eScan™

Enterprise Security

eScan Vision Core XDR

User Guide

Product Version: 22.0.0000.xxxx

Document Version: 22.0.0000.xxxx

24x7 FREE
Online Technical Support

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

An ISO 27001 Certified Company

www.escanav.com

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

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

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

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

Document Number:	5BUG/30.10.2024/22.x
Current Software Version:	22.0.xxxx.xxxx
Technical Support:	**support@escanav.com**
Sales:	**sales@escanav.com**
Forums:	**https://forums.escanav.com**
eScan Wiki:	**https://wiki.escanav.com/wiki/index.php/**
Live Chat:	**https://www.escanav.com/english/livechat.asp**
Published by:	MicroWorld Software Services Private Limited
Date:	January, 2025

Table of Contents

Introduction

eScan Vision Core XDR (eXtended Detection and Response) is a broader and layered endpoint security solution that delivers real-time visibility, analysis, protection, and remediation for endpoints. This provides deeper insights and alerts the admin about malicious activity, which facilitates quicker investigation and restricts the attacks on endpoints as soon as detected.

The Vision Core XDR consists of the latest modules like Phishing simulation and IP Radar. Additionally, a MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is included to give your network an expanded cybersecurity coverage. As an enterprise-grade security solution, it supports automated and manual actions to restrict the potential threats on the endpoint. It proactively reduces the attack, prevents malware infection, and neutralizes potential threats by detecting them in real-time. eScan Vision Core XDR is designed using in-demand and futuristic technologies available for Windows, Mac, and Linux based endpoints across the enterprise.

eScan Management Console, a web-based centralized management console for Vision Core XDR empowers an administrator to install and manage eScan clients on the computers connected across the network. With this console, you can perform following activities–

- Install eScan client application on computers.
- Monitor the security status of computers.
- Create and manage policies or tasks for computers.
- Create and view customized reports of the security status of the computers.
- Manage notifications for alerts and warnings of suspicious activities.
- Detection and remediation of malicious activities
- Incident data investigation and search

Pre-requisites for eScan Vision Core XDR Server

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

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

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

System Requirements

Windows Server and Endpoints	Mac Endpoints	Linux Endpoints
Microsoft® Windows® 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)	OS X Snow Leopard (10.6 or later) OS X Lion (10.7 or later) OS X Mountain Lion (10.8 or later) OS X Mavericks (10.9 or later) OS X Yosemite (10.10 or later) OS X El Capitan (10.11 or later) macOS Sierra (10.12 or later) macOS High Sierra (10.13 or later) macOS Mojave (10.14 or later) macOS Catalina (10.15 or later) macOS Big Sur (11.0 or later) macOS Monterey (12.0 or later) macOS Ventura (13.0 or later) macOS Sonoma (14.0 or later)	RHEL 4 and above (32 and 64-bit) CentOS 5.10 and above (32 and 64-bit) SLES 10 SP3 and above (32 and 64-bit) Debian 4.0 and above (32 and 64-bit) openSUSE 10.1 and above (32 and 64-bit) Fedora 5.0 and above (32 and 64-bit) Ubuntu 6.06 and above (32 and 64-bit) Mint 12 and above (32 and 64 bit) Oracle 7.x and above (32 and 64 bit) Red Hat Linux server (32 and 64 bit)
Hardware Requirements for eScan Server: **CPU -** 2GHz Intel™ Core™ Duo processor or equivalent **Memory -** 4 GB and above **Disk Space** (Free) – 8 GB and above **Hardware Requirements for eScan Client:** **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	**Hardware Requirements for eScan Client:** **CPU -** Intel based Macintosh **Memory** –2 GB and More recommended **Disk Space** – 2 GB and above	**Hardware Requirements for eScan Client:** **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

eScan Management Console can be accessed by using following browsers:

- Firefox latest version
- Google Chrome latest version

Installing eScan Vision Core XDR Server

- **Installing eScan Vision Core XDR Server from CD/DVD**

  Installing eScan Vision Core XDR from the CD/DVD is very simple, insert the CD/DVD in the ROM and wait few seconds for the Autorun to run the installation wizard. In case the installation wizard does not run automatically, locate and double-click the **XDRcwnxxxxx.exe** on CD-ROM. This will run the installation wizard based setup of eScan Vision Core XDR. To complete the installation, follow the instructions on screen.

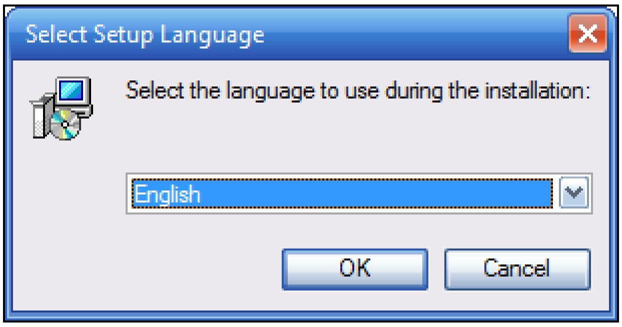
- **Installing eScan Vision Core XDR Server from internet**

  To install eScan Server from the downloaded setup file, double click the **XDRcwnxxxxx.exe** and follow the instructions on screen to complete the installation process.

Installation

To install eScan Vision Core XDR, follow the steps given below:

1. The installation wizard displays following window:



Select Setup Language

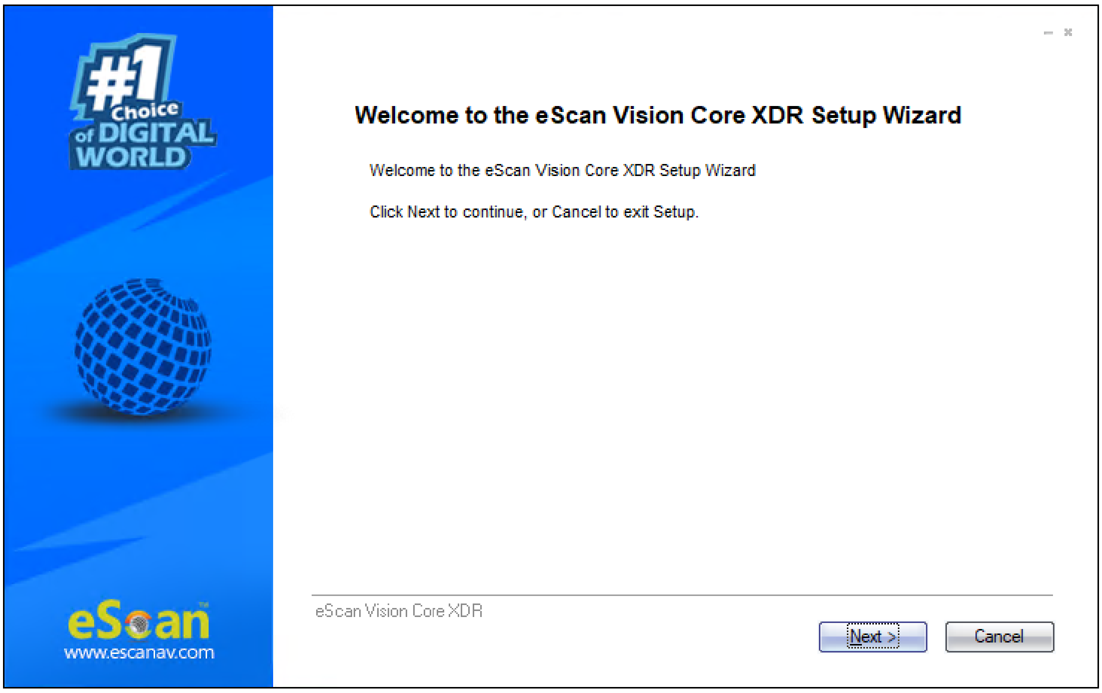
Select the language to use during the installation:

English

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.



Welcome to the eScan Vision Core XDR Setup Wizard

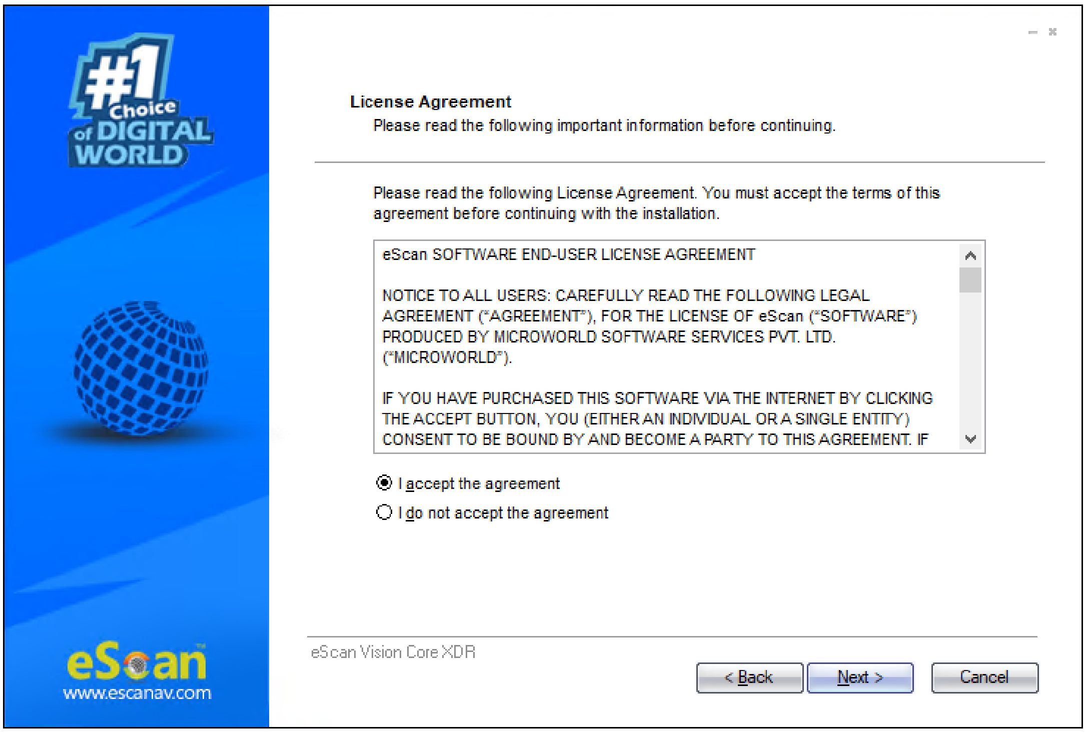
Welcome to the eScan Vision Core XDR Setup Wizard

Click Next to continue, or Cancel to exit Setup.

eScan Vision Core XDR

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

License Agreement screen appears.



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

eScan SOFTWARE END-USER LICENSE AGREEMENT

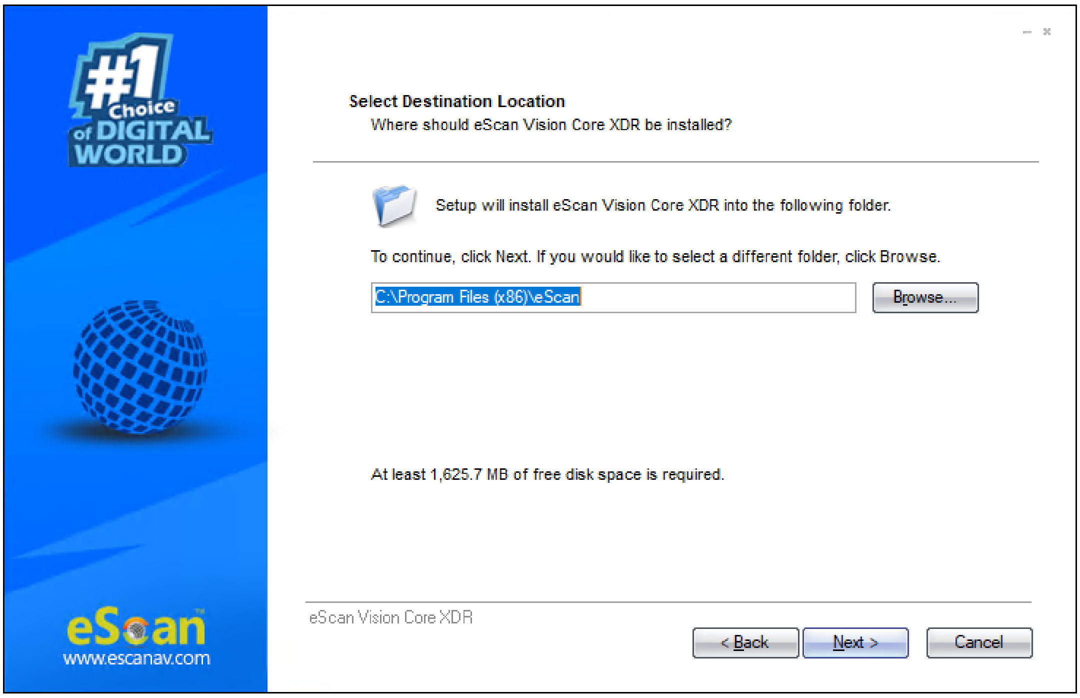
NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF eScan ("SOFTWARE") PRODUCED BY MICROWORLD SOFTWARE SERVICES PVT. LTD. ("MICROWORLD").

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF

● I accept the agreement

○ I do not accept the agreement

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



Select Destination Location

Where should eScan Vision Core XDR be installed?

Setup will install eScan Vision Core XDR into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

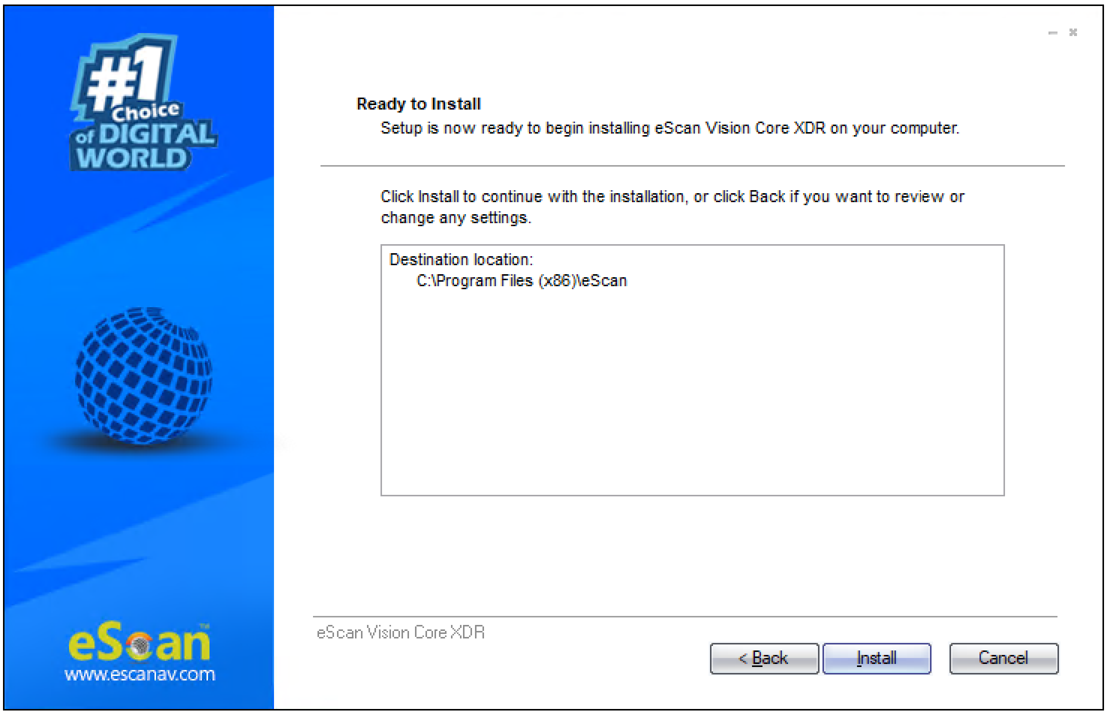
C:\Program Files (x86)\eScan

At least 1,625.7 MB of free disk space is required.

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

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

Ready to Install screen appears displaying destination location.



Ready to Install

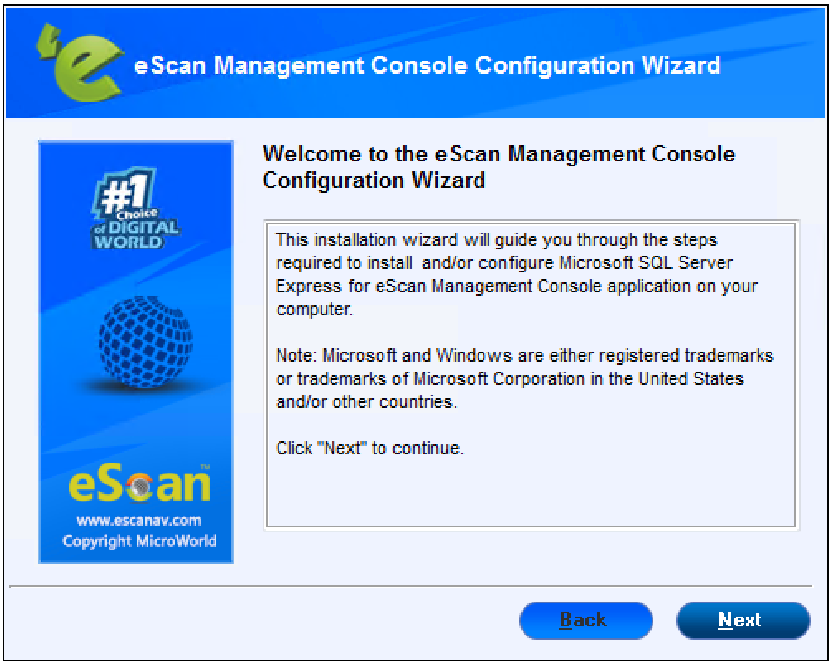
Setup is now ready to begin installing eScan Vision Core XDR on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\Program Files (x86)\eScan

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

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



eScan Management Console Configuration Wizard

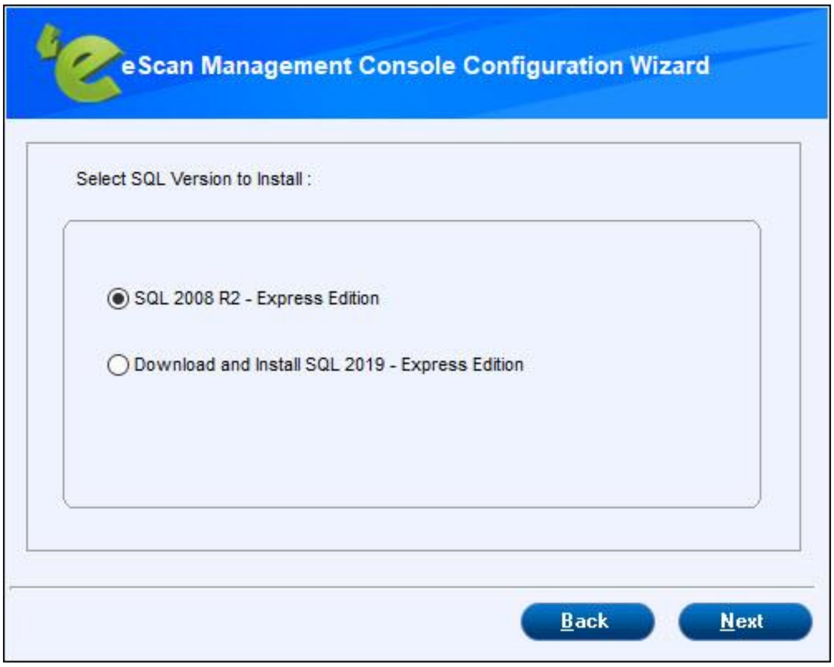
Welcome to the eScan Management Console Configuration Wizard

This installation wizard will guide you through the steps required to install and/or configure Microsoft SQL Server Express for eScan Management Console application on your computer.

Note: Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Click "Next" to continue.

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.



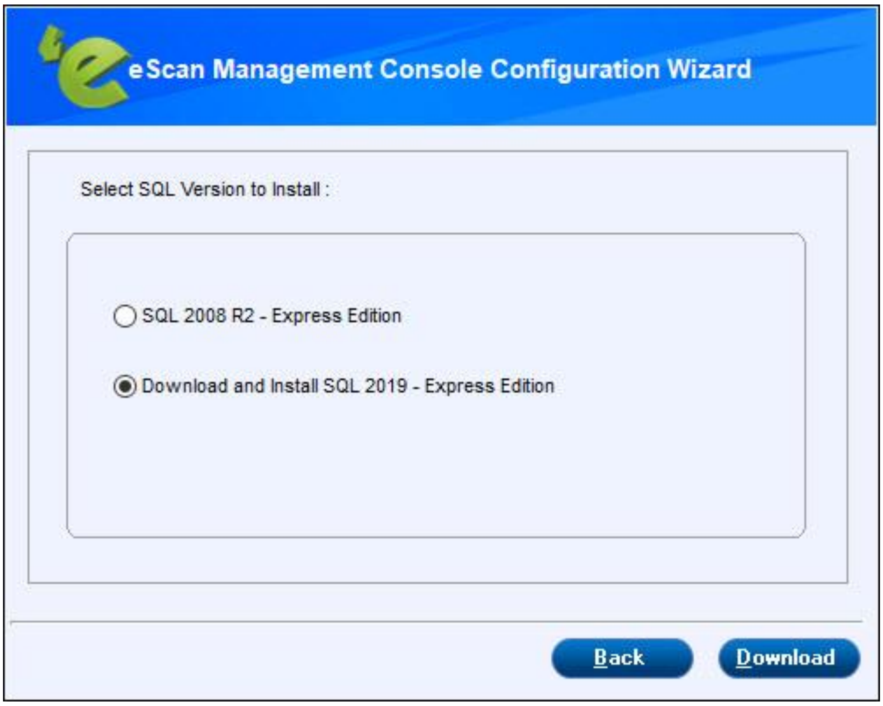
eScan Management Console Configuration Wizard

Select SQL Version to Install :

● SQL 2008 R2 - Express Edition

○ Download and Install SQL 2019 - 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**.



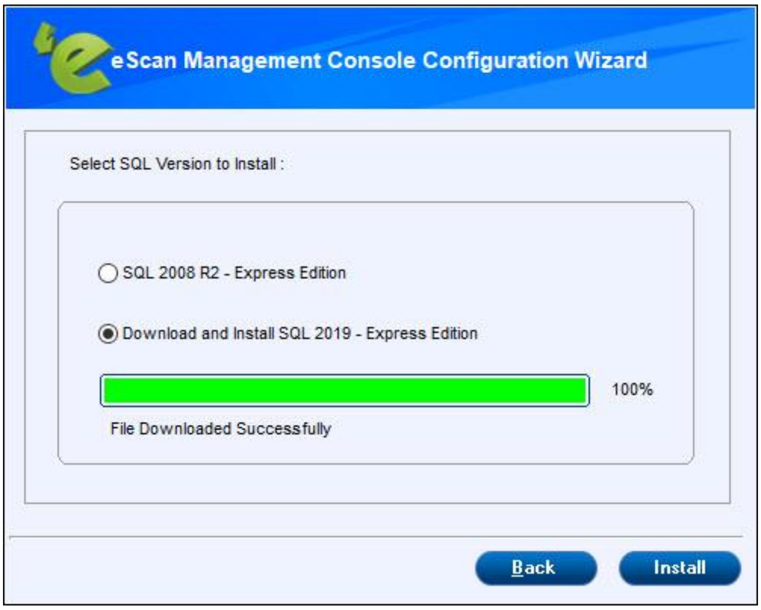
eScan Management Console Configuration Wizard

Select SQL Version to Install :

○ SQL 2008 R2 - Express Edition

● Download and Install SQL 2019 - Express Edition

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



eScan Management Console Configuration Wizard

Select SQL Version to Install :

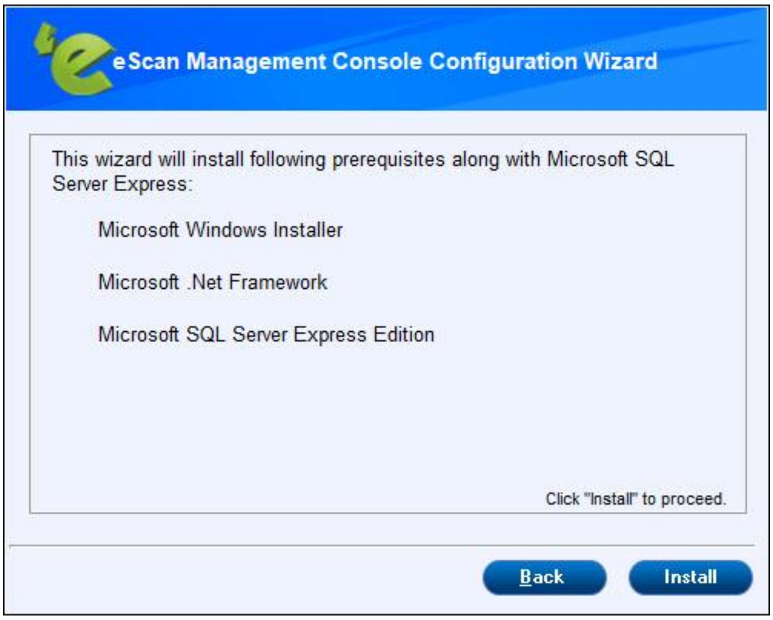
○ SQL 2008 R2 - Express Edition

● Download and Install SQL 2019 - Express Edition

100%

File Downloaded Successfully

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



eScan Management Console Configuration Wizard

This wizard will install following prerequisites along with Microsoft SQL Server Express:

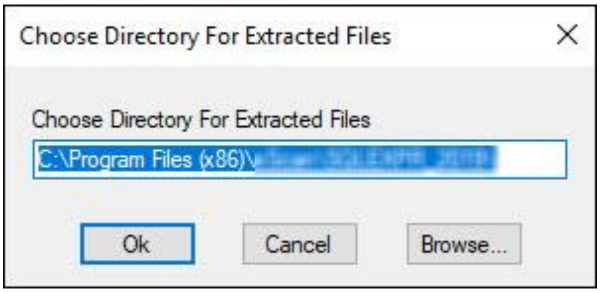
Microsoft Windows Installer

Microsoft .Net Framework

Microsoft SQL Server Express Edition

Click "Install" to proceed.

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



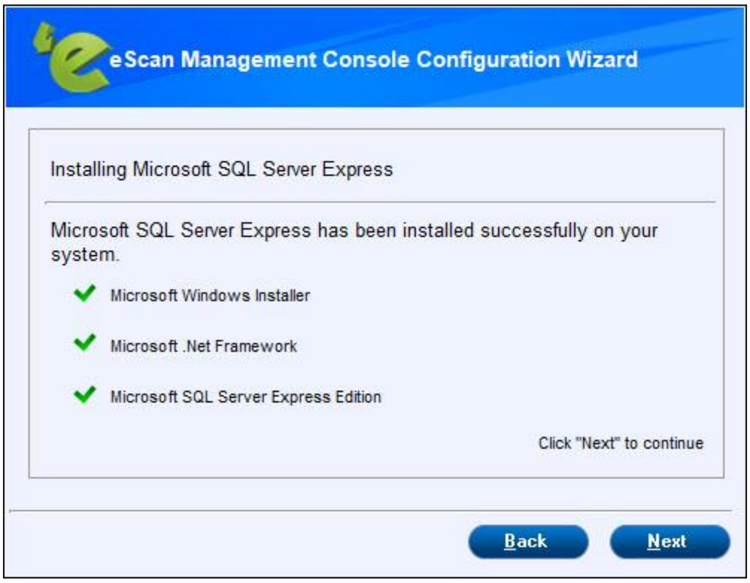
Choose Directory For Extracted Files

Choose Directory For Extracted Files

C:\Program Files (x86)\[redacted]

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

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



Installing Microsoft SQL Server Express

Microsoft SQL Server Express has been installed successfully on your system.

✓ Microsoft Windows Installer

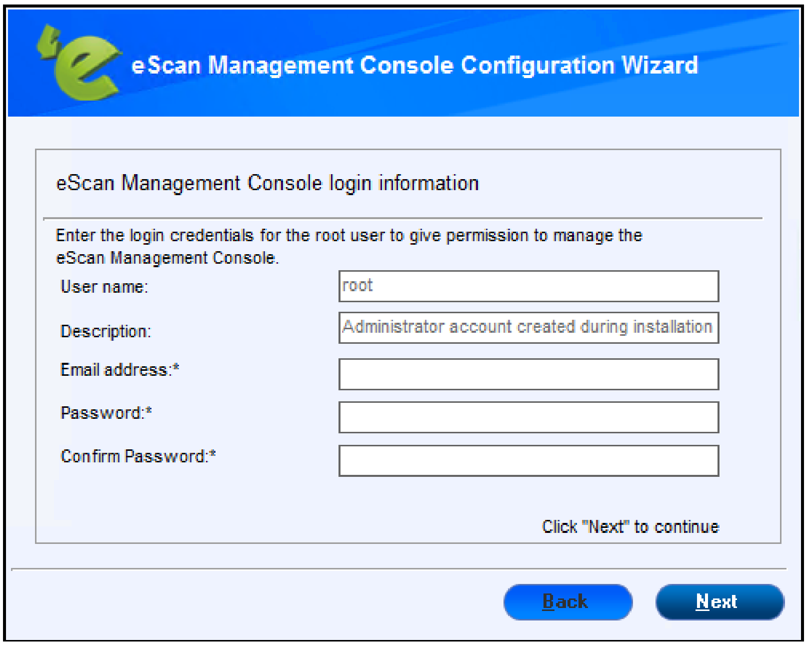
✓ Microsoft .Net Framework

✓ Microsoft SQL Server Express Edition

Click "Next" to continue

13. To proceed, click **Next**.
    The wizard requests you to enter the login credentials for the root user.

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



eScan Management Console login information

Enter the login credentials for the root user to give permission to manage the eScan Management Console.

User name: root

Description: Administrator account created during installation

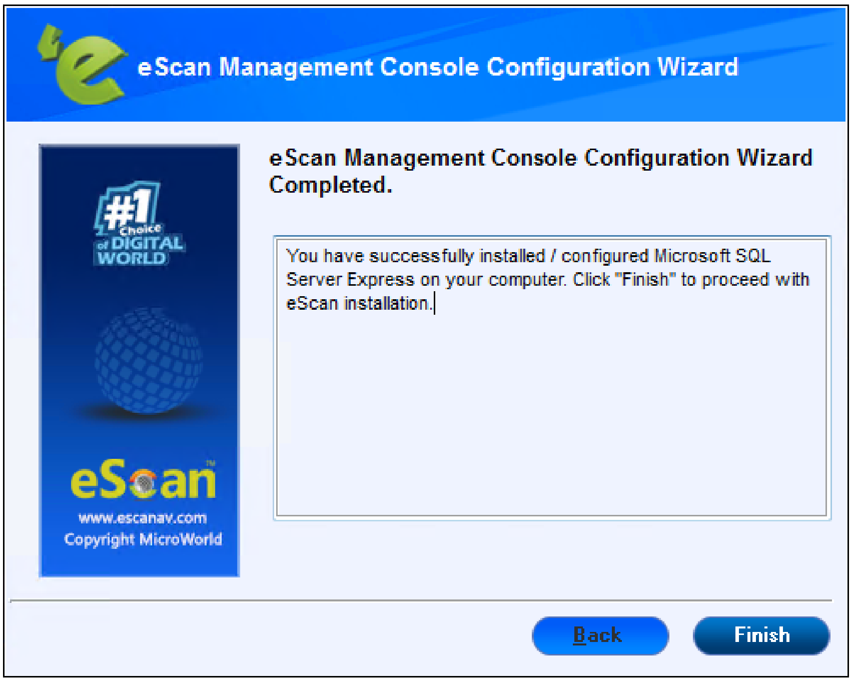
Email address:*

Password:*

Confirm Password:*

Click "Next" to continue

14. After filling all the details, click **Next**.
    The installation successful window appears.

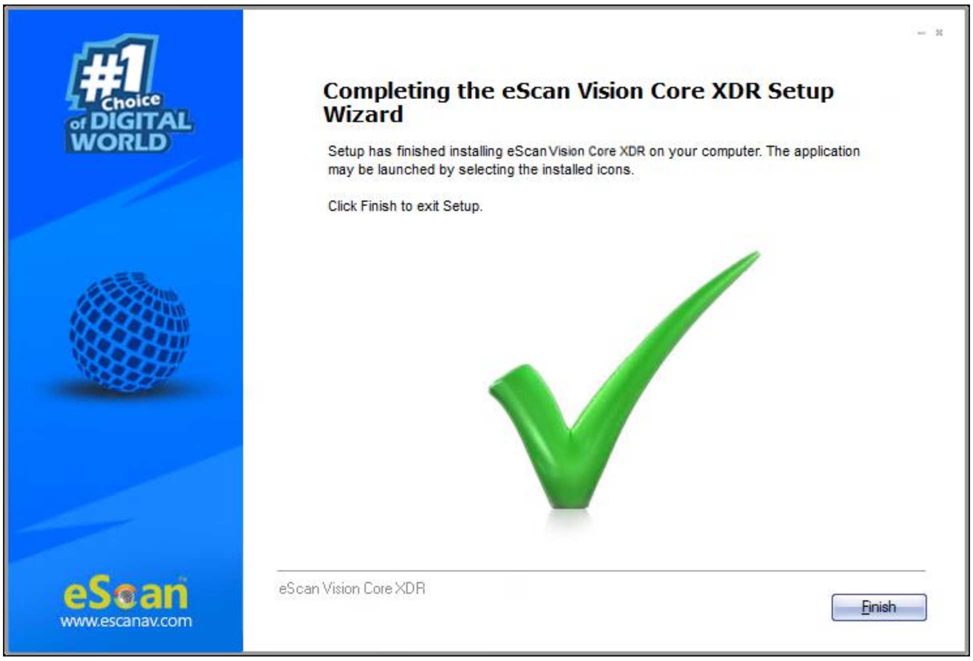


eScan Management Console Configuration Wizard
#1 Choice of DIGITAL WORLD
eScan
www.escanav.com
Copyright MicroWorld
Back
Finish

eScan Management Console Configuration Wizard Completed.

You have successfully installed / configured Microsoft SQL Server Express on your computer. Click "Finish" to proceed with eScan installation.

15. Click **Finish** to exit the installation wizard and proceed further.

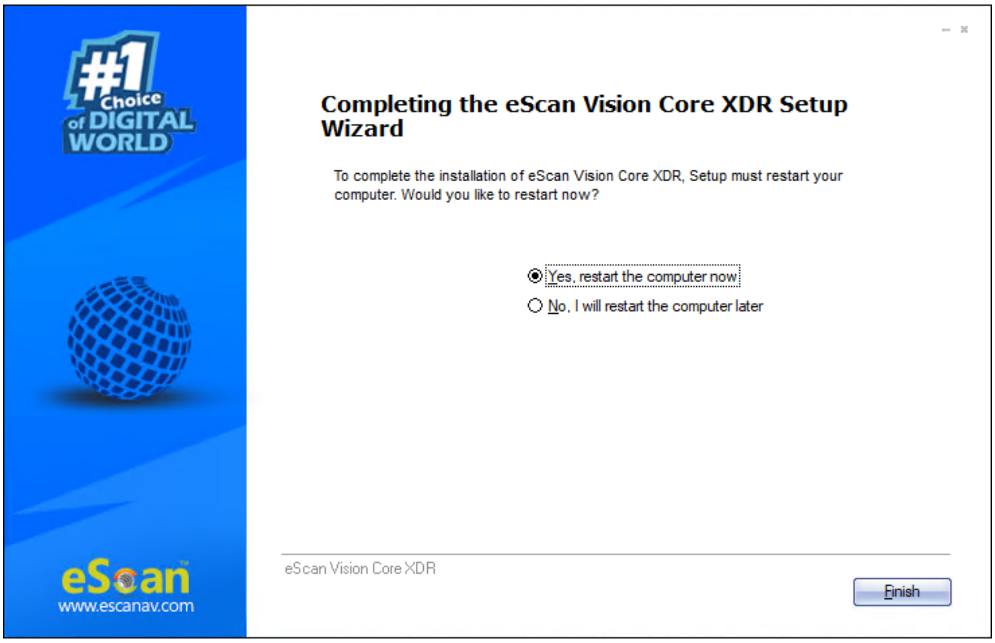


Completing the eScan Vision Core XDR Setup Wizard

Setup has finished installing eScan Vision Core XDR on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

16. Click **Finish**. The wizard asks you to restart the PC for completing the installation process.



Completing the eScan Vision Core XDR Setup Wizard

To complete the installation of eScan Vision Core XDR, Setup must restart your computer. Would you like to restart now?

● Yes, restart the computer now

○ No, I will restart the computer later

17. To restart your PC, click **Yes**.

    After the computer restarts, launch the eScan Enterprise XDR and enter the license key for activation.

NOTE	To run eScan services without any interruption 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 allows you manage, deploy and configure eScan client on computers. It stores the configuration information and log files about the computers connected across the network. Being the core component, it communicates with the following components.

- **Agent**
  It manages the connection between the eScan server and the client computers.

- **eScan Management Console**
  It is a Web-based application hosted on the eScan Server. With this application, administrators can manage and configure eScan on computers in the network.

- **Microsoft SQL Server Express Edition**
  It is a database for storing events and logs already included in the eScan Setup file.

- **Apache**
  It is an open source, cross-platform web server software essential for running eScan Management Console. It's included in the eScan Setup file.

NOTE	For Windows 11 / 10 / 8 / 8.1 / 2008 / 2012 / 2016 / 2019 operating systems, the SQL 2008 Express edition will be installed.

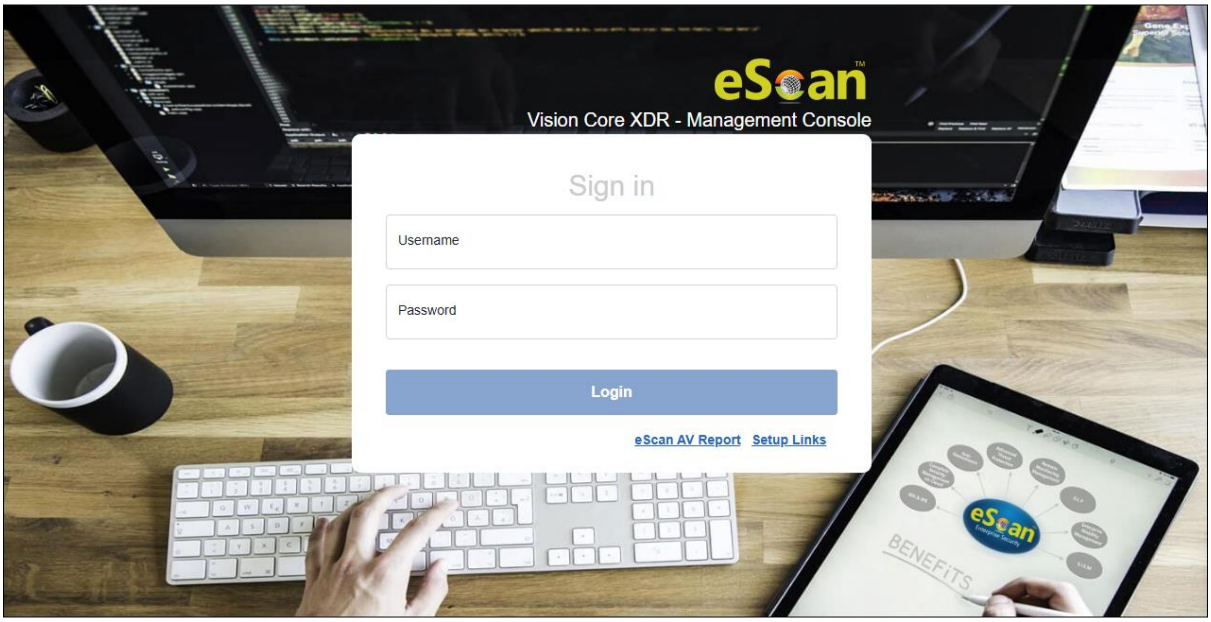
	For Windows 7 and below, SQL 2005 Express edition will be installed. Uninstallation of eScan server won't remove SQL and APACHE from the endpoint. The user will have to uninstall these components manually.

Web Console Login

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

Method 1:

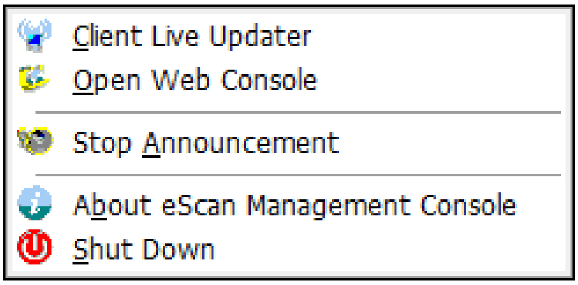
1. Launch a web browser.
2. Enter the following URL: <*IP address of the eScan Server installed system*>:10443
   Web console login page appears.



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

Method 2:

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

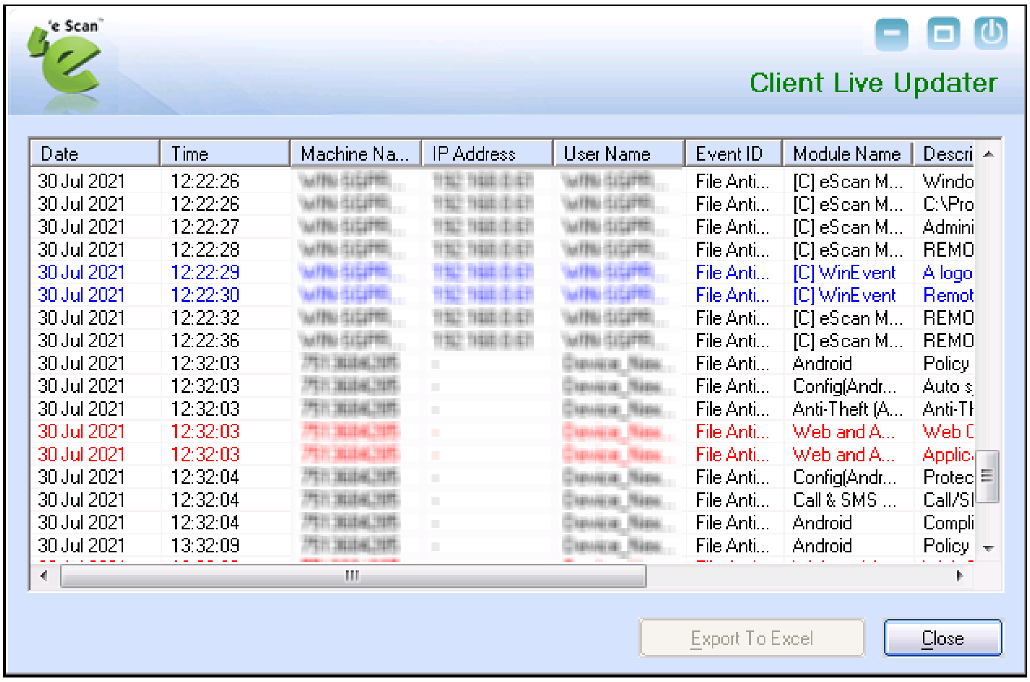


2. Click **Open Web Console**.
   Default browser launches and displays web console login page.

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

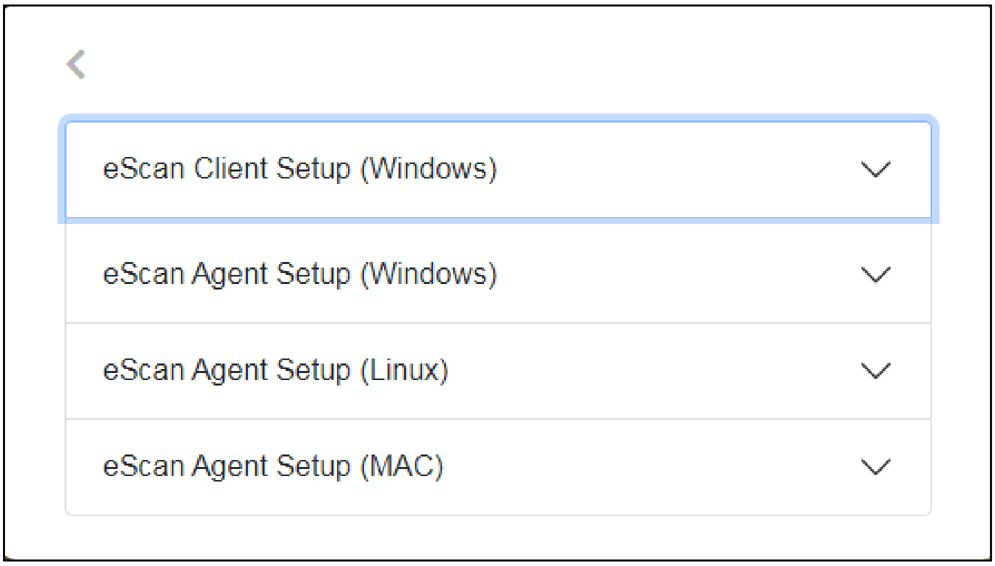
Shut Down

Clicking this option shuts down the eScan Management console.

❗ NOTE	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)

eScan Agent Setup (Windows)

eScan Agent Setup (Linux)

eScan Agent Setup (MAC)

- **eScan Client Setup (Windows)**
  This link can be shared via email to the computer users where remote installation is impossible. By clicking this link users can download the eScan Client Setup and install it manually on their computers. Users can also directly access the eScan Management console from their desktop.

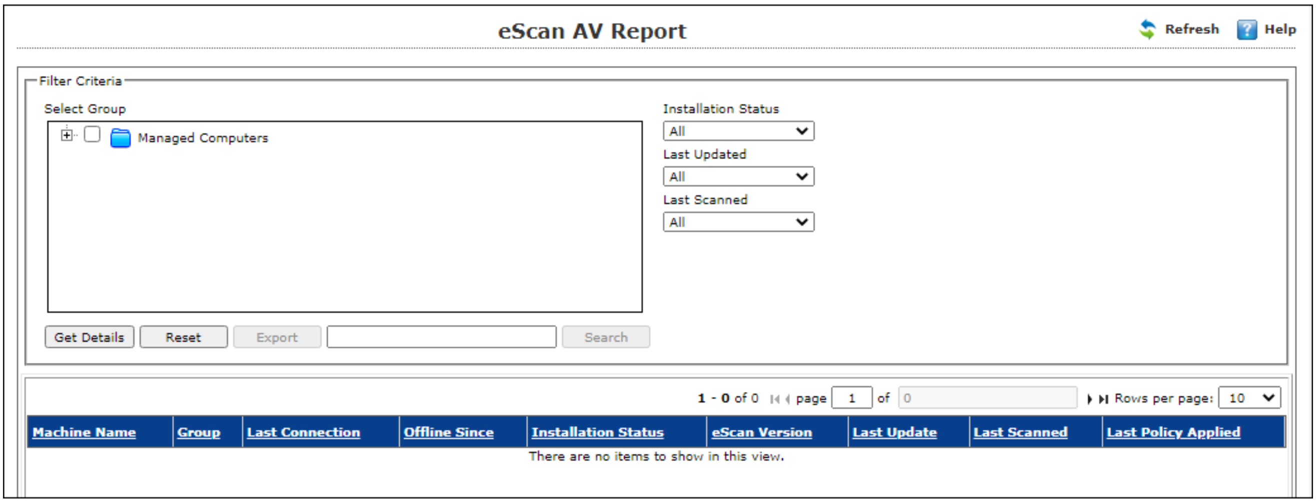
- **eScan Agent Setup (Windows)**
  This link can be shared via email to the computer user where you are unable to get system information or communication is breaking frequently. After the eScan Agent Setup is downloaded and installed on the Managed Computer, it establishes the connection between the server and client computers.

- **eScan Agent Setup (Linux)**
  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.

eScan AV Report

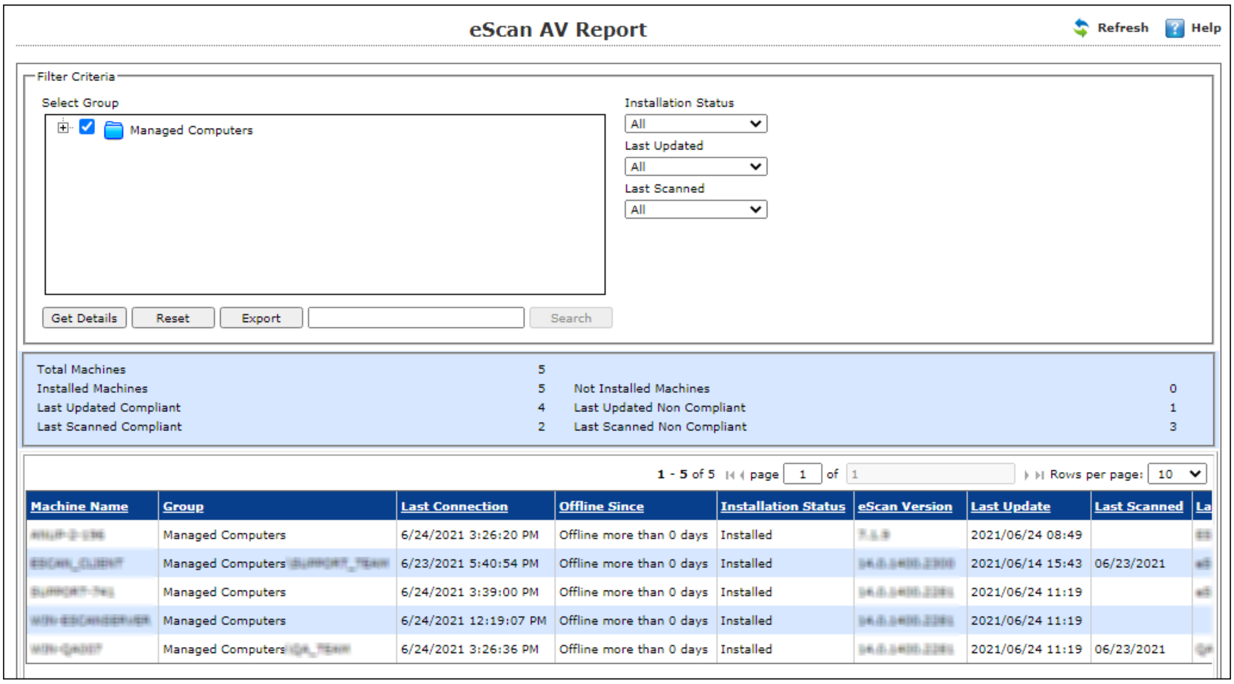
Clicking this link redirects you to the eScan AV Report webpage that displays Anti-Virus report for eScan installed computers.



Machine Name	Group	Last Connection	Offline Since	Installation Status	eScan Version	Last Update	Last Scanned	Last Policy Applied

There are no items to show in this view.

Select a group and then click **Get Details** to get the details of the endpoints.



Total Machines	5		
Installed Machines	5	Not Installed Machines	0
Last Updated Compliant	4	Last Updated Non Compliant	1
Last Scanned Compliant	2	Last Scanned Non Compliant	3

1 - 5 of 5 page 1 of 1 Rows per page: 10

Machine Name	Group	Last Connection	Offline Since	Installation Status	eScan Version	Last Update	Last Scanned	La
[redacted]	Managed Computers	6/24/2021 3:26:20 PM	Offline more than 0 days	Installed	[redacted]	2021/06/24 08:49		[redacted]
[redacted]	Managed Computers [redacted]	6/23/2021 5:40:54 PM	Offline more than 0 days	Installed	[redacted]	2021/06/14 15:43	06/23/2021	[redacted]
[redacted]	Managed Computers	6/24/2021 3:39:00 PM	Offline more than 0 days	Installed	[redacted]	2021/06/24 11:19		[redacted]
[redacted]	Managed Computers	6/24/2021 12:19:07 PM	Offline more than 0 days	Installed	[redacted]	2021/06/24 11:19		
[redacted]	Managed Computers [redacted]	6/24/2021 3:26:36 PM	Offline more than 0 days	Installed	[redacted]	2021/06/24 11:19	06/23/2021	[redacted]

Select a group and then click **Get Details** > **Export**. A detailed **.xls** report will be downloaded to computer.

Exported Successfully Click here to Open/Download

Main Interface

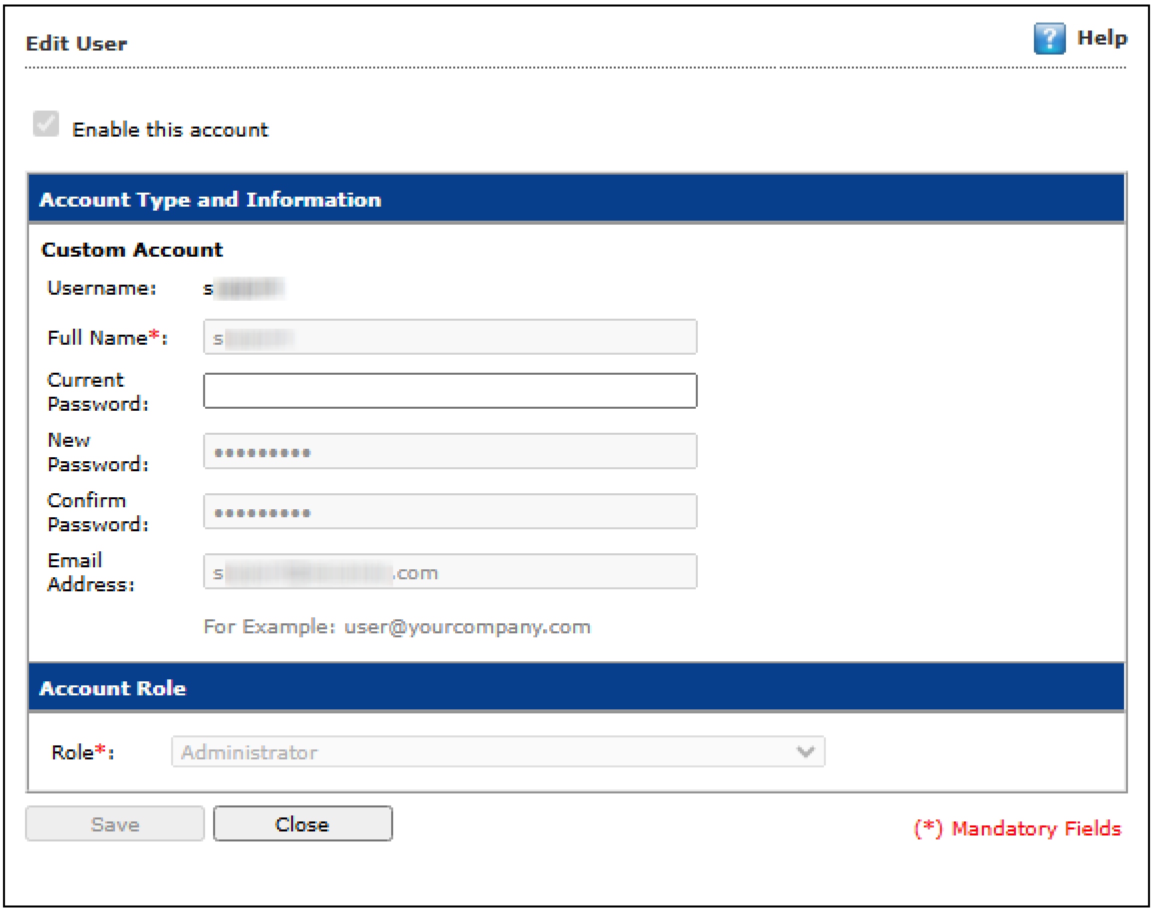
Upon first login, console displays Setup Wizard that familiarizes you with the basic procedures. The links in the top right corner are explained below:

About eScan

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

Username

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



Edit User

Help

☑ Enable this account

Account Type and Information

Custom Account

Username: s[redacted]

Full Name*: s[redacted]

Current Password:

New Password: •••••••••

Confirm Password: •••••••••

Email Address: s[redacted].com

For Example: user@yourcompany.com

Account Role

Role*: Administrator

Save | Close

(*) Mandatory Fields

Log off

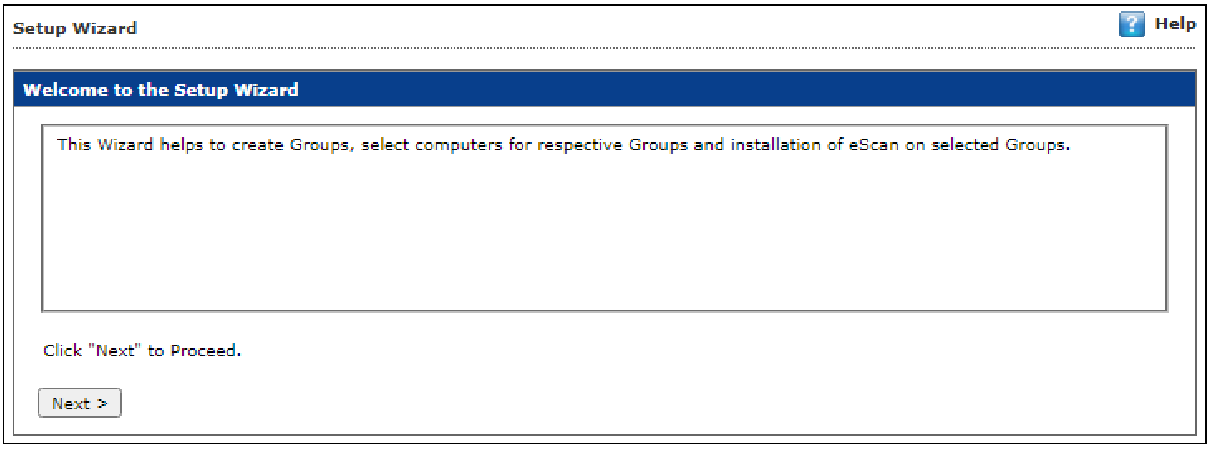
Clicking **Log off** logs you out of the eScan Management Console.

Date of Virus Signatures

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

Setup Wizard

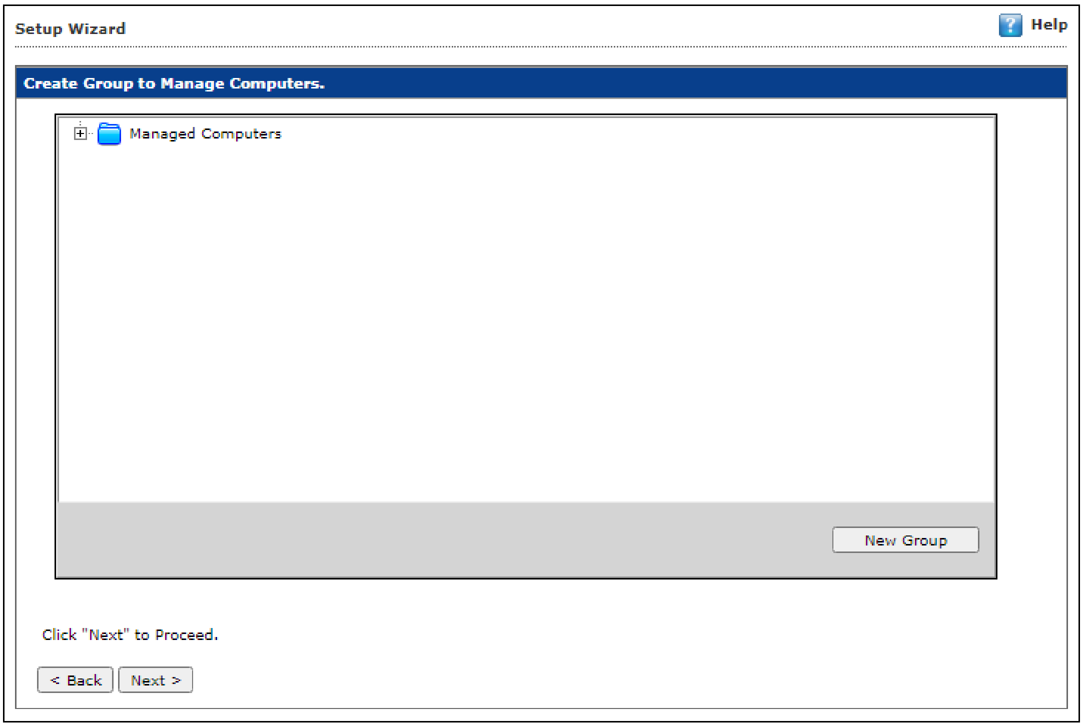
The Setup Wizard helps you to quick start with the eScan Management Console, by allowing admin to perform basic functions such as creating groups, adding computers to it, and installing eScan on it. It is recommended that you follow the steps displayed, before proceeding to the other modules.



This Wizard helps to create Groups, select computers for respective Groups and installation of eScan on selected Groups.

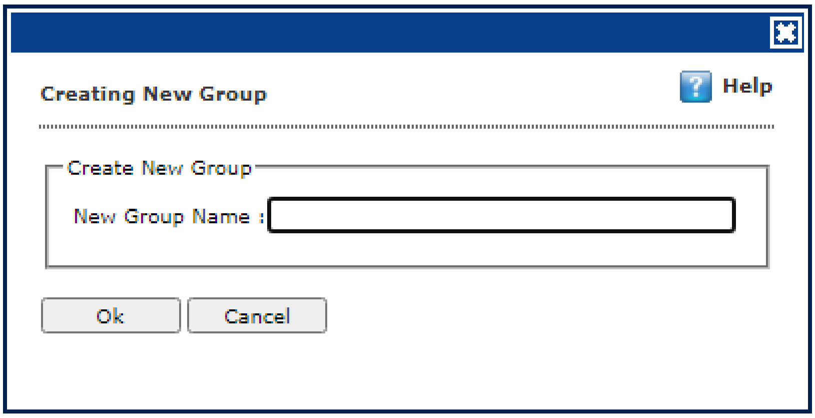
Click "Next" to Proceed.

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

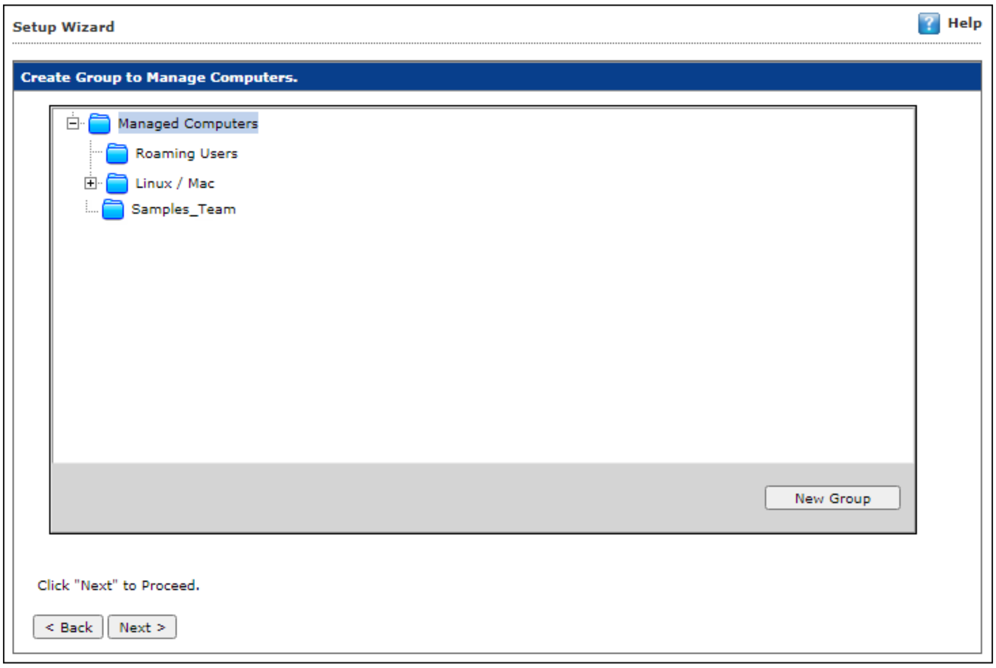


Click "Next" to Proceed.

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



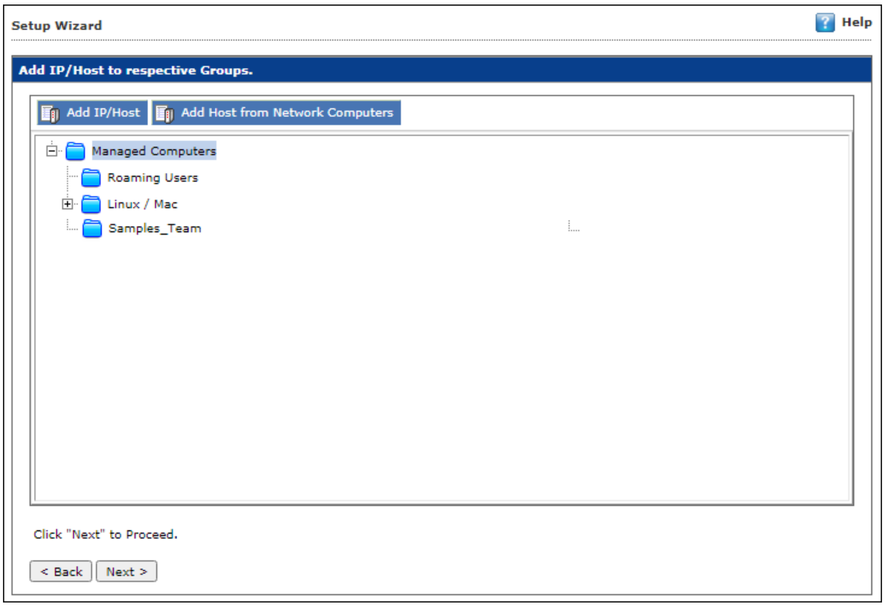
Enter the name of the group and click **OK**.
After creating group, click **Next>** to add computers to the respective group.
Add IP/Host to respective Groups window appears.



Click "Next" to Proceed.

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

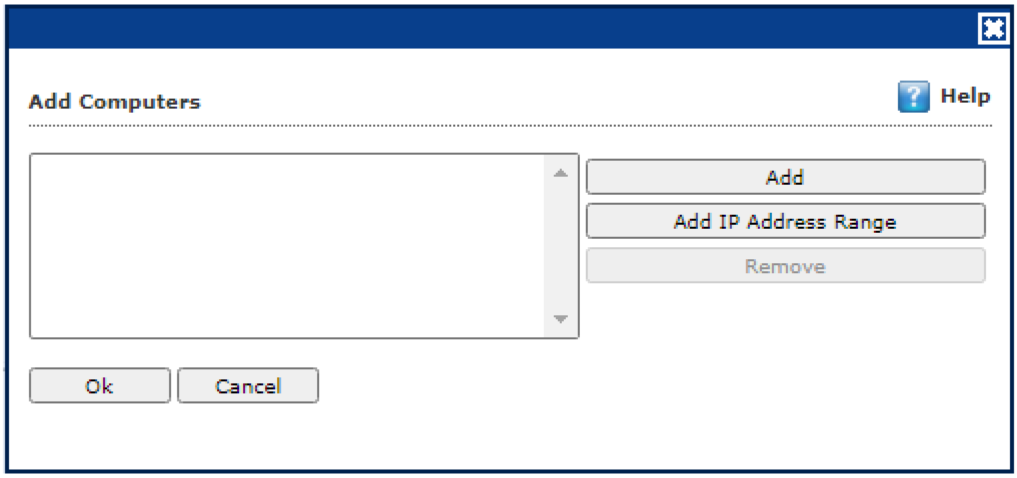
- IP Address/Host name
- Host from Network Computers



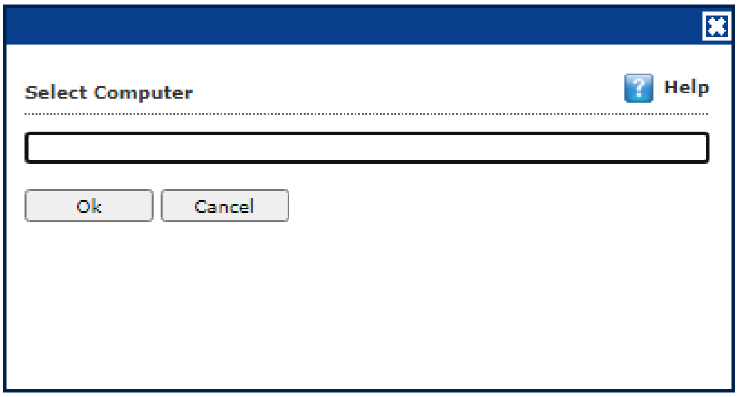
Adding computers via IP Address/Host Name

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

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



2. Click **Add**. Add Computers window appears.

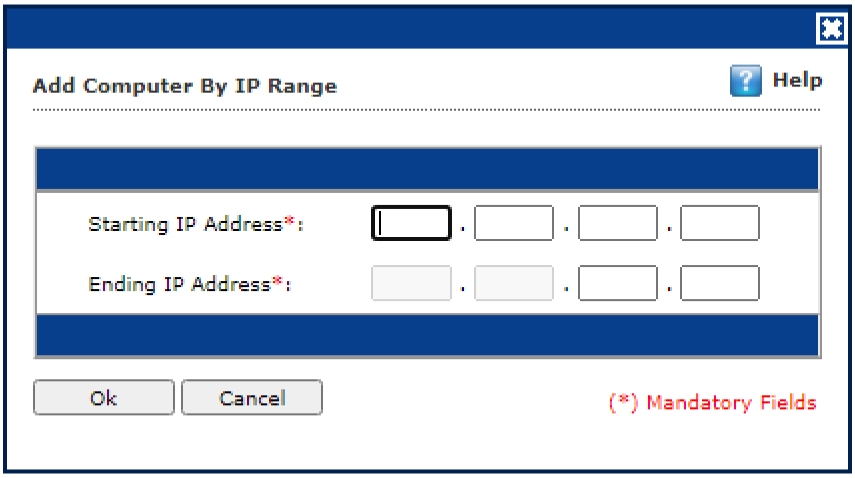


Select Computer

3. Enter the 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 window appears.



Add Computer By IP Range

Starting IP Address*: . . .

Ending IP Address*: . . .

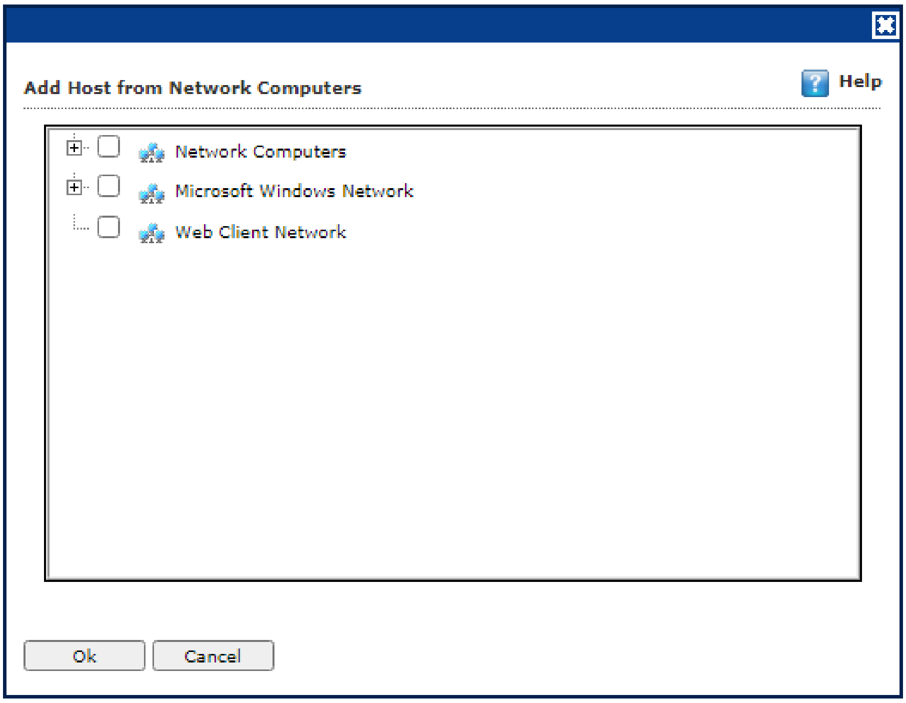
(*) Mandatory Fields

5. Enter the first and the last IP Address of the range.
6. Click **Ok**.
   The computers will be added in the group.

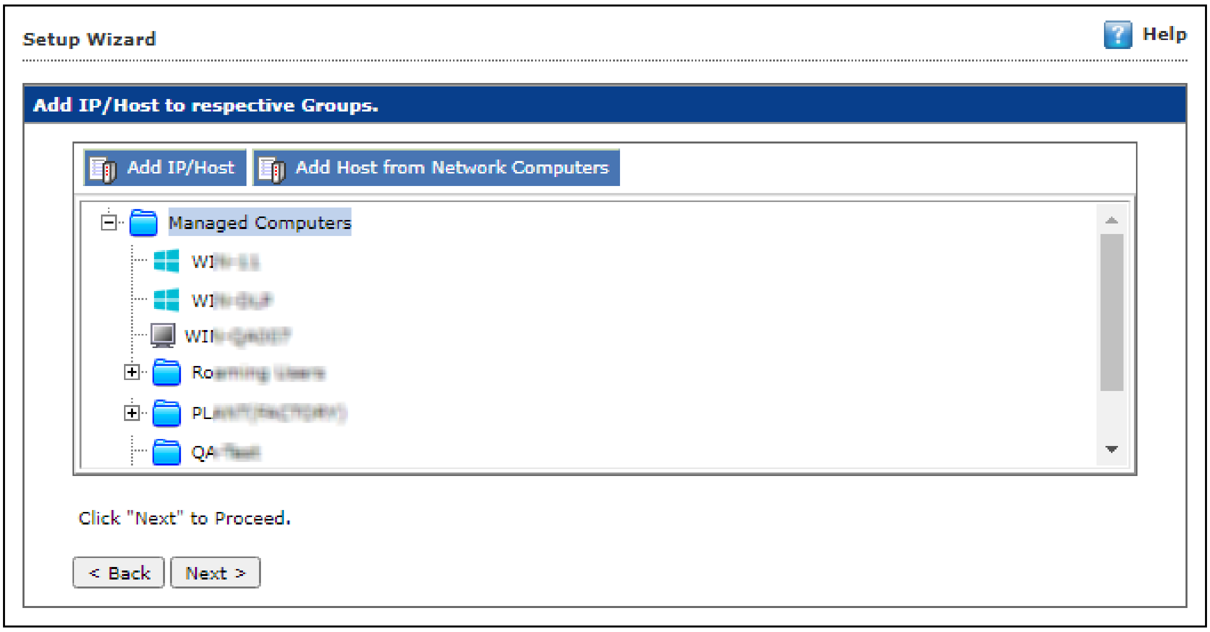
Adding Host Name from Network Computers

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

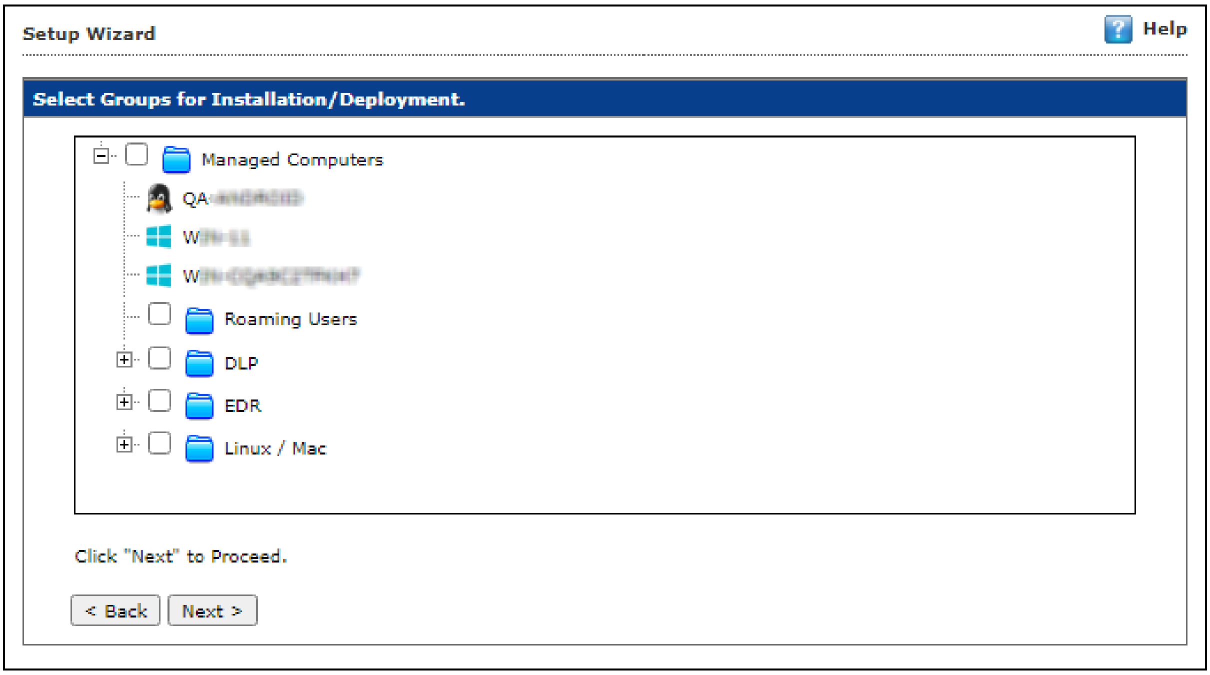
1. Select the group and click **Add Host from Network Computers**.
   Add Host from Network Computers window appears.



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



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



Setup Wizard

Help

Select Groups for Installation/Deployment.

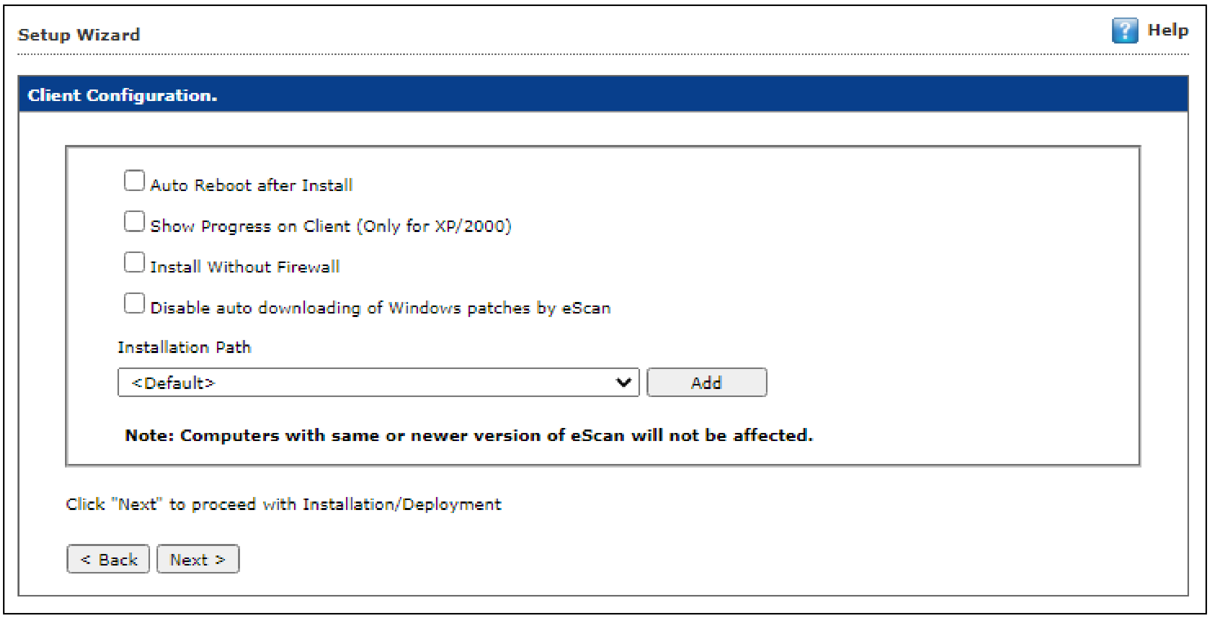
- □ Managed Computers
  - QA-[redacted]
  - W[redacted]
  - W[redacted]
  - □ Roaming Users
- □ DLP
- □ EDR
- □ Linux / Mac

Click "Next" to Proceed.

< Back | Next >

Select the group having client computers then click **Next.**

Client Configuration window appears



Setup Wizard

Help

Client Configuration.

□ Auto Reboot after Install

□ Show Progress on Client (Only for XP/2000)

□ Install Without Firewall

□ Disable auto downloading of Windows patches by eScan

Installation Path

<Default> | Add

Note: Computers with same or newer version of eScan will not be affected.

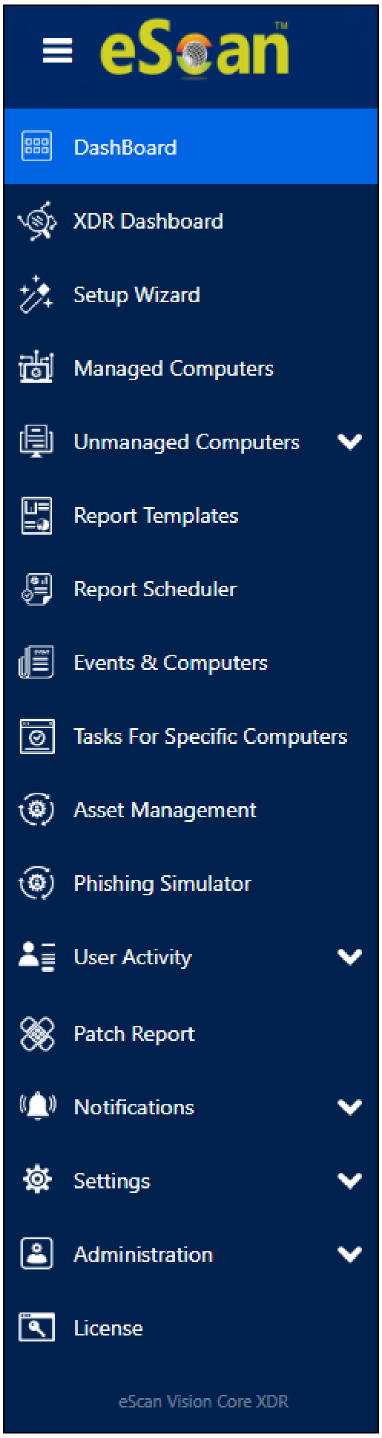
Click "Next" to proceed with Installation/Deployment

< Back | Next >

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

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, Live Status, and IP Radar. The monitoring is done by Management Console of the computers for virus infections and security violations. To learn more, click here.

XDR Dashboard

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

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 define/configure Policies for computers. It provides you various options for creating groups, adding tasks, moving computers from one group to another 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 allows you to 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 allows 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. 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**.

Phishing Simulator

The Phishing Simulator enables your threat intelligence team conduct an internal activity where a mock phishing email is sent to employees to assess whether they click on embedded links or ignore the email. These phishing mails are created by mimicking the actual phishing emails. If the employees respond to the mail by clicking the email links, the action gets stored for further analysis of conducting Phishing awareness program. 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**.

Patch Report

The Patch Report module displays the number of windows security patches installed and not installed on managed computers. This will help an administrator to identify the number of vulnerable systems in the network and install the critical patches quickly. To learn more, **click here**.

Notifications

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

Settings

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

Administration

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

License

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

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

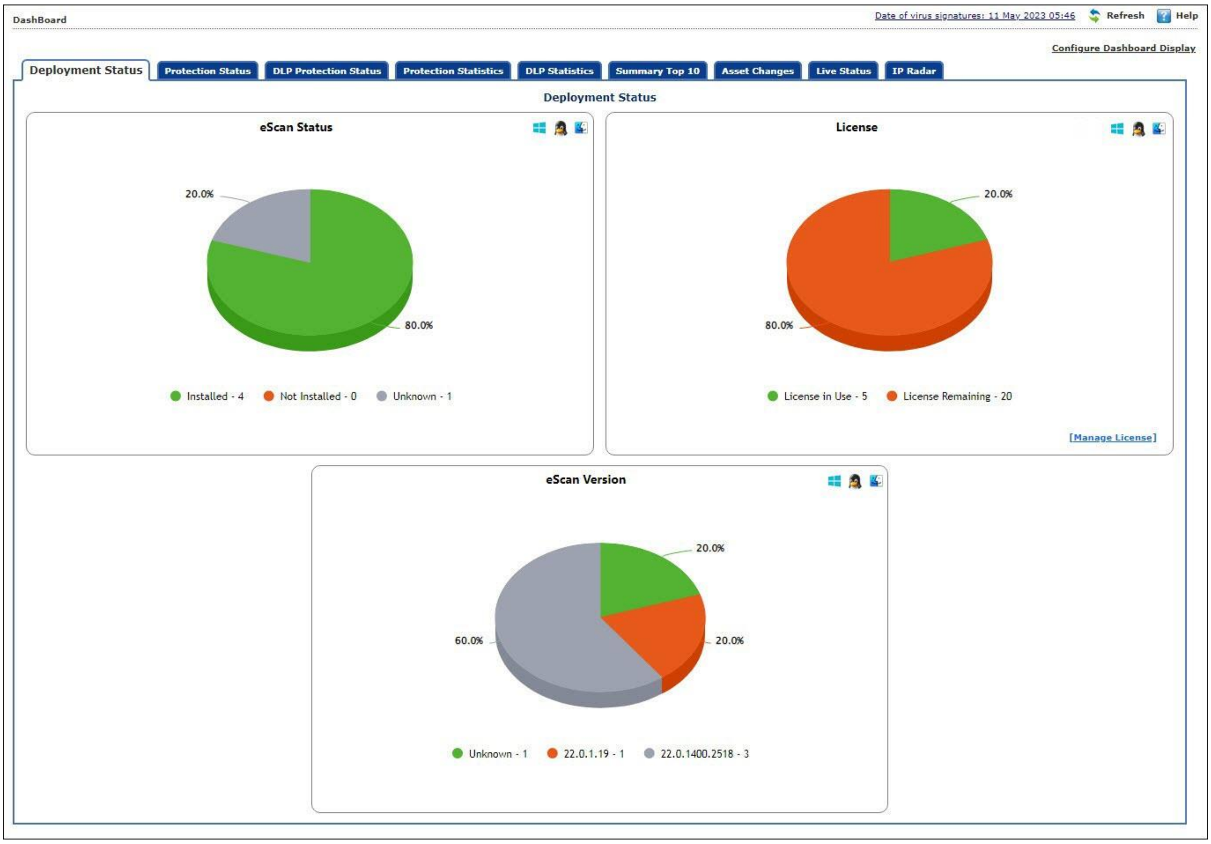
Dashboard

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

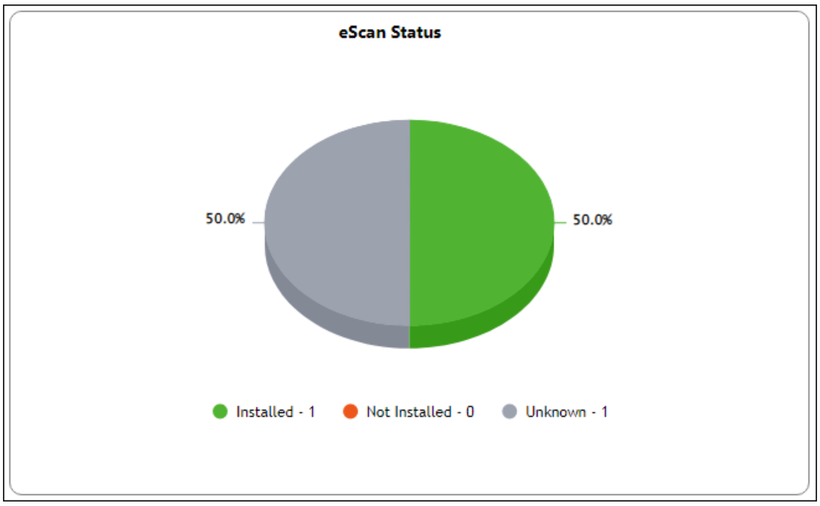
- **Deployment Status**
- **Protection Status**
- **DLP Protection Status**
- **Protection Statistics**
- **DLP Statistics**
- **Summary Top 10**
- **Asset Changes**
- **Live Status**
- **IP Radar**

Deployment Status

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



eScan Status

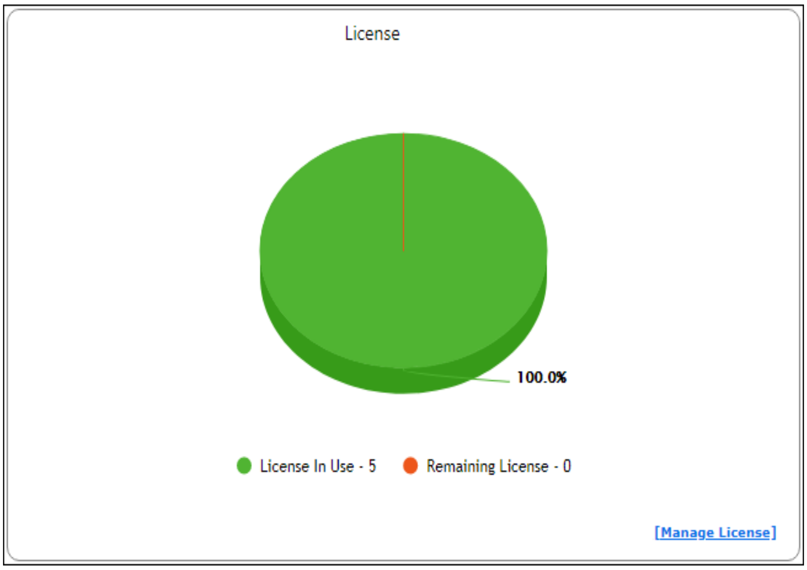


Installed – It displays the number of computers on which eScan Client is installed.

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

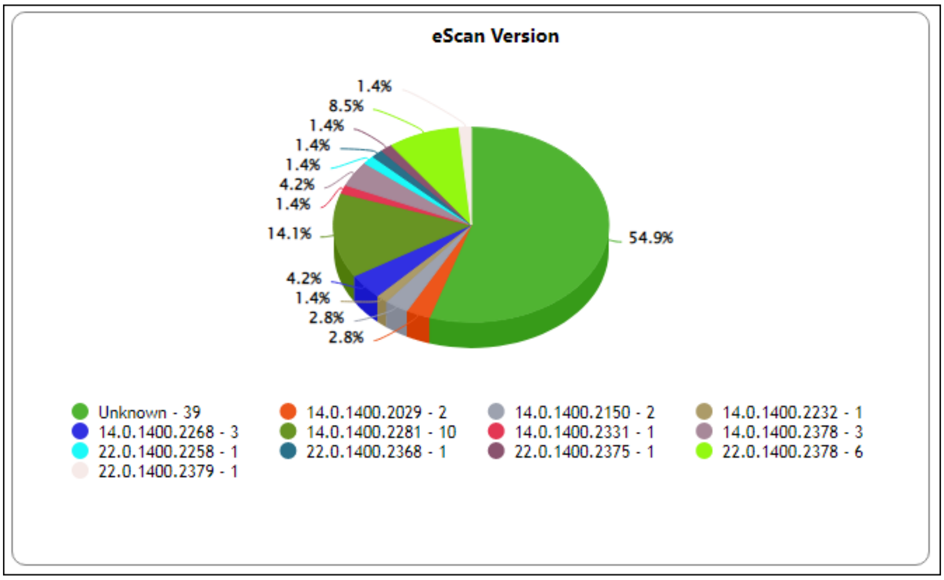


License in Use - It displays the number of licenses that are active.

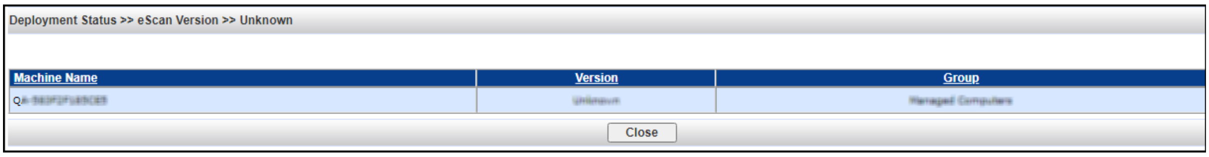
Licenses Remaining - It displays the number of remaining licenses.

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.



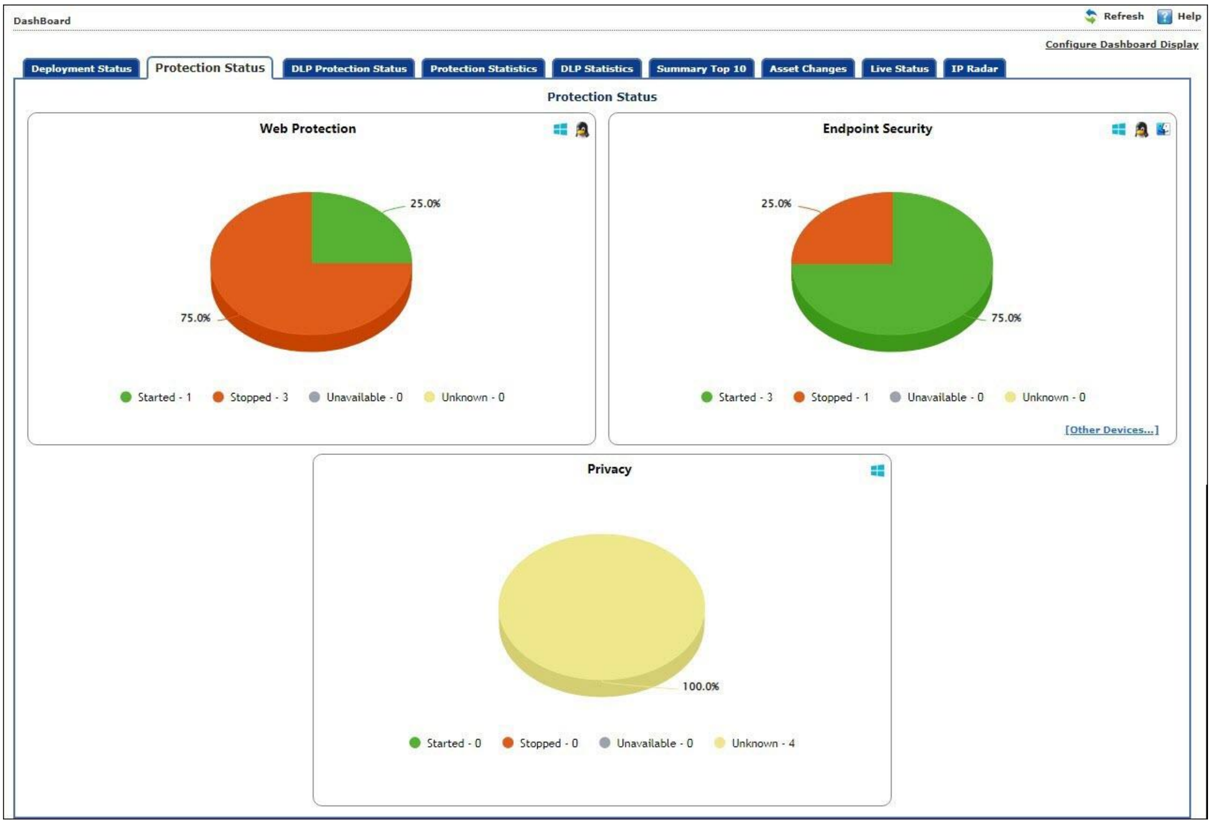
Deployment Status >> eScan Version >> Unknown

Machine Name	Version	Group
Q[redacted]	[redacted]	[redacted]

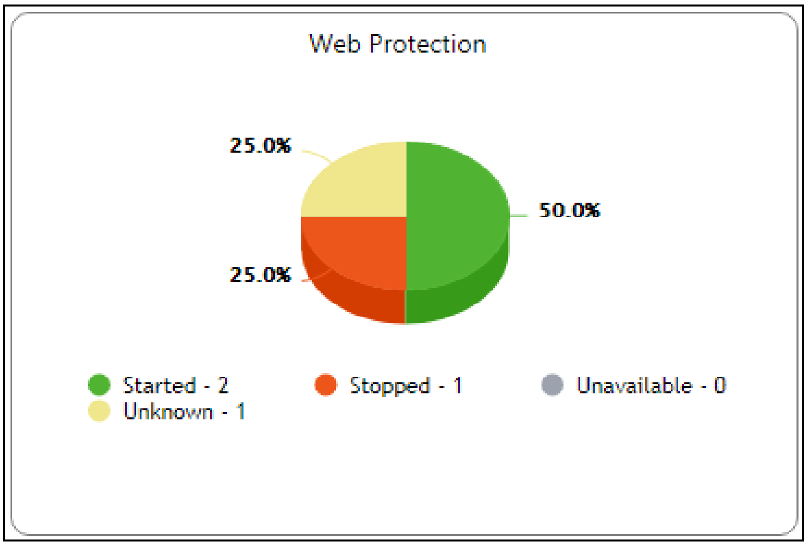
NOTE	Clicking underlined numerical displays detailed information for computers.

Protection Status

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



Web Protection



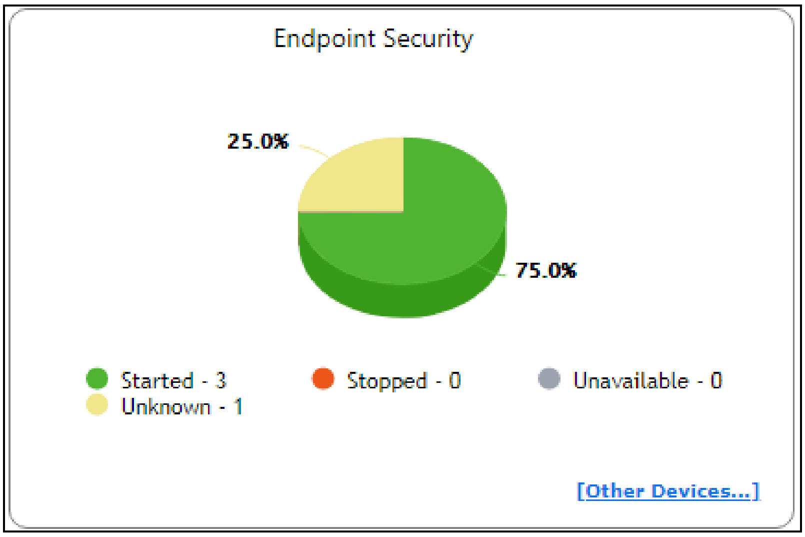
Started – It displays the number of computers on which the Web Protection module is in started state.

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

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

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

Endpoint Security



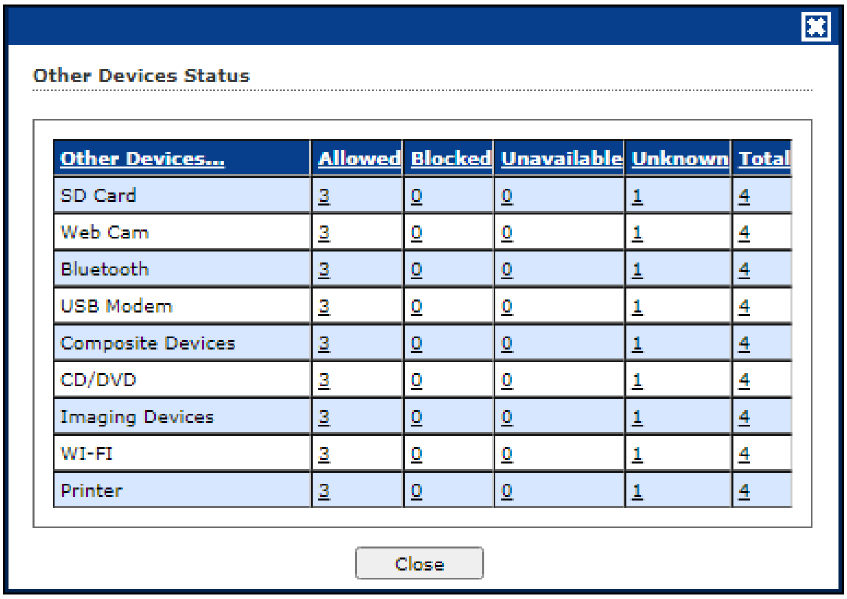
Started - It displays the number of computers on which the Endpoint Security module is in started state.

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

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

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

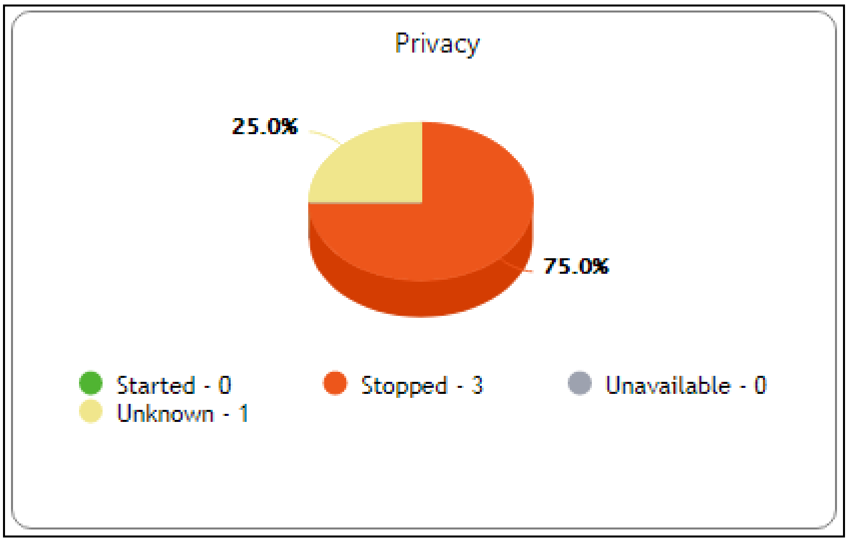
Clicking **Other Devices** displays details about other devices.



Other Devices Status

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

Privacy



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

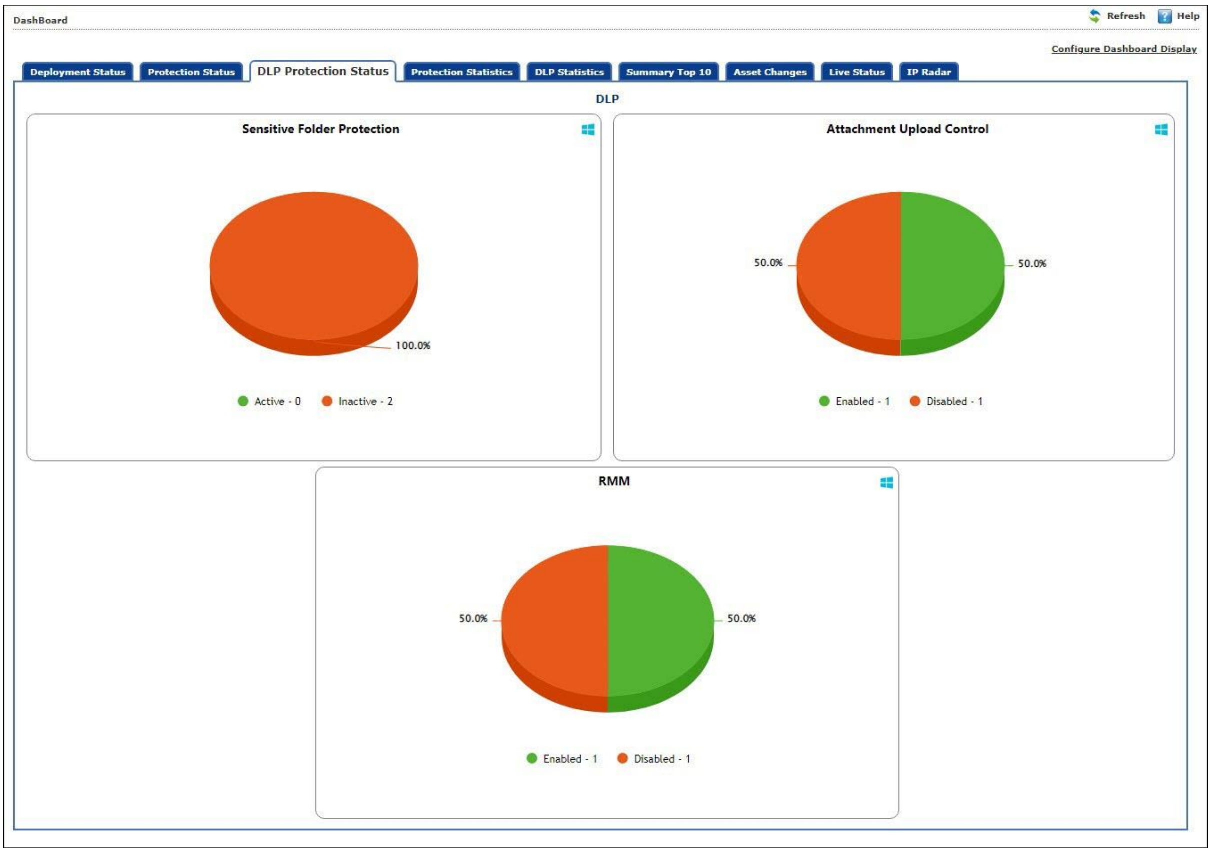
Stopped - It displays the number of computers on which the Privacy Control module is in stopped state.

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

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

DLP Protection Status

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

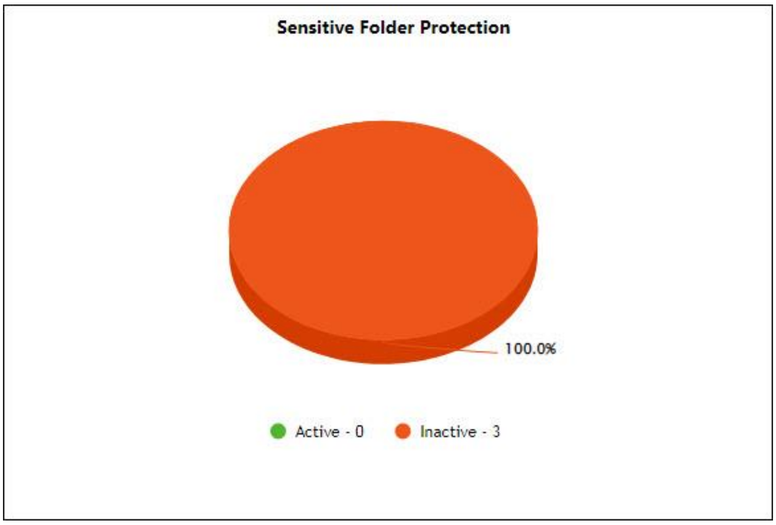


The DLP Protection Status tab contains the status information of the following modules:

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

Sensitive Folder Protection

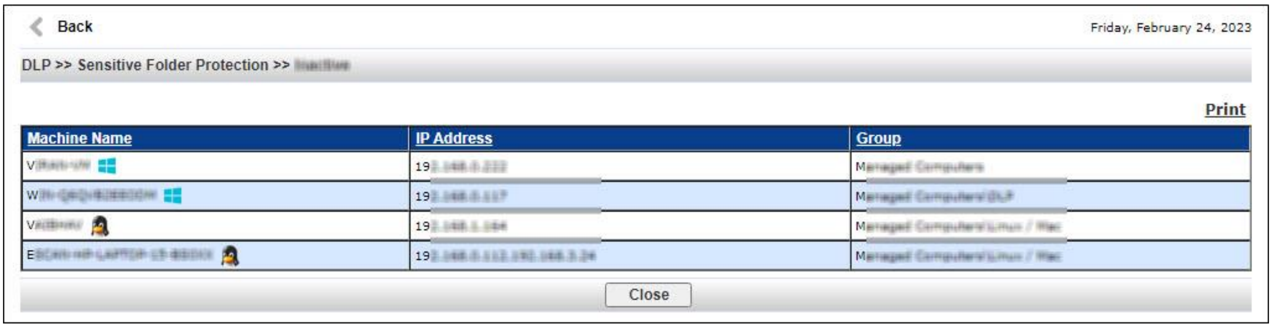
This chart displays the protection status of Sensitive Folder Protection module:



- **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.

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

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



Friday, February 24, 2023

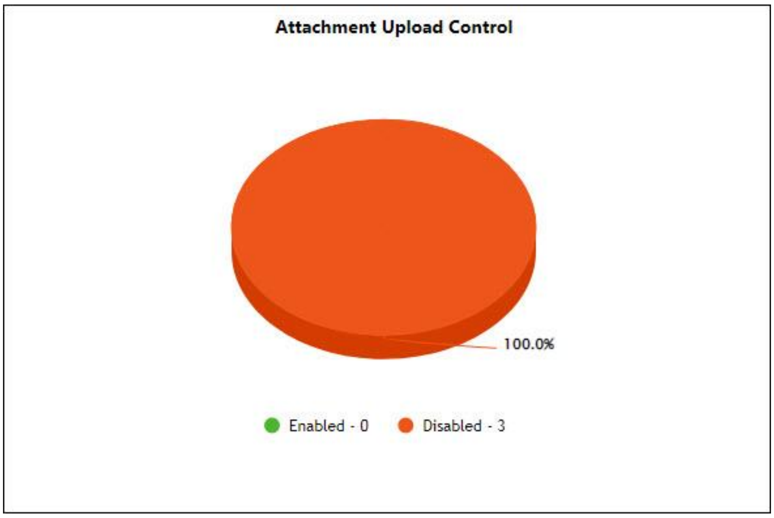
DLP >> Sensitive Folder Protection >> [redacted]

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

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

Attachment Upload Control

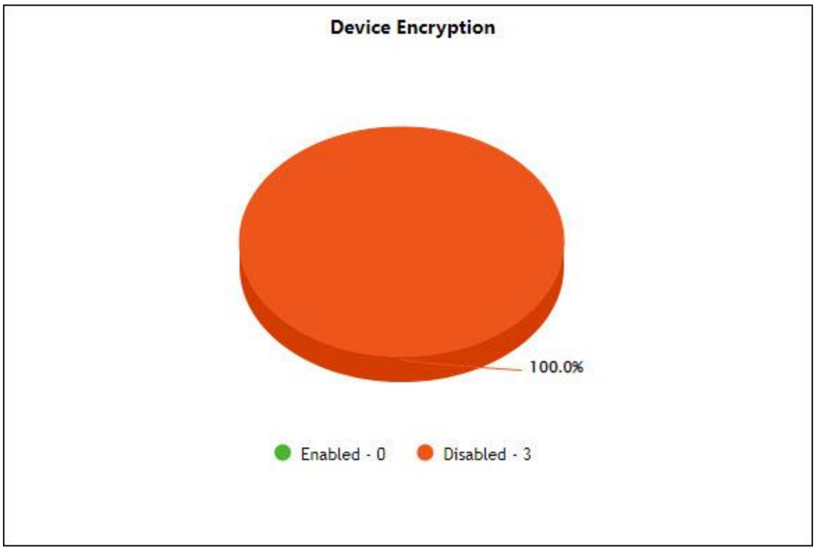
This chart displays the protection status of Attachment Upload Control module:



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

Device Encryption

This chart displays the protection status of Device Encryption module:

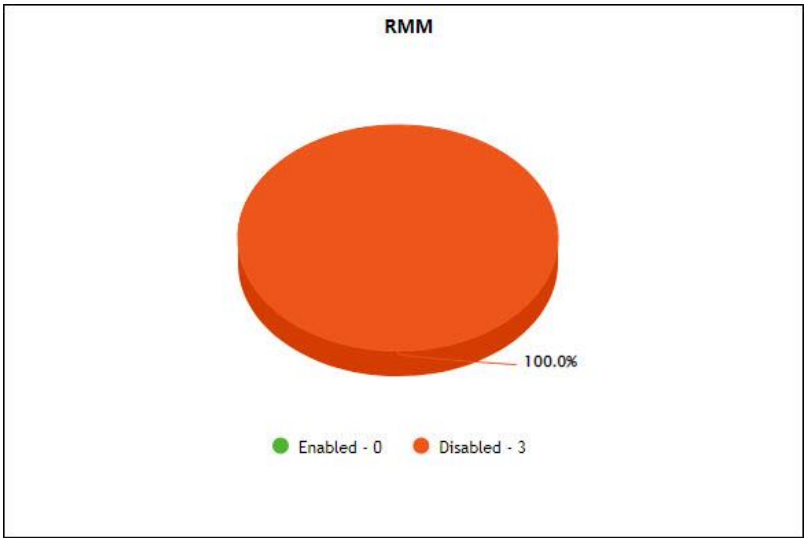


- **Enabled:** It shows the number of computers on which the Device Encryption is turned on.
- **Disabled:** It shows the number of computers on which the Device Encryption is turned off.

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

RMM

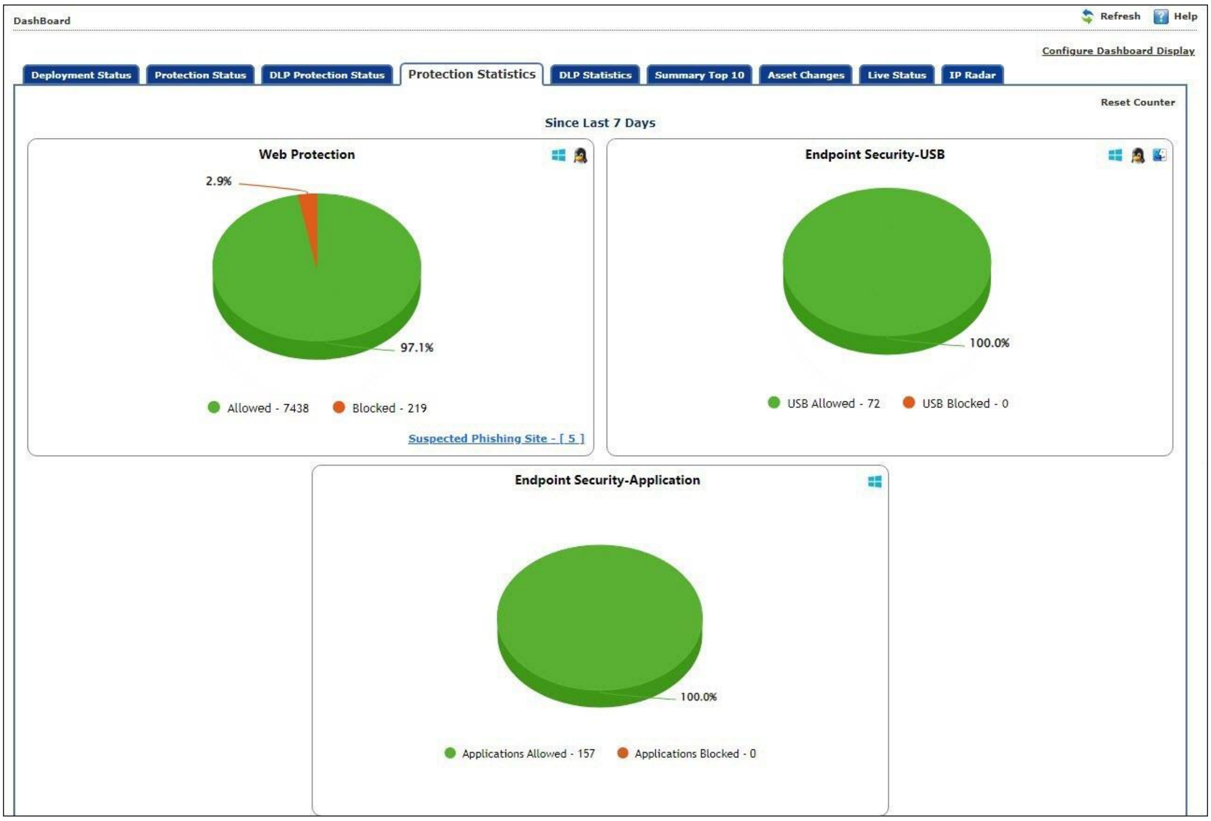
This chart displays the protection status of RMM (Remote Monitoring & Management) module:



- **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.

Protection Statistics

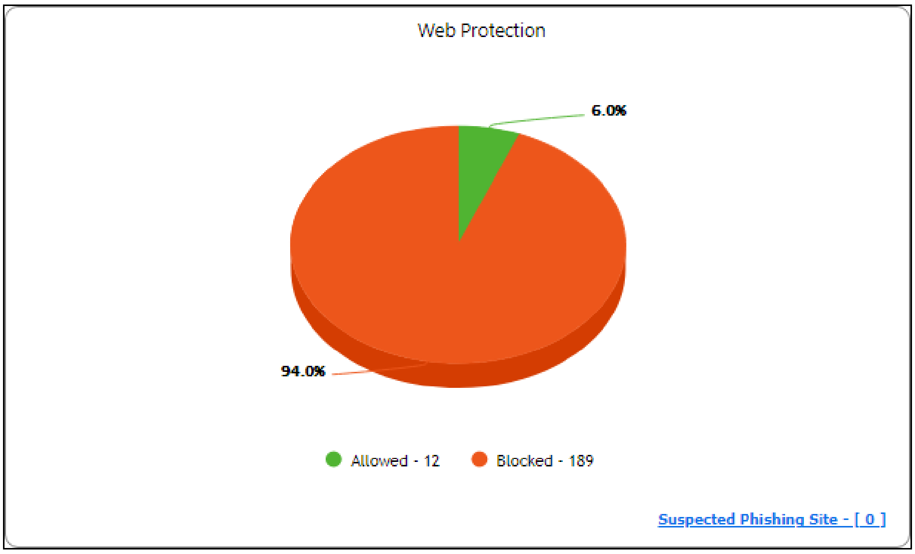
This tab displays activity statistics and action taken by all modules of eScan Client since last seven days in pie chart format.



Reset Counter

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

Web Protection



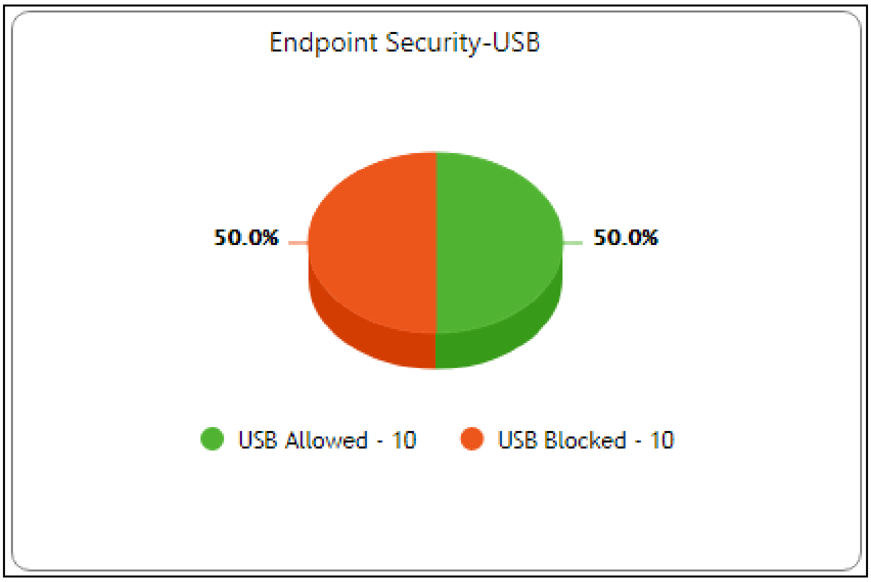
Allowed – It displays the number of websites to which access was allowed by Web Protection module.

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

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

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

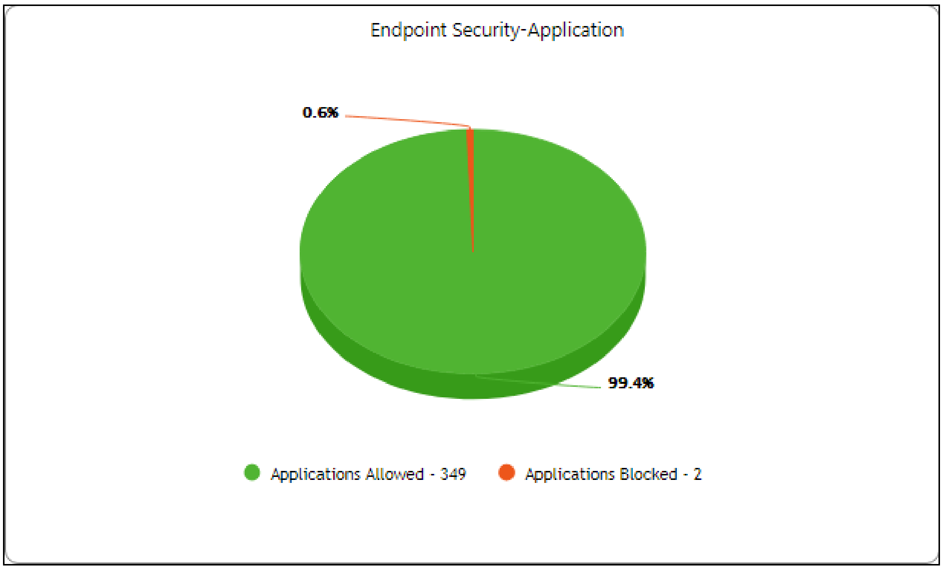
Endpoint Security-USB



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

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

Endpoint Security-Application

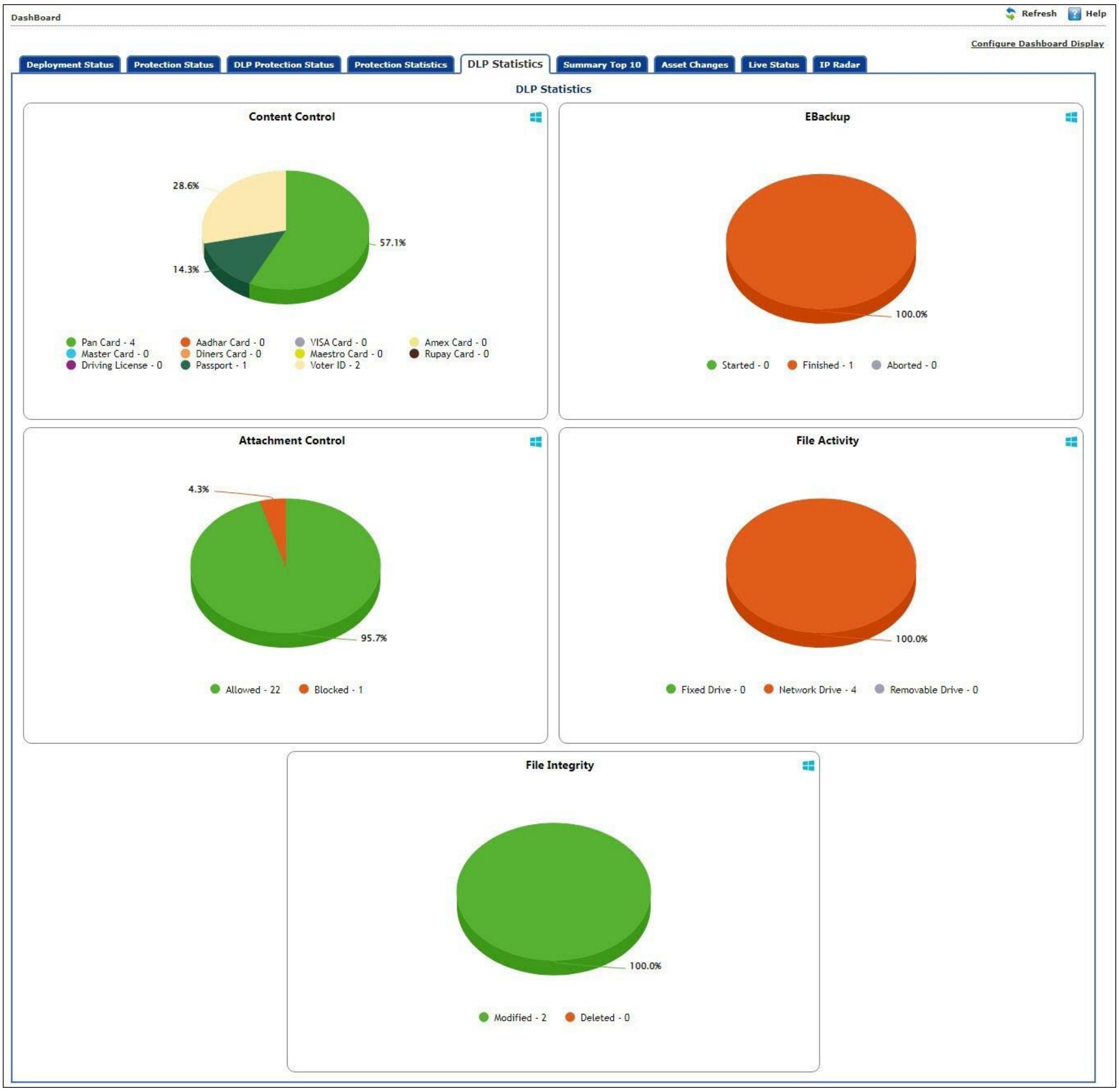


Applications Allowed – It displays the number of applications allowed by Endpoint Security-Application module.

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

DLP Statistics

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

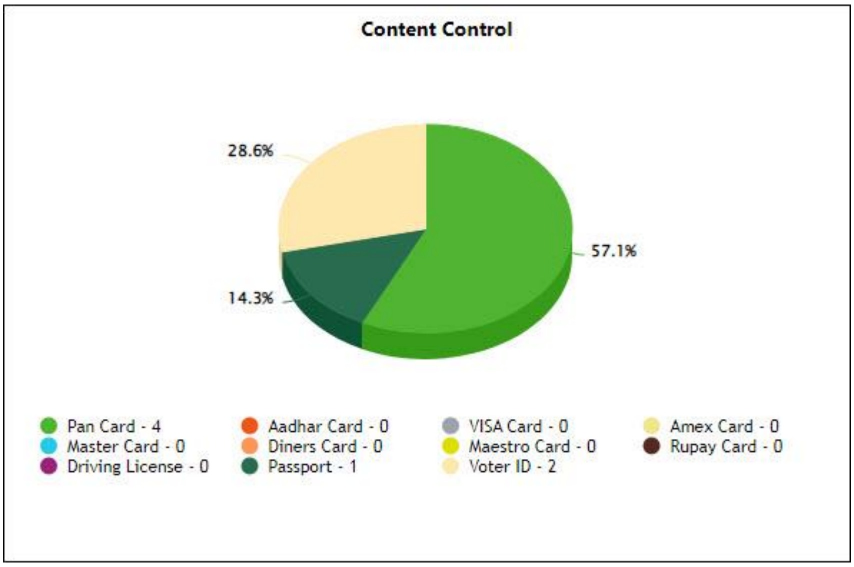


The DLP Statistics tab contains the statistical information of the following modules:

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

Content Control

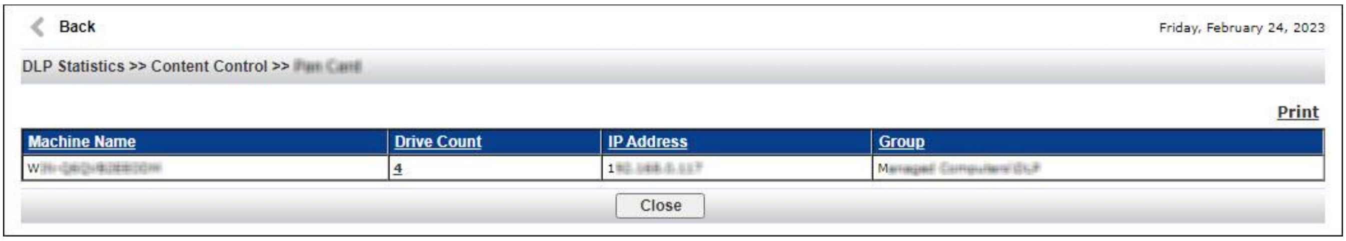
This chart displays the protection statistics of Content Control module:



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

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

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

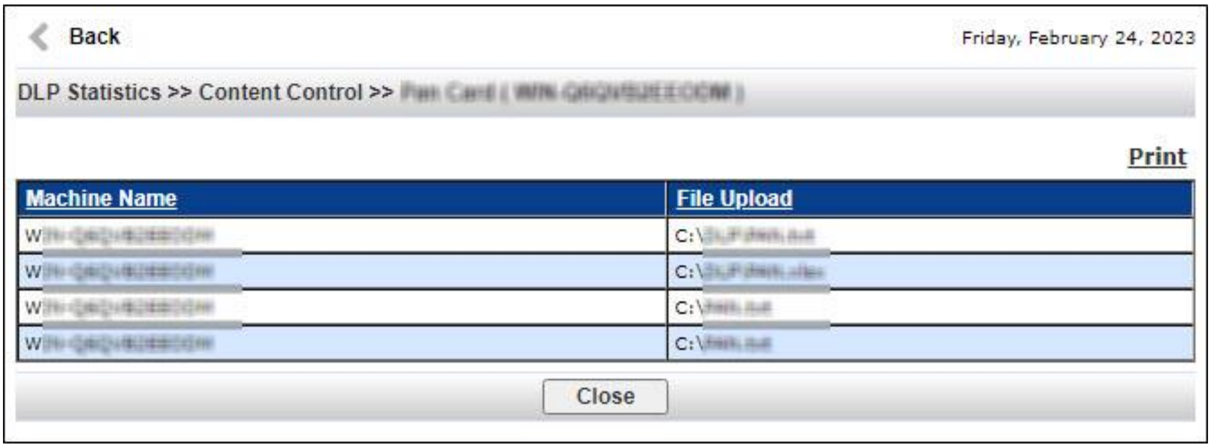


DLP Statistics >> Content Control >> [redacted]

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

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

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



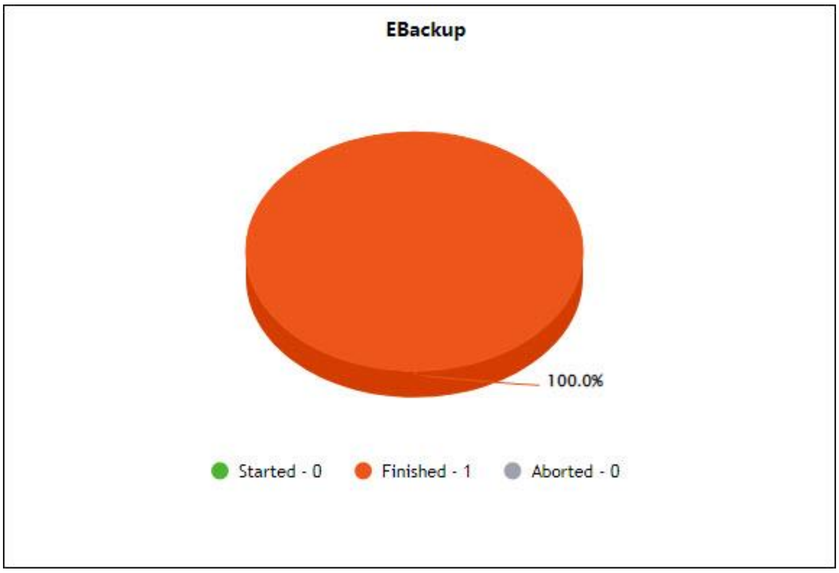
DLP Statistics >> Content Control >> [redacted]

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

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

EBackup

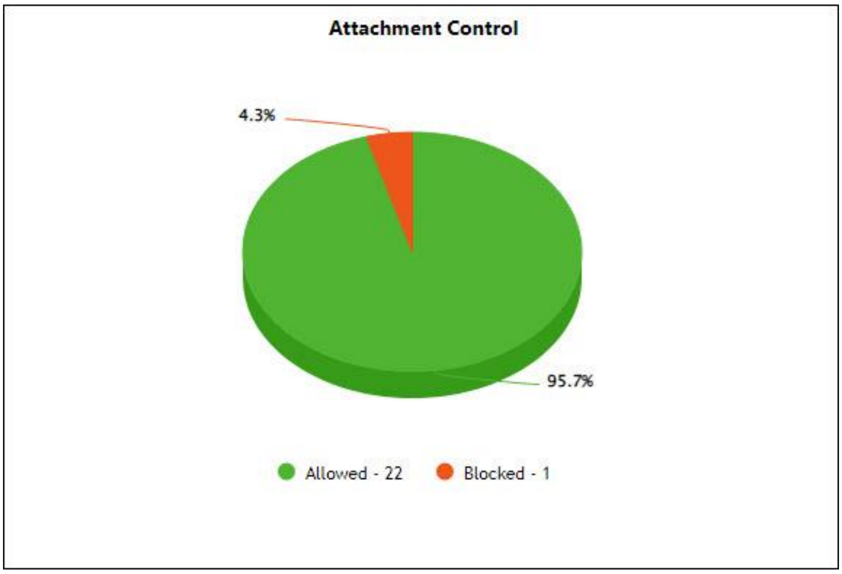
This chart displays the protection statistics of EBackup module:



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

Attachment Control

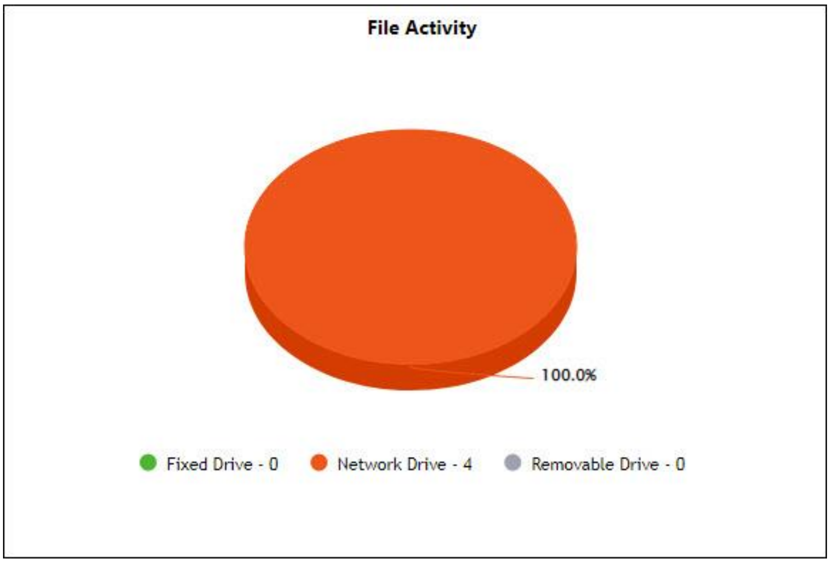
This chart displays the protection statistics of Attachment Control module:



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

File Activity

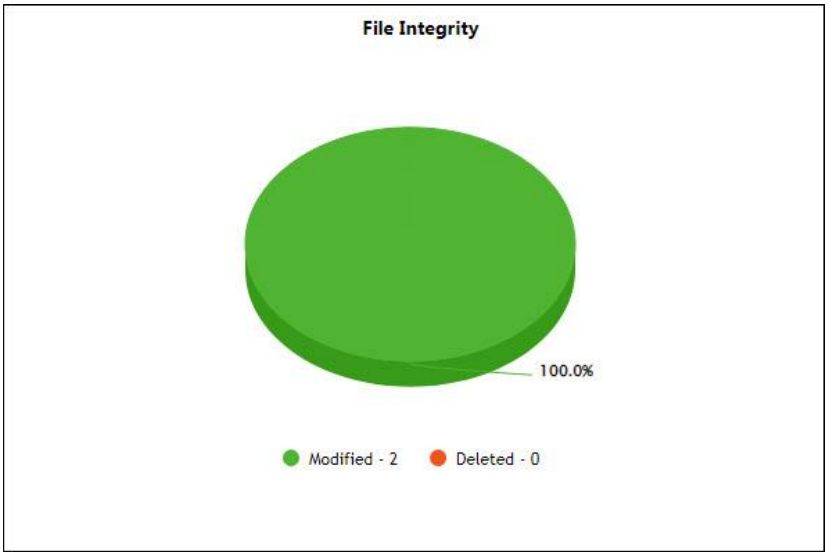
This chart displays the protection statistics of File Activity module:



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

File Integrity

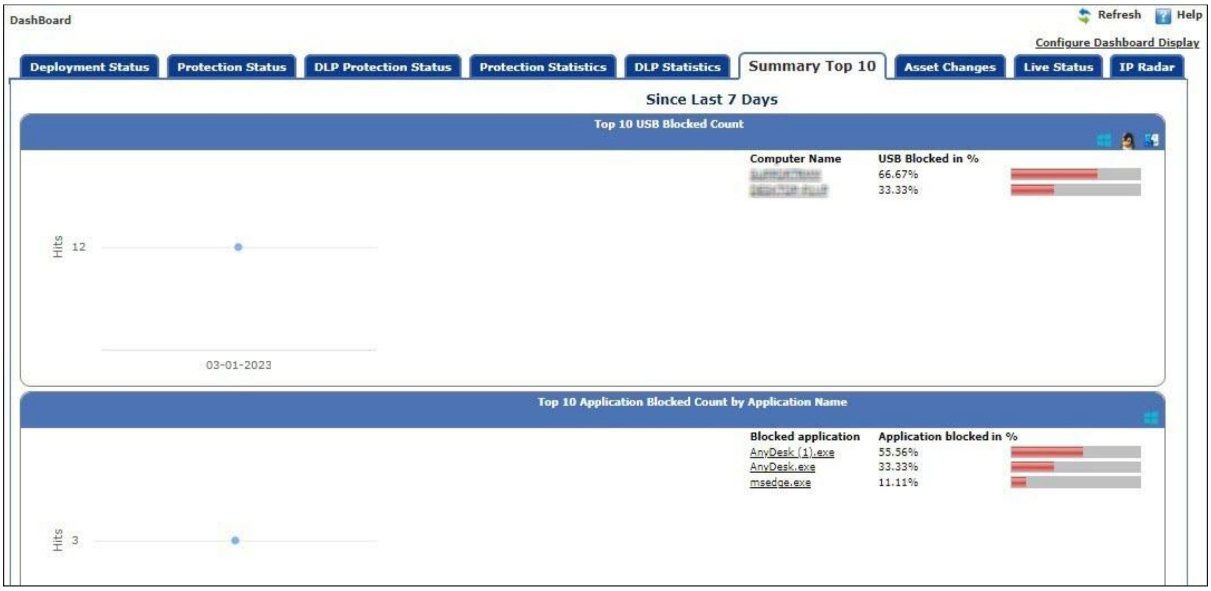
This chart displays the protection statistics of File Integrity module:



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

Summary Top 10

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



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

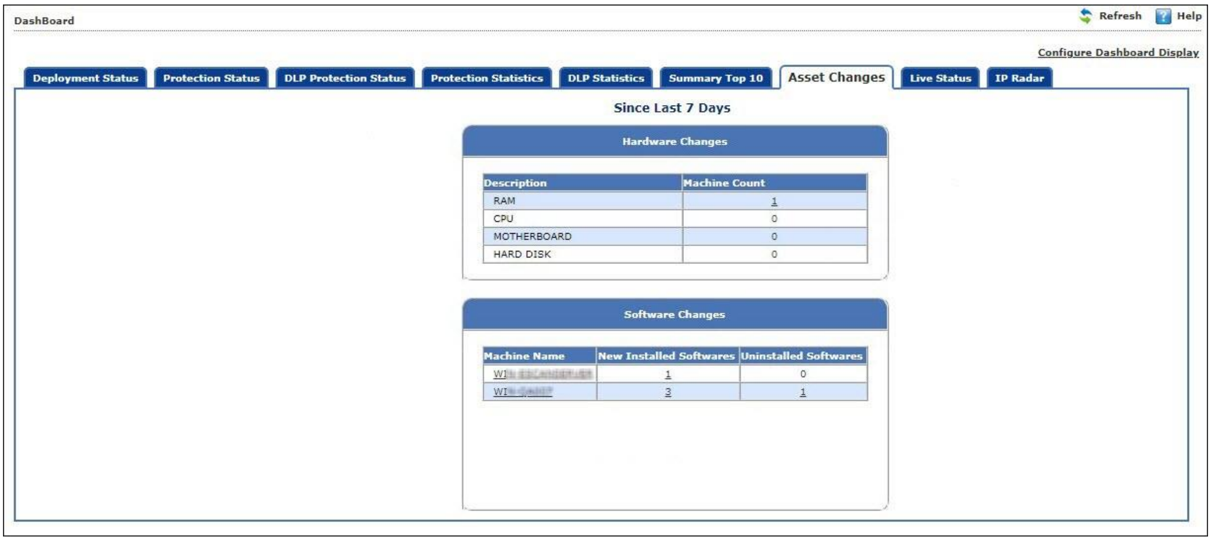
Blocked application	Application blocked in %
AnyDesk (1).exe	55.56%
AnyDesk.exe	33.33%
msedge.exe	11.11%

The tab displays the summary for following parameters:

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

Asset Changes

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



DashBoard

Since Last 7 Days

Hardware Changes

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

Software Changes

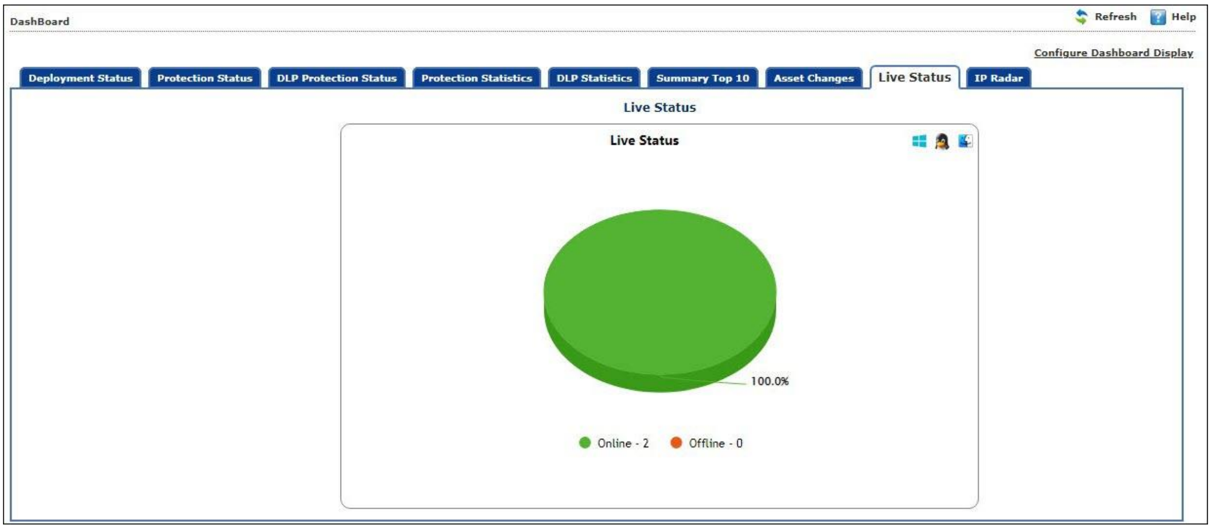
Machine Name	New Installed Softwares	Uninstalled Softwares
WI[redacted]	1	0
WI[redacted]	3	1

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

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

Live Status

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

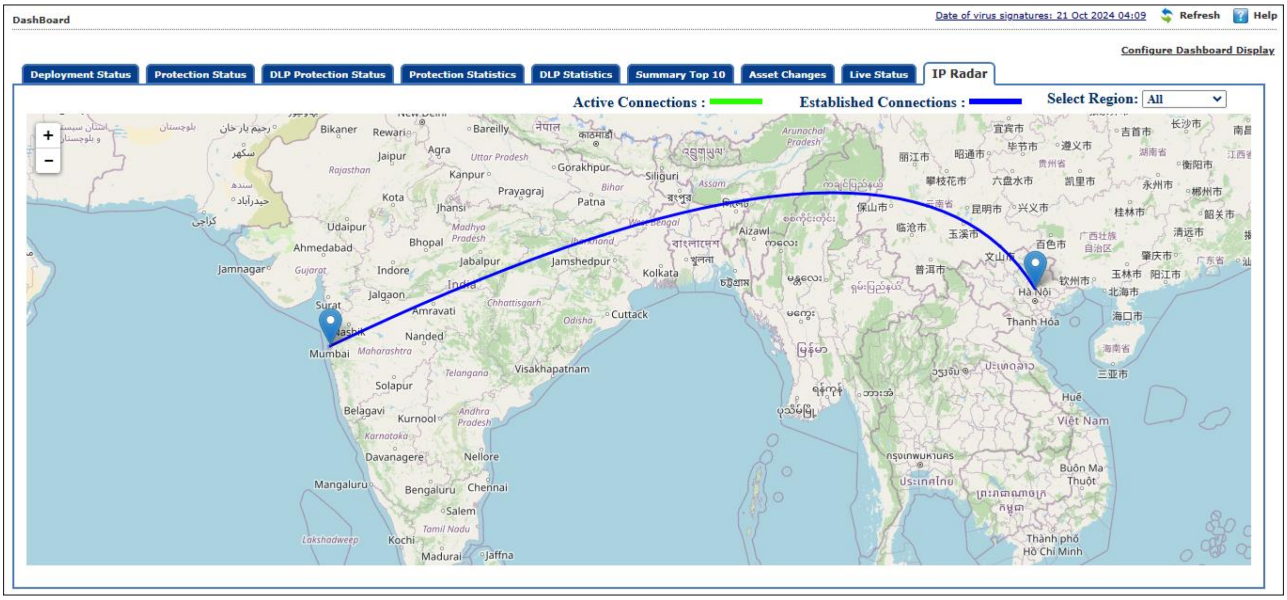


DashBoard

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

IP Radar

The IP Radar is a global map where you can view all the active and established IP connections initiated and connected to eScan server. This feature allows you to trace all the connections that are currently running via eScan server. In simple terms, when IP communication is initiated between XDR sensor and external resource globally, it will be captured and displayed on the map in real-time. IP Radar does not require any 3rd party vendor service(s) for functioning.



DashBoard

Date of virus signatures: 21 Oct 2024 04:09 Refresh Help

Configure Dashboard Display

Deployment Status | Protection Status | DLP Protection Status | Protection Statistics | DLP Statistics | Summary Top 10 | Asset Changes | Live Status | IP Radar

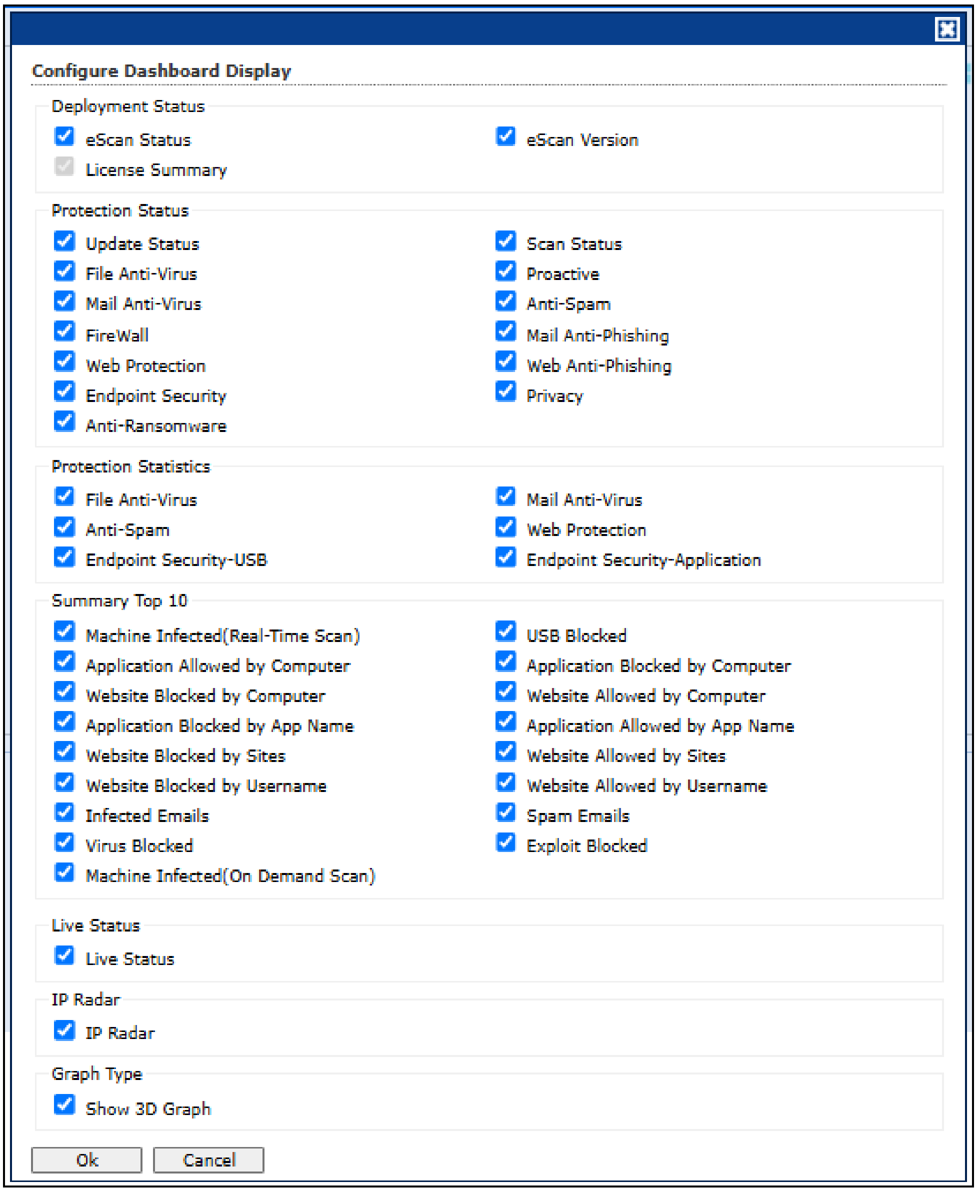
Active Connections : 🟩 Established Connections : 🟦 Select Region: All

The green marked connections are active connections and the blue ones are established connections. You can easily choose the region between **Domestic** and **Foreign** for specific view on the map. Or choose **All** for a broader view. For region selection, simply use provided drop-down at the top-right corner on the map. An active internet connection is required on the server machine for IP radar to work.

Configure the Dashboard Display

To configure the Dashboard display, follow the steps given below:

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



Configure Dashboard Display

Deployment Status
☑ eScan Status
☑ eScan Version
☑ License Summary

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

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

Summary Top 10
☑ Machine Infected(Real-Time Scan)
☑ USB Blocked
☑ Application Allowed by Computer
☑ Application Blocked by Computer
☑ Website Blocked by Computer
☑ Website Allowed by Computer
☑ Application Blocked by App Name
☑ Application Allowed by App Name
☑ Website Blocked by Sites
☑ Website Allowed by Sites
☑ Website Blocked by Username
☑ Website Allowed by Username
☑ Infected Emails
☑ Spam Emails
☑ Virus Blocked
☑ Exploit Blocked
☑ Machine Infected(On Demand Scan)

Live Status
☑ Live Status

IP Radar
☑ IP Radar

Graph Type
☑ Show 3D Graph

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

XDR Dashboard

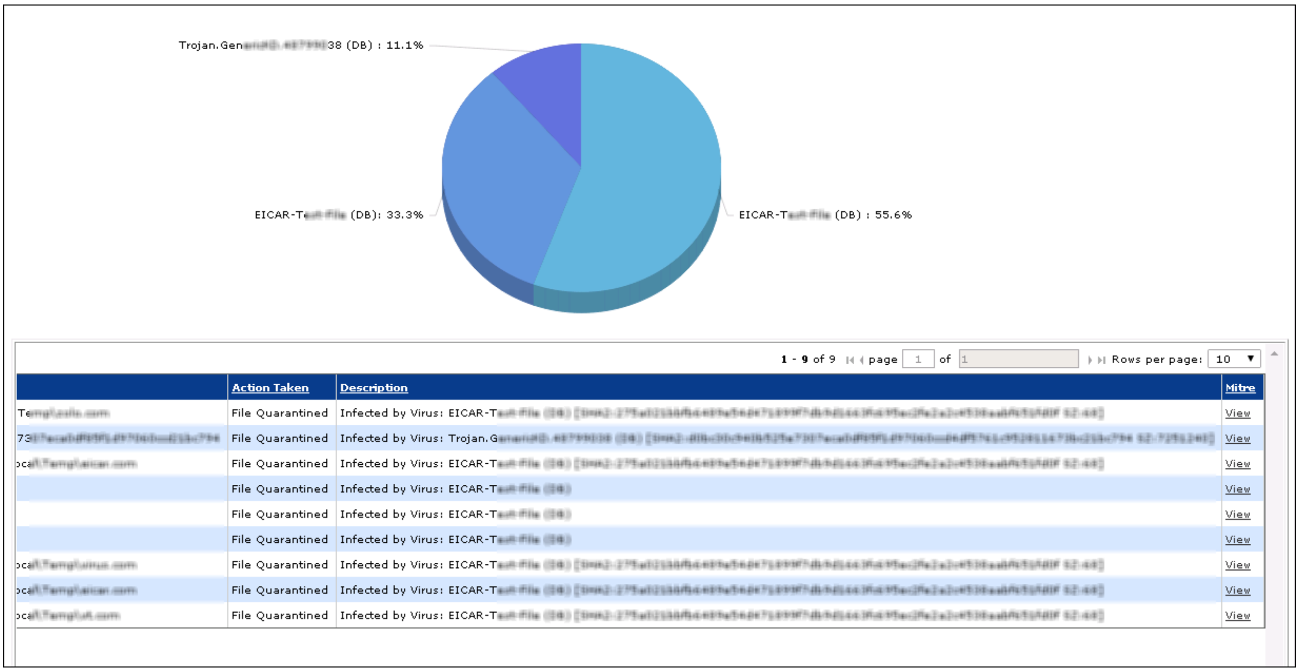
The XDR dashboard is primarily used to keep track of malicious activities and potential attacks by keeping a close eye on network. It analyses the detected threat and helps to determine the root cause of attacks. This dashboard consists of different tabs having multiple summary reports that are as follows:

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

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

Incident - eScan

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


Trojan.Gen[redacted]38 (DB) : 11.1%
EICAR-T[redacted] (DB): 33.3%
EICAR-T[redacted] (DB) : 55.6%

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

	Action Taken	Description	Mitre
Te[redacted]	File Quarantined	Infected by Virus: EICAR-T[redacted]	View
73[redacted]	File Quarantined	Infected by Virus: Trojan.G[redacted]	View
ocal[redacted]	File Quarantined	Infected by Virus: EICAR-T[redacted]	View
	File Quarantined	Infected by Virus: EICAR-T[redacted]	View
	File Quarantined	Infected by Virus: EICAR-T[redacted]	View
	File Quarantined	Infected by Virus: EICAR-T[redacted]	View
ocal[redacted]	File Quarantined	Infected by Virus: EICAR-T[redacted]	View
ocal[redacted]	File Quarantined	Infected by Virus: EICAR-T[redacted]	View
ocal[redacted]	File Quarantined	Infected by Virus: EICAR-T[redacted]	View

Filtering Incident – eScan Report

To filter the Incident – eScan as per your requirements, click **Filter Criteria** field.
Filter Criteria field expands.
Select the parameters you want to be included in the filtered report.

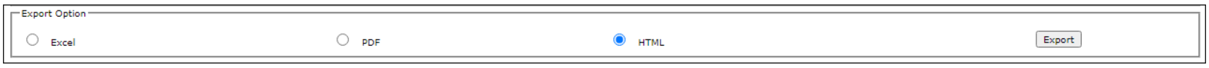
Include/Exclude
Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After making the necessary selections, click **Search**.
The Incident – eScan will be filtered according to your preferences.

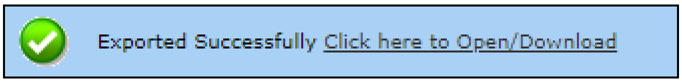
After applying filter the following type of the summary report will be generated. It consists of general information such as Client Date, Computer Name / IP, IP Address, User Name, Event Description, Action Taken, etc.

Exporting the Report

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


Export Option
○ Excel ○ PDF ● HTML

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


Exported Successfully Click here to Open/Download

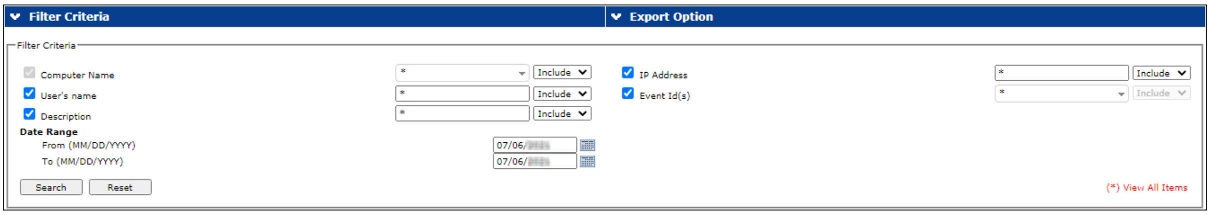
Click the link to open/download the file.

Incident - Windows

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

Filtering Incident – Windows Report

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



Filter Criteria
☑ Computer Name * Include
☑ User's name * Include
☑ Description * Include
☑ IP Address * Include
☑ Event Id(s) * Include
Date Range
From (MM/DD/YYYY) 07/06/[redacted]
To (MM/DD/YYYY) 07/06/[redacted]

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

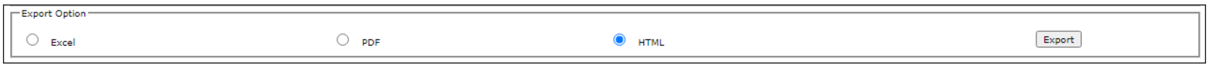
Include/Exclude
Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After making the necessary selections, click **Search**.
The Incident – Windows will be filtered according to your preferences.

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

Exporting the Report

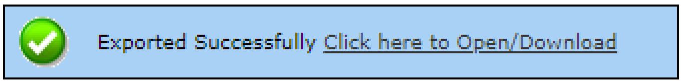
To export the Incident – Windows Report, click **Export Option**.
Export Option field expands.



Export Option

○ Excel ○ PDF ● HTML

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



Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Incident - EDR

Incident - XDR tab provides the summary report of all the events from the endpoints in the network on the basis of severity for advanced investigation and response. It blocks/remove the suspicious files and then alerts the admin for further investigation and analysis of it.
eScan Vision Core XDR solution provides different types of report such as Virus, PowerShell, and many more based on the different types of threats and malicious activities. The admin can select the report from the drop-down menu according to the requirement and get the detailed report about the same. The types of reports are as follow:

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

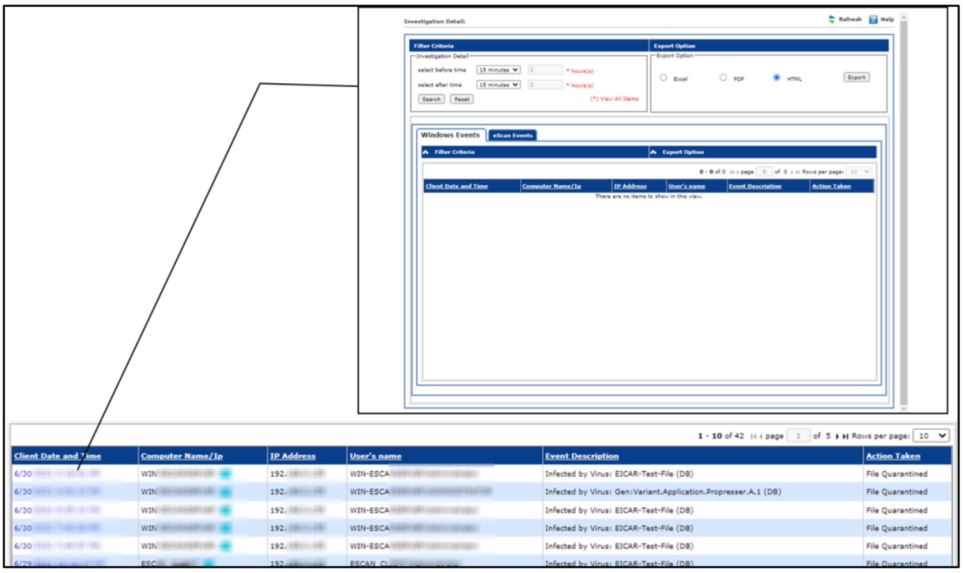
- Password Archive: Blocked
- User: Blocked

Report Type

Each report is unique and used for in-depth analysis of the potential attacks or suspicious activities. For example, Proactive Behavioral Analysis Engine (PBAE) generates the report based on the collected events that are blocked due to suspicious behavior in the endpoints. The Virus report generates the summary for the virus that were detected and blocked in the network.

For example, the following figure gives the summary of the virus report:

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



Investigation Detail:

Filter Criteria

Investigation Detail

select before time 15 minutes 2 * hours(s)

select after time 15 minutes 2 * hours(s)

(*) View All Items

Export Option

Export Option

○ Excel ○ PDF ● HTML

0 - 0 of 0 page 0 of 0 Rows per page: 10

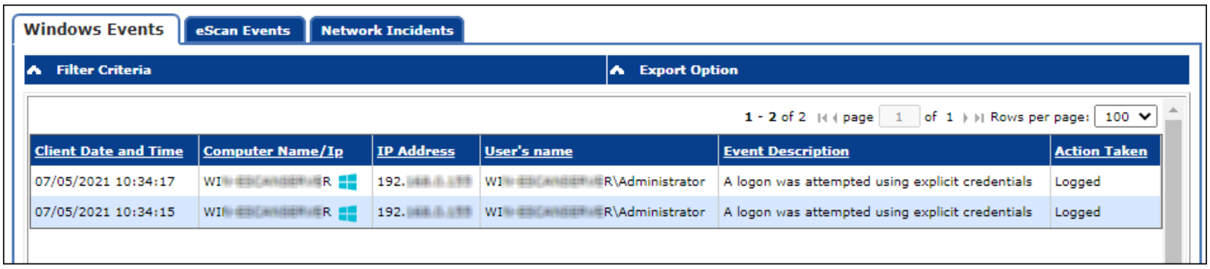
Client Date and Time	Computer Name/Ip	IP Address	User's name	Event Description	Action Taken

There are no items to show in this view.

1 - 10 of 42 page 1 of 5 Rows per page: 10

Client Date and Time	Computer Name/Ip	IP Address	User's name	Event Description	Action Taken
6/30 [redacted]	WIN [redacted]	192. [redacted]	WIN-ESCA [redacted]	Infected by Virus: EICAR-Test-File (DB)	File Quarantined
6/30 [redacted]	WIN [redacted]	192. [redacted]	WIN-ESCA [redacted]	Infected by Virus: Gen:Variant.Application.Propresser.A.1 (DB)	File Quarantined
6/30 [redacted]	WIN [redacted]	192. [redacted]	WIN-ESCA [redacted]	Infected by Virus: EICAR-Test-File (DB)	File Quarantined
6/30 [redacted]	WIN [redacted]	192. [redacted]	WIN-ESCA [redacted]	Infected by Virus: EICAR-Test-File (DB)	File Quarantined
6/30 [redacted]	WIN [redacted]	192. [redacted]	WIN-ESCA [redacted]	Infected by Virus: EICAR-Test-File (DB)	File Quarantined
6/29 [redacted]	ESC [redacted]	192. [redacted]	ESCAN_CL [redacted]	Infected by Virus: EICAR-Test-File (DB)	File Quarantined

The detailed report will be generated.



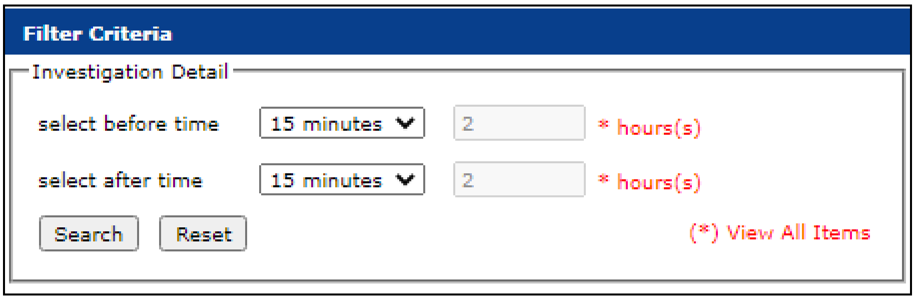
1 - 2 of 2 page 1 of 1 Rows per page: 100

Client Date and Time	Computer Name/Ip	IP Address	User's name	Event Description	Action Taken
07/05/2021 10:34:17	WI [redacted] R	192. [redacted]	WI [redacted] R\Administrator	A logon was attempted using explicit credentials	Logged
07/05/2021 10:34:15	WI [redacted] R	192. [redacted]	WI [redacted] R\Administrator	A logon was attempted using explicit credentials	Logged

Windows Events: It displays the Windows event for the filtered time frame.
eScan Events: It displays the eScan events for the filtered time frame.
Network Incident: It displays the Network Incident events for the filtered time frame.

Filtering Incident – EDR Report for Specific Incident

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



select before time: 15 minutes, 2 * hours(s)

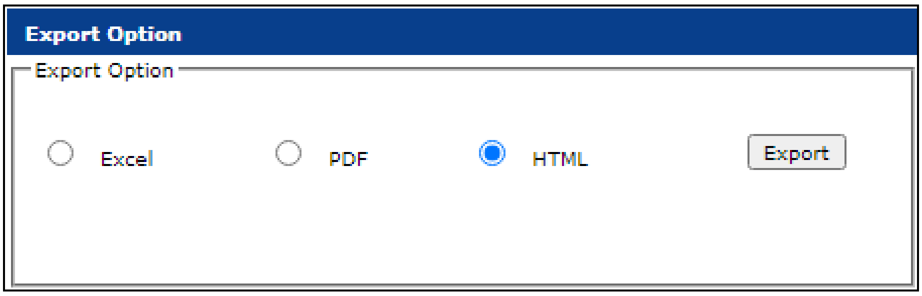
select after time: 15 minutes, 2 * hours(s)

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

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

Exporting Incident – EDR Report for Specific Incident

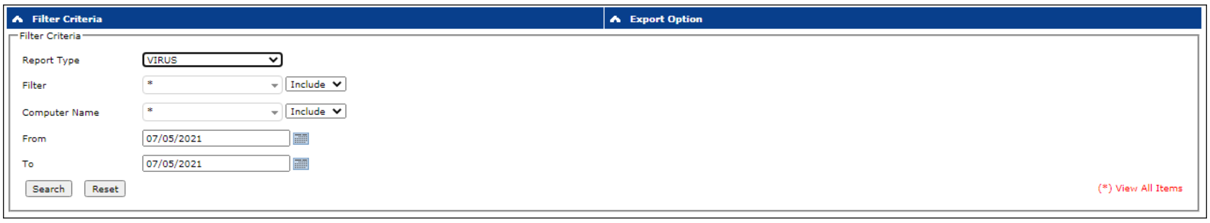
eScan EDR provides investigation details based on the Windows event and eScan events. It allows the admin to export the investigation reports in various formats such as HTML, PDF, or Excel.



○ Excel ○ PDF ● HTML

Filtering Incident – EDR Report

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



Report Type: VIRUS

Filter: * Include

Computer Name: * Include

From: 07/05/2021

To: 07/05/2021

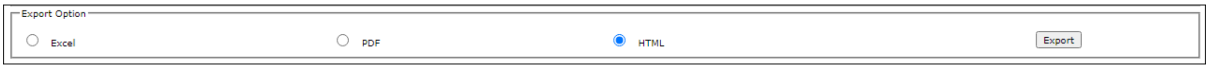
Select the parameters you want to be included in the filtered report.

Include/Exclude
Selecting Include/Exclude for a parameter lets you include or exclude it from the report.77

After making the necessary selections, click **Search.**
The Incident – EDR will be filtered according to your preferences.

Exporting the Report

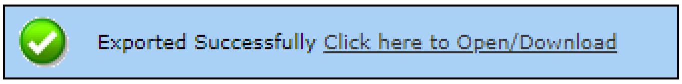
To export the Incident – EDR Report, click **Export Option**.
Export Option field expands.



Export Option

○ Excel ○ PDF ● HTML

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

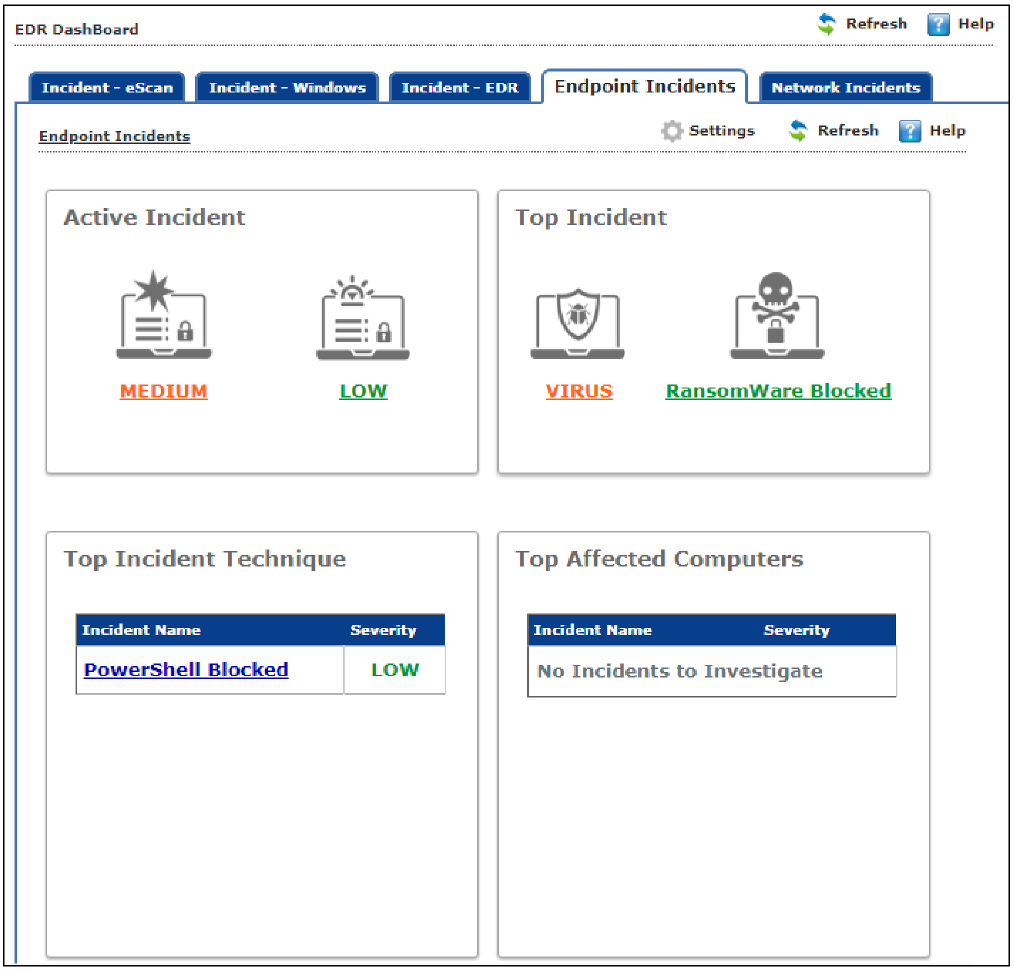


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Endpoint Incidents

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



Incident Name	Severity
PowerShell Blocked	LOW

Incident Name	Severity
No Incidents to Investigate	

Active Incidents

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

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

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

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

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

Adding Specific Incident for Monitoring

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

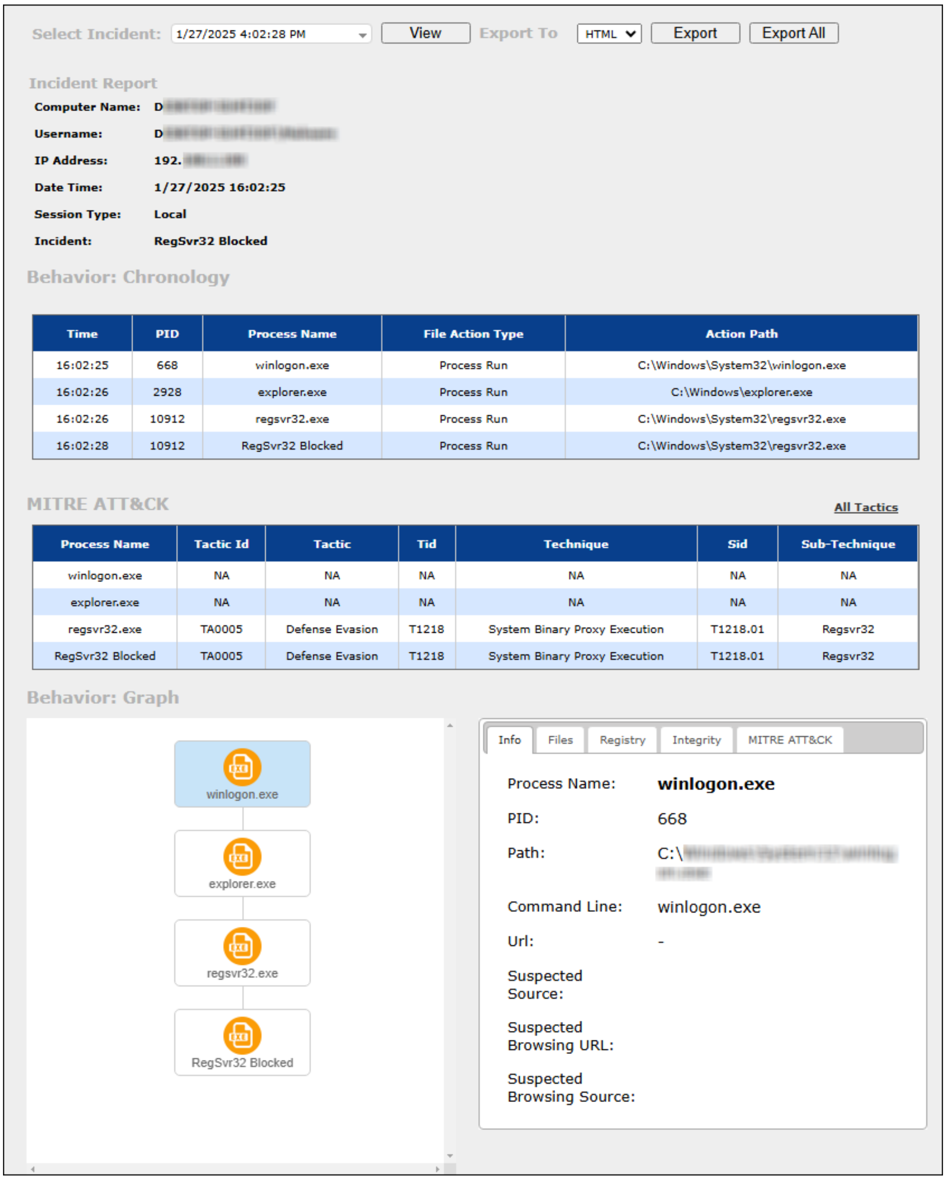
1. From the list of the detected incident, select the specific incident according to the requirement.
2. Click **Add To Monitor**.
   The specific incident will be added to the monitoring list.

Viewing the Details of the Specific Incident

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

To view the detailed process tree follow the below steps:

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



Select Incident: 1/27/2025 4:02:28 PM

Incident Report

Computer Name:	D[redacted]
Username:	D[redacted]
IP Address:	192.[redacted]
Date Time:	1/27/2025 16:02:25
Session Type:	Local
Incident:	RegSvr32 Blocked

Behavior: Chronology

Time	PID	Process Name	File Action Type	Action Path
16:02:25	668	winlogon.exe	Process Run	C:\Windows\System32\winlogon.exe
16:02:26	2928	explorer.exe	Process Run	C:\Windows\explorer.exe
16:02:26	10912	regsvr32.exe	Process Run	C:\Windows\System32\regsvr32.exe
16:02:28	10912	RegSvr32 Blocked	Process Run	C:\Windows\System32\regsvr32.exe

MITRE ATT&CK

All Tactics

Process Name	Tactic Id	Tactic	Tid	Technique	Sid	Sub-Technique
winlogon.exe	NA	NA	NA	NA	NA	NA
explorer.exe	NA	NA	NA	NA	NA	NA
regsvr32.exe	TA0005	Defense Evasion	T1218	System Binary Proxy Execution	T1218.01	Regsvr32
RegSvr32 Blocked	TA0005	Defense Evasion	T1218	System Binary Proxy Execution	T1218.01	Regsvr32

Behavior: Graph

Process Name:	winlogon.exe
PID:	668
Path:	C:\[redacted]
Command Line:	winlogon.exe
Url:	-
Suspected Source:	
Suspected Browsing URL:	
Suspected Browsing Source:	

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

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

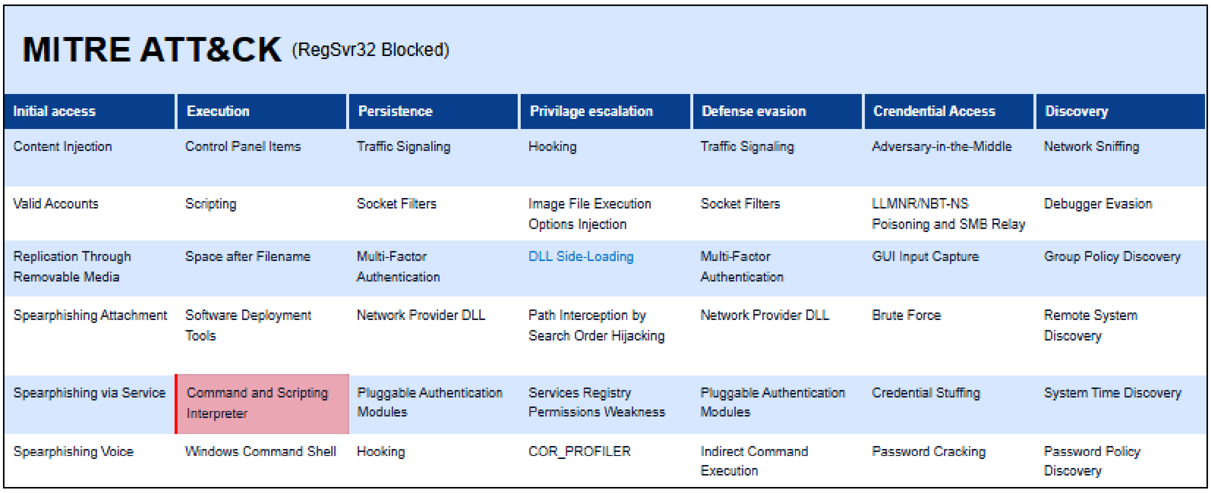
The same report can be exported into different format such as HTML and PDF.

MITRE ATT&CK Framework

The MITRE ATT&CK framework analyzes the events and incidents on a server machine and distributes their packet information i.e. TTPs (Tactics, Techniques, and Procedures) used in the incident to eScan protected endpoints. Further, the endpoints with the help of XDR, take appropriate action to stay alert regarding the suspected events and the incidents. It is an Auto-remediation process which involves advanced framing of the incidents.

Organization's threat intelligence team can use this framework to detect adversarial behavior and to map observed activity to specific ATT&CK techniques. To view all the MITRE ATT&CK tactics, follow the steps given below:

1. In the Incident Report window, click on **All tactics** option under ‘MITRE ATT&CK’ section. The MITRE ATT&CK window opens, highlighting the correct tactic used among all tactics.



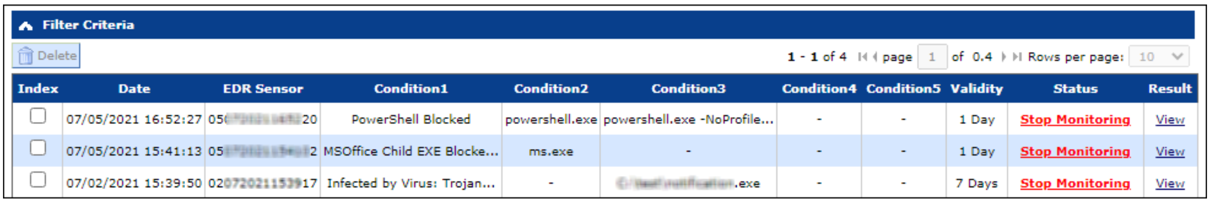
MITRE ATT&CK (RegSvr32 Blocked)

Initial access	Execution	Persistence	Privilage escalation	Defense evasion	Crendential Access	Discovery
Content Injection	Control Panel Items	Traffic Signaling	Hooking	Traffic Signaling	Adversary-in-the-Middle	Network Sniffing
Valid Accounts	Scripting	Socket Filters	Image File Execution Options Injection	Socket Filters	LLMNR/NBT-NS Poisoning and SMB Relay	Debugger Evasion
Replication Through Removable Media	Space after Filename	Multi-Factor Authentication	DLL Side-Loading	Multi-Factor Authentication	GUI Input Capture	Group Policy Discovery
Spearphishing Attachment	Software Deployment Tools	Network Provider DLL	Path Interception by Search Order Hijacking	Network Provider DLL	Brute Force	Remote System Discovery
Spearphishing via Service	Command and Scripting Interpreter	Pluggable Authentication Modules	Services Registry Permissions Weakness	Pluggable Authentication Modules	Credential Stuffing	System Time Discovery
Spearphishing Voice	Windows Command Shell	Hooking	COR_PROFILER	Indirect Command Execution	Password Cracking	Password Policy Discovery

This information can also be used to share intelligence on emerging threats, helping organizations stay up-to-date with evolving attack methods.

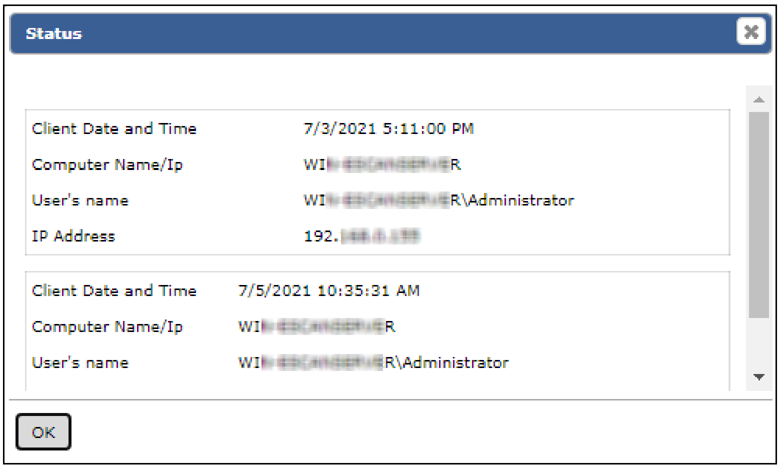
Viewing the Details of Monitoring Incident

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



Index	Date	EDR Sensor	Condition1	Condition2	Condition3	Condition4	Condition5	Validity	Status	Result
□	07/05/2021 16:52:27	05[redacted]20	PowerShell Blocked	powershell.exe	powershell.exe -NoProfile...	-	-	1 Day	Stop Monitoring	View
□	07/05/2021 15:41:13	05[redacted]2	MSOffice Child EXE Blocke...	ms.exe	-	-	-	1 Day	Stop Monitoring	View
□	07/02/2021 15:39:50	02[redacted]17	Infected by Virus: Trojan...	-	[redacted].exe	-	-	7 Days	Stop Monitoring	View

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



Status

Client Date and Time	7/3/2021 5:11:00 PM
Computer Name/Ip	WI[redacted]R
User's name	WI[redacted]R\Administrator
IP Address	192.[redacted]

Client Date and Time	7/5/2021 10:35:31 AM
Computer Name/Ip	WI[redacted]R
User's name	WI[redacted]R\Administrator

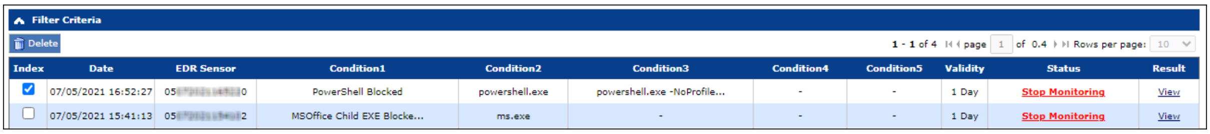
This will display the details of the same incident that were detected from all the endpoints in the network.

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

Deleting the Monitoring Incident

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

1. Select the specific incident from the list.



1 - 1 of 4 page 1 of 0.4 Rows per page: 10

Index	Date	EDR Sensor	Condition1	Condition2	Condition3	Condition4	Condition5	Validity	Status	Result
☑	07/05/2021 16:52:27	05[redacted]0	PowerShell Blocked	powershell.exe	powershell.exe -NoProfile...	-	-	1 Day	Stop Monitoring	View
□	07/05/2021 15:41:13	05[redacted]2	MSOffice Child EXE Blocke...	ms.exe	-	-	-	1 Day	Stop Monitoring	View

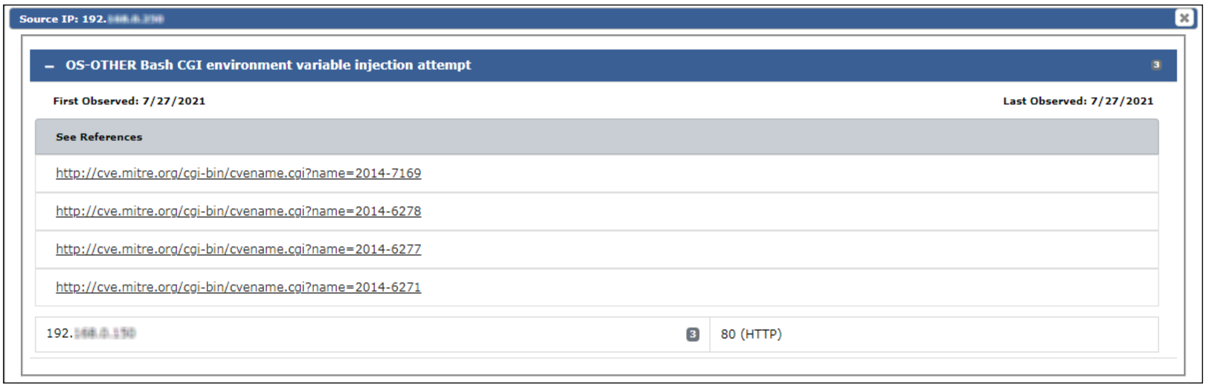
2. Click **Delete**.
   The specific incident will be deleted.

Network Incidents

In this tab, multiple network incident records are displayed with information about the incident such as source and destination IP address, port number, incident name, and more. Integrated with the Nemasis Passive Vulnerability Scanner (PVS), eScan Server gathers all the security events that help the administrators for centralized monitoring, analysis, and reporting.

Top Source

This will display the list of sources that were detected based on different pre-defined threshold values. To get the details, click the specific IP address.



Source IP: 192.[redacted]

– OS-OTHER Bash CGI environment variable injection attempt 3

First Observed: 7/27/2021 Last Observed: 7/27/2021

See References

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-7169

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6278

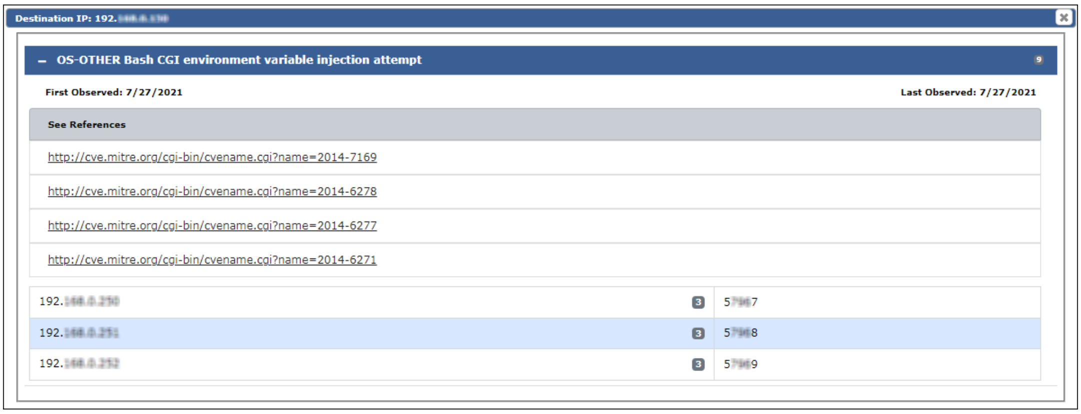
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6271

192.[redacted]	3	80 (HTTP)

Top Destination

This will display the list of destinations that were detected based on different pre-defined threshold values. To get the details, click the specific IP address.



Destination IP: 192.[redacted]

– OS-OTHER Bash CGI environment variable injection attempt 9

First Observed: 7/27/2021 Last Observed: 7/27/2021

See References

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-7169

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6278

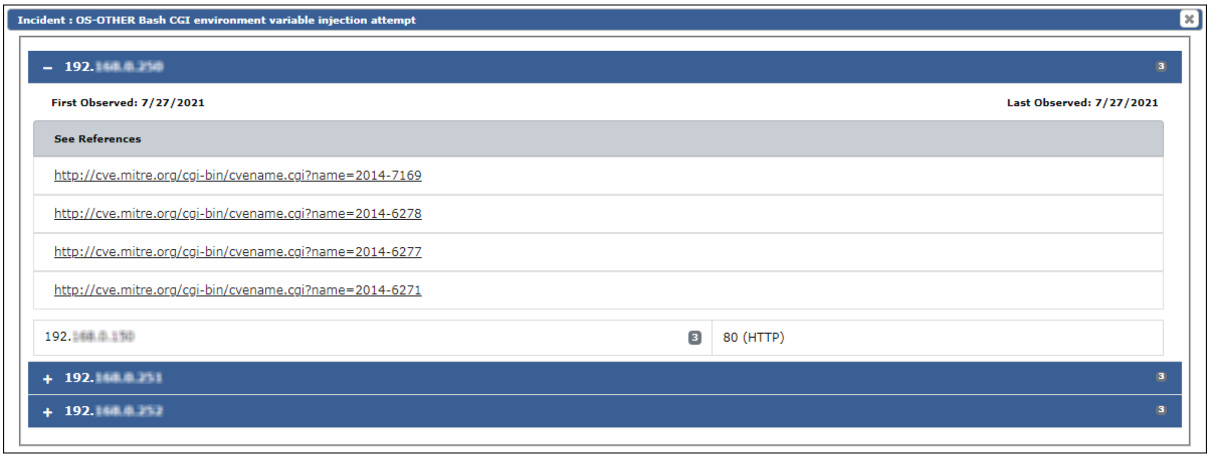
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6271

192.[redacted]	3	5[redacted]7
192.[redacted]	3	5[redacted]8
192.[redacted]	3	5[redacted]9

Top Incident

This will display the list of top incidents that were detected based on different pre-defined threshold values. To get the details, click the specific incident.



Incident : OS-OTHER Bash CGI environment variable injection attempt

– 192.[redacted] 3

First Observed: 7/27/2021 Last Observed: 7/27/2021

See References

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-7169

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6278

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6271

192.[redacted] 3 80 (HTTP)

+ 192.[redacted] 3

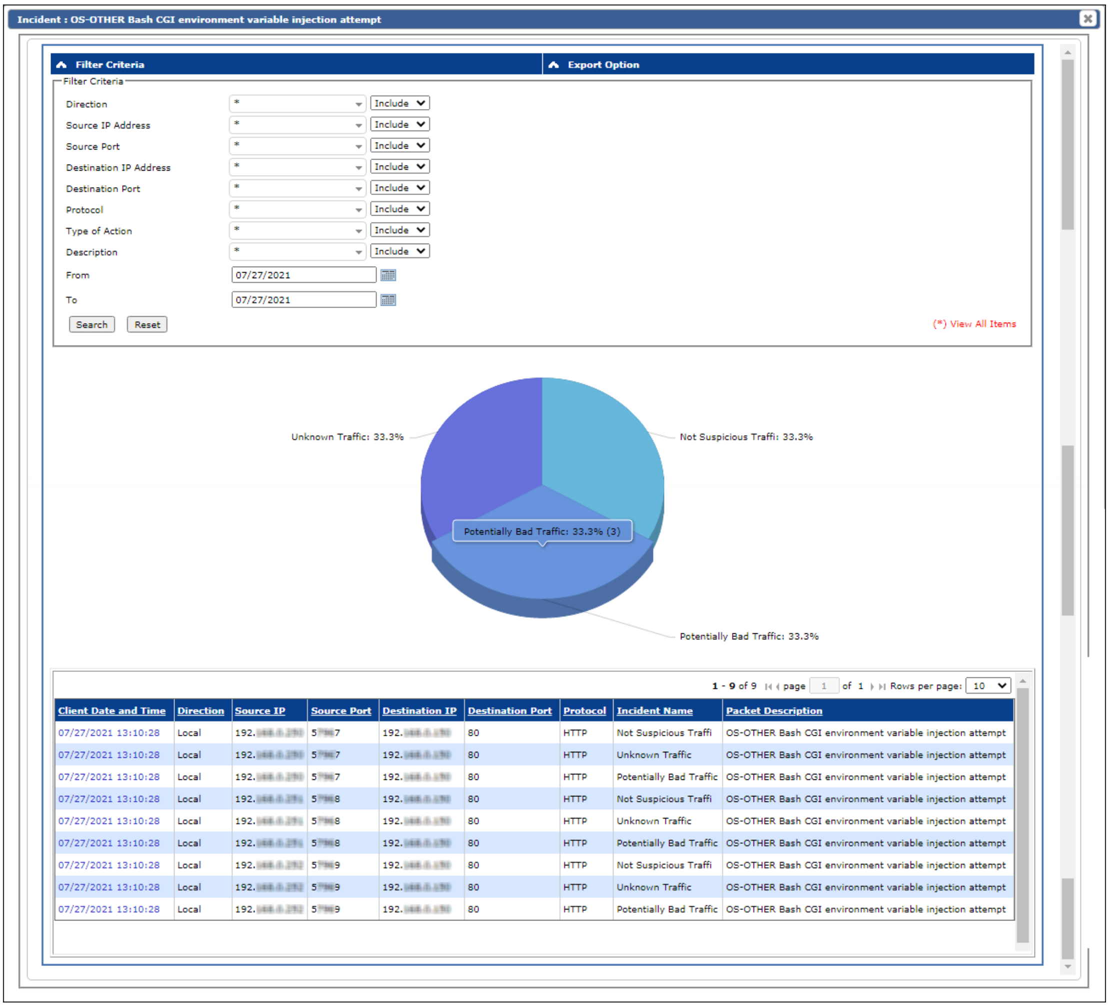
+ 192.[redacted] 3

All Incident

This will have an option to view all the incidents without of specific filter. To view the incidents, click on **View All Records**.

Viewing the Network Incident

To view all the incident, click **view all records**. The record window will be displayed.



Incident : OS-OTHER Bash CGI environment variable injection attempt

Filter Criteria
Export Option

Filter Criteria

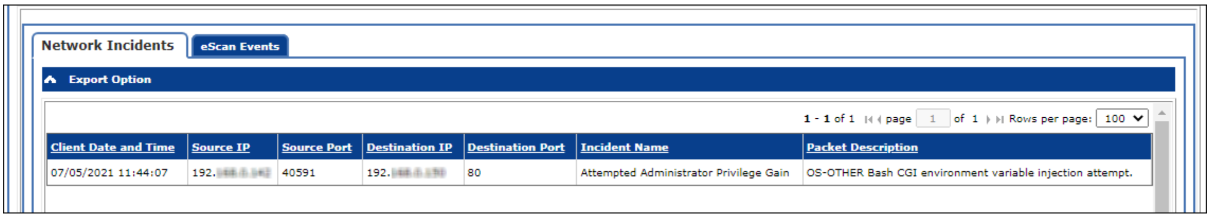
Direction	*	Include
Source IP Address	*	Include
Source Port	*	Include
Destination IP Address	*	Include
Destination Port	*	Include
Protocol	*	Include
Type of Action	*	Include
Description	*	Include
From	07/27/2021	
To	07/27/2021	

Search
Reset
(*) View All Items
Unknown Traffic: 33.3%
Not Suspicious Traffi: 33.3%
Potentially Bad Traffic: 33.3% (3)
Potentially Bad Traffic: 33.3%

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

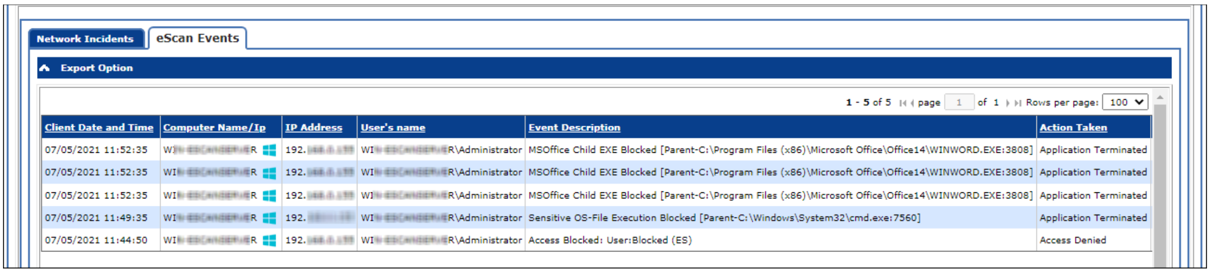
Client Date and Time	Direction	Source IP	Source Port	Destination IP	Destination Port	Protocol	Incident Name	Packet Description
07/27/2021 13:10:28	Local	192.[redacted]	5[redacted]7	192.[redacted]	80	HTTP	Not Suspicious Traffi	OS-OTHER Bash CGI environment variable injection attempt
07/27/2021 13:10:28	Local	192.[redacted]	5[redacted]7	192.[redacted]	80	HTTP	Unknown Traffic	OS-OTHER Bash CGI environment variable injection attempt
07/27/2021 13:10:28	Local	192.[redacted]	5[redacted]7	192.[redacted]	80	HTTP	Potentially Bad Traffic	OS-OTHER Bash CGI environment variable injection attempt
07/27/2021 13:10:28	Local	192.[redacted]	5[redacted]8	192.[redacted]	80	HTTP	Not Suspicious Traffi	OS-OTHER Bash CGI environment variable injection attempt
07/27/2021 13:10:28	Local	192.[redacted]	5[redacted]8	192.[redacted]	80	HTTP	Unknown Traffic	OS-OTHER Bash CGI environment variable injection attempt
07/27/2021 13:10:28	Local	192.[redacted]	5[redacted]8	192.[redacted]	80	HTTP	Potentially Bad Traffic	OS-OTHER Bash CGI environment variable injection attempt
07/27/2021 13:10:28	Local	192.[redacted]	5[redacted]9	192.[redacted]	80	HTTP	Not Suspicious Traffi	OS-OTHER Bash CGI environment variable injection attempt
07/27/2021 13:10:28	Local	192.[redacted]	5[redacted]9	192.[redacted]	80	HTTP	Unknown Traffic	OS-OTHER Bash CGI environment variable injection attempt
07/27/2021 13:10:28	Local	192.[redacted]	5[redacted]9	192.[redacted]	80	HTTP	Potentially Bad Traffic	OS-OTHER Bash CGI environment variable injection attempt

To get the detailed view of incident click the hyperlink of **Client Date and Time** column of the incident list. Investigation Detail window appears.



Client Date and Time	Source IP	Source Port	Destination IP	Destination Port	Incident Name	Packet Description
07/05/2021 11:44:07	192.[redacted]	40591	192.[redacted]	80	Attempted Administrator Privilege Gain	OS-OTHER Bash CGI environment variable injection attempt.

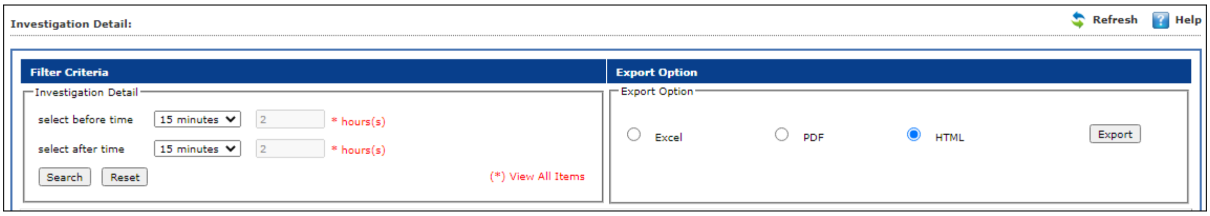
Here, you will get the details of the incidents and also the eScan events generated during that period of time.



Client Date and Time	Computer Name/Ip	IP Address	User's name	Event Description	Action Taken
07/05/2021 11:52:35	WI[redacted]R	192.[redacted]	WI[redacted]R\Administrator	MSOffice Child EXE Blocked [Parent-C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE:3808]	Application Terminated
07/05/2021 11:52:35	WI[redacted]R	192.[redacted]	WI[redacted]R\Administrator	MSOffice Child EXE Blocked [Parent-C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE:3808]	Application Terminated
07/05/2021 11:52:35	WI[redacted]R	192.[redacted]	WI[redacted]R\Administrator	MSOffice Child EXE Blocked [Parent-C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE:3808]	Application Terminated
07/05/2021 11:49:35	WI[redacted]R	192.[redacted]	WI[redacted]R\Administrator	Sensitive OS-File Execution Blocked [Parent-C:\Windows\System32\cmd.exe:7560]	Application Terminated
07/05/2021 11:44:50	WI[redacted]R	192.[redacted]	WI[redacted]R\Administrator	Access Blocked: User:Blocked (ES)	Access Denied

In the eScan events tab, you will get the details about the computer name, IP address, events details, action taken, and infected source.

You can filter the events based on time it occurred and also export the report in different format such as HTML, PDF, and Excel.



Investigation Detail

select before time 15 minutes 2 * hours(s)

select after time 15 minutes 2 * hours(s)

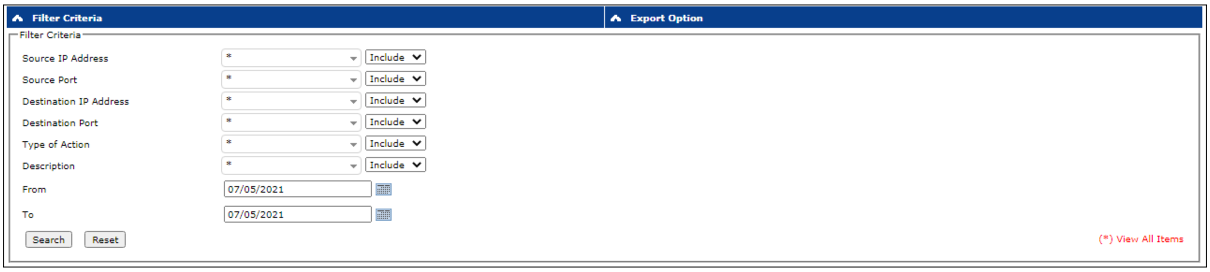
(*) View All Items

Export Option

○ Excel ○ PDF ● HTML

Filtering the Specific Incident

Admin can filter the incidents based on various criteria such as Source IP Address, Source Port, Destination IP Address, Destination port, Type of action, from date and date, and more.



Filter Criteria

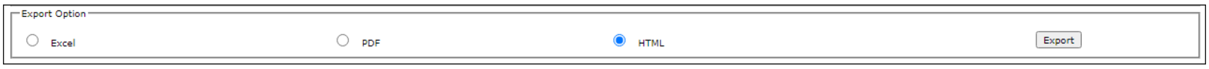
Source IP Address	*	Include
Source Port	*	Include
Destination IP Address	*	Include
Destination Port	*	Include
Type of Action	*	Include
Description	*	Include
From	07/05/2021	
To	07/05/2021	

(*) View All Items

After entering the details, click **Search**. The required result will be displayed accordingly.

Exporting the Network Incident

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



Export Option

○ Excel ○ PDF ● HTML

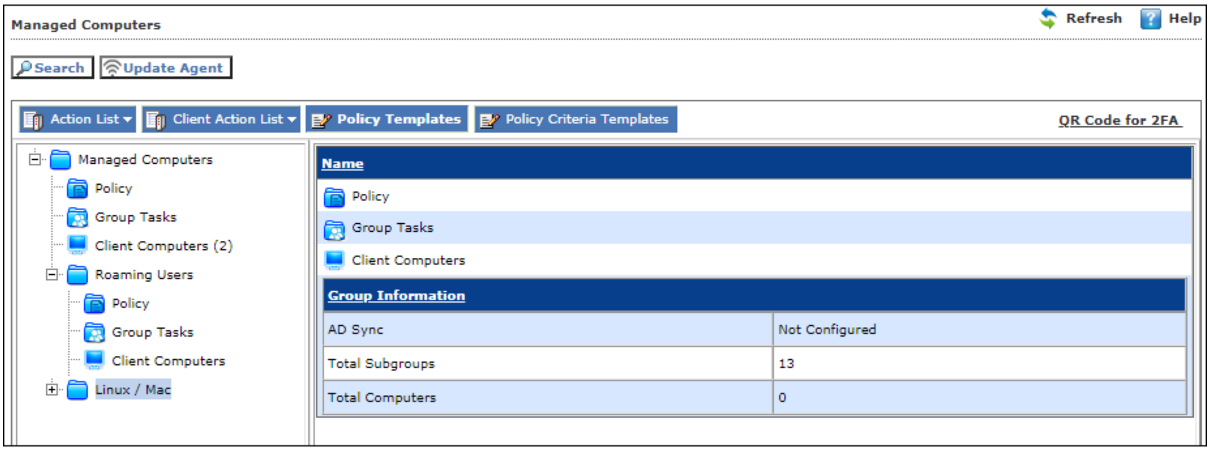
Select the preferred option and then click **Export**. A success message appears.
Click the link to open/download the file.

Managed Computers

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

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

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



Name
Policy
Group Tasks
Client Computers

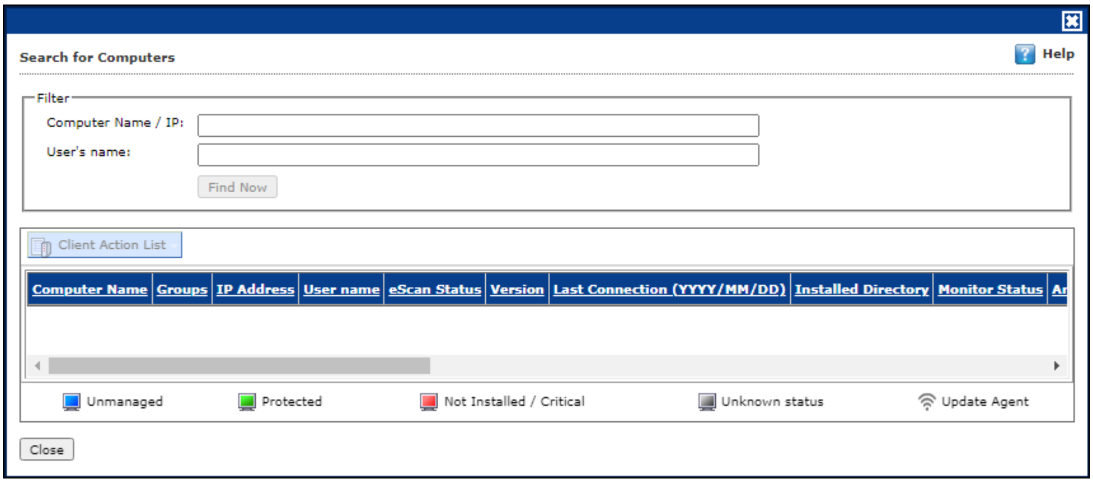
Group Information	
AD Sync	Not Configured
Total Subgroups	13
Total Computers	0

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.



Search for Computers

Help

Filter

Computer Name / IP:

User's name:

Find Now

Client Action List

Computer Name	Groups	IP Address	User name	eScan Status	Version	Last Connection (YYYY/MM/DD)	Installed Directory	Monitor Status	Ar

🟦 Unmanaged 🟩 Protected 🟥 Not Installed / Critical ▨ Unknown status Update Agent

Close

The Filter section displays following fields:

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

Username
Enter a username.

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

Update Agent

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

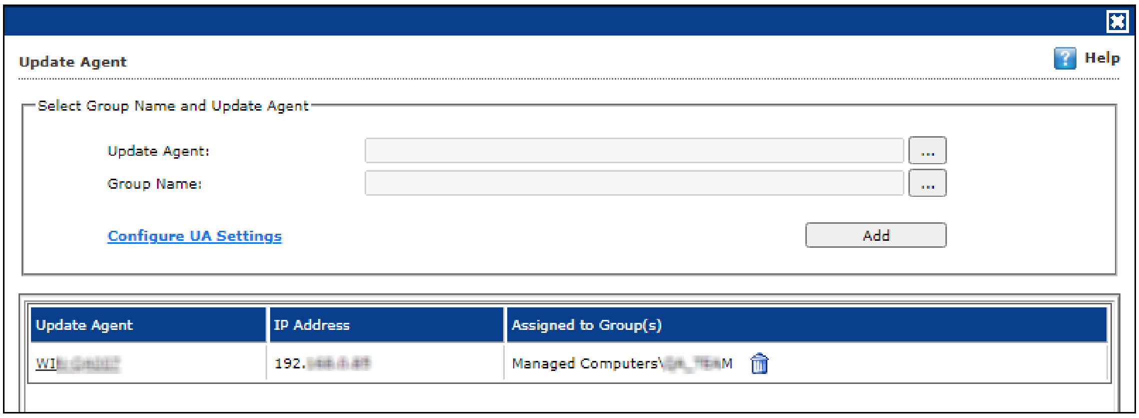
By default, eScan server distributes the virus definitions and policies to all the clients added in the web console. But, if you want to reduce server's workload, you can create an Update Agent for the respective group(s). The Update Agent will receive virus definitions and policies from server and distribute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

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

Adding an Update Agent

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

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



Update Agent

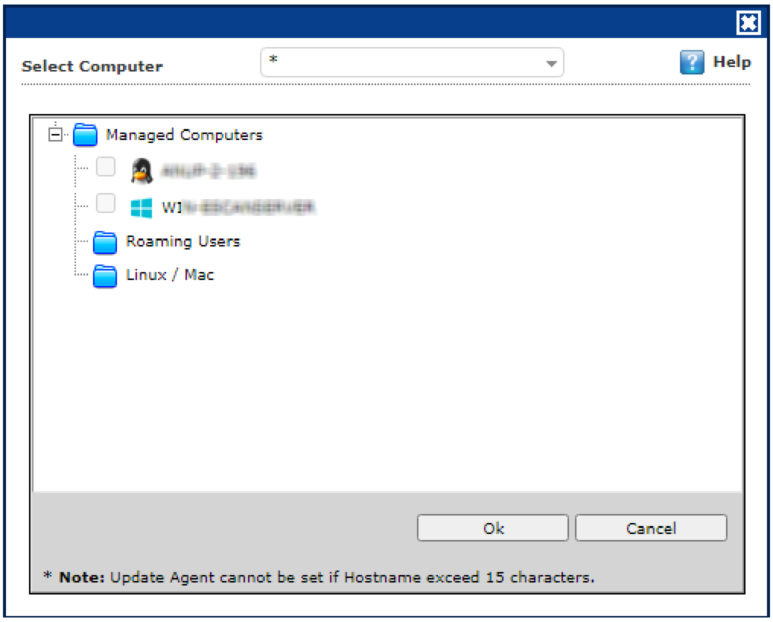
Select Group Name and Update Agent

Update Agent: ...

Group Name: ...

Update Agent	IP Address	Assigned to Group(s)
WI[redacted]	192.[redacted]	Managed Computers\[redacted]M

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



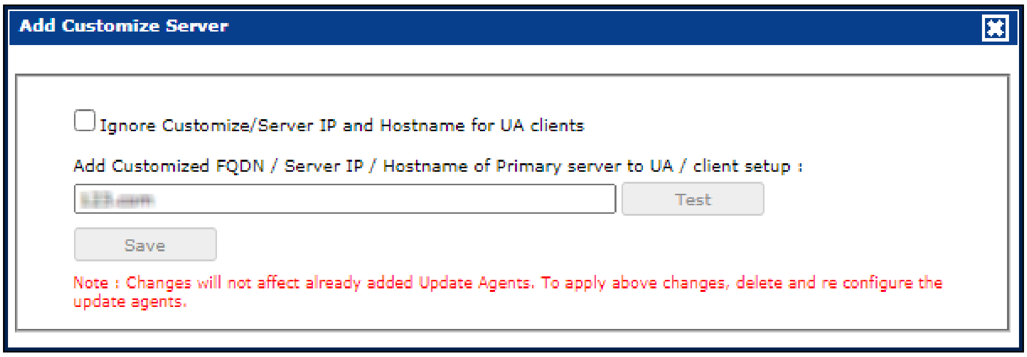
Select Computer *

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

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

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.



Add Customize Server

□ Ignore Customize/Server IP and Hostname for UA clients

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

[redacted]

Note : Changes will not affect already added Update Agents. To apply above changes, delete and re configure the update agents.

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.

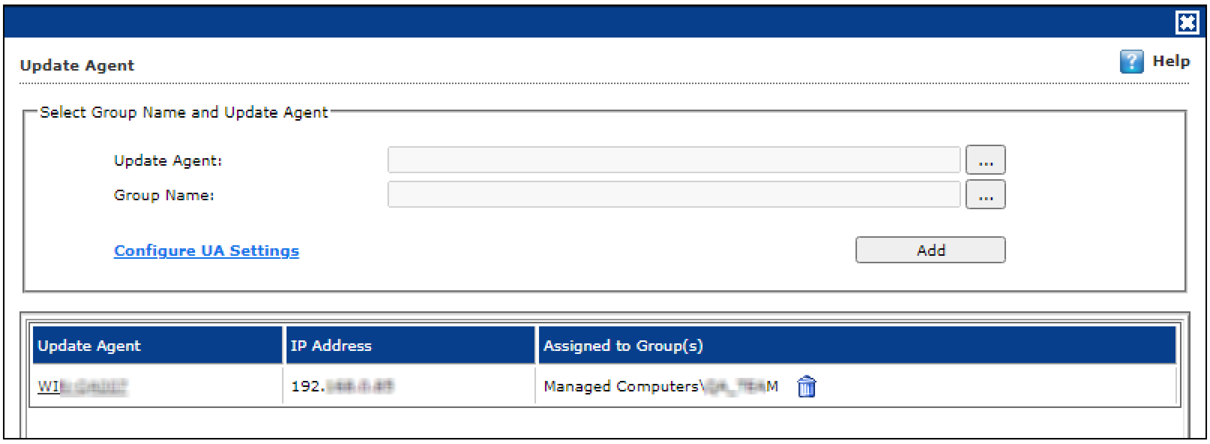
Add Customized FQDN / Server IP / Hostname of Primary server to UA / client setup
Enter the public address that has been assigned to the eScan Server through which clients can download the updates directly.

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.



Update Agent

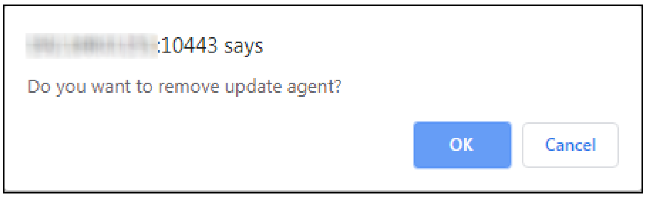
Select Group Name and Update Agent

Update Agent:

Group Name:

Update Agent	IP Address	Assigned to Group(s)
WI[redacted]	192.[redacted]	Managed Computers\[redacted]M 🗑

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



[redacted]:10443 says

Do you want to remove update agent?

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

Action List

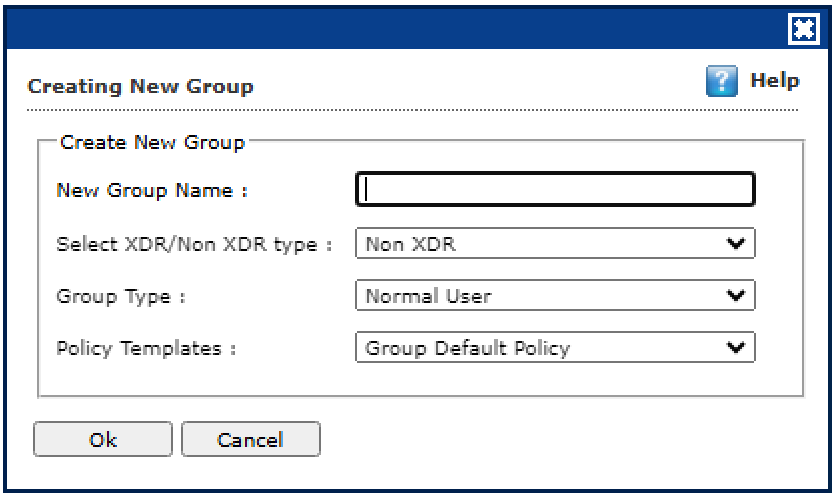
The Action List takes you action for a group. The drop-down contains following options:

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

New Subgroup

To create a group, follow the steps given below:

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



Creating New Group

Create New Group

New Group Name :

Select XDR/Non XDR type : Non XDR

Group Type : Normal User

Policy Templates : Group Default Policy

2. Enter a name for the group in the provided field.
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.

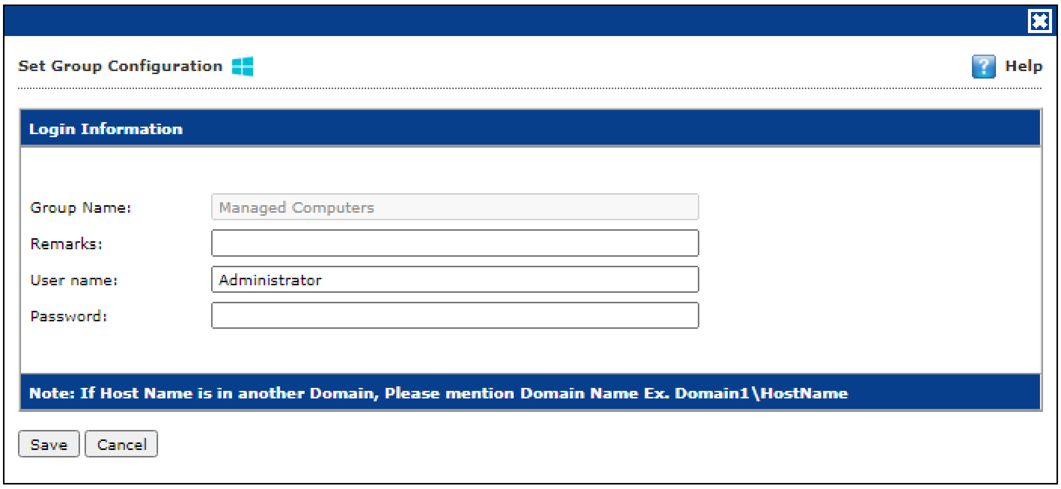
NOTE	If the Group type is set to **Normal User**, then server will try to connect to the client computer using the hostname. If the Group type is set to **Roaming User**, then server will try to connect to the client computer using the IP address. Multiple groups can be created within a group.

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.



Set Group Configuration

Login Information

Group Name: Managed Computers

Remarks:

User name: Administrator

Password:

Note: If Host Name is in another Domain, Please mention Domain Name Ex. Domain1\HostName

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

Managing Installations

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

This section will give you an overview on following activities:

Installing eScan Client

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

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

To initiate Force download, in the **Managed Computers** module**,** select the client computer and click **Client Action list** > **Force Download**.
It will initiate the forced download process on selected Client computers.

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

Remote Installation of eScan Client

Pre-Installation

To prepare a client computer for the remote deployment of eScan Enterprise EDR; 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.

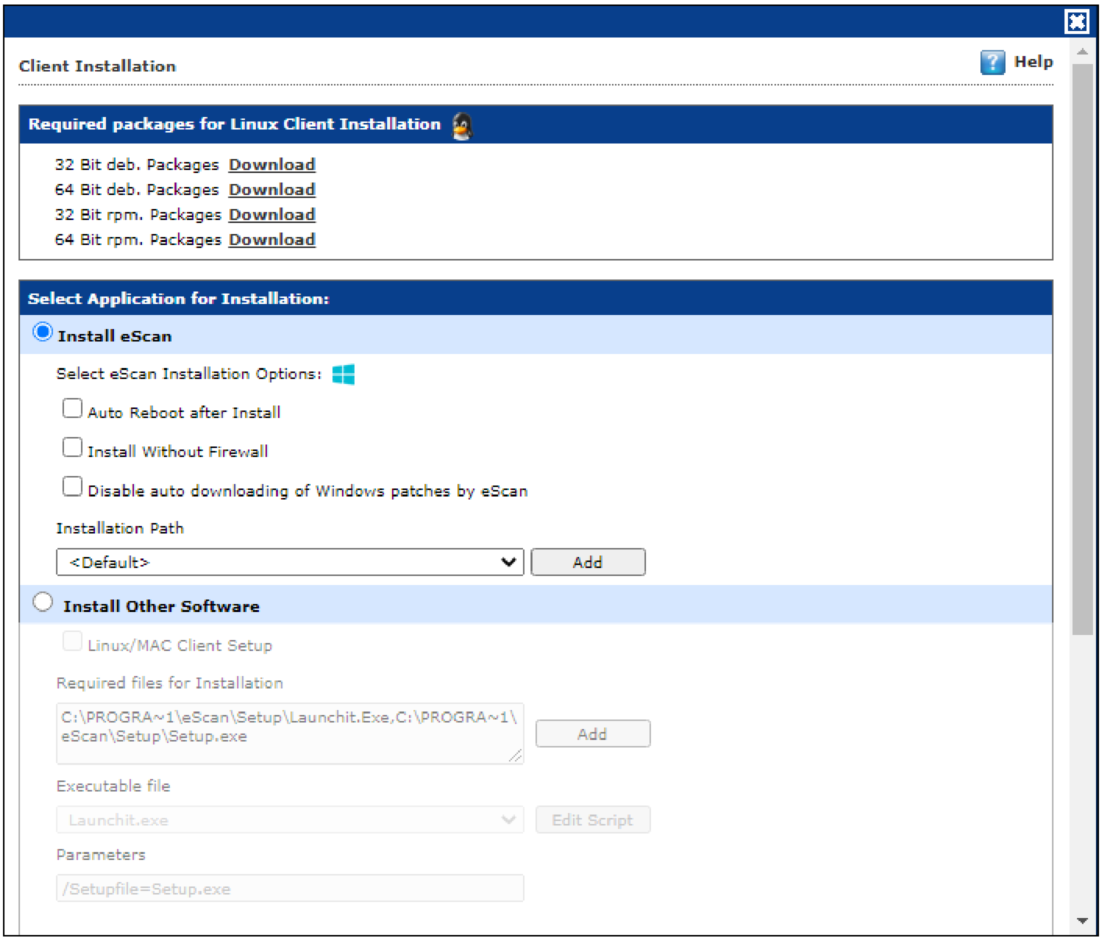
4. Double-click **Network access: Sharing and security model for local accounts** policy.
5. Select Classic - Local users authenticate as themselves option present in the drop-down.
6. Click **Apply** > **OK**.
7. Double-click **Accounts: Limit local account use of blank passwords to console logon only** 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 (Windows)

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



Client Installation

Required packages for Linux Client Installation

32 Bit deb. Packages Download
64 Bit deb. Packages Download
32 Bit rpm. Packages Download
64 Bit rpm. Packages Download

Select Application for Installation:

● **Install eScan**

Select eScan Installation Options:

□ Auto Reboot after Install

□ Install Without Firewall

□ Disable auto downloading of Windows patches by eScan

Installation Path

<Default>

○ **Install Other Software**

□ Linux/MAC Client Setup

Required files for Installation

C:\PROGRA~1\eScan\Setup\Launchit.Exe,C:\PROGRA~1\eScan\Setup\Setup.exe

Executable file

Launchit.exe

Parameters

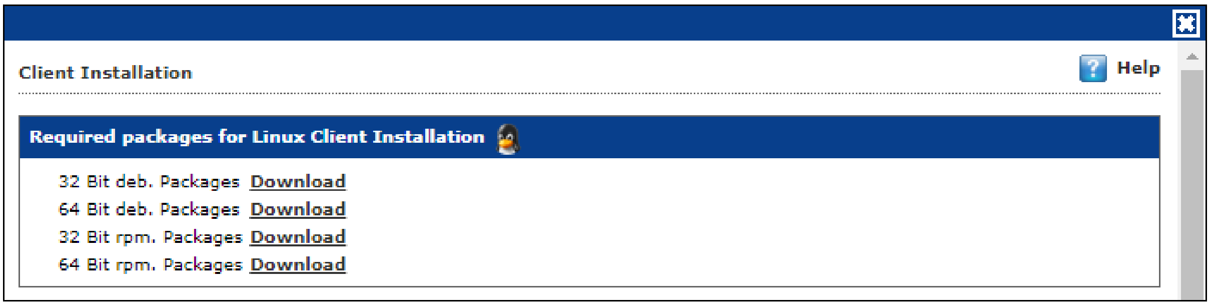
/Setupfile=Setup.exe

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 Linux Computers

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

1. Login to the EMC with your username and password.
2. Click Managed Computers on the navigation panel and select a group.
3. To deploy the setup, click **Action List** > **Deploy/ Upgrade Client**.
4. Download respective agent link from **Required package for Linux Client Installation** option.

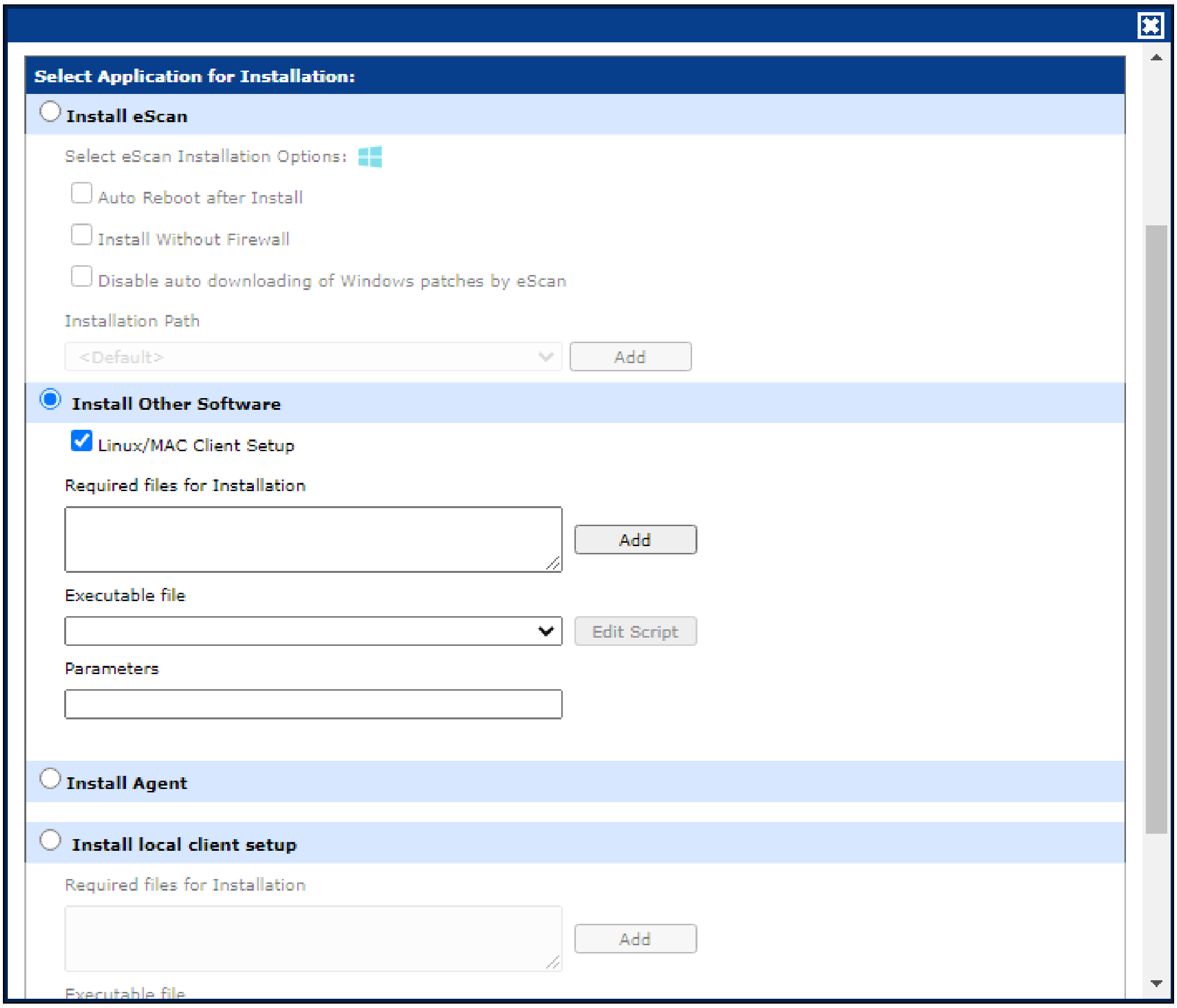


Client Installation

Required packages for Linux Client Installation

32 Bit deb. Packages	Download
64 Bit deb. Packages	Download
32 Bit rpm. Packages	Download
64 Bit rpm. Packages	Download

5. Click **Install Other Software** and select **Linux/MAC Client setup** option.



Select Application for Installation:

○ Install eScan

Select eScan Installation Options:

□ Auto Reboot after Install

□ Install Without Firewall

□ Disable auto downloading of Windows patches by eScan

Installation Path

<Default>

● Install Other Software

☑ Linux/MAC Client Setup

Required files for Installation

Executable file

Parameters

○ Install Agent

○ Install local client setup

Required files for Installation

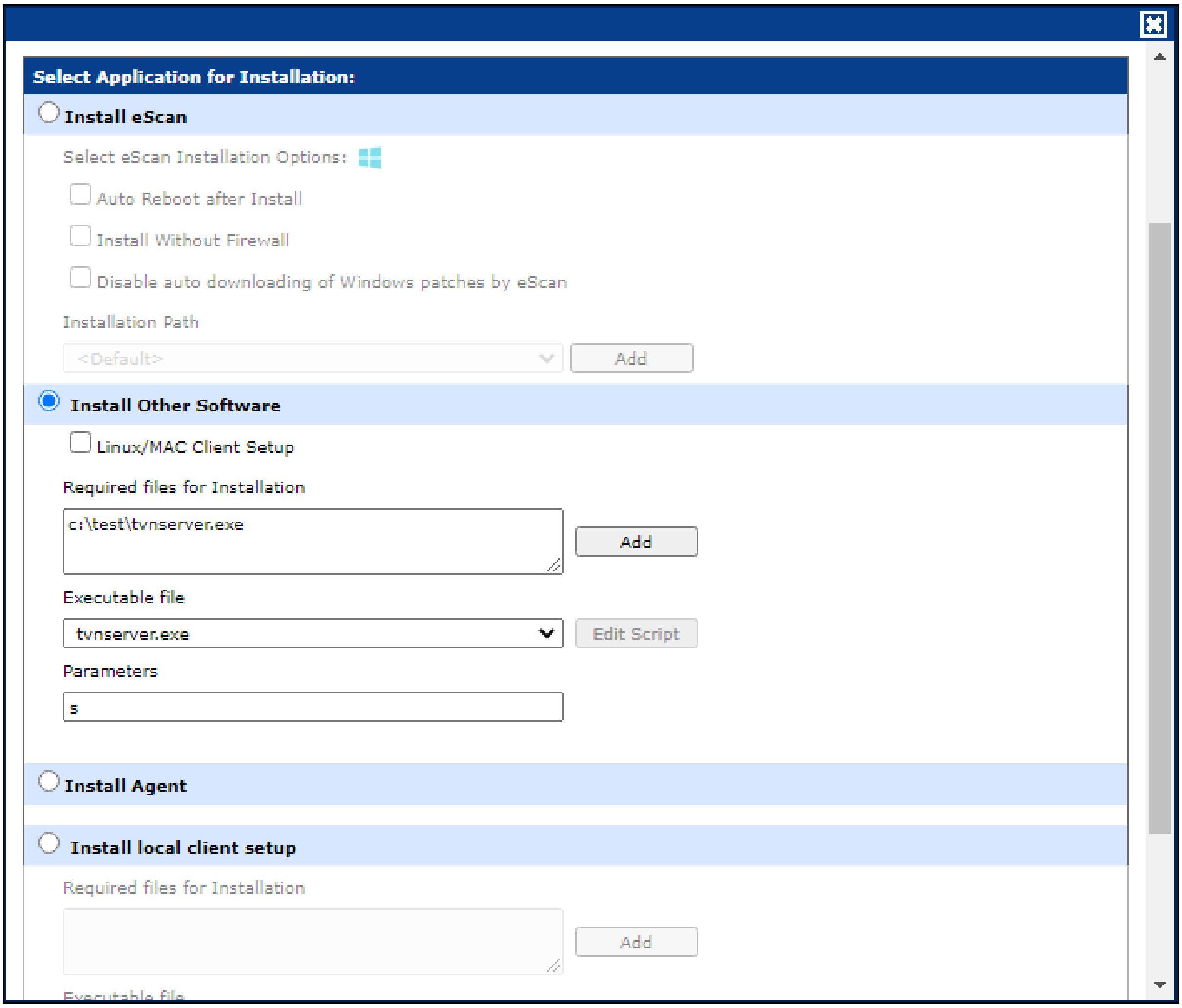
Executable file

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

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 **Action List** > **Deploy/Upgrade Client**. Client Installation window appears.
4. Select **Install Other Software** option.



Select Application for Installation:

○ **Install eScan**

Select eScan Installation Options:

□ Auto Reboot after Install

□ Install Without Firewall

□ Disable auto downloading of Windows patches by eScan

Installation Path

<Default>

● **Install Other Software**

□ Linux/MAC Client Setup

Required files for Installation

c:\test\tvnserver.exe

Executable file

tvnserver.exe

Parameters

s

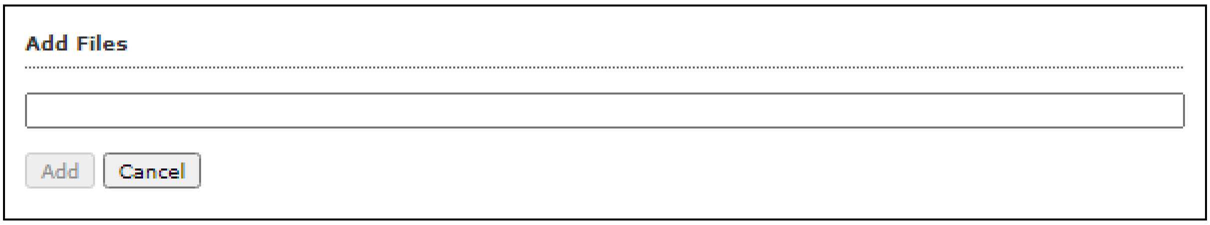
○ **Install Agent**

○ **Install local client setup**

Required files for Installation

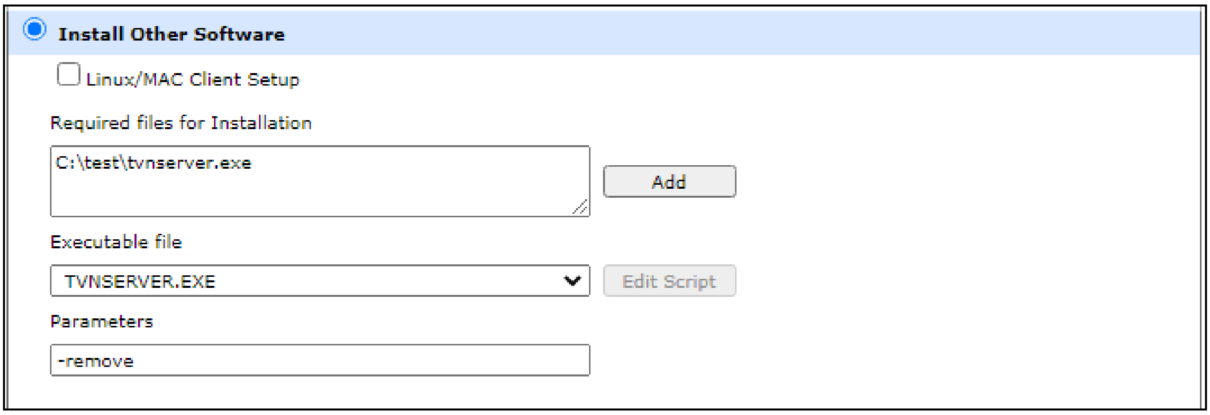
Executable file

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



Add Files

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

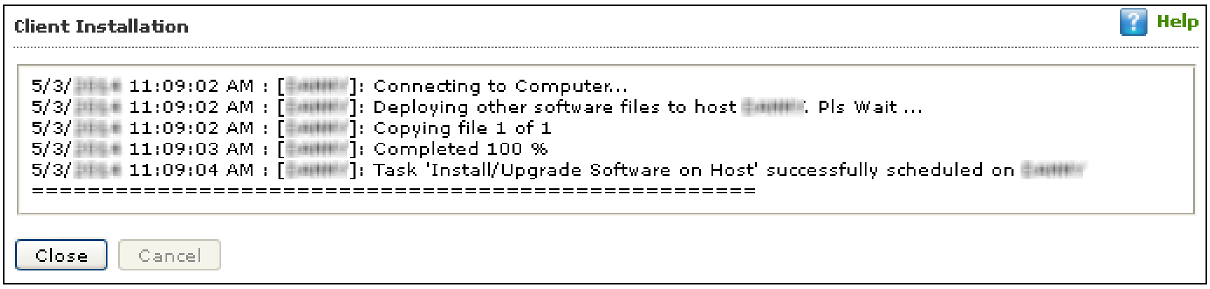
□ Linux/MAC Client Setup

Required files for Installation: C:\test\tvnserver.exe

Executable file: TVNSERVER.EXE

Parameters: -remove

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.

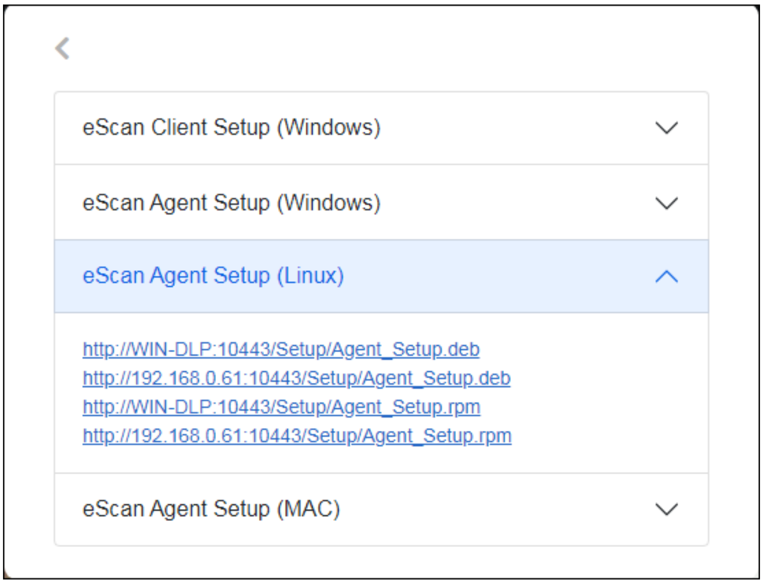


Client Installation

```
5/3/[redacted] 11:09:02 AM : [[redacted]]: Connecting to Computer...
5/3/[redacted] 11:09:02 AM : [[redacted]]: Deploying other software files to host [redacted]. Pls Wait ...
5/3/[redacted] 11:09:02 AM : [[redacted]]: Copying file 1 of 1
5/3/[redacted] 11:09:03 AM : [[redacted]]: Completed 100 %
5/3/[redacted] 11:09:04 AM : [[redacted]]: Task 'Install/Upgrade Software on Host' successfully scheduled on [redacted]
====================================================
```

Installing Agent on Linux

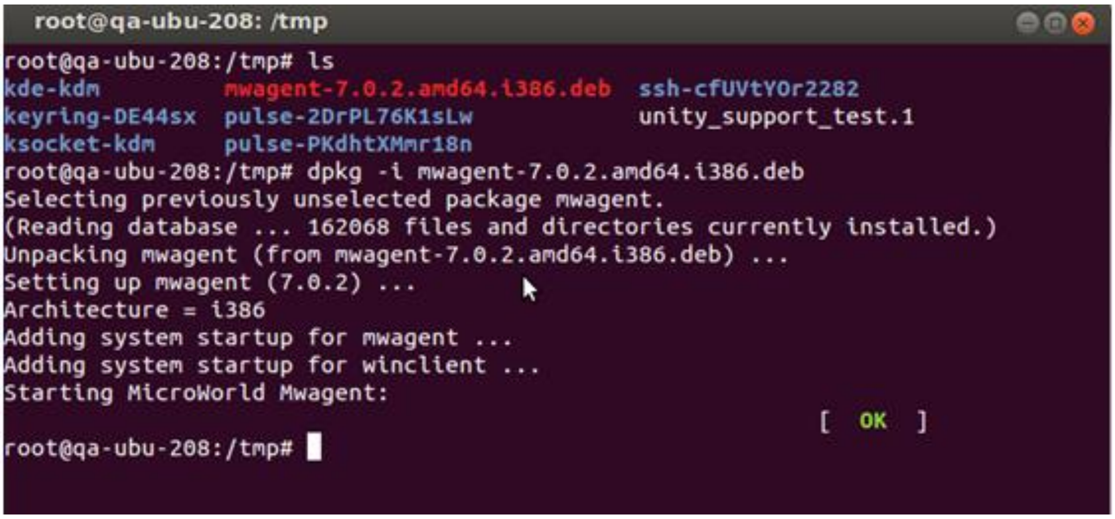
1. To manually install eScan Agent on Linux endpoint, please download the agent setup displayed on the **Login Page** > **Setup Links** of eScan Management Console and Save to the Linux client.



eScan Client Setup (Windows)
eScan Agent Setup (Windows)
eScan Agent Setup (Linux)

http://WIN-DLP:10443/Setup/Agent_Setup.deb
http://192.168.0.61:10443/Setup/Agent_Setup.deb
http://WIN-DLP:10443/Setup/Agent_Setup.rpm
http://192.168.0.61:10443/Setup/Agent_Setup.rpm

2. Open the terminal for installing Agent.
3. Installation of Agent requires root or sudo user authentication. After Login as **root** or **sudo user**, go to the path where the **Agent_setup.deb** file has been saved.
4. Install the agent from the path using the following command – ***dpkg – i***. (**for RPM based setup – Rpm-ivh)** –



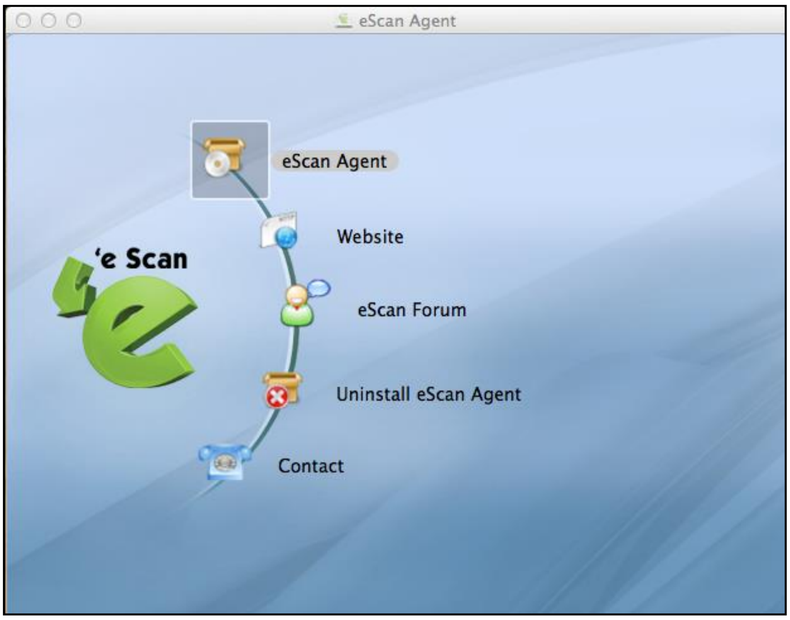
```
root@qa-ubu-208: /tmp
root@qa-ubu-208:/tmp# ls
kde-kdm          mwagent-7.0.2.amd64.i386.deb  ssh-cfUVtYOr2282
keyring-DE44sx   pulse-2DrPL76K1sLw            unity_support_test.1
ksocket-kdm      pulse-PKdhtXMmr18n
root@qa-ubu-208:/tmp# dpkg -i mwagent-7.0.2.amd64.i386.deb
Selecting previously unselected package mwagent.
(Reading database ... 162068 files and directories currently installed.)
Unpacking mwagent (from mwagent-7.0.2.amd64.i386.deb) ...
Setting up mwagent (7.0.2) ...
Architecture = i386
Adding system startup for mwagent ...
Adding system startup for winclient ...
Starting MicroWorld Mwagent:
                                                           [  OK  ]
root@qa-ubu-208:/tmp# 
```

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

Installing eScan Agent on Mac Computers

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

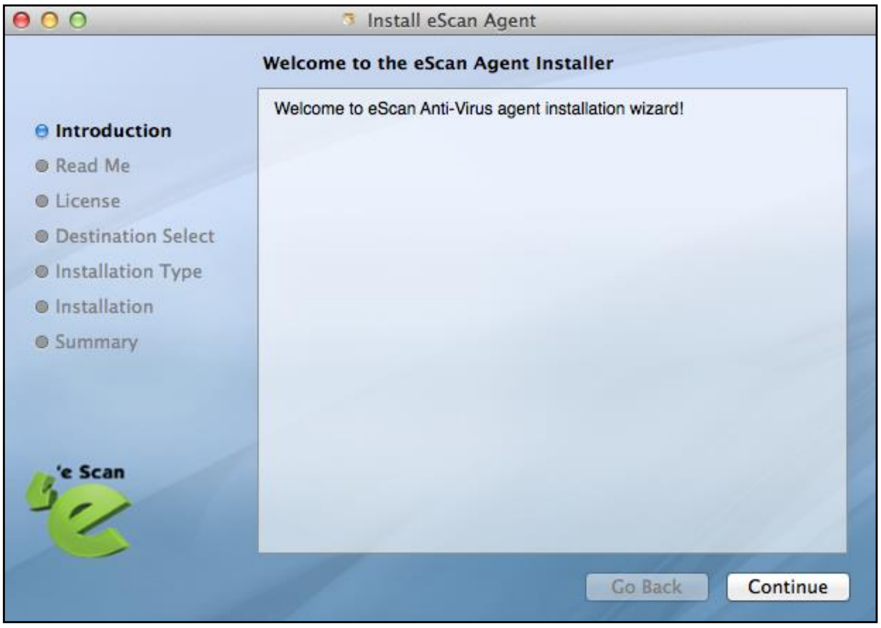
1. Download agent from the link received via mail and save it at the desired path on the computer where you wish to install eScan Client.
2. Go to the path where Agent is saved.
3. Double-click **Agent_Setup.dmg** file to run the installation wizard.
   Agent Installation Wizard will run.



4. Double-click **eScan Agent**. This will start the installation process.

Introduction window appears.

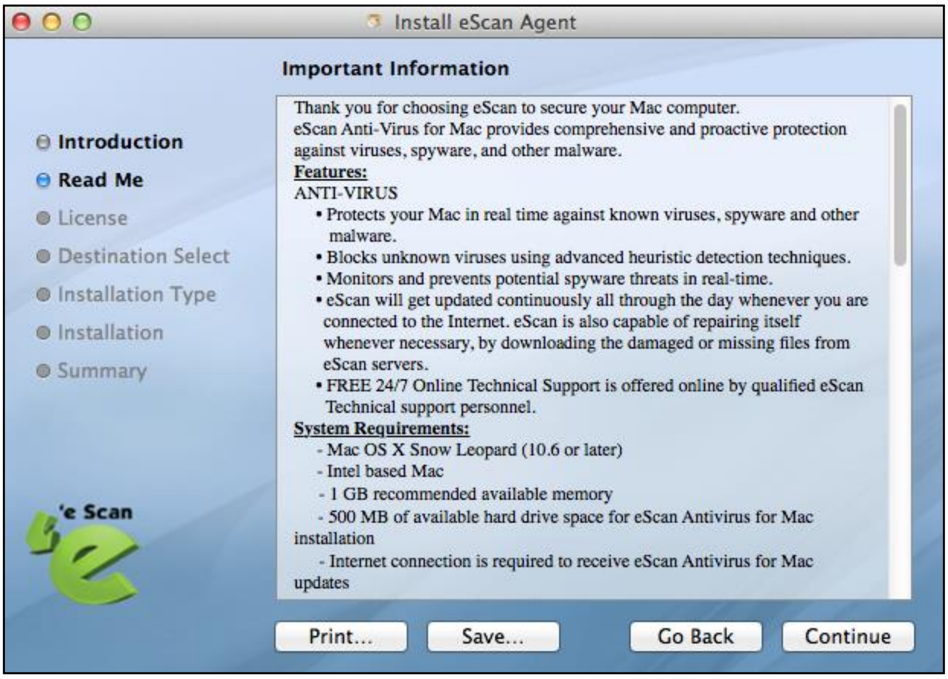
5. To proceed, click **Continue**.



Welcome to eScan Anti-Virus agent installation wizard!

The installation wizard displays Read Me window.

6. Please read the system requirements and click **Continue**.
   License window appears.



Thank you for choosing eScan to secure your Mac computer.
eScan Anti-Virus for Mac provides comprehensive and proactive protection against viruses, spyware, and other malware.

Features:

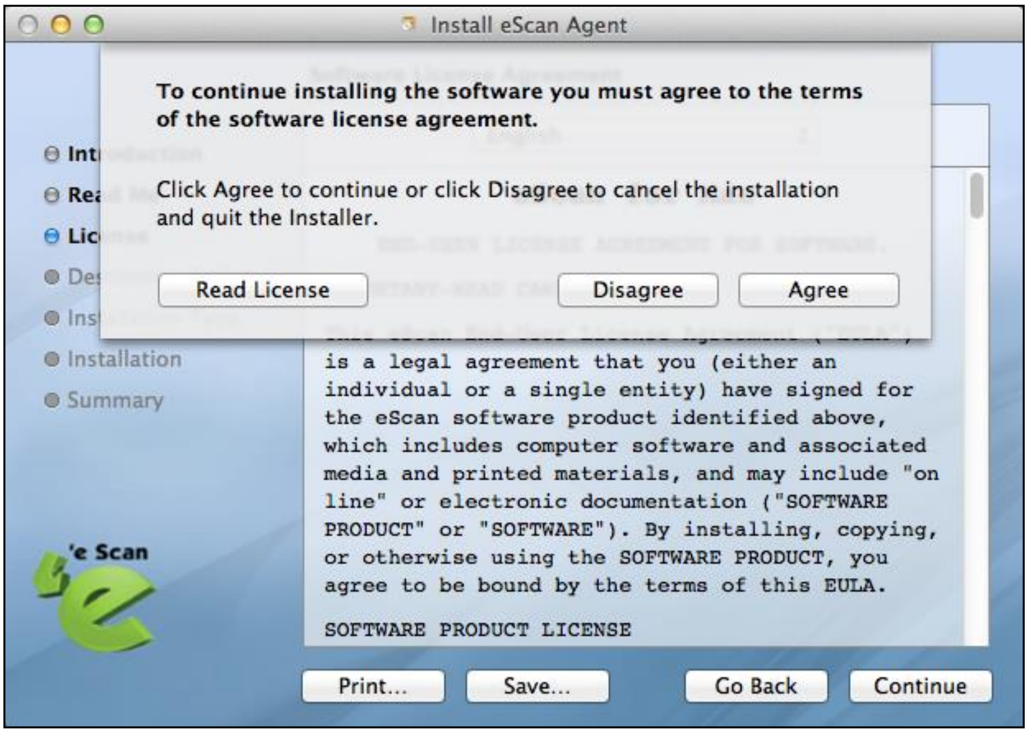
ANTI-VIRUS

- Protects your Mac in real time against known viruses, spyware and other malware.
- Blocks unknown viruses using advanced heuristic detection techniques.
- Monitors and prevents potential spyware threats in real-time.
- eScan will get updated continuously all through the day whenever you are connected to the Internet. eScan is also capable of repairing itself whenever necessary, by downloading the damaged or missing files from eScan servers.
- FREE 24/7 Online Technical Support is offered online by qualified eScan Technical support personnel.

System Requirements:

- Mac OS X Snow Leopard (10.6 or later)
- Intel based Mac
- 1 GB recommended available memory
- 500 MB of available hard drive space for eScan Antivirus for Mac installation
- Internet connection is required to receive eScan Antivirus for Mac updates

7. Please read the agreement completely and then click **Continue**.
8. Agree to terms and conditions by clicking **Agree**.



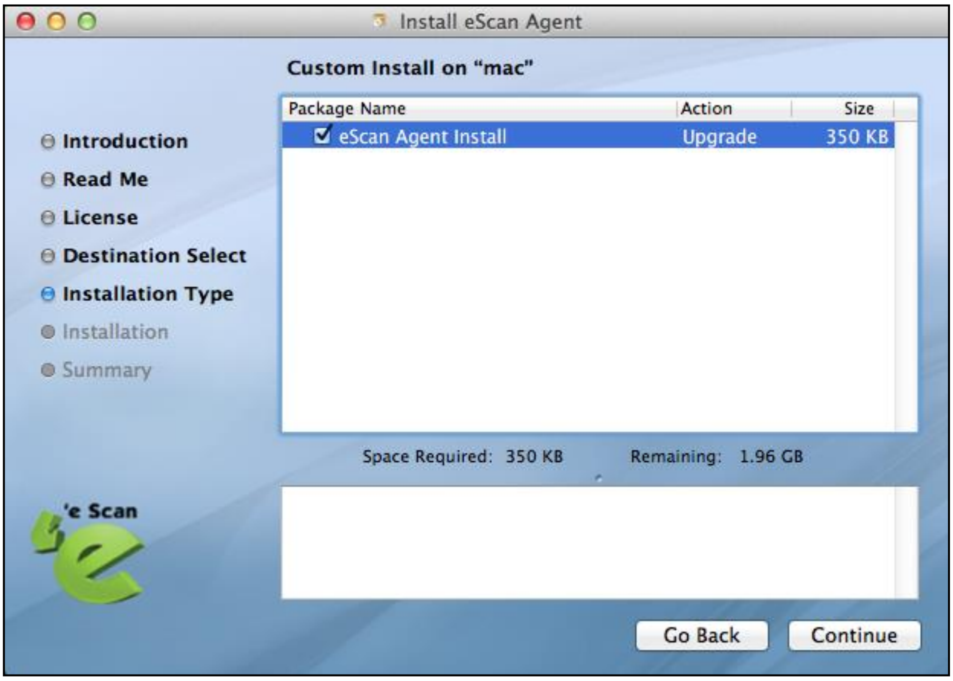
To continue installing the software you must agree to the terms of the software license agreement.

Click Agree to continue or click Disagree to cancel the installation and quit the Installer.

is a legal agreement that you (either an individual or a single entity) have signed for the eScan software product identified above, which includes computer software and associated media and printed materials, and may include "on line" or electronic documentation ("SOFTWARE PRODUCT" or "SOFTWARE"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA.

SOFTWARE PRODUCT LICENSE

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

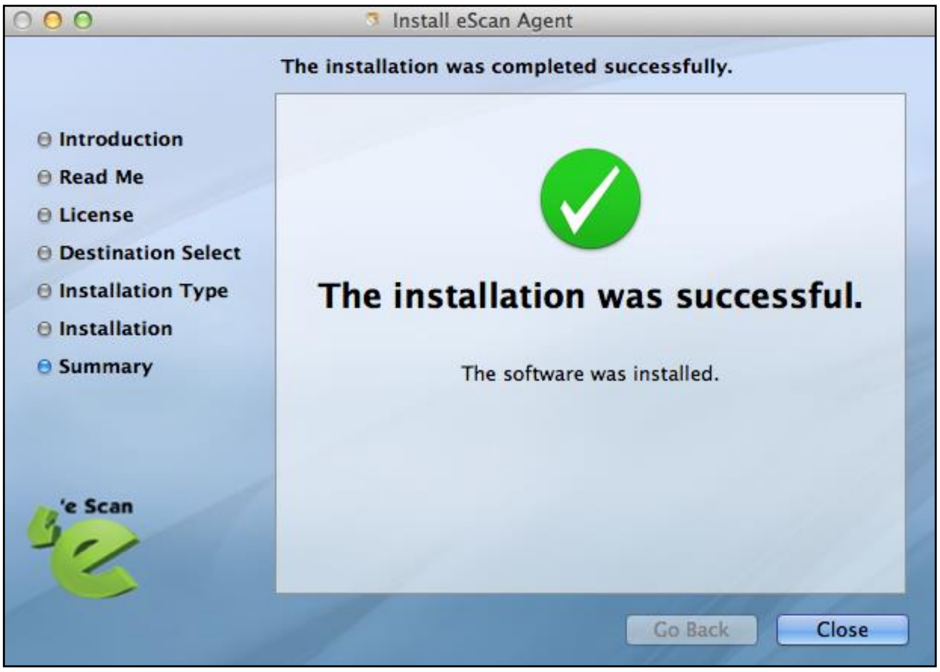


Custom Install on “mac”

Package Name	Action	Size
☑ eScan Agent Install	Upgrade	350 KB

Space Required: 350 KB Remaining: 1.96 GB

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



Install eScan Agent

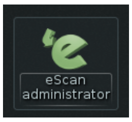
The installation was completed successfully.

The installation was successful.

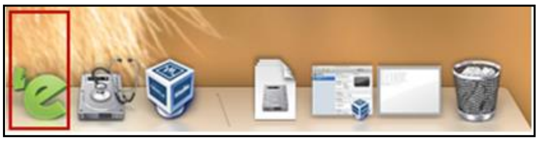
The software was installed.

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

    In Linux, eScan Administrator Icon will be displayed on desktop.



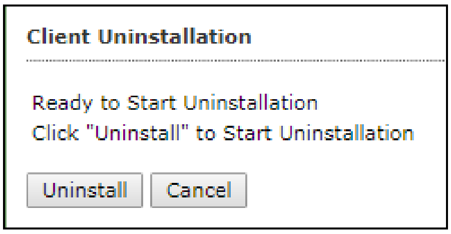
In Mac, eScan icon will be displayed in the **Dock**. Double-click it to launch eScan.



Uninstall eScan Client (Windows, Mac, and Linux)

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

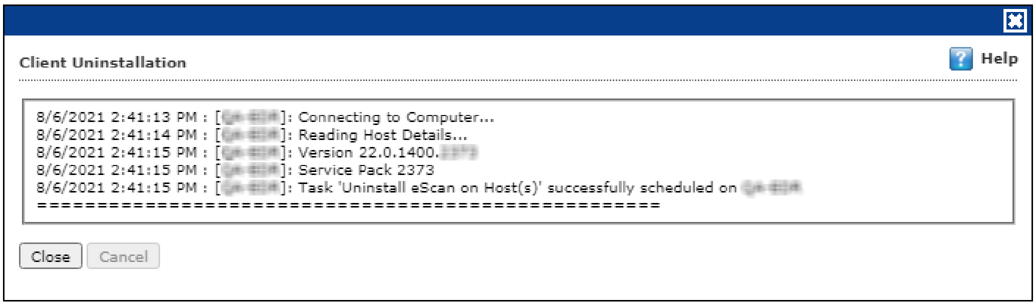
1. Select the group of computers for uninstallation.
2. Click **Action List** > **Uninstall eScan Client**.
   Client Uninstallation window appears.



Client Uninstallation

Ready to Start Uninstallation
Click "Uninstall" to Start Uninstallation

3. Click **Uninstall**.
   The Client Uninstallation window displays the progress.



Client Uninstallation

```
8/6/2021 2:41:13 PM : [[redacted]]: Connecting to Computer...
8/6/2021 2:41:14 PM : [[redacted]]: Reading Host Details...
8/6/2021 2:41:15 PM : [[redacted]]: Version 22.0.1400.[redacted]
8/6/2021 2:41:15 PM : [[redacted]]: Service Pack 2373
8/6/2021 2:41:15 PM : [[redacted]]: Task 'Uninstall eScan on Host(s)' successfully scheduled on [redacted]
====================================================
```

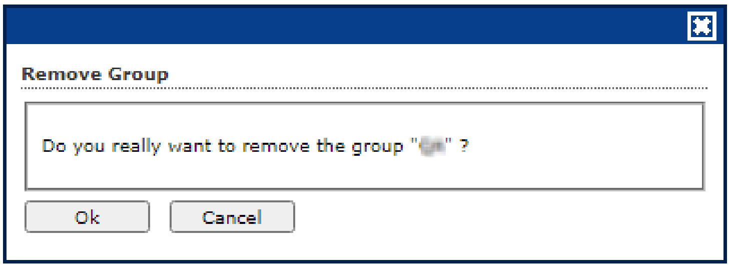
After the uninstallation process is over, click **Close**.

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**.

Remove Group

To remove a group, follow the steps given below:

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



Remove Group

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

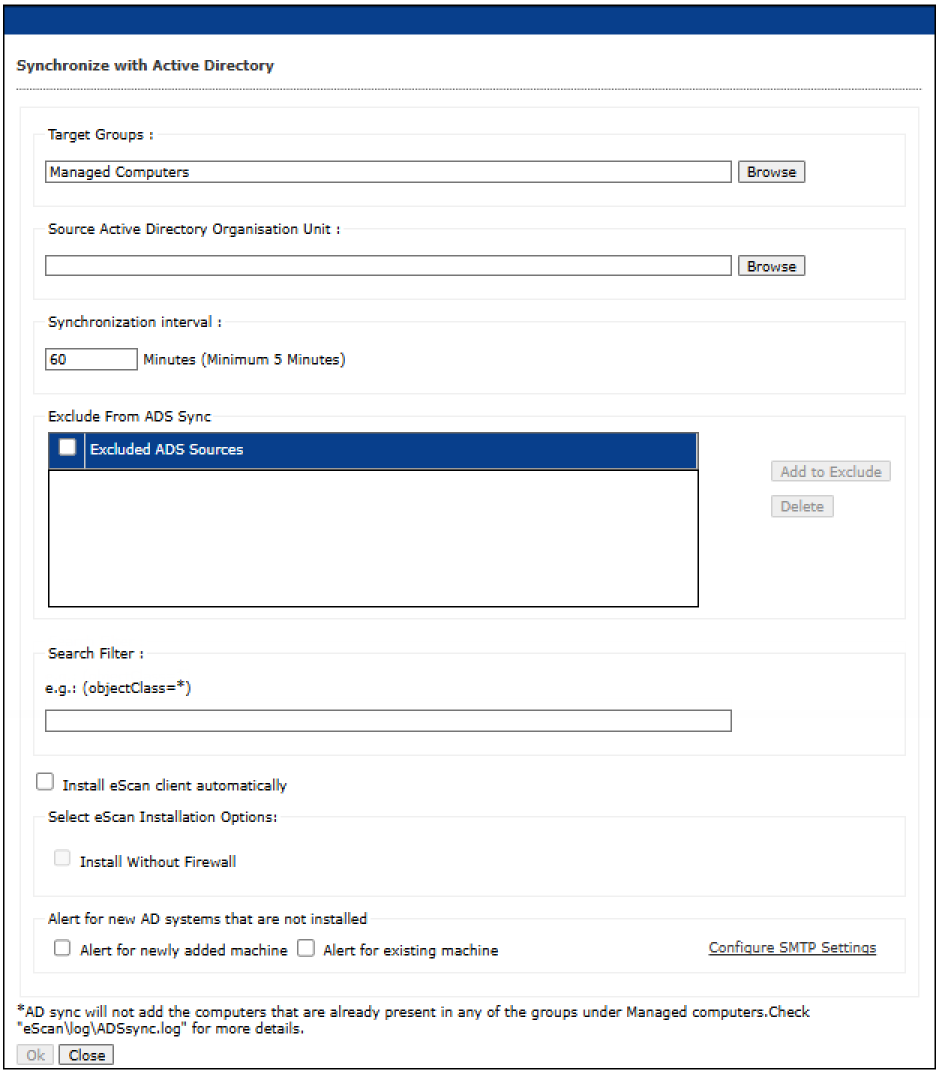
NOTE	A group will be removed only if it contains no computers.

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

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
□ Excluded ADS Sources

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

□ Install eScan client automatically
Select eScan Installation Options:
□ Install Without Firewall

Alert for new AD systems that are not installed
□ Alert for newly added machine □ Alert for existing machine

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

4. Under Source Active Directory Organization Unit section click **Browse** and select an Active Directory.
5. Under Synchronization Interval section enter the preferred duration (in minutes). After filling the above details, proceed to following sections:

   Exclude from ADS Sync
   This field displays a list of excluded Active Directory sources.
   To delete a source, select the checkbox Excluded ADS Sources. Select a source(s) and then click **Delete**.

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

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

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

Install without Firewall
Selecting this option lets you install eScan without firewall.

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

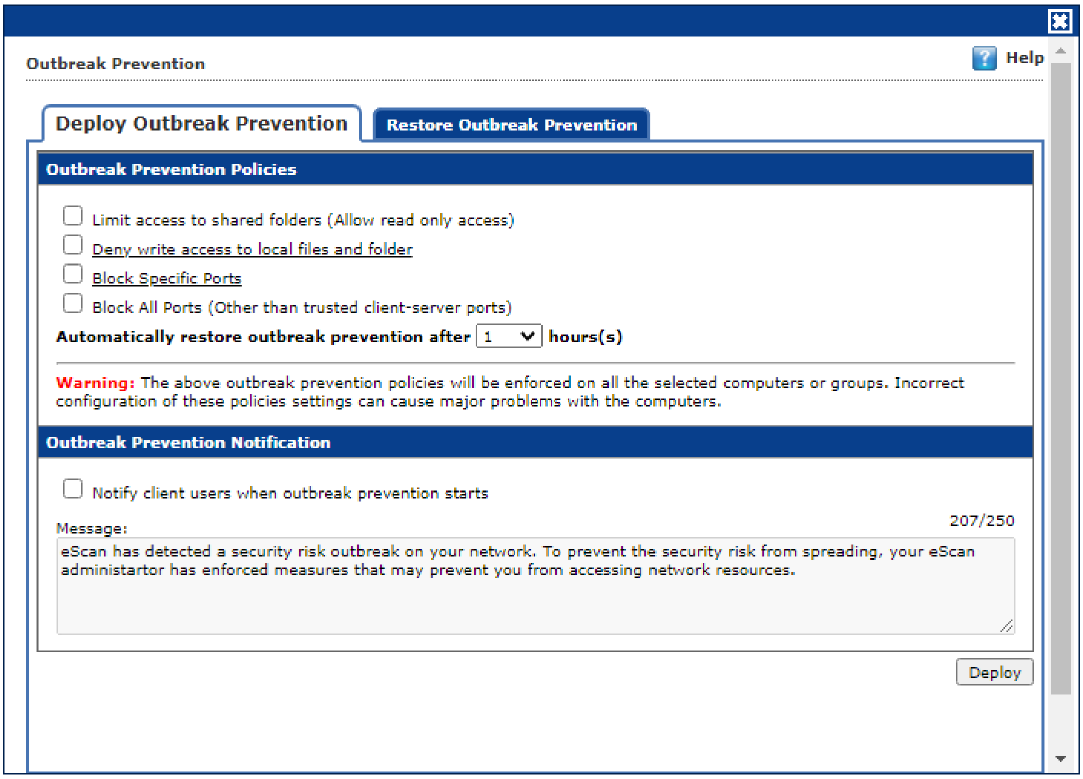
Outbreak Prevention

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

Deploying Outbreak Prevention

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

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



Outbreak Prevention Policies

□ Limit access to shared folders (Allow read only access)
□ Deny write access to local files and folder
□ Block Specific Ports
□ Block All Ports (Other than trusted client-server ports)

Automatically restore outbreak prevention after 1 **hours(s)**

Warning: The above outbreak prevention policies will be enforced on all the selected computers or groups. Incorrect configuration of these policies settings can cause major problems with the computers.

Outbreak Prevention Notification

□ Notify client users when outbreak prevention starts

Message: 207/250
eScan has detected a security risk outbreak on your network. To prevent the security risk from spreading, your eScan administartor has enforced measures that may prevent you from accessing network resources.

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

Deny write access to local files and folder

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

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

Block All Ports (Other than trusted client-server ports)
Select this checkbox to block all ports other than trusted client server ports.

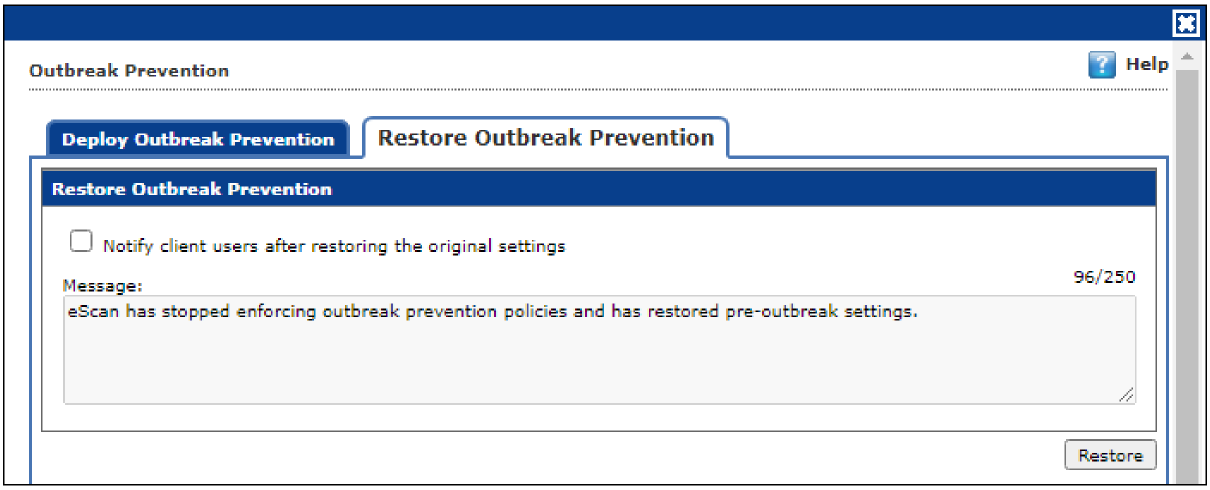
Automatically restore the outbreak prevention after hour(s)
This feature lets you restore outbreak prevention automatically after set duration (hours). Click the drop-down and select the preferred duration.

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

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

Restore Outbreak Prevention

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



Outbreak Prevention

Restore Outbreak Prevention

□ Notify client users after restoring the original settings

Message: 96/250

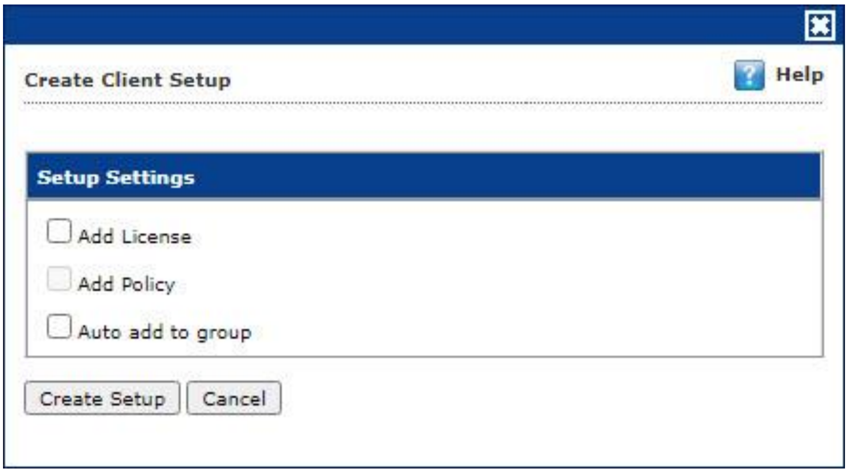
eScan has stopped enforcing outbreak prevention policies and has restored pre-outbreak settings.

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

Create Client Setup

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

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



Create Client Setup

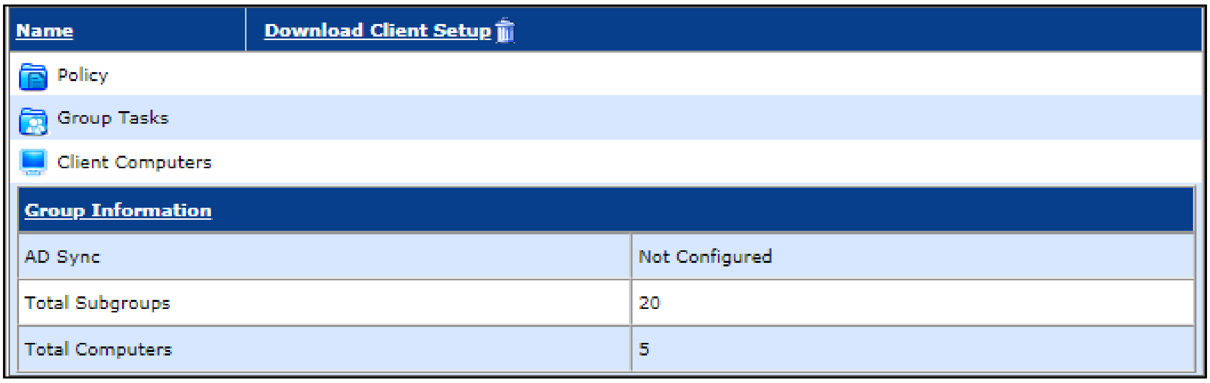
Setup Settings

☐ Add License

☐ Add Policy

☐ Auto add to group

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



Name	Download Client Setup
Policy	
Group Tasks	
Client Computers	

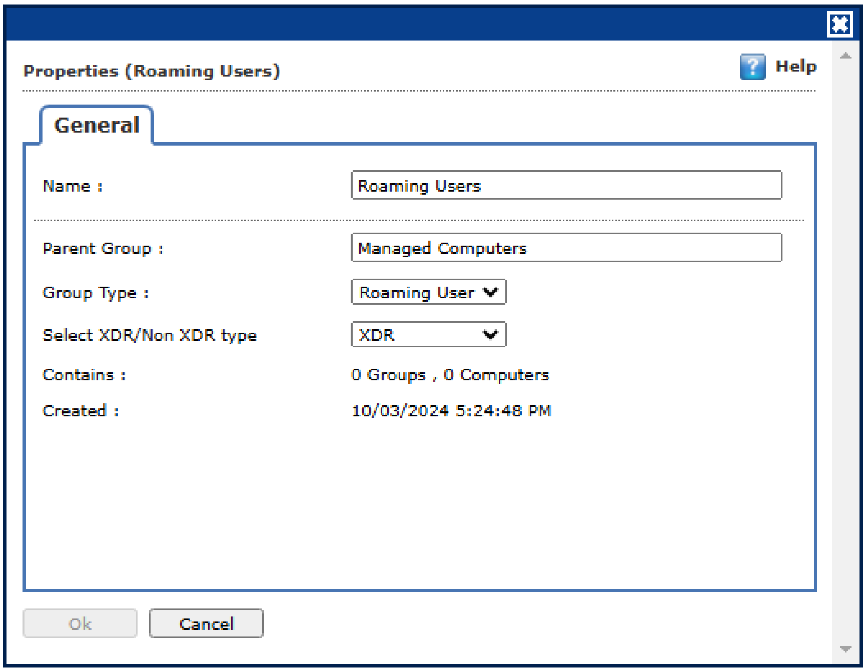
Group Information

AD Sync	Not Configured
Total Subgroups	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 (Roaming Users)

Name : Roaming Users

Parent Group : Managed Computers

Group Type : Roaming User

Select XDR/Non XDR type XDR

Contains : 0 Groups , 0 Computers

Created : 10/03/2024 5:24:48 PM

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

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

Creation date of the Group

Group Tasks

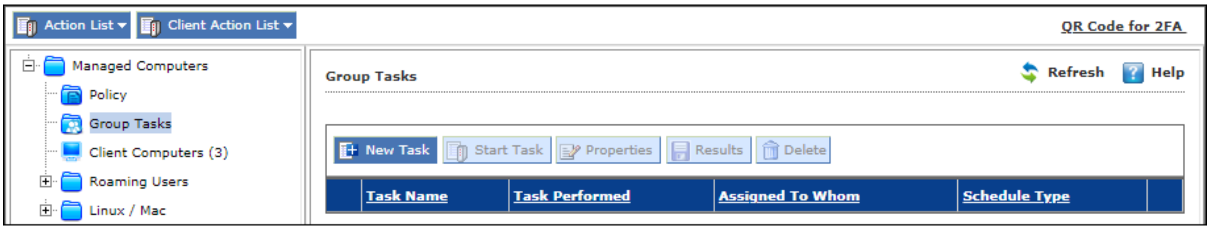
With the **Group Tasks** option, you can create a task, start a task, select a task and view its properties, view task results as well as delete an already created task. Tasks can include the following.

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

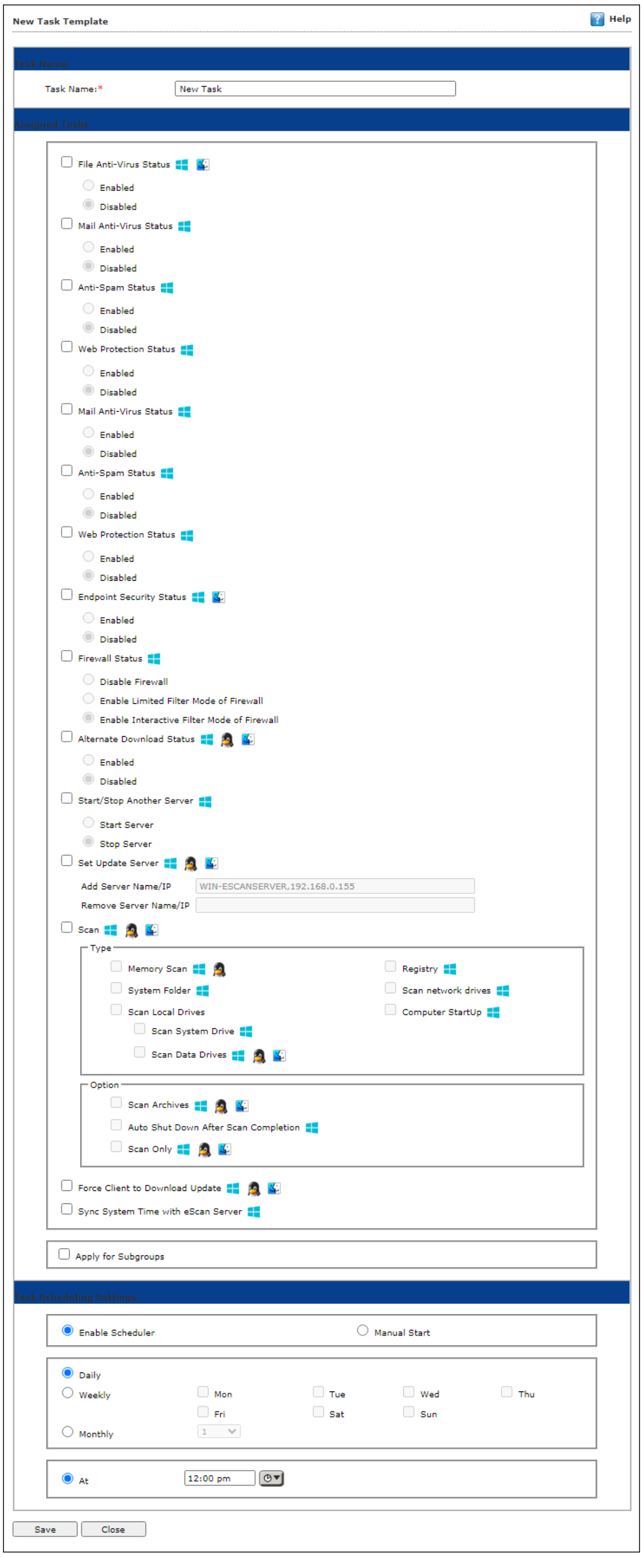
Creating a Group Task

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

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



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



New Task Template
Help

Task Name

Task Name:* New Task

Assigned Tasks

□ File Anti-Virus Status
○ Enabled
● Disabled

□ Mail Anti-Virus Status
○ Enabled
● Disabled

□ Anti-Spam Status
○ Enabled
● Disabled

□ Web Protection Status
○ Enabled
● Disabled

□ Mail Anti-Virus Status
○ Enabled
● Disabled

□ Anti-Spam Status
○ Enabled
● Disabled

□ Web Protection Status
○ Enabled
● Disabled

□ Endpoint Security Status
○ Enabled
● Disabled

□ Firewall Status
○ Disable Firewall
○ Enable Limited Filter Mode of Firewall
● Enable Interactive Filter Mode of Firewall

□ Alternate Download Status
○ Enabled
● Disabled

□ Start/Stop Another Server
○ Start Server
● Stop Server

□ Set Update Server
Add Server Name/IP WIN-ESCANSERVER,192.168.0.155
Remove Server Name/IP

□ Scan

Type
□ Memory Scan □ Registry
□ System Folder □ Scan network drives
□ Scan Local Drives □ Computer StartUp
□ Scan System Drive
□ Scan Data Drives

Option
□ Scan Archives
□ Auto Shut Down After Scan Completion
□ Scan Only

□ Force Client to Download Update
□ Sync System Time with eScan Server

□ Apply for Subgroups

Task Scheduling Settings

● Enable Scheduler ○ Manual Start

● Daily
○ Weekly □ Mon □ Tue □ Wed □ Thu
□ Fri □ Sat □ Sun
○ Monthly 1

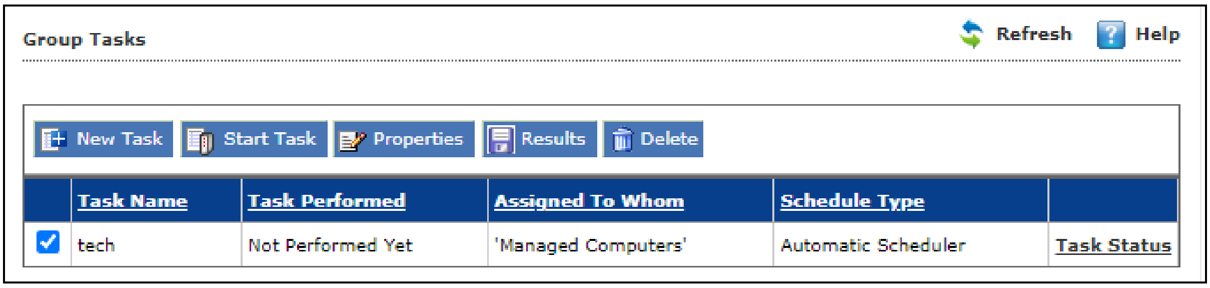
● At 12:00 pm

Save Close

5. Enter the Task Name and configure the desired task settings.
6. 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.



	Task Name	Task Performed	Assigned To Whom	Schedule Type	
☑	tech	Not Performed Yet	'Managed Computers'	Automatic Scheduler	Task Status

Start Task

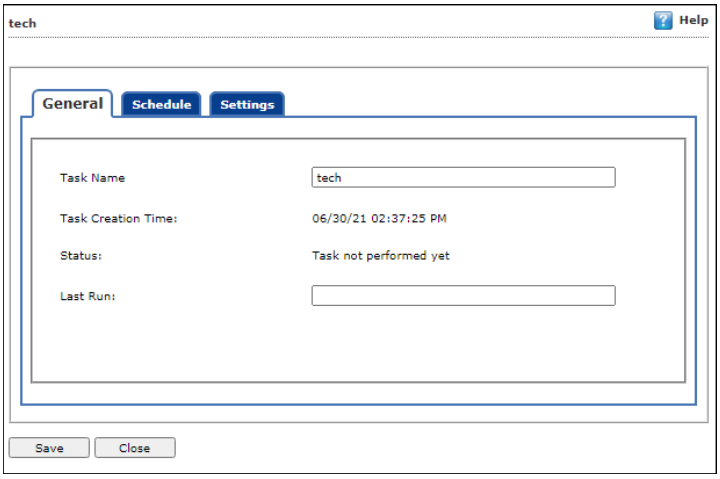
To start a task manually, select a task and then click **Start Task**.

Delete Task

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

Properties

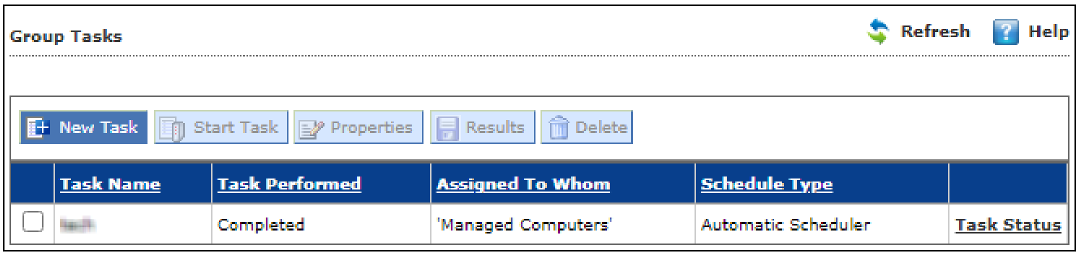
To view the properties of a task, select a task and then click **Properties**. It also lets you modify or redefine the entire settings configured. After making the necessary changes, click **Save**. The properties for the group task will be saved and updated.



Task Name	tech
Task Creation Time:	06/30/21 02:37:25 PM
Status:	Task not performed yet
Last Run:	

Results

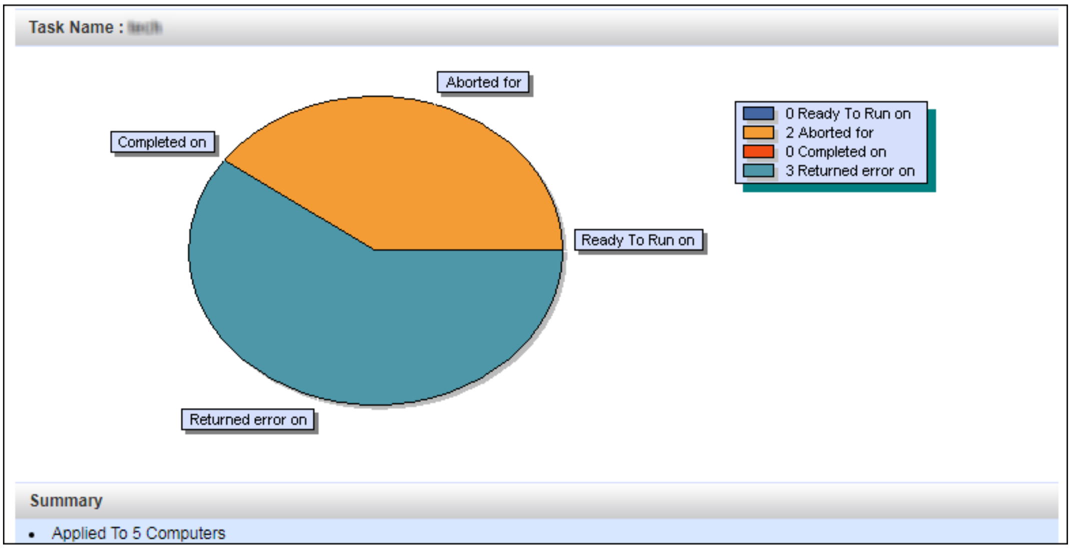
To view the results of a completed task, select a task and then click **Results**.



	Task Name	Task Performed	Assigned To Whom	Schedule Type	
□	[redacted]	Completed	'Managed Computers'	Automatic Scheduler	Task Status

Task Status

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



Task Name : [redacted]

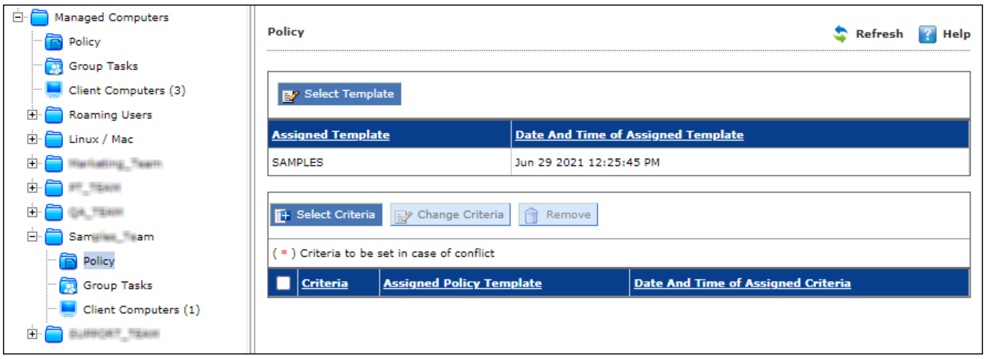
Summary

- Applied To 5 Computers

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.

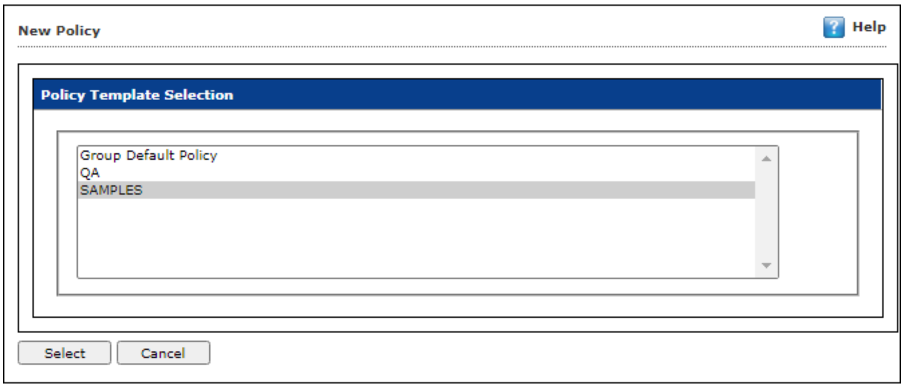


Assigned Template	Date And Time of Assigned Template
SAMPLES	Jun 29 2021 12:25:45 PM

(*) Criteria to be set in case of conflict

□	Criteria	Assigned Policy Template	Date And Time of Assigned Criteria

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



New Policy

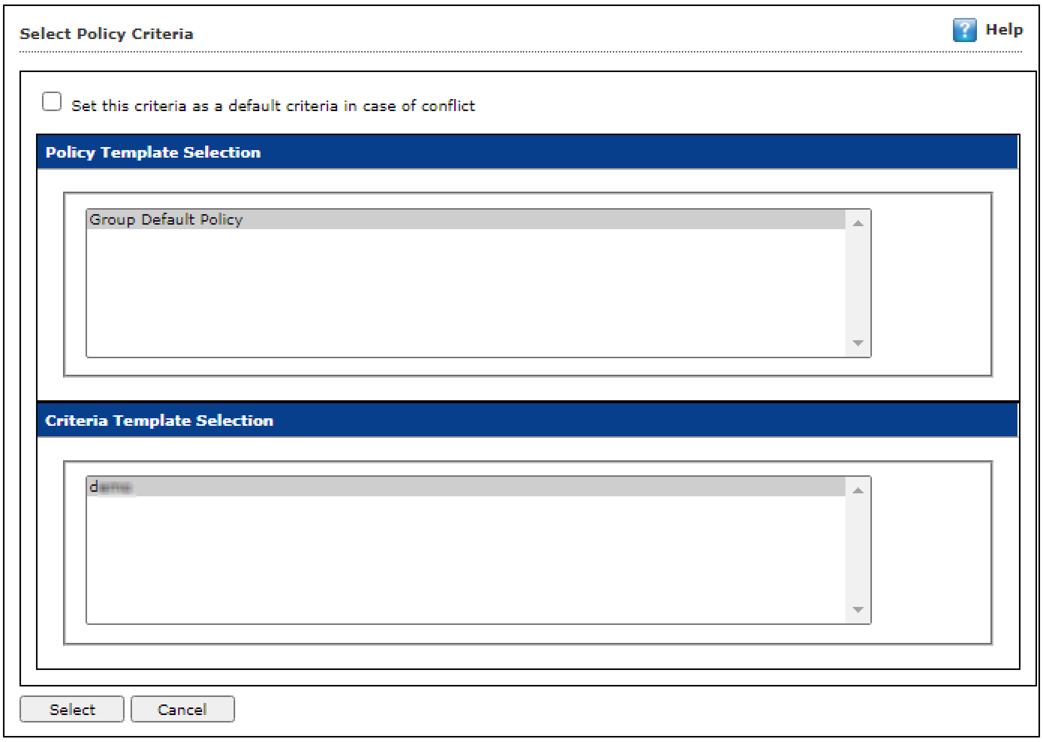
Help

Policy Template Selection

Group Default Policy
QA
SAMPLES

Select Cancel

4. Select a policy template and then click **Select**.
5. To assign criteria to 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

[redacted]

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.

Client Action List

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

- **Set Host Configuration**
- **Deploy/Upgrade Client**
- **Uninstall eScan Client**
- **Connect to Client (RMM)**
- **Move to Group**
- **Remove from Group**
- **Refresh Client**
- **Assign Policy Template**
- **Show Critical Incidents Events**
- **Show Critical Security Events**
- **Export**
- **Show Installed Software**
- **Force Download**
- **Check Vulnerability**
- **Forensic-Port/Communication**
- **Collect Debug/Logs**
- **Check eScan Port(s)**
- **Remediation Console**
- **Search IOC**
- **On Demand Scanning**
- **Send Message**
- **Outbreak Prevention**
- **Delete All Quarantine Files**
- **Create OTP**
- **Pause Protection**
- **Resume Protection**
- **Properties**

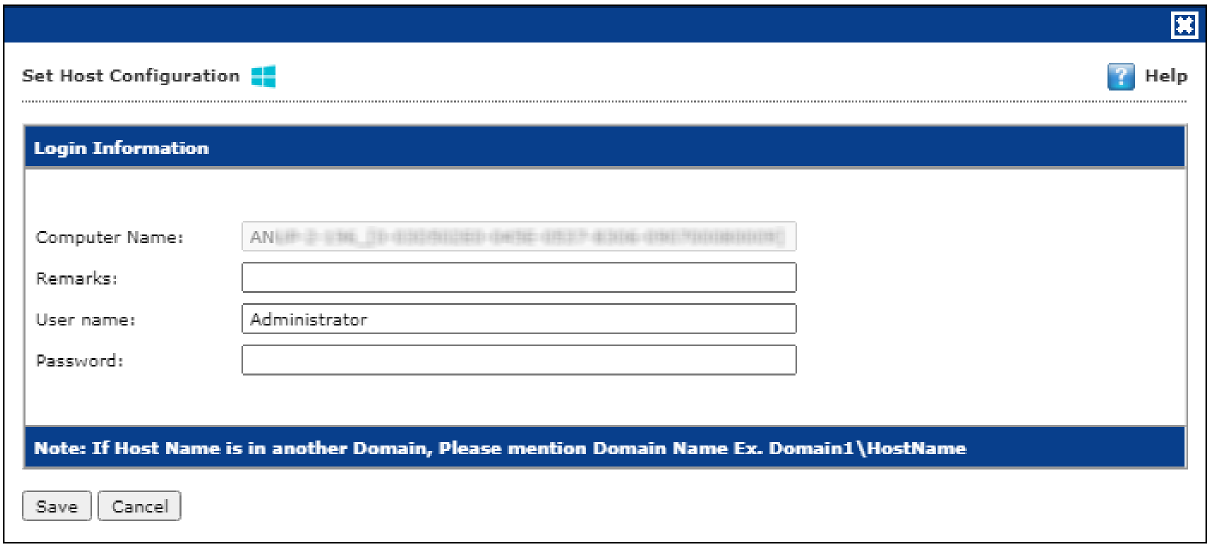
The Client Action List contains few options similar to Action List. These options perform same, except they perform the action only for selected computer(s).

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.



Set Host Configuration

Login Information

Computer Name: AN[redacted]

Remarks:

User name: Administrator

Password:

Note: If Host Name is in another Domain, Please mention Domain Name Ex. Domain1\HostName

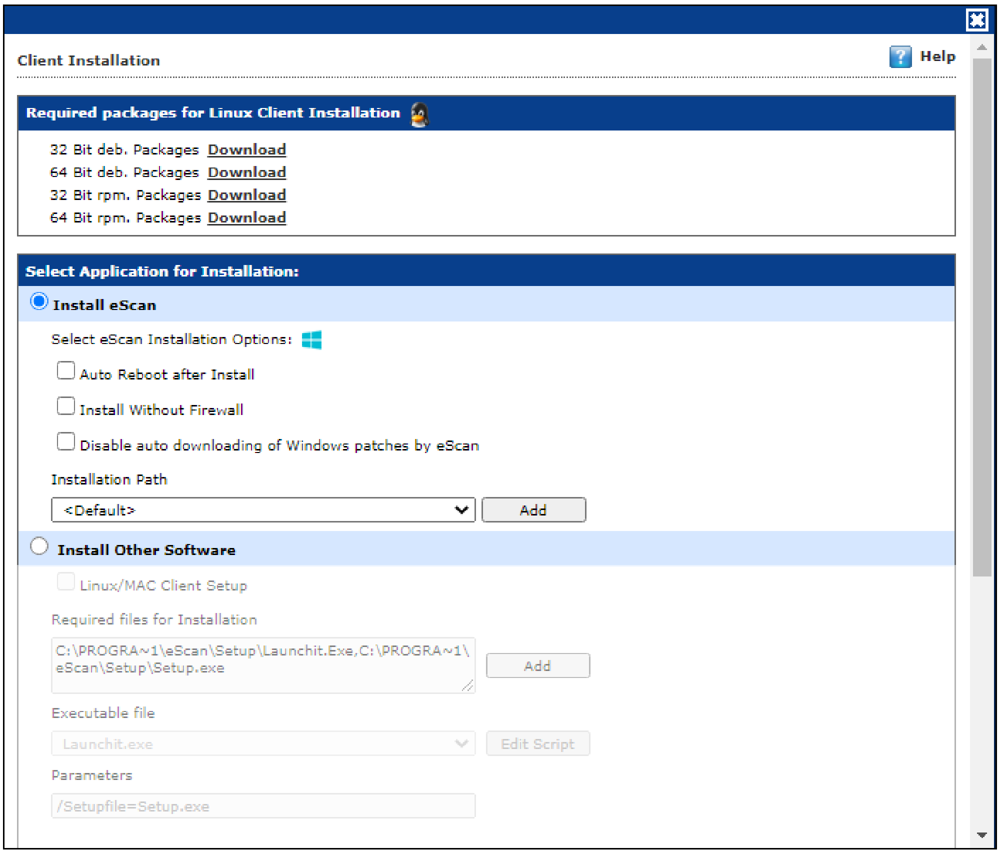
3. Enter Remarks and login credentials.
4. Click **Save**.
   The Host will be configured as per new settings.

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



Client Installation

Help

Required packages for Linux Client Installation

32 Bit deb. Packages Download
64 Bit deb. Packages Download
32 Bit rpm. Packages Download
64 Bit rpm. Packages Download

Select Application for Installation:

● Install eScan

Select eScan Installation Options:

□ Auto Reboot after Install
□ Install Without Firewall
□ Disable auto downloading of Windows patches by eScan

Installation Path

<Default> | Add

○ Install Other Software

□ Linux/MAC Client Setup

Required files for Installation

C:\PROGRA~1\eScan\Setup\Launchit.Exe,C:\PROGRA~1\eScan\Setup\Setup.exe | Add

Executable file

Launchit.exe | Edit Script

Parameters

/Setupfile=Setup.exe

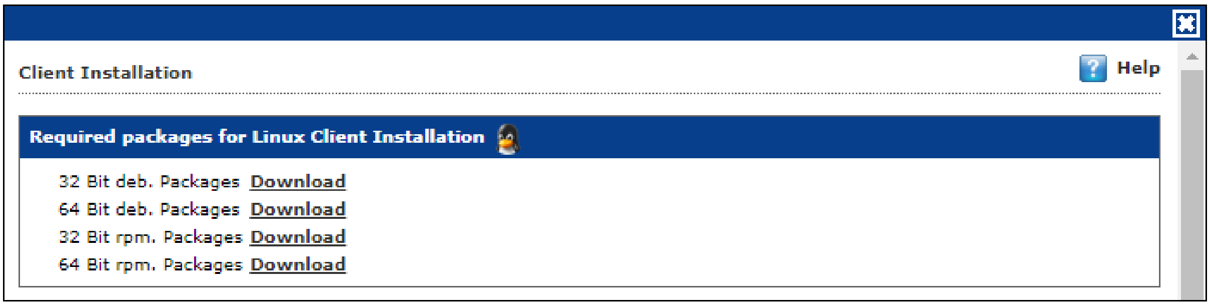
5. Select **Install eScan** option.
   By default eScan is installed at the following path on a Client computer.
   C:\Program Files\eScan (default path for 32-bit computer)
   OR
   C:\Program Files (x86)\eScan (default path for 64-bit computers).
6. To define a different installation path, click **Add**. (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.

Installing eScan Client on Linux Computers

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

6. Login to the EMC with your username and password.
7. Click Managed Computers on the navigation panel and select a group.

8. Under the group, click Client Computer and select a computer.
9. To deploy the setup, click **Client Action List** > **Deploy/ Upgrade Client**.
10. Download respective agent link from **Required package for Linux Client Installation** option.



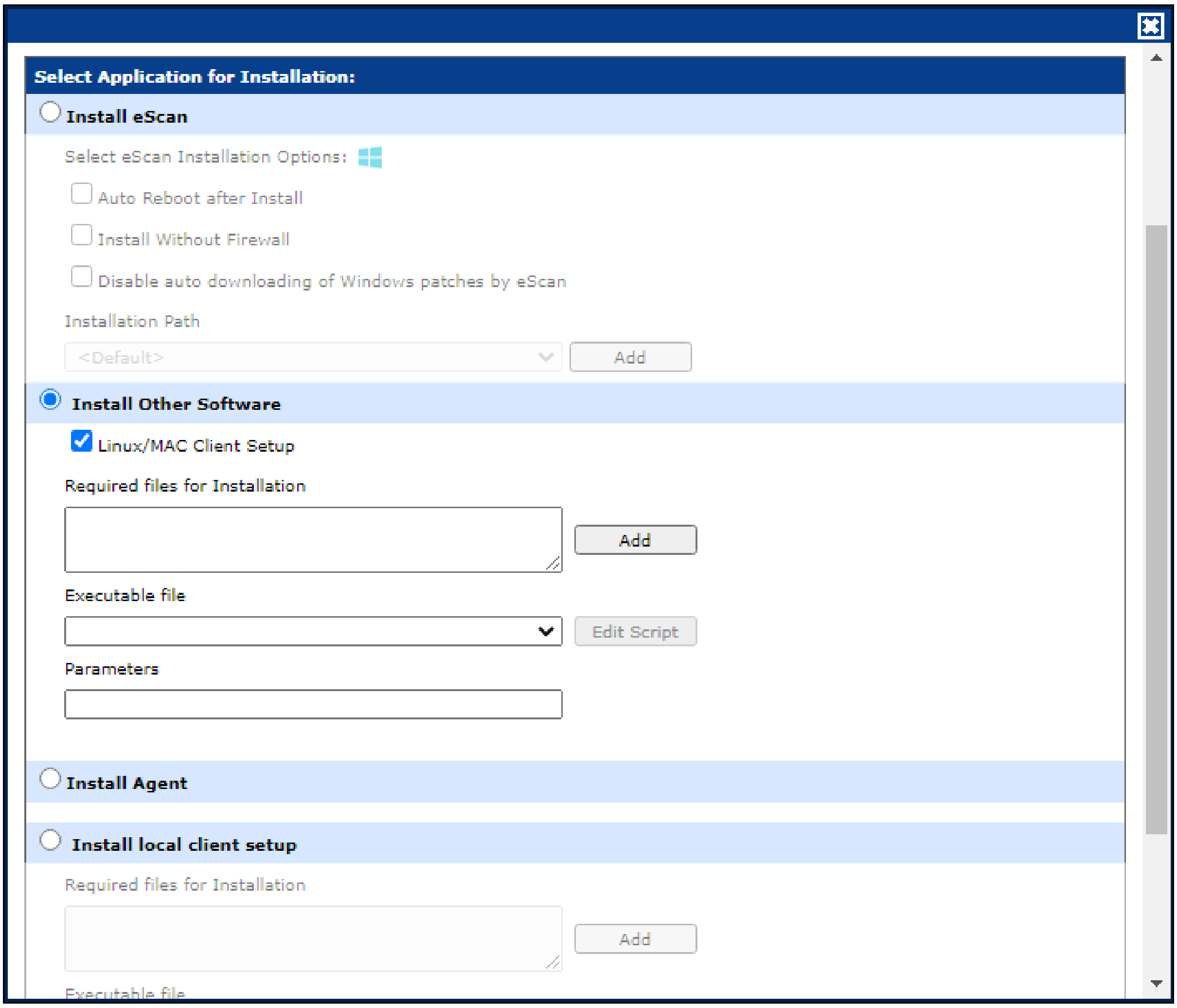
Client Installation

Help

Required packages for Linux Client Installation

32 Bit deb. Packages Download
64 Bit deb. Packages Download
32 Bit rpm. Packages Download
64 Bit rpm. Packages Download

11. Click **Install Other Software** and select **Linux/MAC Client setup** option.



Select Application for Installation:

○ Install eScan

Select eScan Installation Options:

□ Auto Reboot after Install

□ Install Without Firewall

□ Disable auto downloading of Windows patches by eScan

Installation Path

<Default>

● Install Other Software

☑ Linux/MAC Client Setup

Required files for Installation

Executable file

Parameters

○ Install Agent

○ Install local client setup

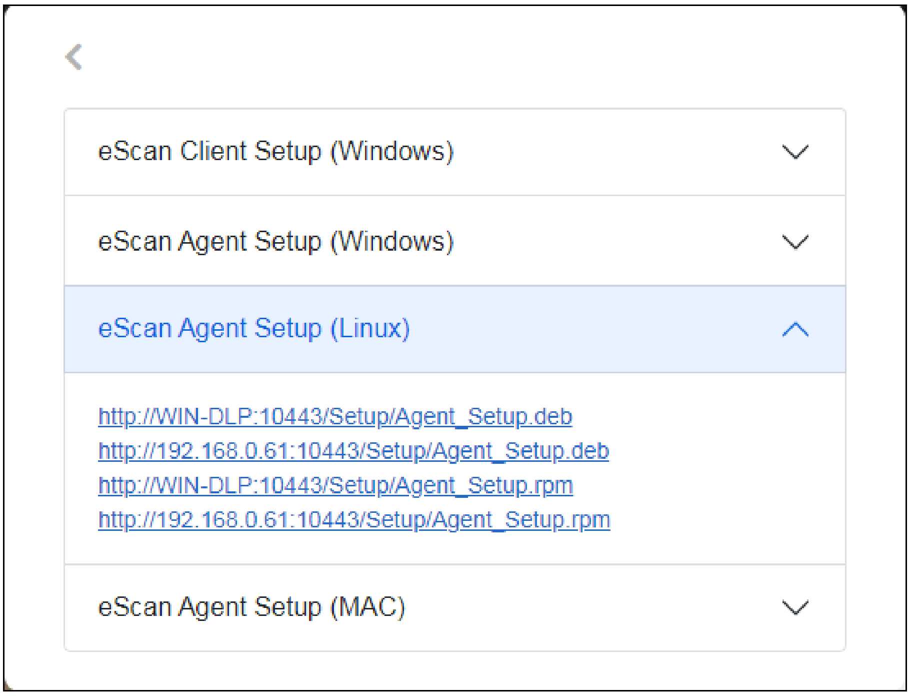
Required files for Installation

Executable file

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

Installing Agent on Linux

5. To manually install eScan Agent on Linux endpoint, please download the agent setup displayed on the **Login Page** > **Setup Links** of eScan Management Console and Save to the Linux client.



eScan Client Setup (Windows)

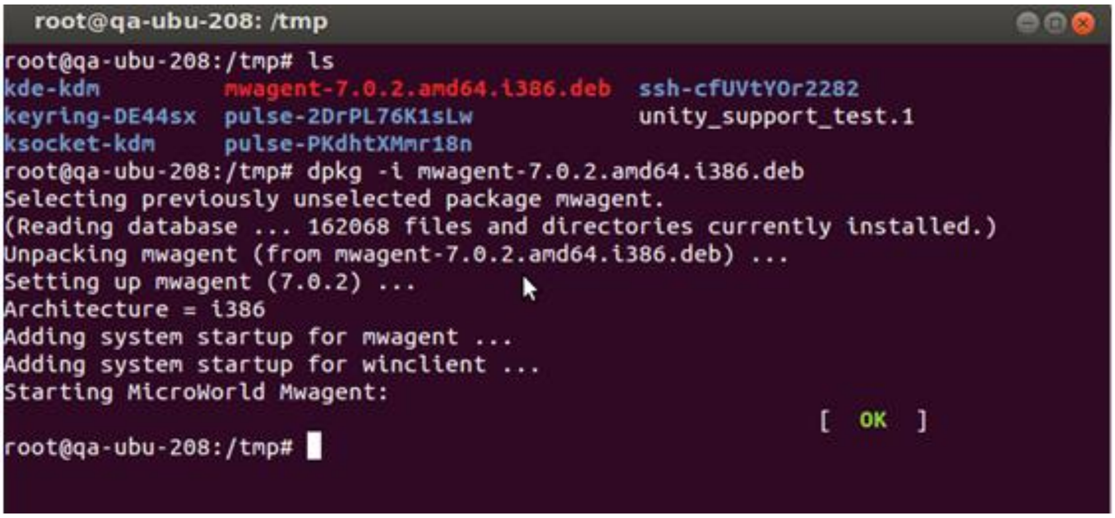
eScan Agent Setup (Windows)

eScan Agent Setup (Linux)

http://WIN-DLP:10443/Setup/Agent_Setup.deb
http://192.168.0.61:10443/Setup/Agent_Setup.deb
http://WIN-DLP:10443/Setup/Agent_Setup.rpm
http://192.168.0.61:10443/Setup/Agent_Setup.rpm

eScan Agent Setup (MAC)

6. Open the terminal for installing Agent.
7. Installation of Agent requires root or sudo user authentication. After Login as **root** or **sudo user**, go to the path where the **Agent_setup.deb** file has been saved.
8. Install the agent from the path using the following command – ***dpkg – i***. (**for RPM based setup – Rpm-ivh)** –



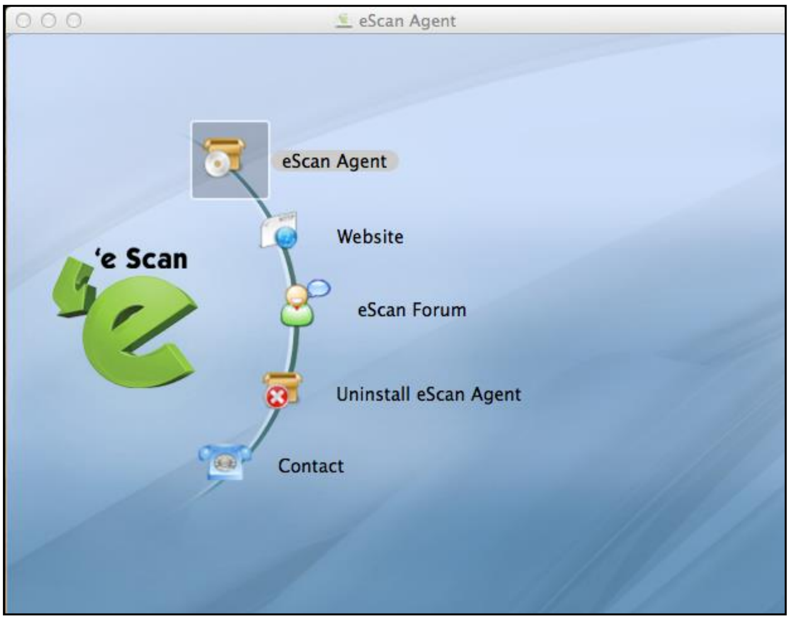
```
root@qa-ubu-208: /tmp
root@qa-ubu-208:/tmp# ls
kde-kdm         mwagent-7.0.2.amd64.i386.deb  ssh-cfUVtYOr2282
keyring-DE44sx  pulse-2DrPL76K1sLw            unity_support_test.1
ksocket-kdm     pulse-PKdhtXMmr18n
root@qa-ubu-208:/tmp# dpkg -i mwagent-7.0.2.amd64.i386.deb
Selecting previously unselected package mwagent.
(Reading database ... 162068 files and directories currently installed.)
Unpacking mwagent (from mwagent-7.0.2.amd64.i386.deb) ...
Setting up mwagent (7.0.2) ...
Architecture = i386
Adding system startup for mwagent ...
Adding system startup for winclient ...
Starting MicroWorld Mwagent:
                                                           [  OK  ]
root@qa-ubu-208:/tmp# █
```

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

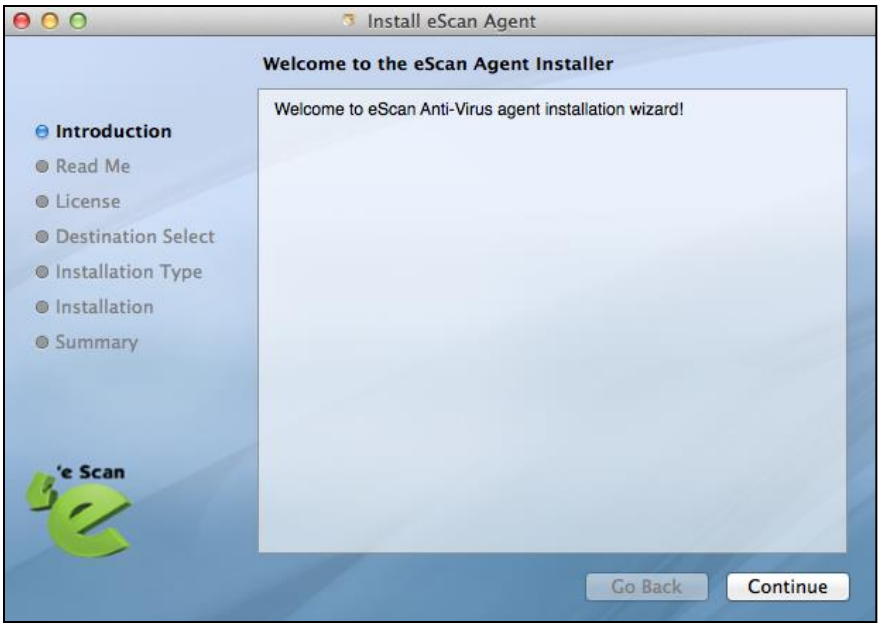
Installing eScan Agent on Mac Computers

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

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



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



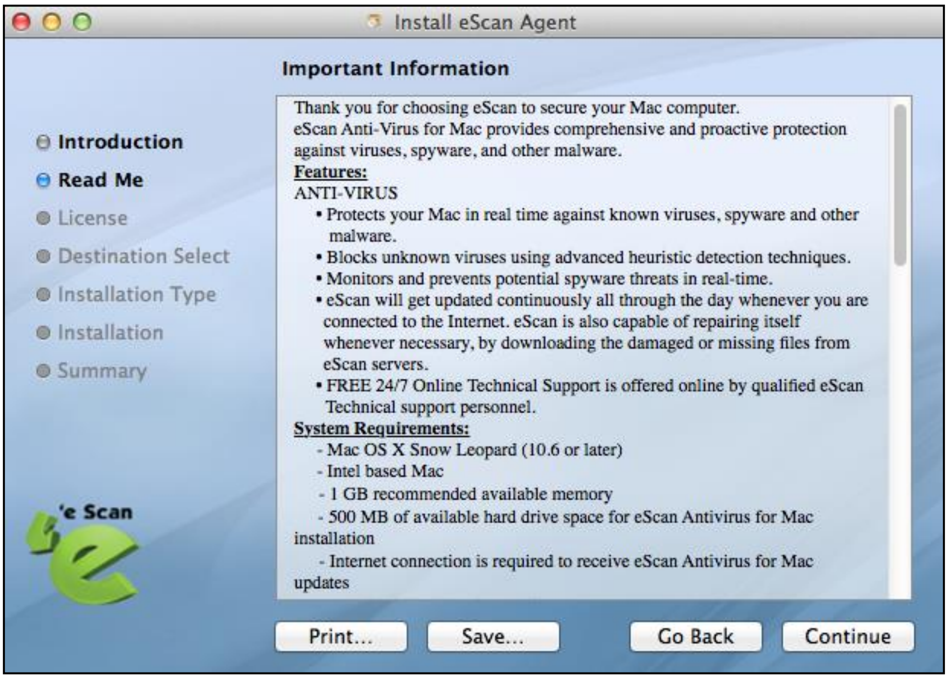
Welcome to the eScan Agent Installer

Welcome to eScan Anti-Virus agent installation wizard!

The installation wizard displays Read Me window.

17. Please read the system requirements and click **Continue**.

License window appears.



Thank you for choosing eScan to secure your Mac computer.
eScan Anti-Virus for Mac provides comprehensive and proactive protection against viruses, spyware, and other malware.

Features:

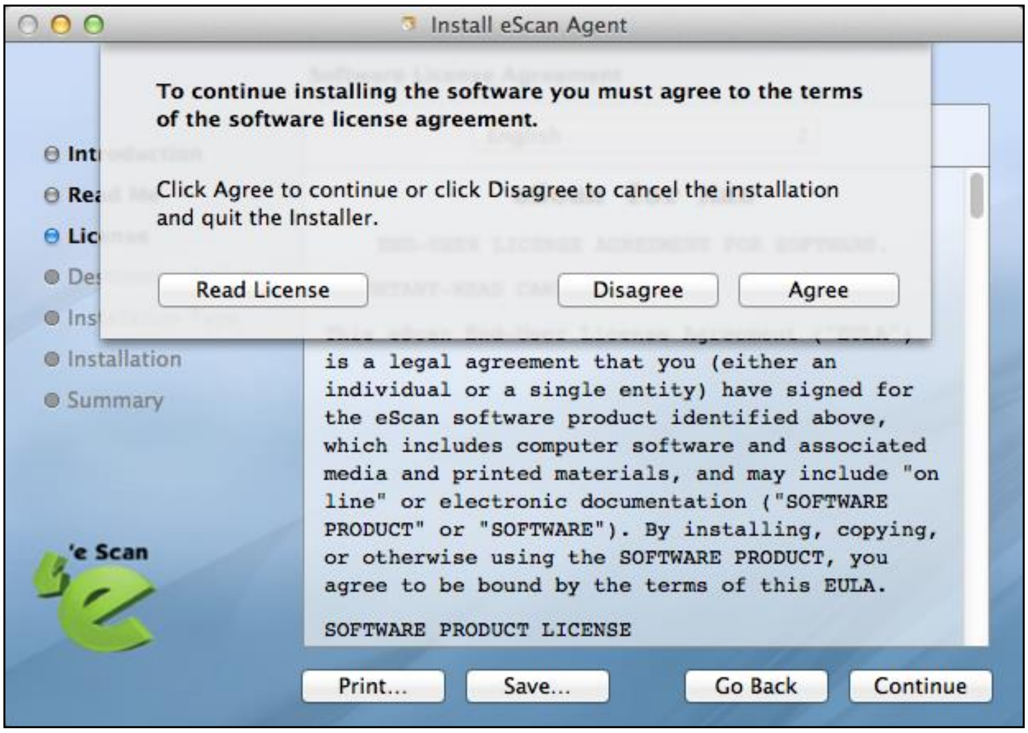
ANTI-VIRUS

- Protects your Mac in real time against known viruses, spyware and other malware.
- Blocks unknown viruses using advanced heuristic detection techniques.
- Monitors and prevents potential spyware threats in real-time.
- eScan will get updated continuously all through the day whenever you are connected to the Internet. eScan is also capable of repairing itself whenever necessary, by downloading the damaged or missing files from eScan servers.
- FREE 24/7 Online Technical Support is offered online by qualified eScan Technical support personnel.

System Requirements:

- Mac OS X Snow Leopard (10.6 or later)
- Intel based Mac
- 1 GB recommended available memory
- 500 MB of available hard drive space for eScan Antivirus for Mac installation
- Internet connection is required to receive eScan Antivirus for Mac updates

18. Please read the agreement completely and then click **Continue**.
19. Agree to terms and conditions by clicking **Agree**.



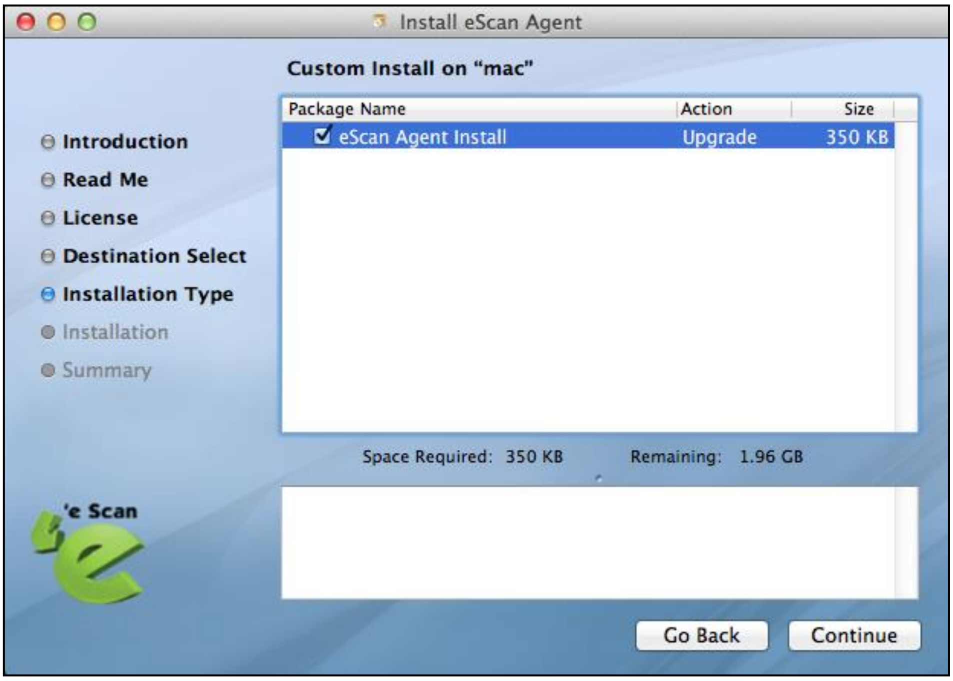
To continue installing the software you must agree to the terms of the software license agreement.

Click Agree to continue or click Disagree to cancel the installation and quit the Installer.

is a legal agreement that you (either an individual or a single entity) have signed for the eScan software product identified above, which includes computer software and associated media and printed materials, and may include "on line" or electronic documentation ("SOFTWARE PRODUCT" or "SOFTWARE"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA.

SOFTWARE PRODUCT LICENSE

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



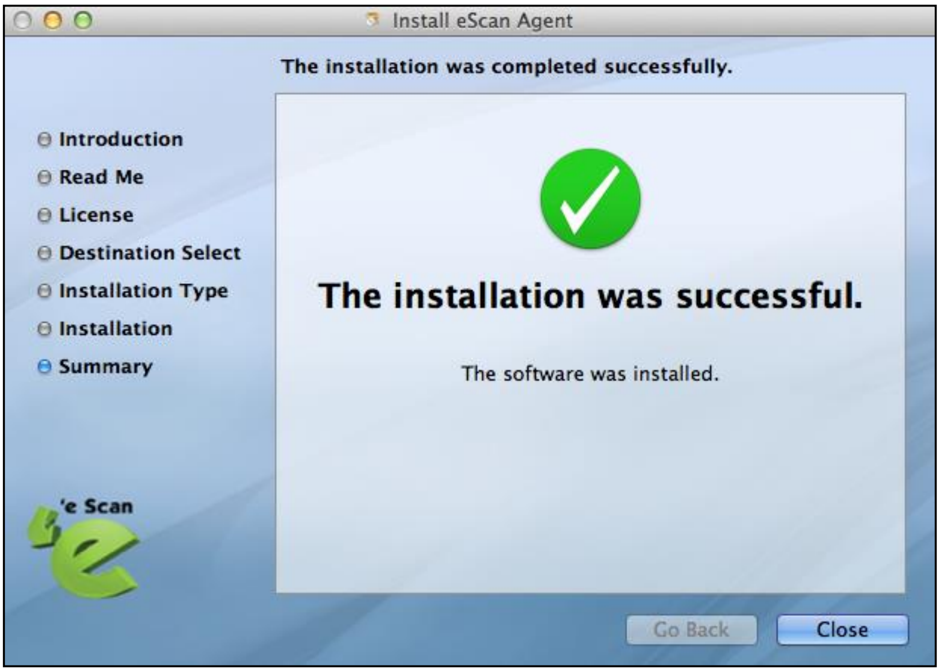
Install eScan Agent

Custom Install on “mac”

Package Name	Action	Size
☑ eScan Agent Install	Upgrade	350 KB

Space Required: 350 KB Remaining: 1.96 GB

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



Install eScan Agent

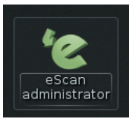
The installation was completed successfully.

The installation was successful.

The software was installed.

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

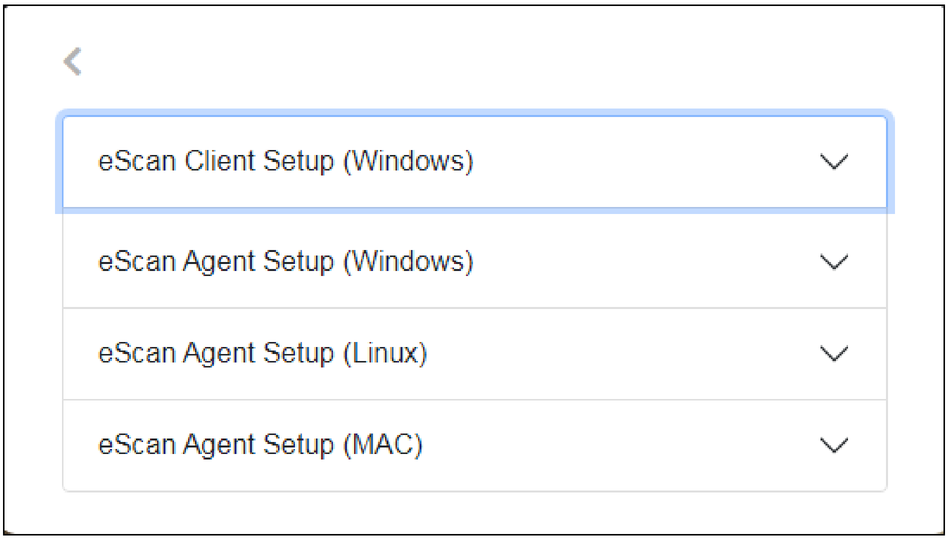
In Linux, eScan Administrator Icon will be displayed on desktop.



In Mac, eScan icon will be displayed in the **Dock**. Double-click it to launch eScan.

Manual installation of eScan Client on network computers

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


eScan Client Setup (Windows)
eScan Agent Setup (Windows)
eScan Agent Setup (Linux)
eScan Agent Setup (MAC)

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)

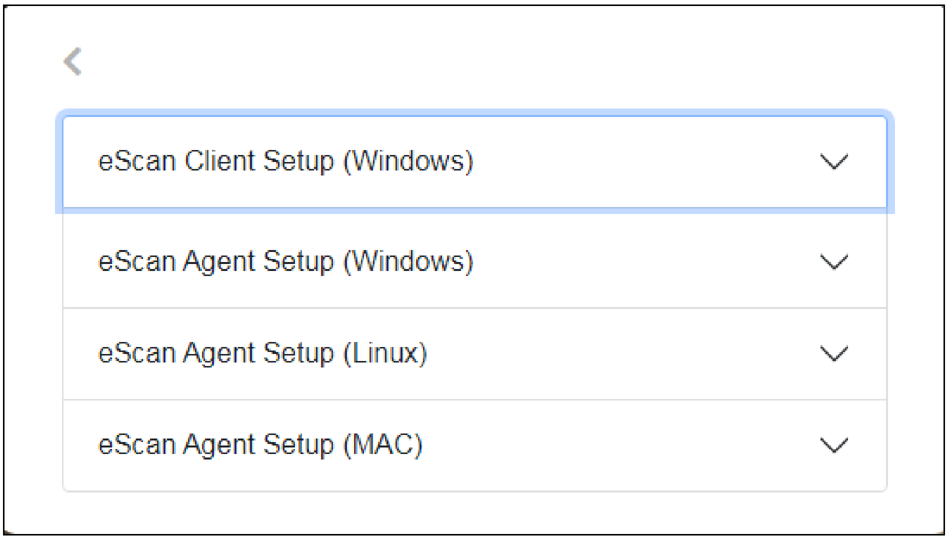
Remotely installing agent on Client computer(s)

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.

NOTE	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.

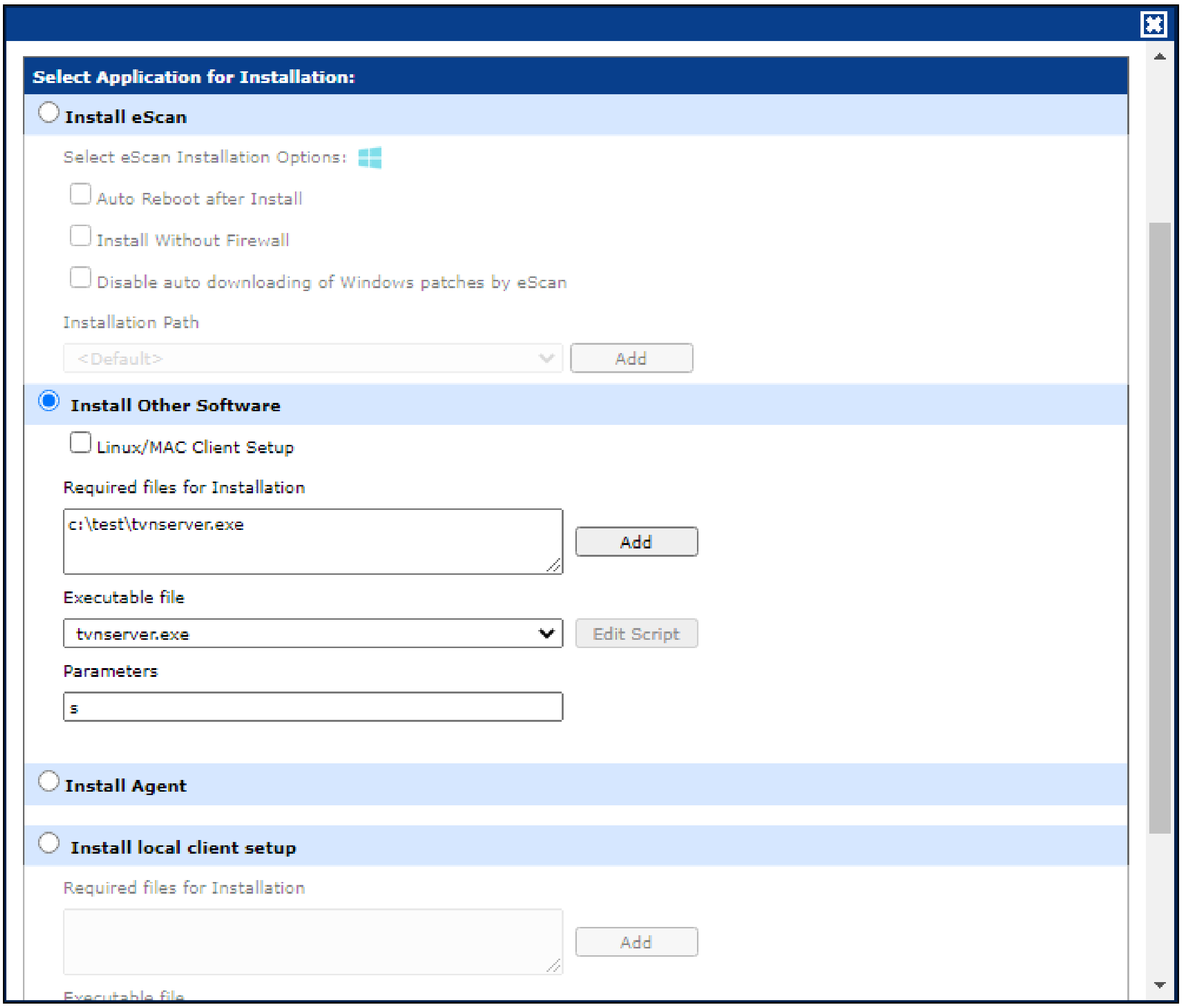

eScan Client Setup (Windows)
eScan Agent Setup (Windows)
eScan Agent Setup (Linux)
eScan Agent Setup (MAC)

Installing other Software (Third Party Software)

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

10. Click Managed Computers.
11. Select a computer from a group.
12. Click **Client Action List** > **Deploy/Upgrade Client**. Client Installation window appears.

13. Select **Install Other Software** option.



Select Application for Installation:

○ Install eScan

Select eScan Installation Options:

□ Auto Reboot after Install

□ Install Without Firewall

□ Disable auto downloading of Windows patches by eScan

Installation Path

<Default> [Add]

● Install Other Software

□ Linux/MAC Client Setup

Required files for Installation

c:\test\tvnserver.exe [Add]

Executable file

tvnserver.exe [Edit Script]

Parameters

s

○ Install Agent

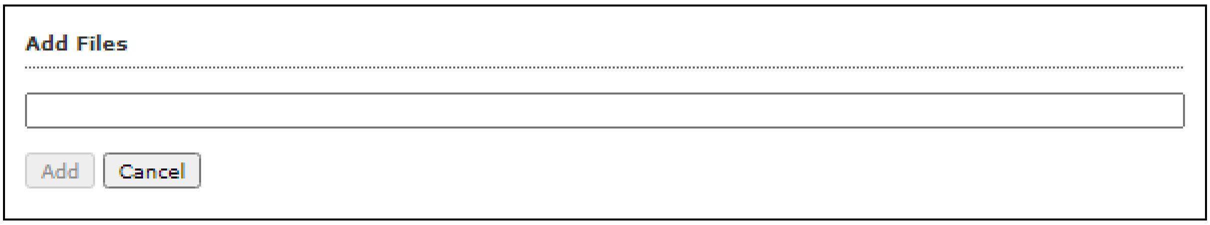
○ Install local client setup

Required files for Installation

[Add]

Executable file

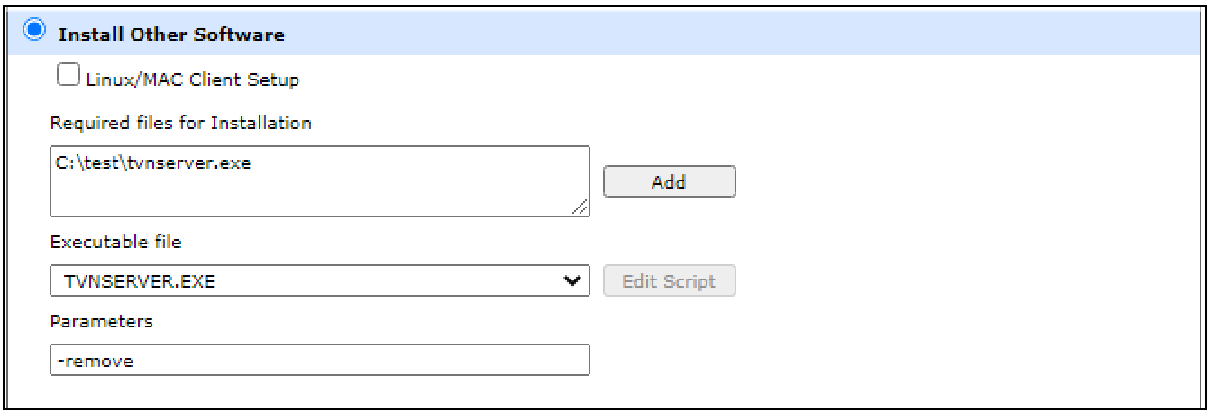
14. Click **Add.**
    Add Files window appears.



Add Files

[Add] [Cancel]

15. 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**

□ Linux/MAC Client Setup

Required files for Installation

C:\test\tvnserver.exe

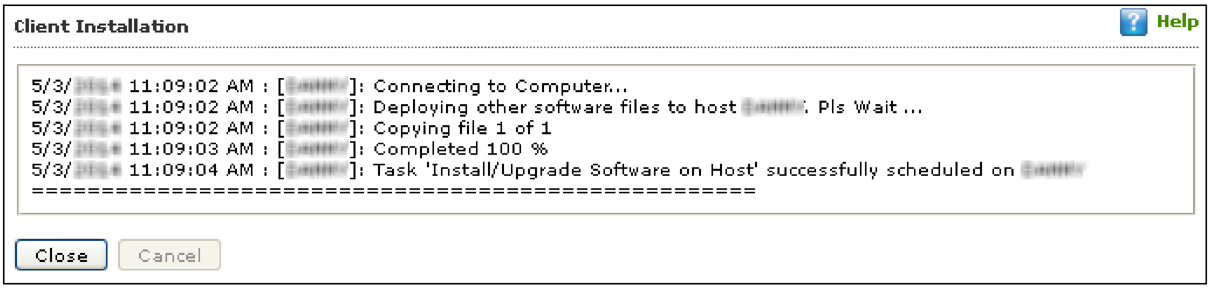
Executable file

TVNSERVER.EXE

Parameters

-remove

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



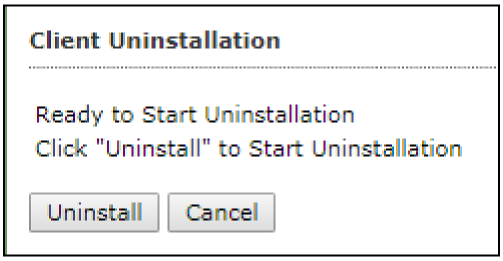
Client Installation

```
5/3/[redacted] 11:09:02 AM : [[redacted]]: Connecting to Computer...
5/3/[redacted] 11:09:02 AM : [[redacted]]: Deploying other software files to host [redacted]. Pls Wait ...
5/3/[redacted] 11:09:02 AM : [[redacted]]: Copying file 1 of 1
5/3/[redacted] 11:09:03 AM : [[redacted]]: Completed 100 %
5/3/[redacted] 11:09:04 AM : [[redacted]]: Task 'Install/Upgrade Software on Host' successfully scheduled on [redacted]
=====================================================
```

Uninstall eScan Client

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

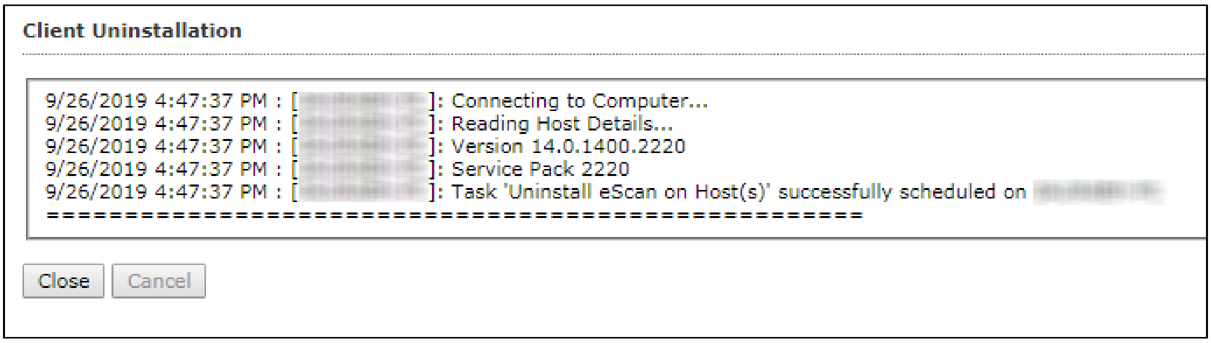
1. Select the computer for uninstallation.
2. Click **Client Action List** > **Uninstall eScan Client**.
   Client Uninstallation window appears.



Client Uninstallation

Ready to Start Uninstallation
Click "Uninstall" to Start Uninstallation

3. Click **Uninstall**.
   The Client Uninstallation window displays the progress.



Client Uninstallation

```
9/26/2019 4:47:37 PM : [[redacted]]: Connecting to Computer...
9/26/2019 4:47:37 PM : [[redacted]]: Reading Host Details...
9/26/2019 4:47:37 PM : [[redacted]]: Version 14.0.1400.2220
9/26/2019 4:47:37 PM : [[redacted]]: Service Pack 2220
9/26/2019 4:47:37 PM : [[redacted]]: Task 'Uninstall eScan on Host(s)' successfully scheduled on [redacted]
=======================================================
```

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**.

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 add to RMM License.
3. Click **Client Action List** > **Connect to Client (RMM)**.
   RMM disclaimer appears.
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 are done performing an activity, click the Disconnect icon to end remote connection.

Move to Group

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

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

Remove from Group

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

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

Refresh Client

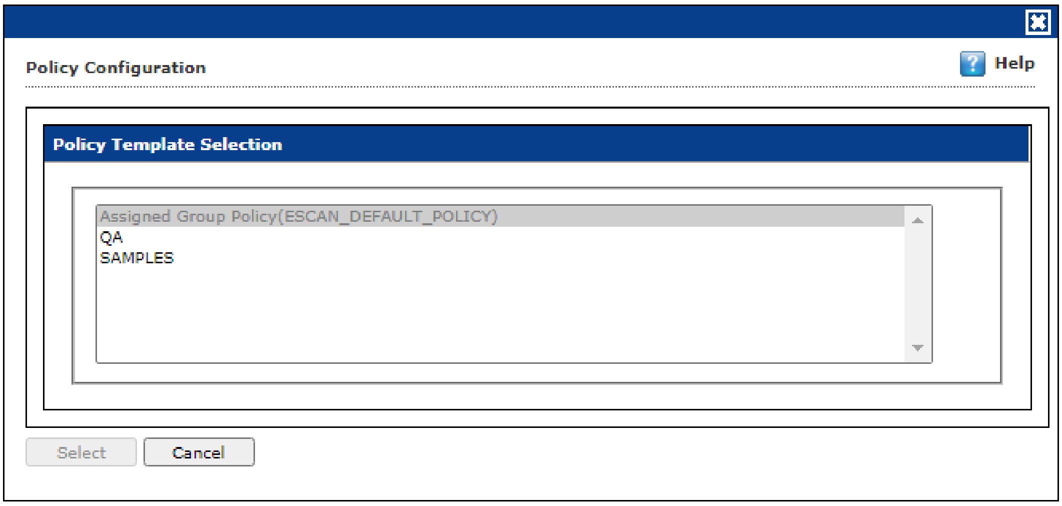
To refresh status of any client computer, follow the steps given below:

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

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 which you want to assign policy template.
3. Click **Client Action List** > **Assign Policy Template**.
4. Manage Add-On License window appears.



Policy Configuration

Policy Template Selection

Assigned Group Policy(ESCAN_DEFAULT_POLICY)
QA
SAMPLES

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

Show Critical Incident Events

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

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

Show Critical Security Events

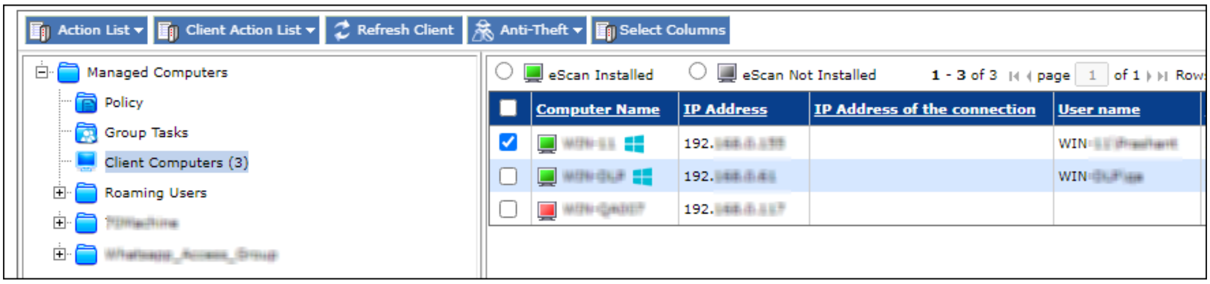
To show critical security events of specific computer, follow the steps given below:

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

Export

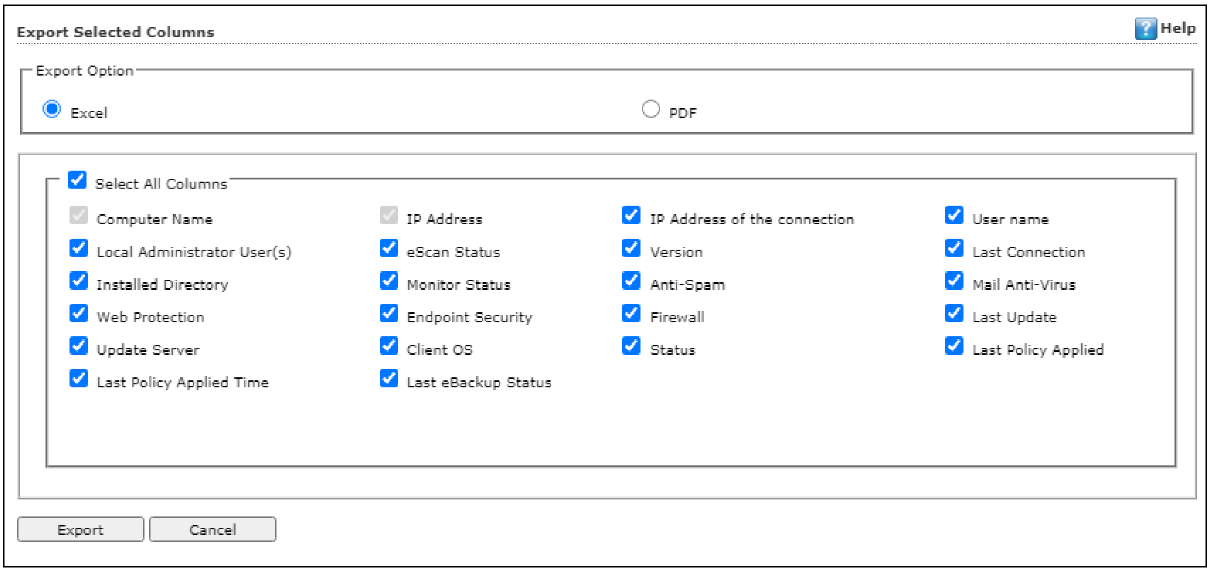
To export a client computer's data, follow the steps given below:

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



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

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



Export Selected Columns — Help

Export Option

● Excel ○ PDF

☑ Select All Columns

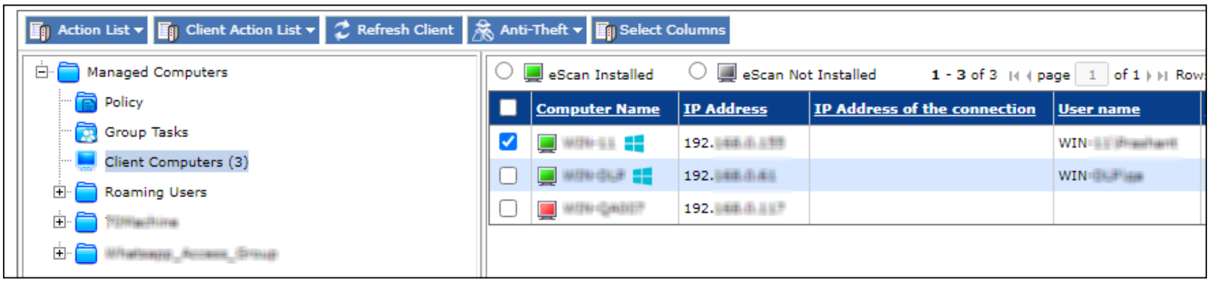
☑ Computer Name
☑ Local Administrator User(s)
☑ Installed Directory
☑ Web Protection
☑ Update Server
☑ Last Policy Applied Time
☑ IP Address
☑ eScan Status
☑ Monitor Status
☑ Endpoint Security
☑ Client OS
☑ Last eBackup Status
☑ IP Address of the connection
☑ Version
☑ Anti-Spam
☑ Firewall
☑ Status
☑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

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

Show Installed Softwares

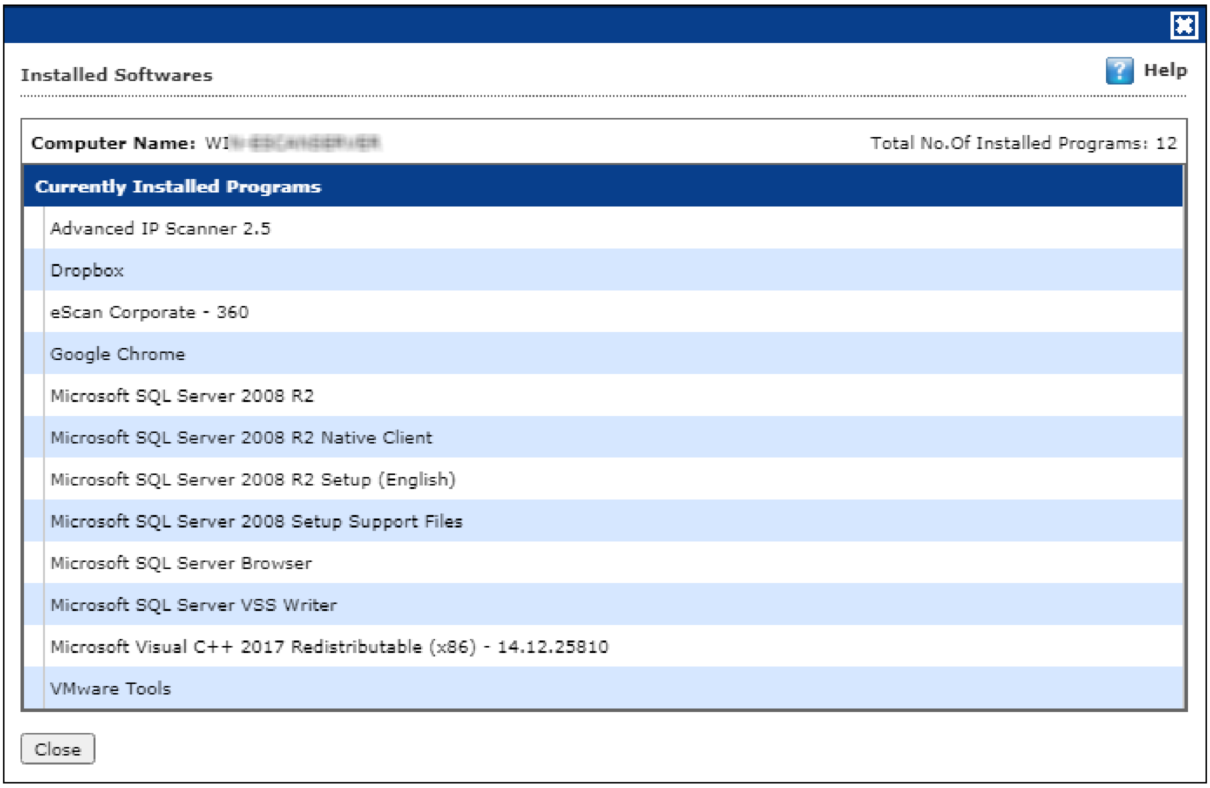
This feature displays a list of installed softwares on a computer. To view the list of installed softwares, follow the steps given below:

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



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

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



Installed Softwares

Computer Name: WI[redacted]

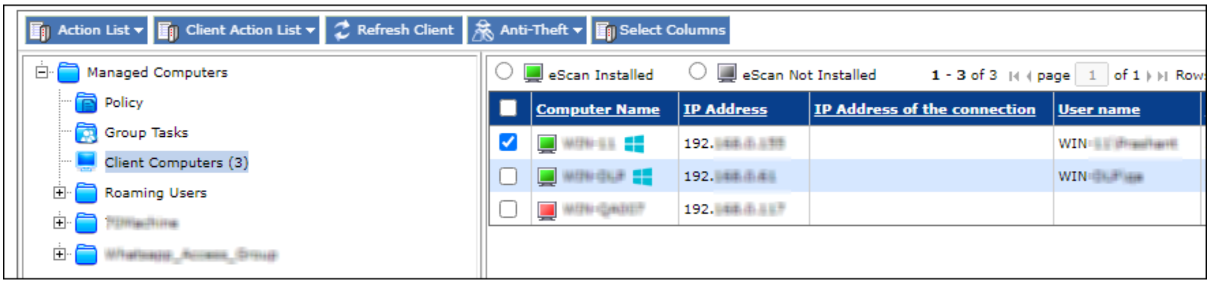
Total No.Of Installed Programs: 12

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

Force Download

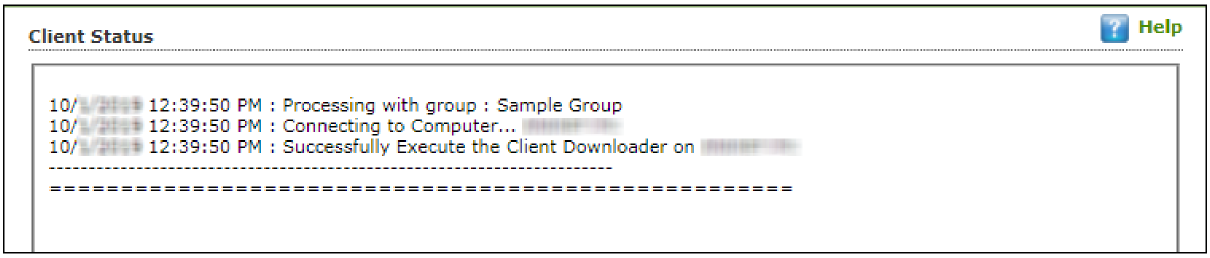
The Force Download feature forces a client computer to download Policy Template modifications (if any) and updated virus signature database. To activate this feature for computers, follow the steps given below:

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



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

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

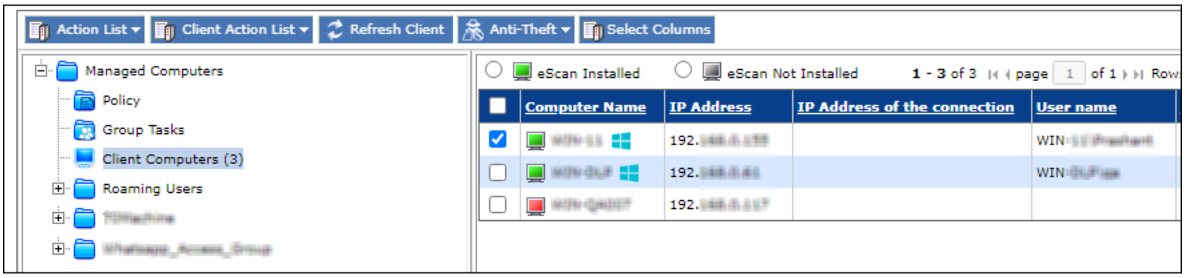


```
10/[redacted] 12:39:50 PM : Processing with group : Sample Group
10/[redacted] 12:39:50 PM : Connecting to Computer... [redacted]
10/[redacted] 12:39:50 PM : Successfully Execute the Client Downloader on [redacted]
---------------------------------------------------------------------------
===================================================
```

Check Vulnerability

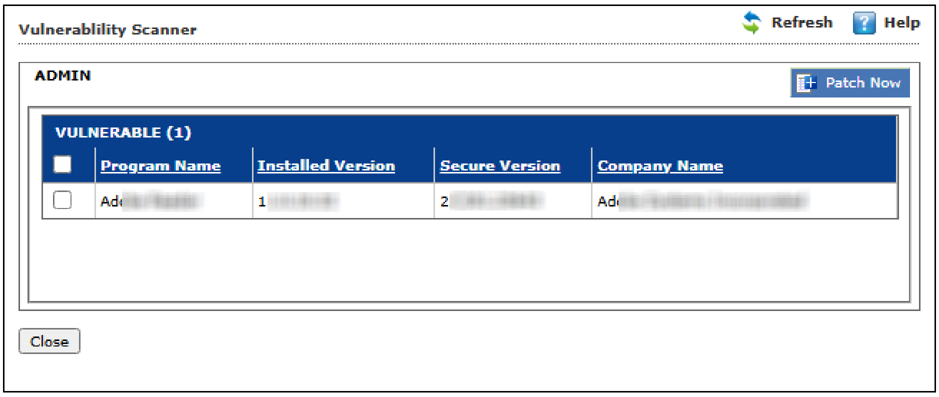
This option helps user to find the present vulnerabilities on managed computers.

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.



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

2. Select client computers and then click **Client Action List** > **Check Vulnerability**. Vulnerability Scanner window appears displaying the result.



Vulnerablility Scanner

ADMIN

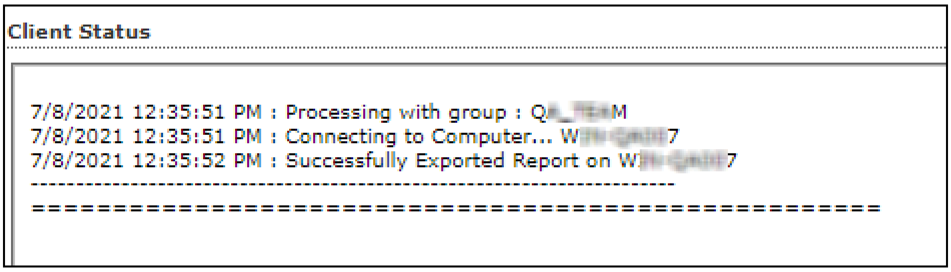
VULNERABLE (1)

☐	Program Name	Installed Version	Secure Version	Company Name
☐	Ad[redacted]	1[redacted]	2[redacted]	Ad[redacted]

The window allows you to patch the vulnerable program using **Patch Now** button on Top-left side.

Forensic-Port/Communication

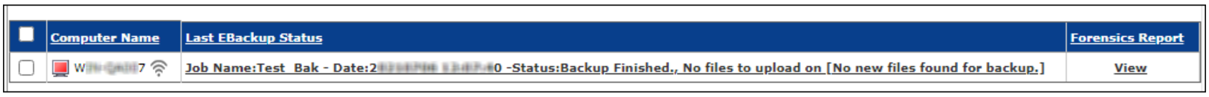
This option generates the Forensic report of the service running on certain port during a particular period for analysis. To generate the report, select the client computer and click **Forensic Port/Communication** option.



Client Status

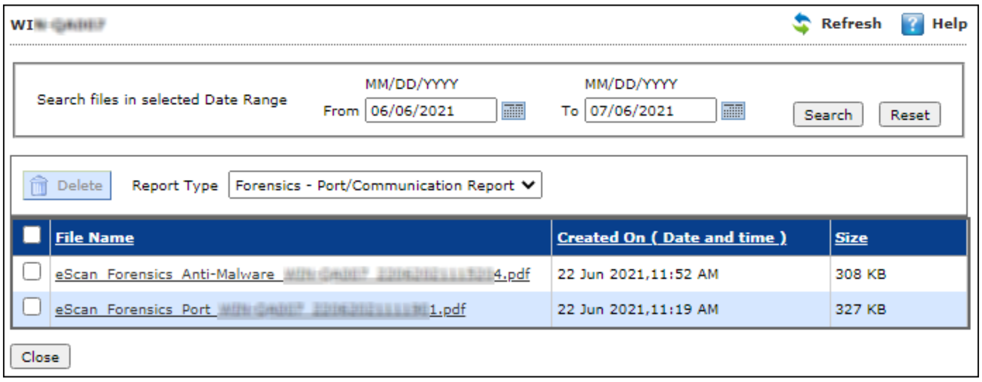
```
7/8/2021 12:35:51 PM : Processing with group : Q[redacted]M
7/8/2021 12:35:51 PM : Connecting to Computer... W[redacted]7
7/8/2021 12:35:52 PM : Successfully Exported Report on W[redacted]7
------------------------------------------------------------------------
=================================================================
```

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



☐	Computer Name	Last EBackup Status	Forensics Report
☐	W[redacted]7	Job Name:Test_Bak - Date:2[redacted]0 -Status:Backup Finished., No files to upload on [No new files found for backup.]	View

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



WI[redacted]

Search files in selected Date Range

MM/DD/YYYY From 06/06/2021

MM/DD/YYYY To 07/06/2021

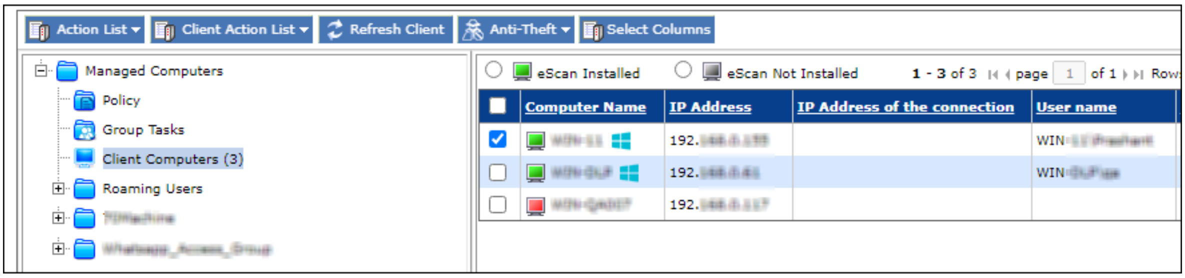
Report Type: Forensics - Port/Communication Report

☐	File Name	Created On (Date and time)	Size
☐	eScan_Forensics_Anti-Malware_[redacted]4.pdf	22 Jun 2021,11:52 AM	308 KB
☐	eScan_Forensics_Port_[redacted]1.pdf	22 Jun 2021,11:19 AM	327 KB

Collect Debug/Logs

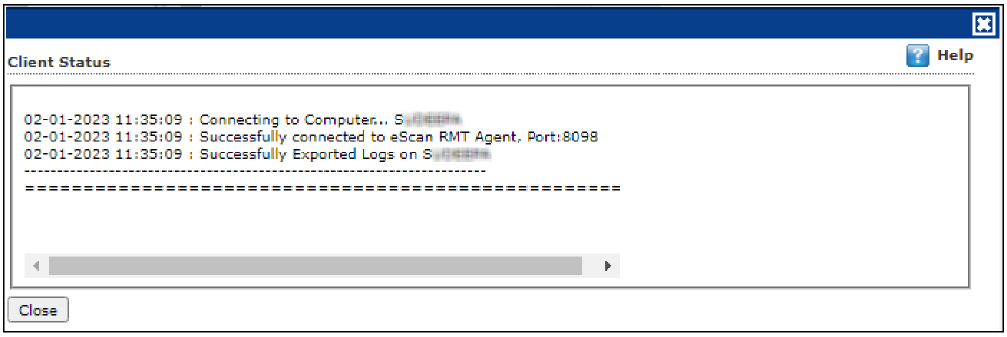
This option helps user to record the system operation and errors that occurs while performing any action on managed computers.

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



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

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

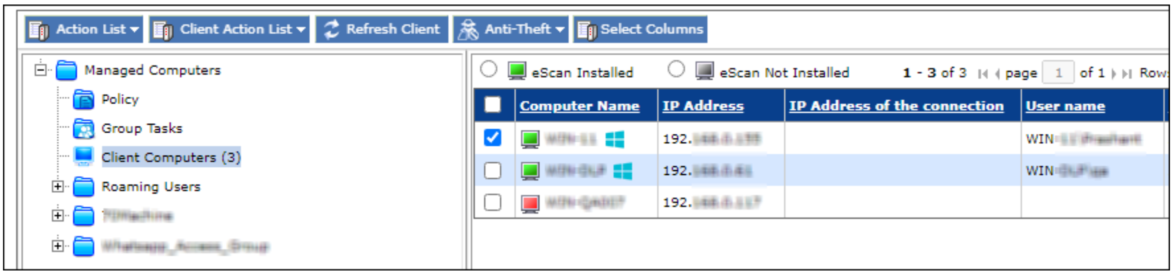


```
02-01-2023 11:35:09 : Connecting to Computer... S[redacted]
02-01-2023 11:35:09 : Successfully connected to eScan RMT Agent, Port:8098
02-01-2023 11:35:09 : Successfully Exported Logs on S[redacted]
-----------------------------------------------------------------
====================================================
```

Check eScan Port(s)

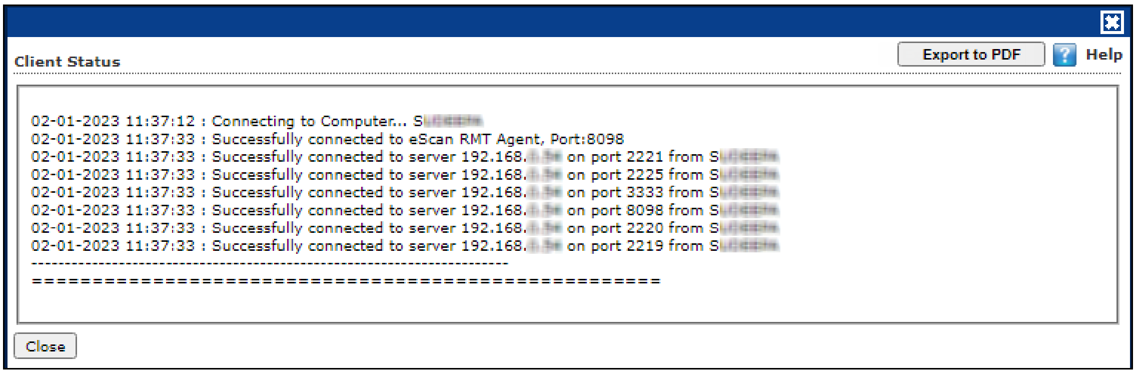
This option used to figure out the opened ports on particular client machine. Checking ports regularly will help you to close the unnecessary ports.

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.



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

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



Client Status

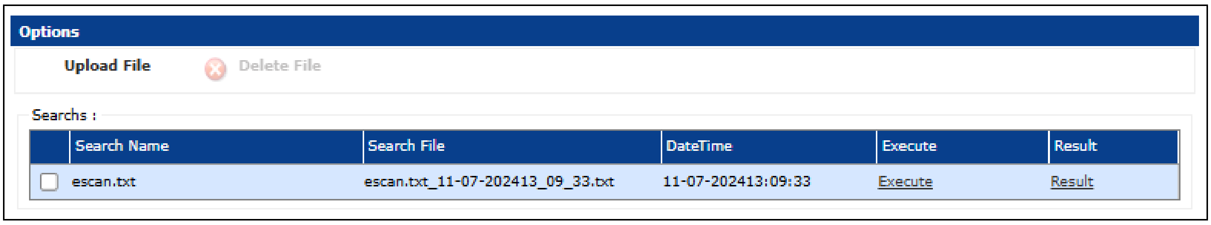
```
02-01-2023 11:37:12 : Connecting to Computer... S[redacted]
02-01-2023 11:37:33 : Successfully connected to eScan RMT Agent, Port:8098
02-01-2023 11:37:33 : Successfully connected to server 192.168.[redacted] on port 2221 from S[redacted]
02-01-2023 11:37:33 : Successfully connected to server 192.168.[redacted] on port 2225 from S[redacted]
02-01-2023 11:37:33 : Successfully connected to server 192.168.[redacted] on port 3333 from S[redacted]
02-01-2023 11:37:33 : Successfully connected to server 192.168.[redacted] on port 8098 from S[redacted]
02-01-2023 11:37:33 : Successfully connected to server 192.168.[redacted] on port 2220 from S[redacted]
02-01-2023 11:37:33 : Successfully connected to server 192.168.[redacted] on port 2219 from S[redacted]
--------------------------------------------------------------------------------
=====================================================
```

Remediation Console

eScan Remediation Console offers unified dashboard for visibility across all endpoints in the network. It helps security team view real-time information and events about a particular client endpoint from a network. This includes system hardware and OS details, task manager activities, task scheduler, network connection activities, and a bunch of other components as well. Click here to learn more.

Search IOC

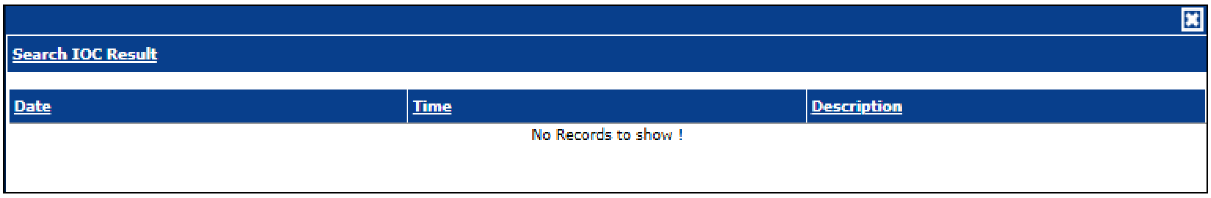
Indicators of Compromise (IOC) are the evidence that indicate potential security breach and malicious activity. It allows you to manually search IOCs and view their results from particular endpoint by uploading IOC scripts of known threats. Follow the steps given below to search IOCs in endpoints:



Searchs :

	Search Name	Search File	DateTime	Execute	Result
□	escan.txt	escan.txt_11-07-202413_09_33.txt	11-07-202413:09:33	Execute	Result

1. Click on **Upload File** to browse and upload script file of the IOC.
   The browse dialogue box appears.
2. Enter search name in provided field for the file to be uploaded.
3. Click on **Choose file** button to browse the script with .txt extension from the computer.
4. Select the file and click on **Save**.
   The IOC script will be available in the IOC list.
5. Select the script from the list and click on the **Execute** button provided under ‘Execute’ column to run the IOC search.
6. Click on the **Result** button provided under ‘Result’ column to view search results.



Search IOC Result

Date	Time	Description

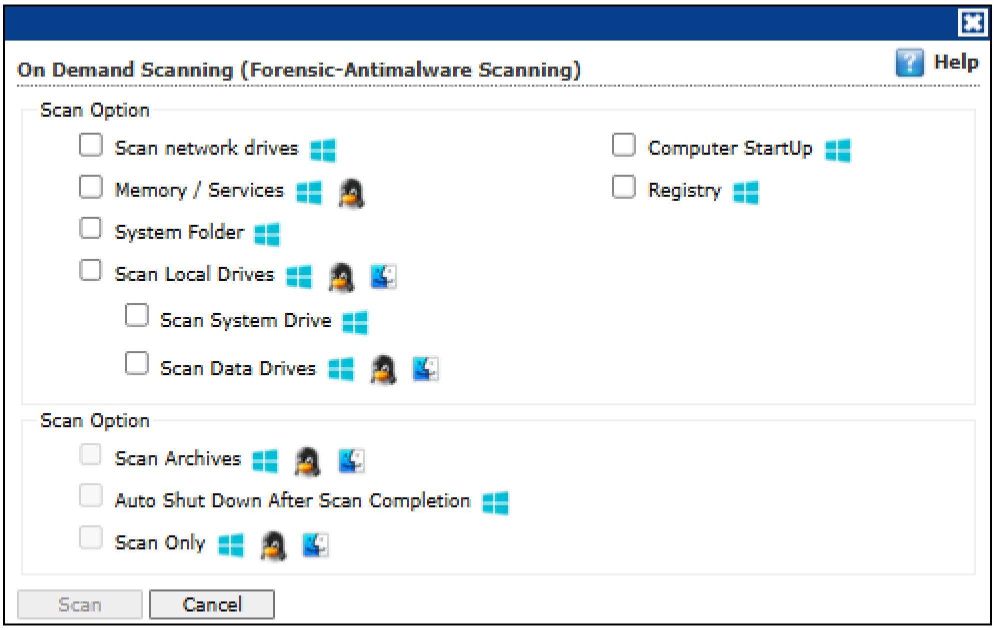
No Records to show !

You can delete IOC script from the list by selecting and clicking on **Delete File** button.

On Demand Scanning

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

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



On Demand Scanning (Forensic-Antimalware Scanning)

Scan Option

- □ Scan network drives
- □ Memory / Services
- □ System Folder
- □ Scan Local Drives
  - □ Scan System Drive
  - □ Scan Data Drives
- □ Computer StartUp
- □ Registry

Scan Option

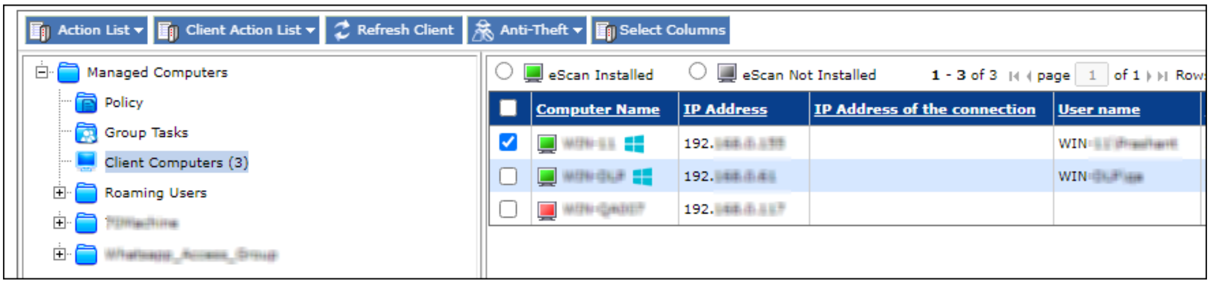
- □ Scan Archives
- □ Auto Shut Down After Scan Completion
- □ Scan Only

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

Send Message

The Send Message feature lets you send a message to computers. To send message to computers, follow the steps given below:

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

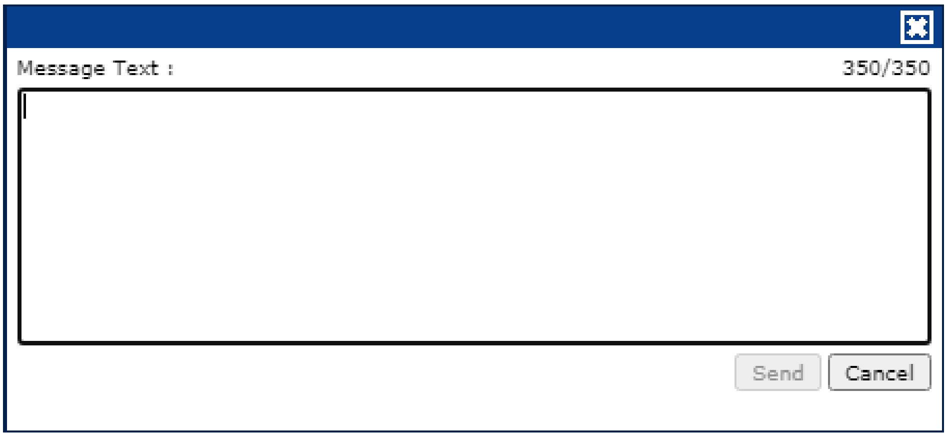


Managed Computers
- Policy
- Group Tasks
- Client Computers (3)
- Roaming Users
- [redacted]
- [redacted]

○ eScan Installed ○ eScan Not Installed 1 - 3 of 3 page 1 of 1

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

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



Message Text : 350/350

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

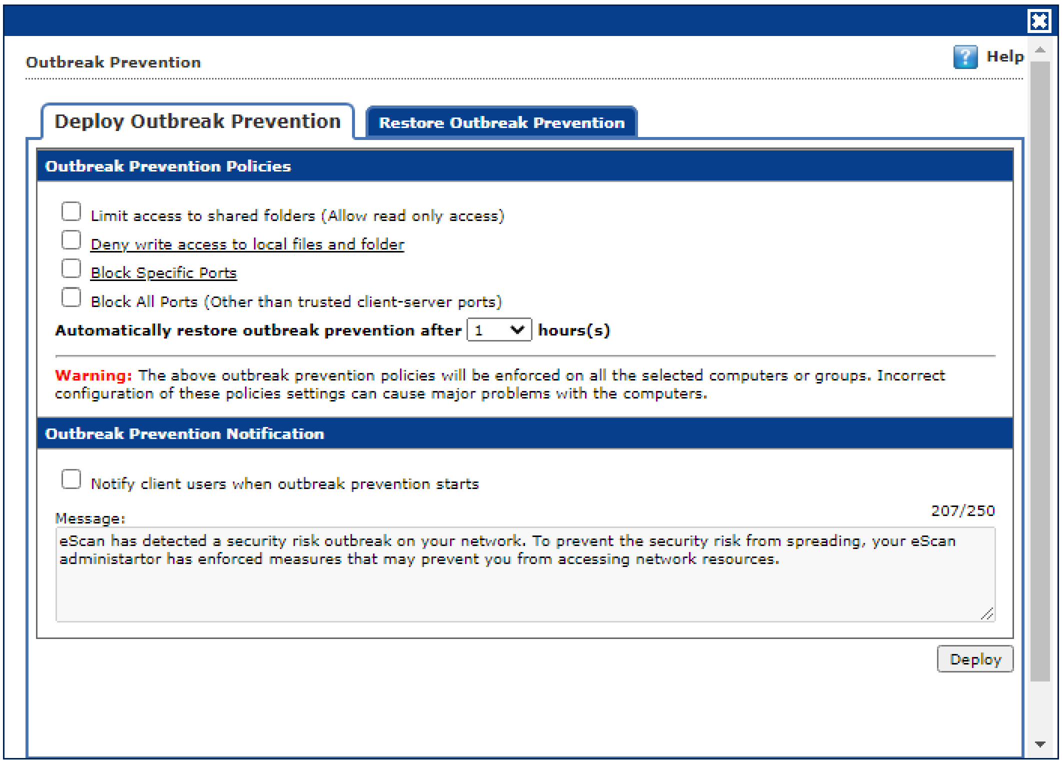
Outbreak Prevention

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

Deploying Outbreak Prevention

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

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



Outbreak Prevention

Outbreak Prevention Policies

□ Limit access to shared folders (Allow read only access)

□ Deny write access to local files and folder

□ Block Specific Ports

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

Automatically restore outbreak prevention after 1 **hours(s)**

Warning: The above outbreak prevention policies will be enforced on all the selected computers or groups. Incorrect configuration of these policies settings can cause major problems with the computers.

Outbreak Prevention Notification

□ Notify client users when outbreak prevention starts

Message: 207/250

eScan has detected a security risk outbreak on your network. To prevent the security risk from spreading, your eScan administartor has enforced measures that may prevent you from accessing network resources.

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

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

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

Block All Ports (Other than trusted client-server ports)
Select this checkbox to block all ports other than trusted client server ports.

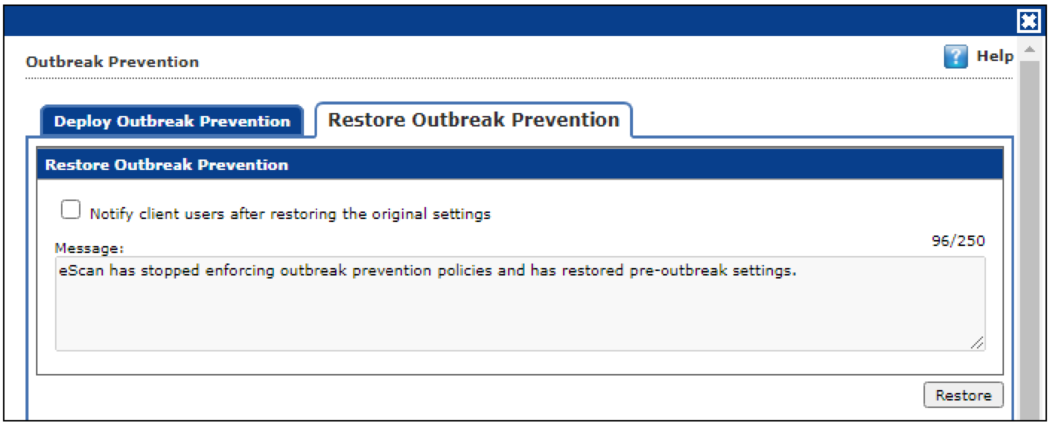
Automatically restore the outbreak prevention after hour(s)
This feature lets you restore outbreak prevention automatically after set duration (hours). Click the drop-down and select the preferred duration.

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

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

Restore Outbreak Prevention

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


Outbreak Prevention
Help
Deploy Outbreak Prevention
Restore Outbreak Prevention
Restore Outbreak Prevention
Restore

□ Notify client users after restoring the original settings

Message: 96/250

eScan has stopped enforcing outbreak prevention policies and has restored pre-outbreak settings.

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

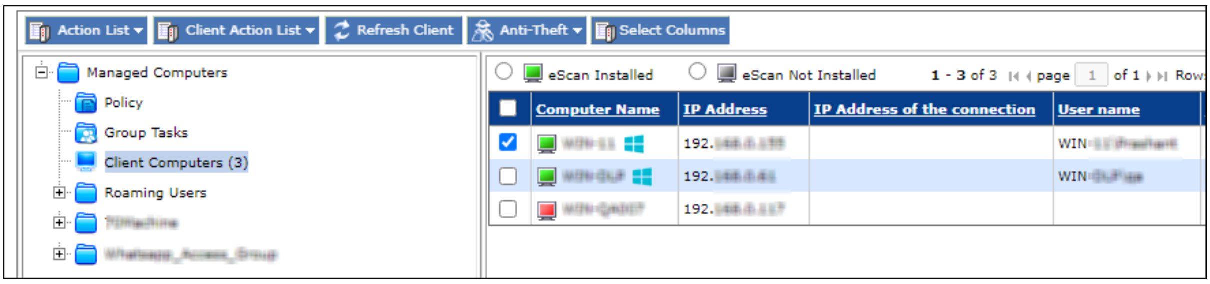
To notify clients about Outbreak Prevention restoration, select the checkbox **Notify client users after the original settings**.

Delete All Quarantine Files

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

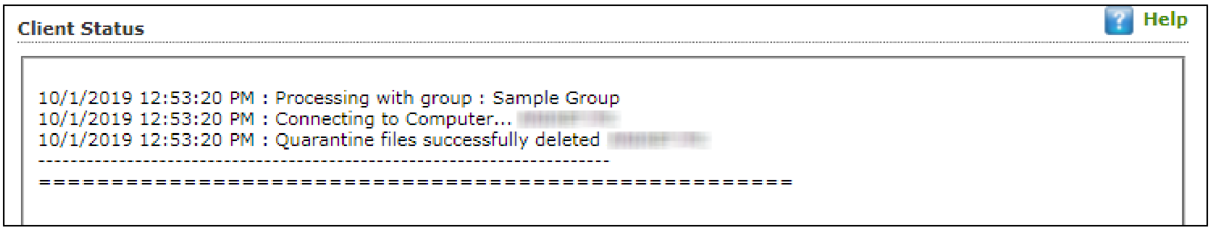
To delete all quarantine files on computers, follow the steps given below:

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



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

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



```
10/1/2019 12:53:20 PM : Processing with group : Sample Group
10/1/2019 12:53:20 PM : Connecting to Computer... [redacted]
10/1/2019 12:53:20 PM : Quarantine files successfully deleted [redacted]
--------------------------------------------------------------------------------
====================================================
```

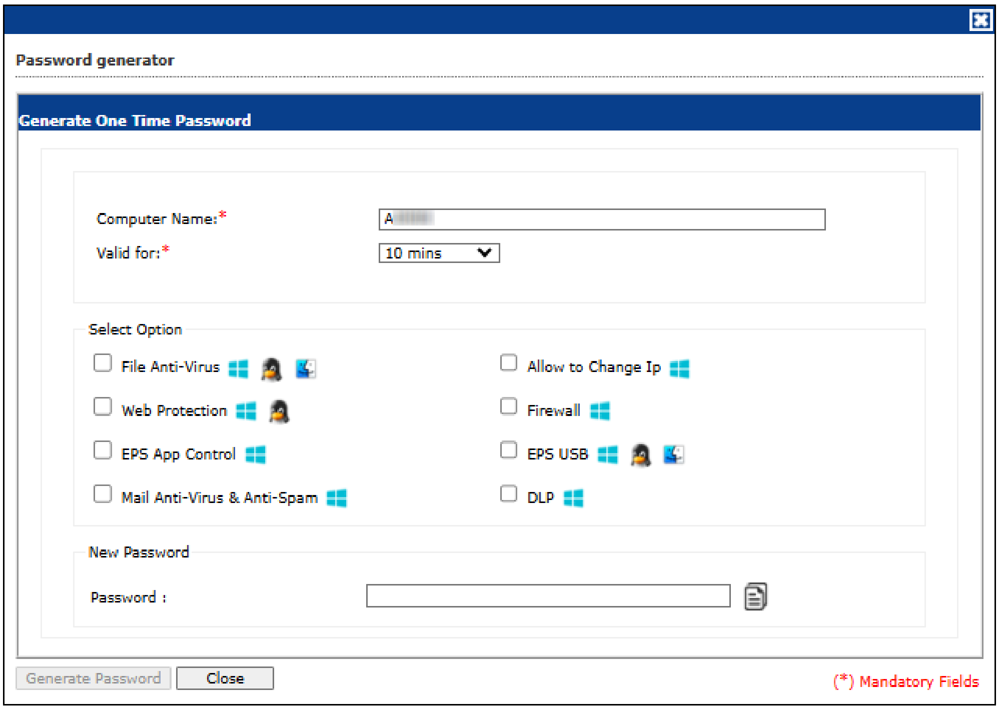
Create OTP

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

Generating an OTP

To generate an OTP, follow the steps given below:

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



Password generator

Generate One Time Password

Computer Name:* A[redacted]

Valid for:* 10 mins

Select Option

☐ File Anti-Virus　☐ Allow to Change Ip

☐ Web Protection　☐ Firewall

☐ EPS App Control　☐ EPS USB

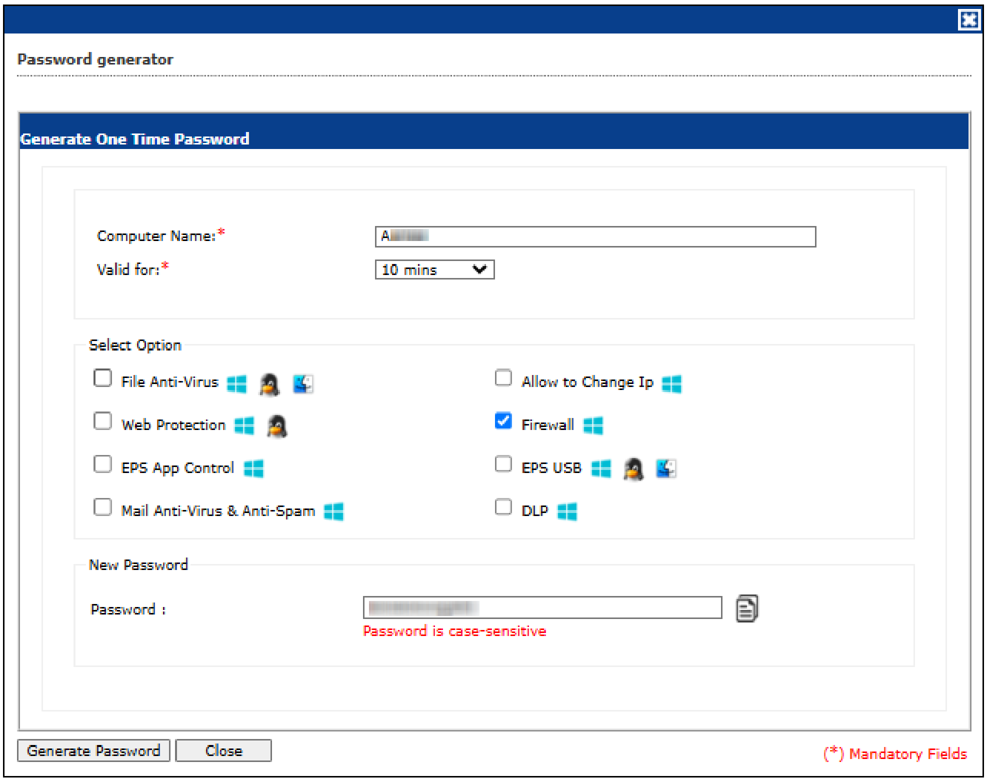
☐ Mail Anti-Virus & Anti-Spam　☐ DLP

New Password

Password :

(*) Mandatory Fields

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



Password generator

Generate One Time Password

Computer Name:* A[redacted]

Valid for:* 10 mins

Select Option

☐ File Anti-Virus　☐ Allow to Change Ip

☐ Web Protection　☑ Firewall

☐ EPS App Control　☐ EPS USB

☐ Mail Anti-Virus & Anti-Spam　☐ DLP

New Password

Password : [redacted]

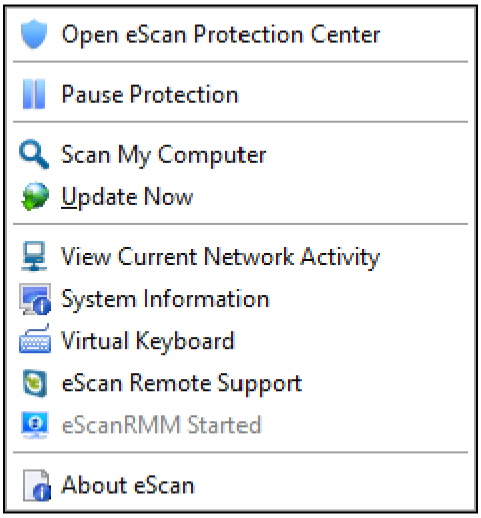
Password is case-sensitive

(*) Mandatory Fields

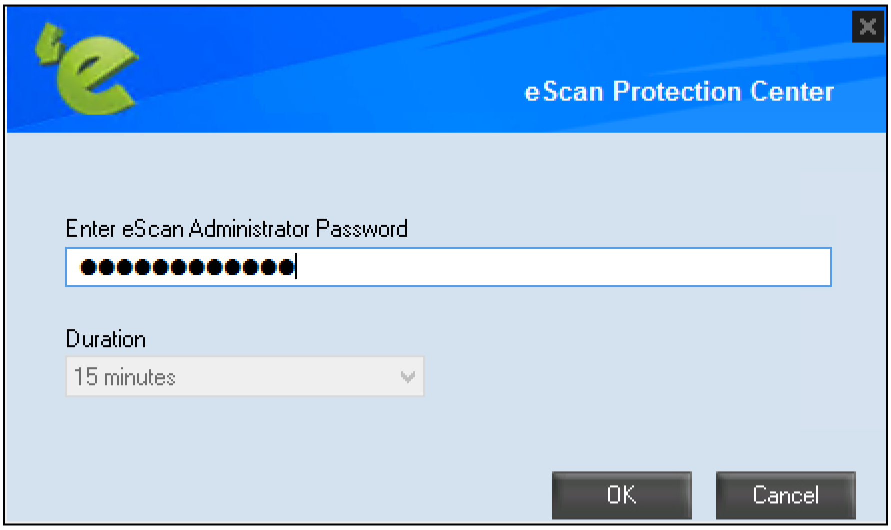
Entering an OTP

To enter an OTP, follow the steps given below:

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



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



Enter eScan Administrator Password: ●●●●●●●●●●●●●

Duration: 15 minutes

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

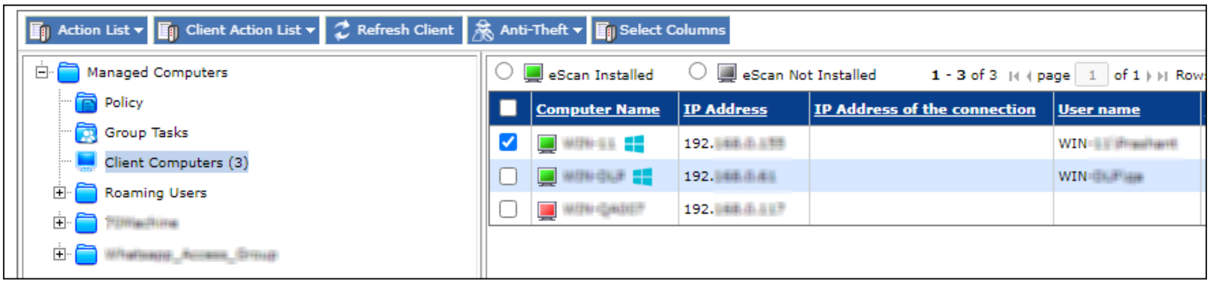
   The selected module will be disabled for set duration.

Pause Protection

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

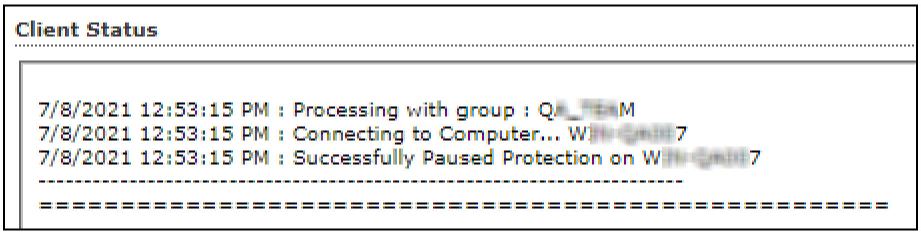
To pause the protection for computers, follow the steps given below:

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.



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

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



Client Status

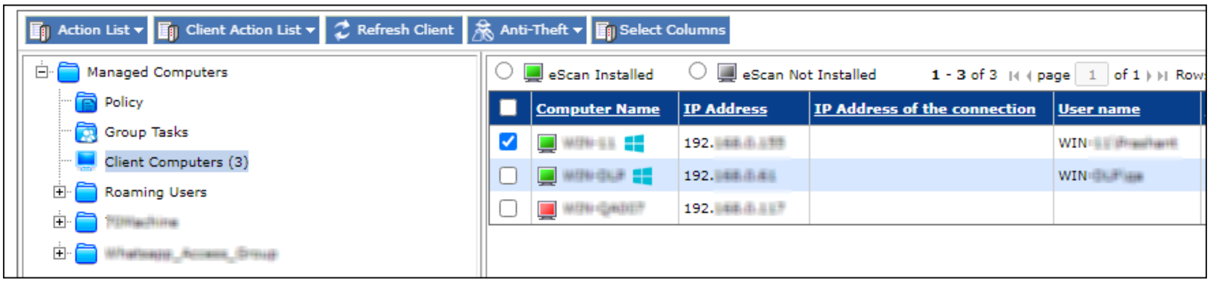
```
7/8/2021 12:53:15 PM : Processing with group : Q[redacted]M
7/8/2021 12:53:15 PM : Connecting to Computer... W[redacted]7
7/8/2021 12:53:15 PM : Successfully Paused Protection on W[redacted]7
-----------------------------------------------------------------------
=======================================================
```

Resume Protection

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

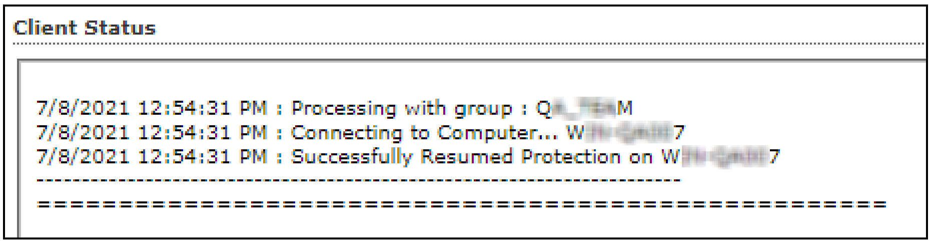
To resume protection for computers, follow the steps given below:

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.



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

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



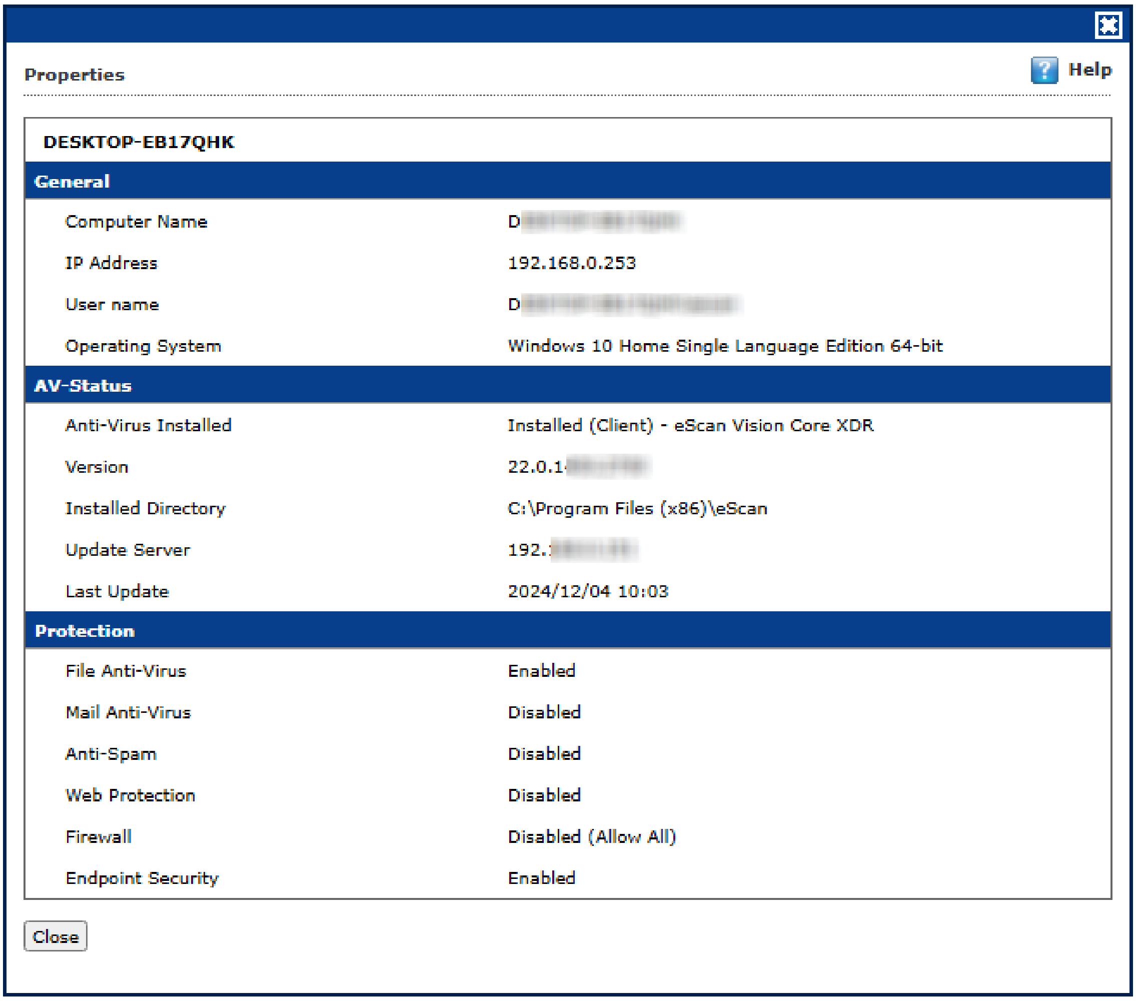
Client Status

```
7/8/2021 12:54:31 PM : Processing with group : Q[redacted]M
7/8/2021 12:54:31 PM : Connecting to Computer... W[redacted]7
7/8/2021 12:54:31 PM : Successfully Resumed Protection on W[redacted]7
-----------------------------------------------------------------------
=======================================================
```

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.



DESKTOP-EB17QHK

General	
Computer Name	D[redacted]
IP Address	192.168.0.253
User name	D[redacted]
Operating System	Windows 10 Home Single Language Edition 64-bit
AV-Status	
Anti-Virus Installed	Installed (Client) - eScan Vision Core XDR
Version	22.0.1[redacted]
Installed Directory	C:\Program Files (x86)\eScan
Update Server	192.[redacted]
Last Update	2024/12/04 10:03
Protection	
File Anti-Virus	Enabled
Mail Anti-Virus	Disabled
Anti-Spam	Disabled
Web Protection	Disabled
Firewall	Disabled (Allow All)
Endpoint Security	Enabled

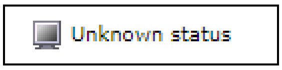
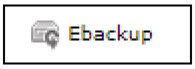
NOTE	If multiple computers are selected, the **Properties** option will be disabled.

Refresh Client

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

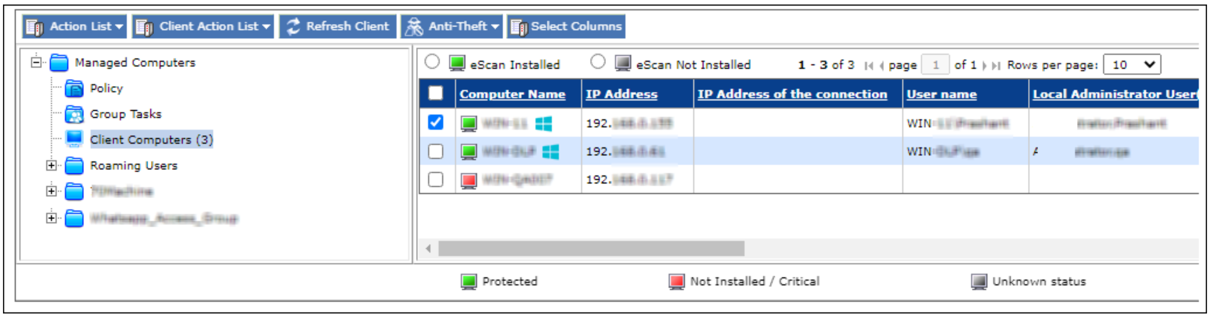
1. Under any group, click **Client Computers**. A list of computers appears on the right pane.
2. Select a computer.
3. Click **Refresh Client**. The Client will be refreshed.

Understanding the eScan Client Protection Status

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

Anti-Theft (requires additional license)

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

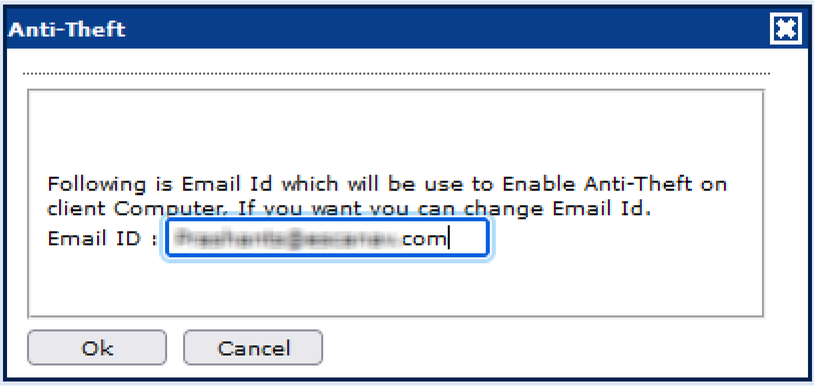


	Computer Name	IP Address	IP Address of the connection	User name	Local Administrator User
☑	[redacted]	192.[redacted]		WIN-[redacted]	[redacted]
□	[redacted]	192.[redacted]		WIN-[redacted]	[redacted]
□	[redacted]	192.[redacted]			

Anti-Theft Options

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

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

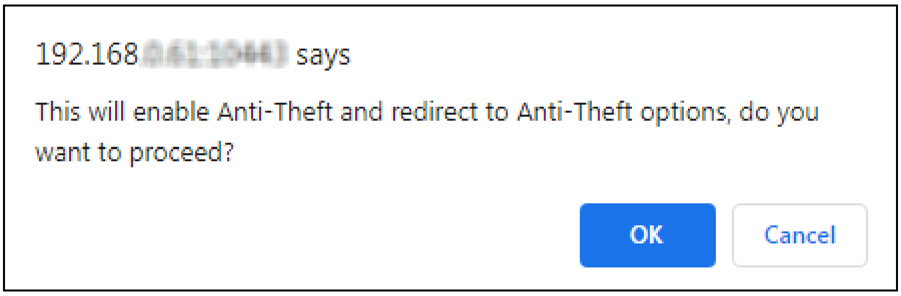


Anti-Theft

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

Email ID : [redacted]com

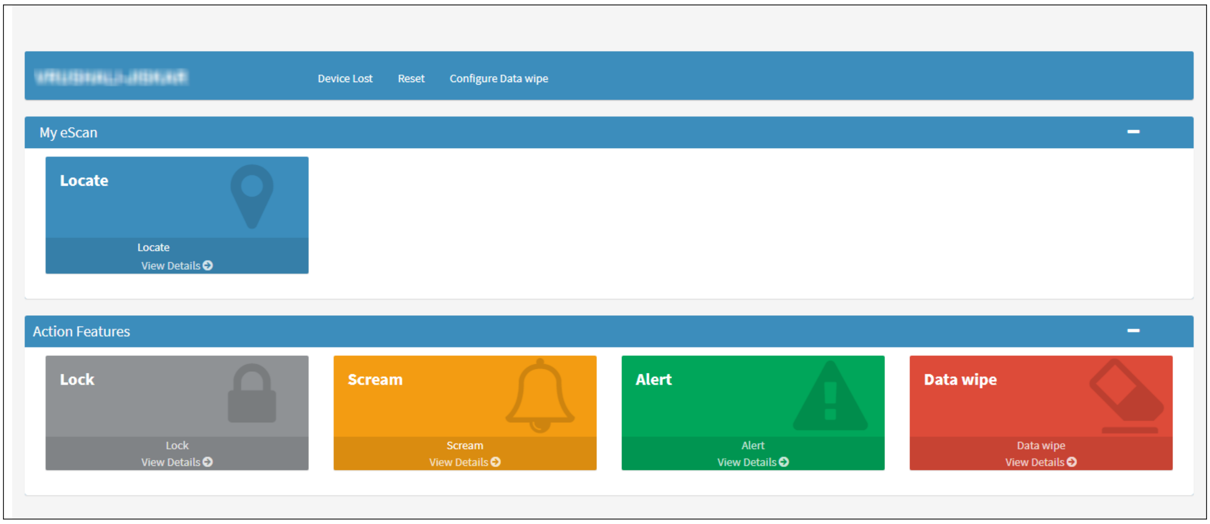
5. A confirmation prompt appears.



192.168[redacted] says

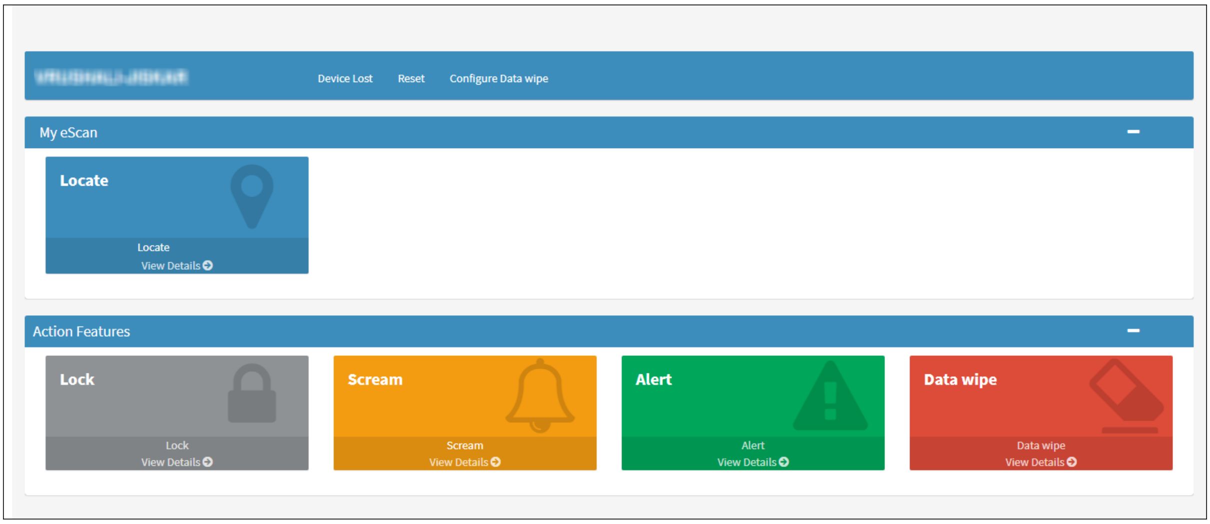
This will enable Anti-Theft and redirect to Anti-Theft options, do you want to proceed?

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



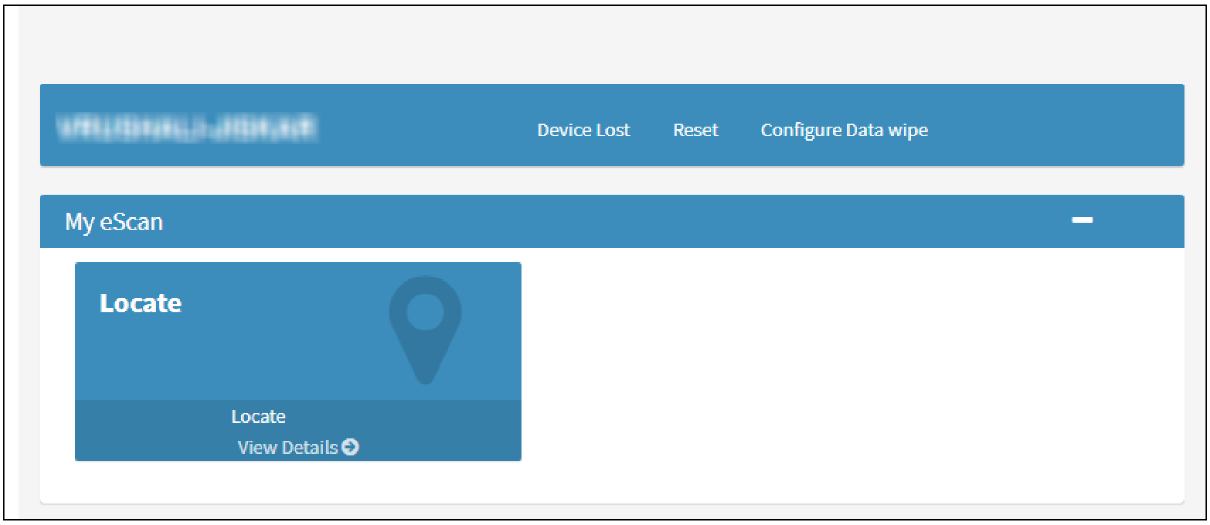
Anti-Theft Portal

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

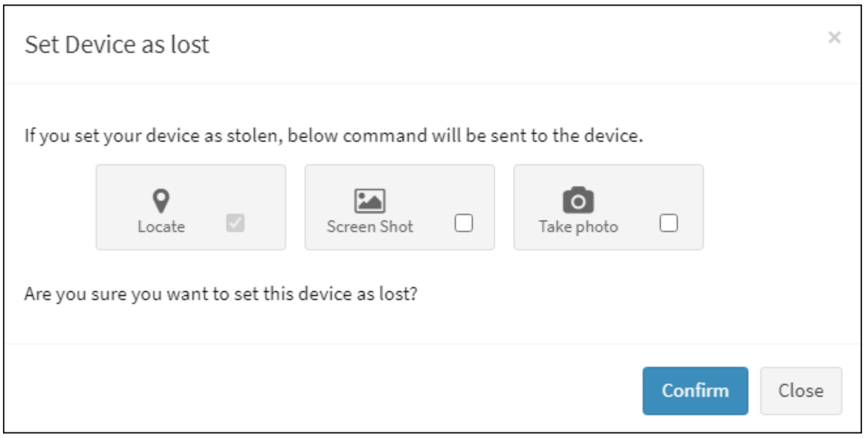


2. In case of loss or theft, click on the system name that has been lost or stolen, the status bar under it will display the system name again and when it was last seen.

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



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



Set Device as lost

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

Locate ☑ Screen Shot □ Take photo □

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

- **Locate**: This option will allow you to locate the system in case of loss/theft. Click on the **Locate** option on the anti-theft portal and the last known location of the system will be displayed on the map. Procedure to Locate the system:

  A. Click **Locate**, the status will change to **Request Pending**; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to locate the system is in progress.

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

- **Screenshot**: This option will take a screen shot of the system whenever it is synced to the server.

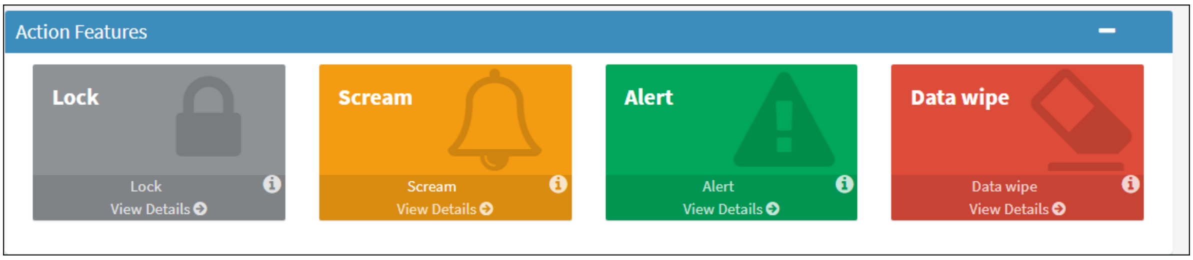
  A. Click **Screenshot**, the status will change to **Request Pending**; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to take a screenshot is in progress.

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

- **Take Photo**: This option will allow you to take a snapshot of the current user of the system from the webcam on clicking the camera option on the anti-theft portal.

  A. Click **Camera**, the status will change to Request Pending; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to take a snapshot is in progress.

  B. **View Details** displays the last two snapshots taken from your system. Click **Reset** to reset the **Action Features** on the system; these actions can be performed on the system when it has been lost or stolen.



There are following action features:

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

Disable Anti-Theft

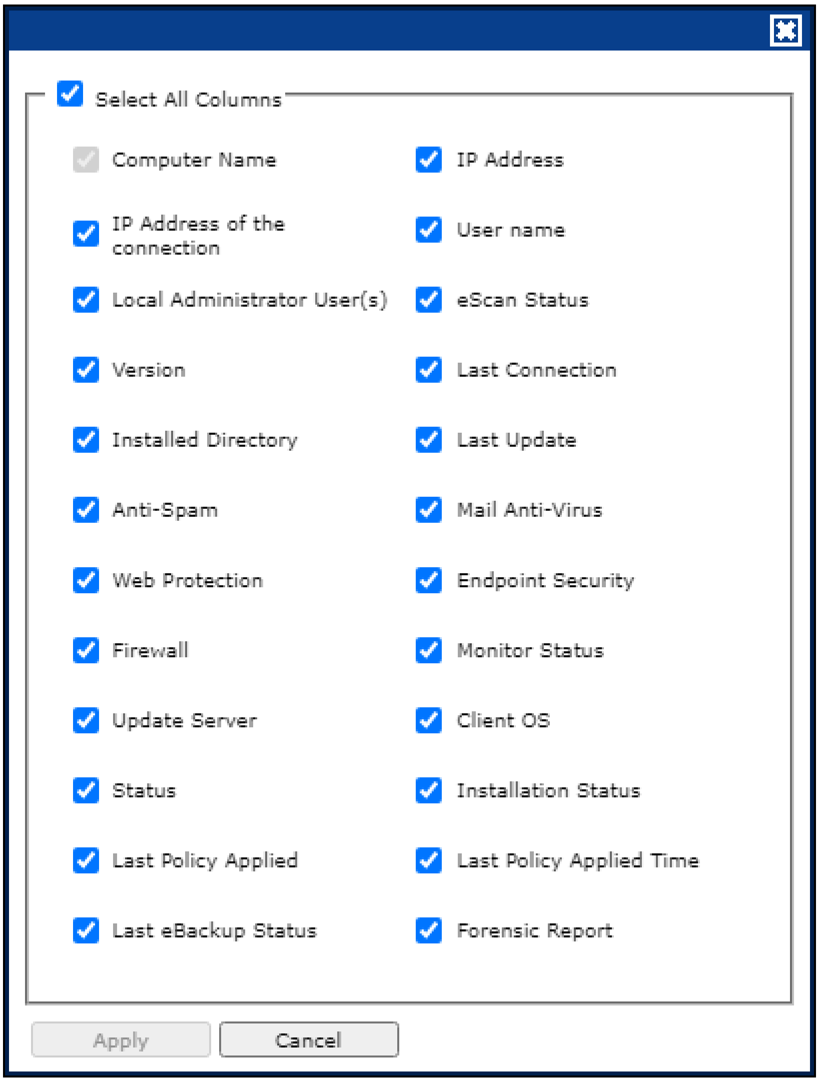
To Disable Anti-Theft, follow the steps given below:

1. Go to Managed Computers.

2. Select the desired computers in Anti-theft Portal.
3. Click **Anti-Theft** > **Disable Anti-Theft**.

Select Columns

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



☑ Select All Columns

☑ Computer Name
☑ IP Address of the connection
☑ Local Administrator User(s)
☑ Version
☑ Installed Directory
☑ Anti-Spam
☑ Web Protection
☑ Firewall
☑ Update Server
☑ Status
☑ Last Policy Applied
☑ Last eBackup Status

☑ IP Address
☑ User name
☑ eScan Status
☑ Last Connection
☑ Last Update
☑ Mail Anti-Virus
☑ Endpoint Security
☑ Monitor Status
☑ Client OS
☑ Installation Status
☑ Last Policy Applied Time
☑ Forensic Report

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

Policy Template

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

Managing Policies

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

Defining Policies Windows computers

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

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

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

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

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

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

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

Advance Security
eScan Advance Security enables you to configure the events for which the alert has be generated. This will help you to create prioritized rules to control which events and processes are monitored, recorded, and alerted. To learn more, **click here**.

Administrator Password

Administrator Password lets you create and change password for administrative login of eScan protection center and Two-Factor Authentication. To learn more, **click here**.

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

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

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

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

Tools
Tools policy let you configure eBackup and RMM Settings. To learn more, **click here**.

Defining Policies Mac or Linux computers

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

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

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

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

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

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

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

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

Web Protection

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

Network Security

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

Tools

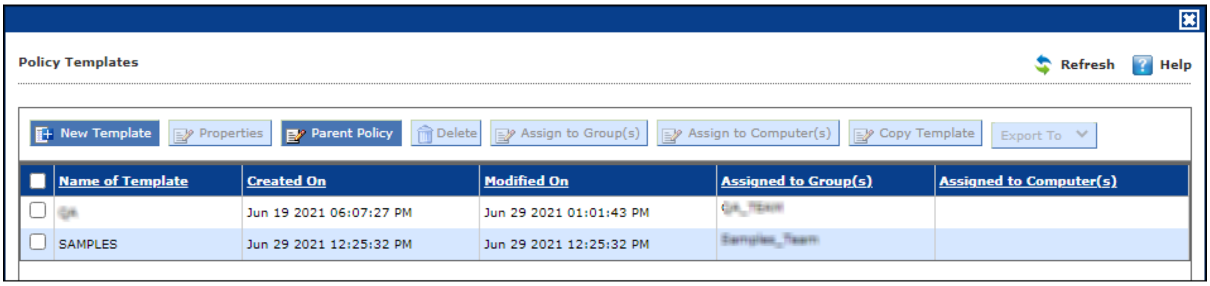
Tools policy let you configure RMM Settings. To learn more, **click here**.

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

Creating Policy Template for a group/specific computer

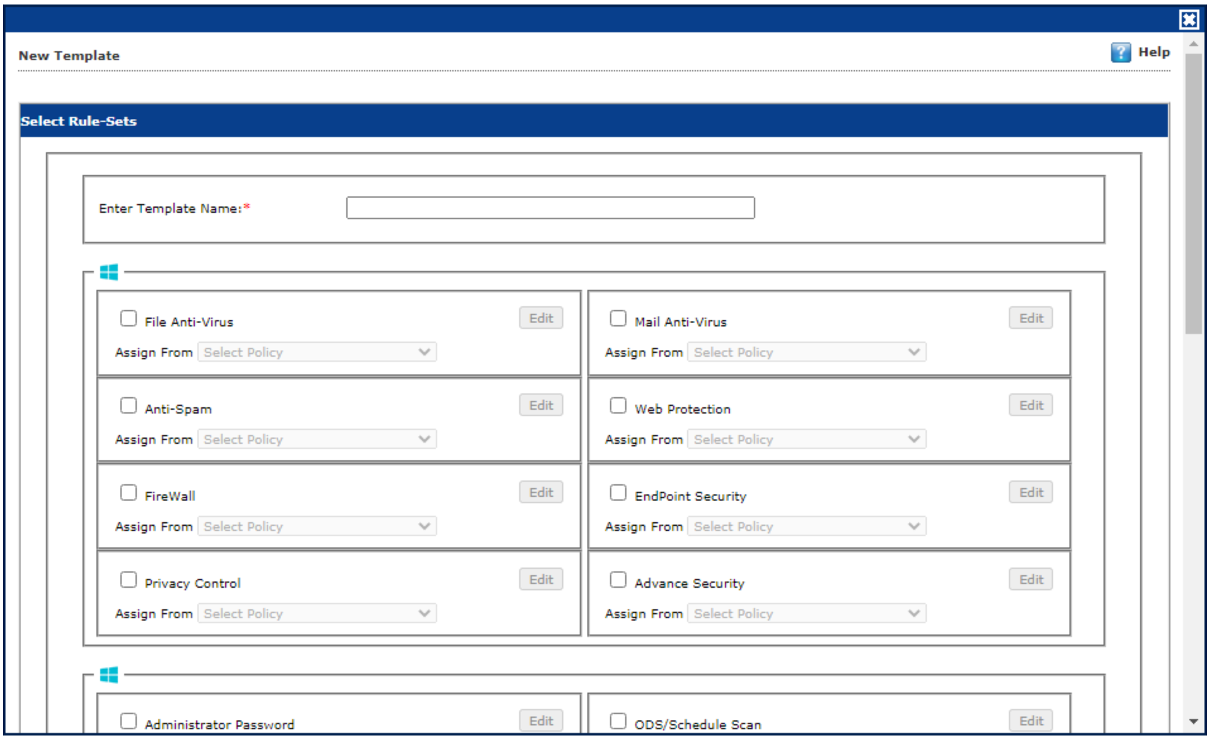
To create a Policy template for a group, follow the steps given below:

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



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

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



Enter Template Name:*

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

☐ Mail Anti-Virus — Assign From: Select Policy — Edit

☐ Anti-Spam — Assign From: Select Policy — Edit

☐ Web Protection — Assign From: Select Policy — Edit

☐ FireWall — Assign From: Select Policy — Edit

☐ EndPoint Security — Assign From: Select Policy — Edit

☐ Privacy Control — Assign From: Select Policy — Edit

☐ Advance Security — Assign From: Select Policy — Edit

☐ Administrator Password — Edit

☐ ODS/Schedule Scan — Edit

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

Configuring eScan Policies for Windows Computers

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

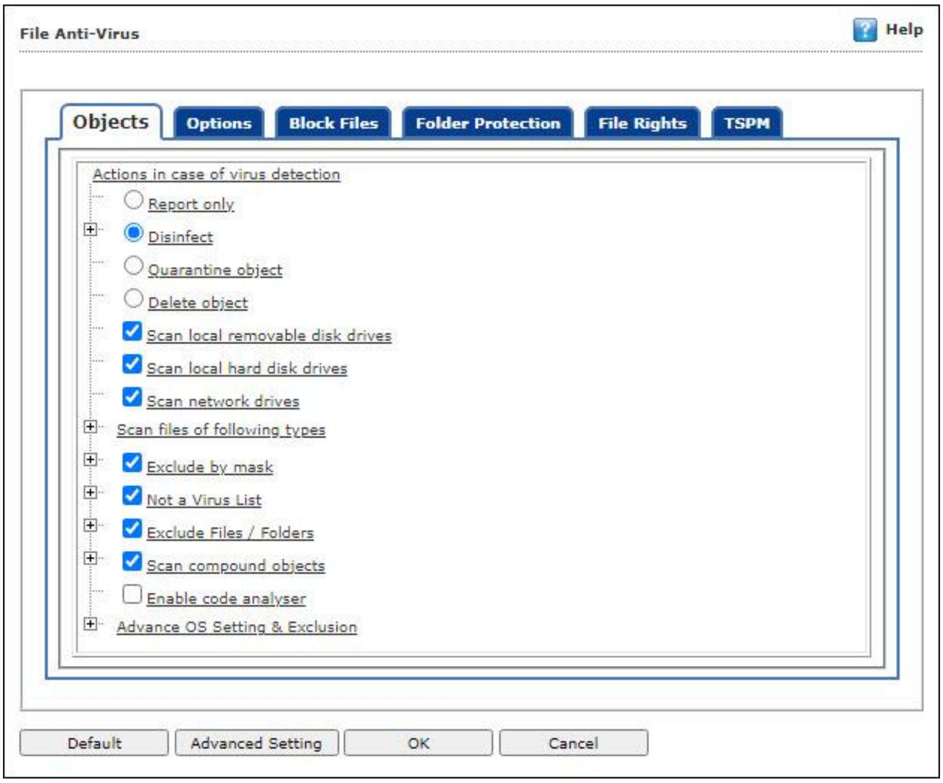
File Anti-Virus

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

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

Objects

The Objects tab lets you configure following options:



File Anti-Virus

Objects | Options | Block Files | Folder Protection | File Rights | TSPM

Actions in case of virus detection

- ○ Report only
- ● Disinfect
- ○ Quarantine object
- ○ Delete object
- ☑ Scan local removable disk drives
- ☑ Scan local hard disk drives
- ☑ Scan network drives
- Scan files of following types
- ☑ Exclude by mask
- ☑ Not a Virus List
- ☑ Exclude Files / Folders
- ☑ Scan compound objects
- □ Enable code analyser
- Advance OS Setting & Exclusion

Actions in case of virus detection

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

Report only

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

Disinfect [Default]

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

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

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

Quarantine object
If disinfection is impossible eScan will quarantine the object. By default, the quarantined files are saved in **C:\Program Files\eScan\Infected folder.** You can select the **Make backup file before disinfection** option if you would like to make a backup of the files before they are disinfected.

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

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

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

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

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

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

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

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

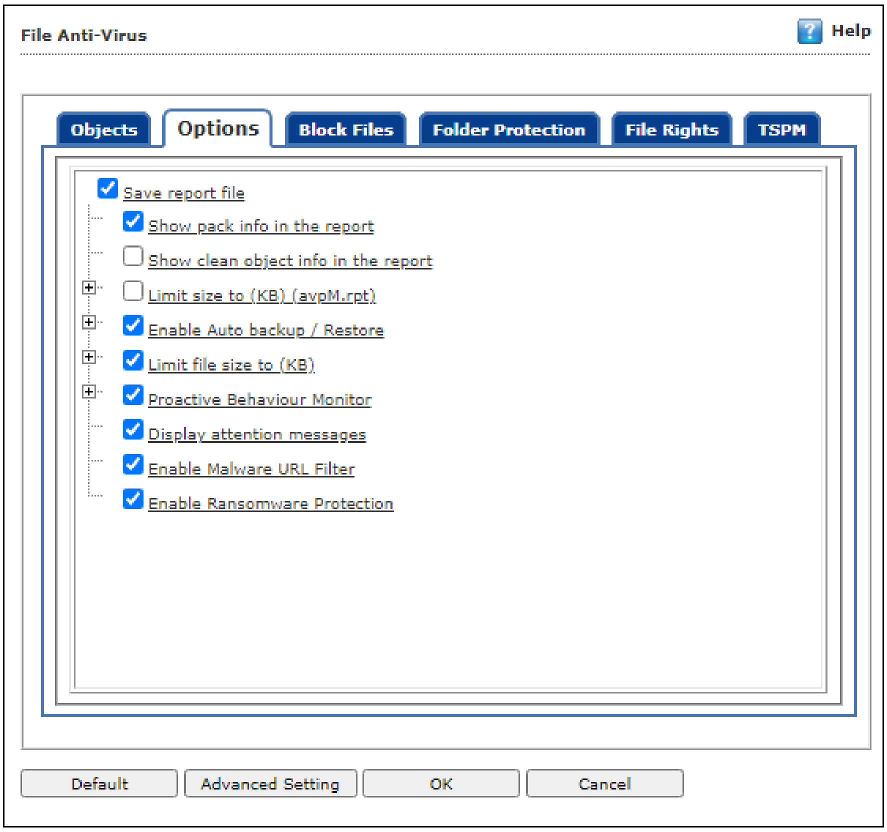
Scan compound objects [Default]
Select this checkbox if you want eScan to scan archives and packed files during scan operations. By default, **Packed** is selected. All the procedures will be followed.

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

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

Options

The Options tab lets you configure following options:



File Anti-Virus

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

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

Show pack info in the report [Default]
Select this checkbox if you want File Anti-Virus to add information regarding scanned compressed files, such as .zip and .rar files to the Monvir.log file.

Show clean object info in the report
Select this checkbox if you want File Anti-Virus to add information regarding uninfected files found during a scan operation to the Monvir.log file. You can select this option to find out which files are not infected.

Limit size to (Kb) (avpM.rpt)
Select this checkbox if you want File Anti-Virus to limit the size of the Monvir.log file and avpM.rpt file. To modify the limit, enter the log file size in field.

Enable Auto backup/Restore [Default]
Selecting this checkbox lets you back up the critical files of the Windows® operating system and then automatically restores the clean files when eScan finds an infection in any of the system files that cannot be disinfected. You can configure the following settings:

- **Do not backup files above size (KB) [Default]:** This option lets you prevent File Anti-Virus from creating backup of files that are larger than the file size that you have specified.
- **Minimum disk space (MB**) **[Default]:** The Auto-backup feature will first check for the minimum available space limit defined for a hard disk drive. If the minimum defined space is available then only the Auto-backup feature will work, if not it will stop without notifying. You can allot the Minimum disk space to be checked from this option. By default, the minimum disk space is 500 MB.

Limit file size to (KB) [Default]
This checkbox lets you set a limit size for the objects or files to be scanned. The default value is set to **20480 Kb**.

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

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

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

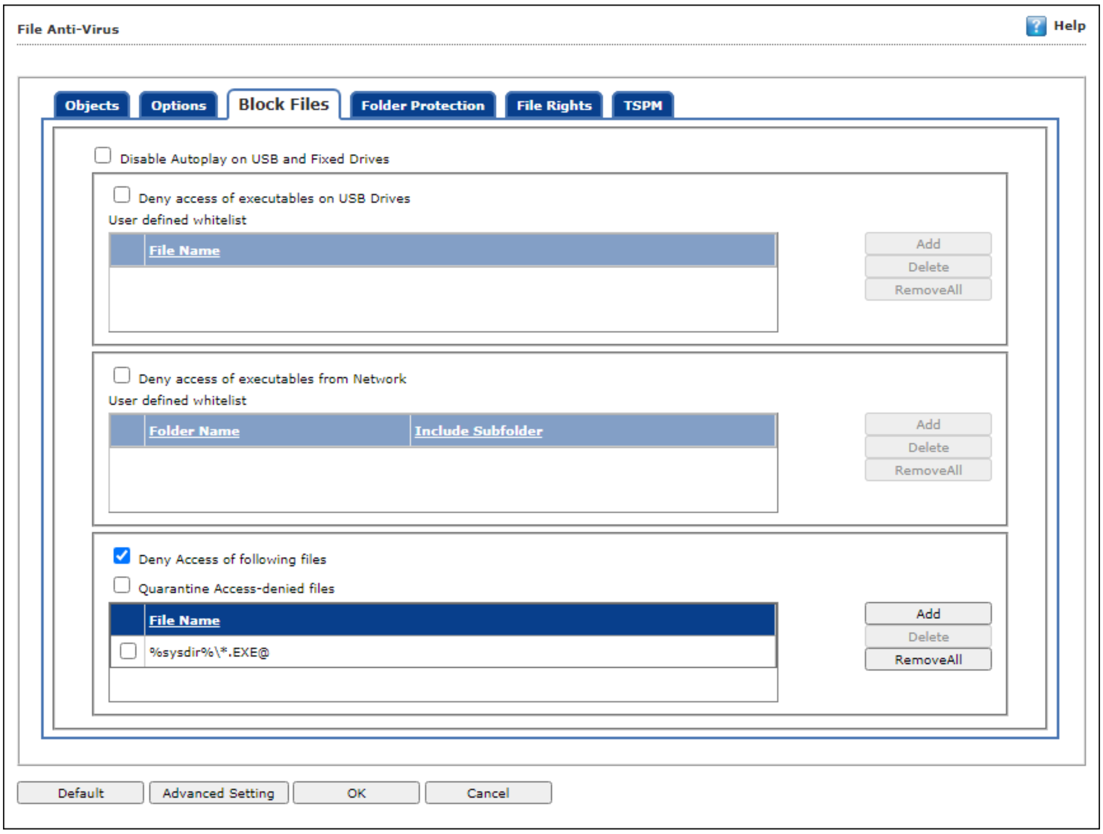
Display attention messages [Default]
When this option is selected, eScan displays an alert consisting the path and name of the infected object and the action taken by the File Anti-Virus module.

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

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

Block Files

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



File Anti-Virus

□ Disable Autoplay on USB and Fixed Drives

□ Deny access of executables on USB Drives

User defined whitelist

File Name

□ Deny access of executables from Network

User defined whitelist

Folder Name	Include Subfolder

☑ Deny Access of following files

□ Quarantine Access-denied files

	File Name
□	%sysdir%*.EXE@

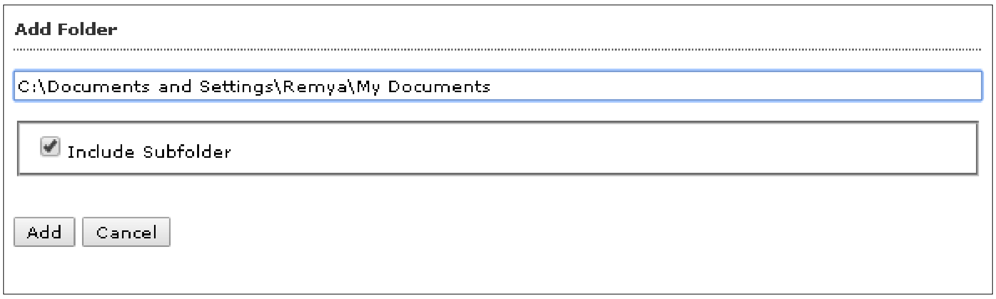
You can configure the following settings:

Disable AutoPlay on USB and Fixed Drives [Default]
Selecting this option will disable AutoPlay when a USB/Fixed Drive is connected.

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

Deny access of executable from Network
Select this checkbox if you want eScan to prevent executables on the client computer from being accessed from the network.

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



Add Folder

C:\Documents and Settings\Remya\My Documents

☑ Include Subfolder

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

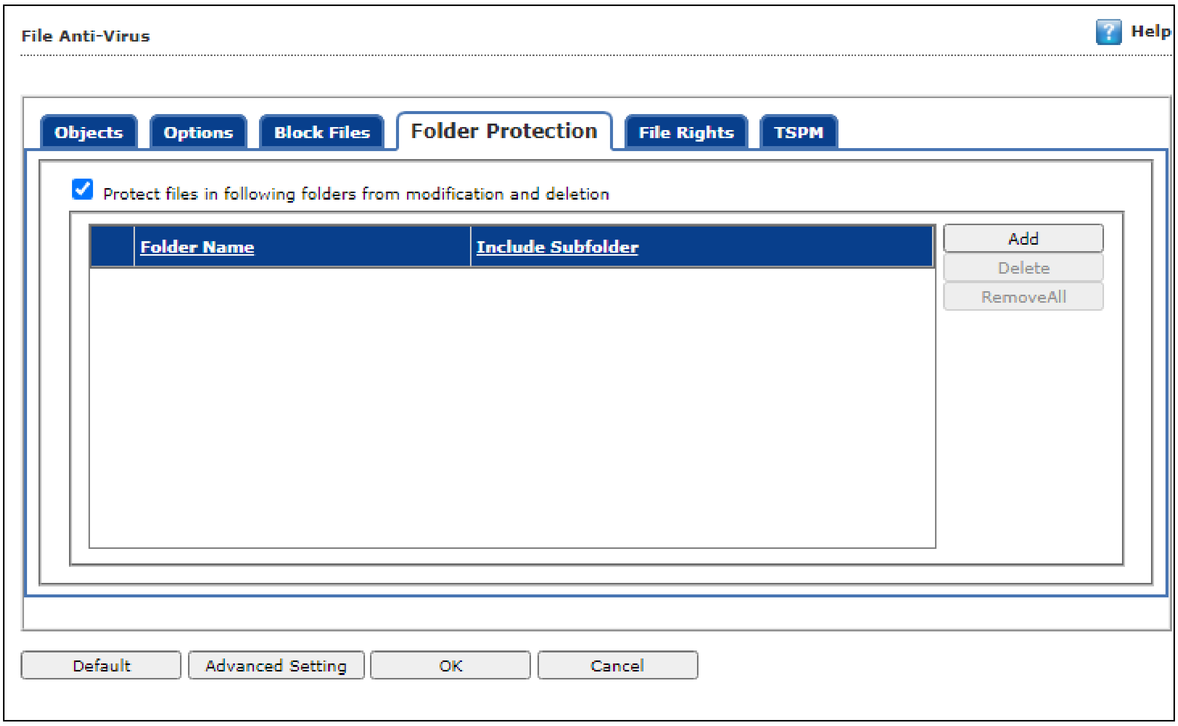
Deny Access of following files [Default]
Select this checkbox if you want eScan to prevent the files in the list from running on the computers.

Quarantine Access-denied files
Select this checkbox if you want eScan to quarantine files to which access is denied.

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

Folder Protection

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



☑ Protect files in following folders from modification and deletion

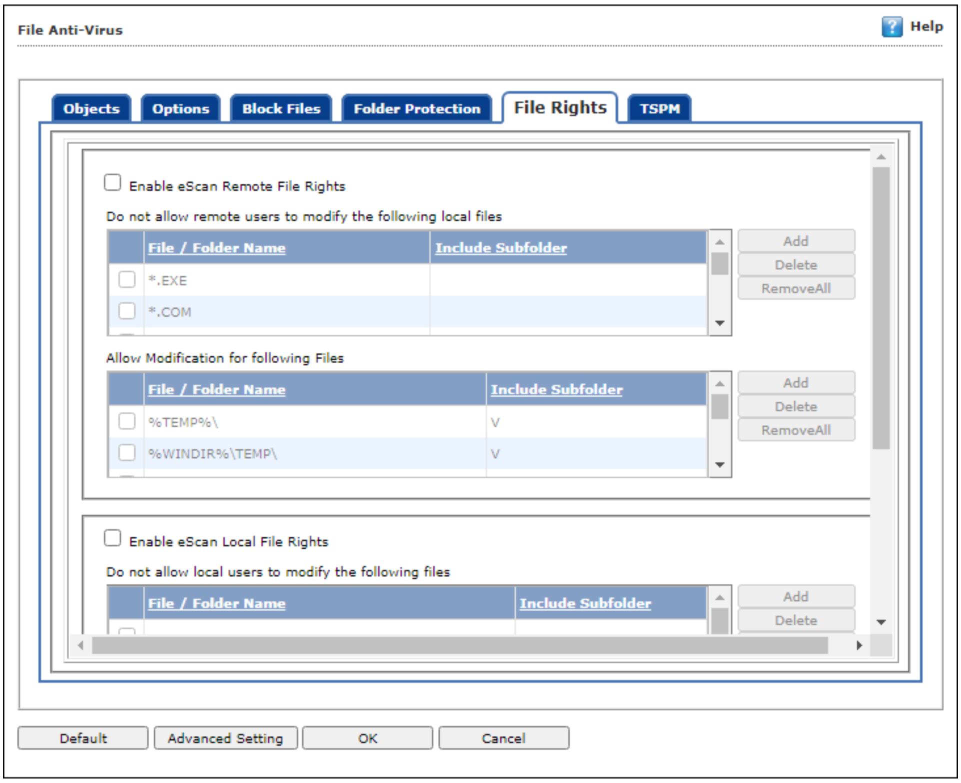
	Folder Name	Include Subfolder

Protect files in following folders from modification and deletion [Default]
This option is selected by default.
Selecting this checkbox enables File Anti-Virus module to protect files in specific folders from being modified or deleted on the client systems. Click **Add**. Enter the complete path of the folder to be

protected on the client systems. You can either protect the parent folder only or select the **Include subfolder** option to protect the subfolders as well.

File Rights

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



□ Enable eScan Remote File Rights

Do not allow remote users to modify the following local files

	File / Folder Name	Include Subfolder
□	*.EXE	
□	*.COM	

Allow Modification for following Files

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

□ Enable eScan Local File Rights

Do not allow local users to modify the following files

	File / Folder Name	Include Subfolder

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

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

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

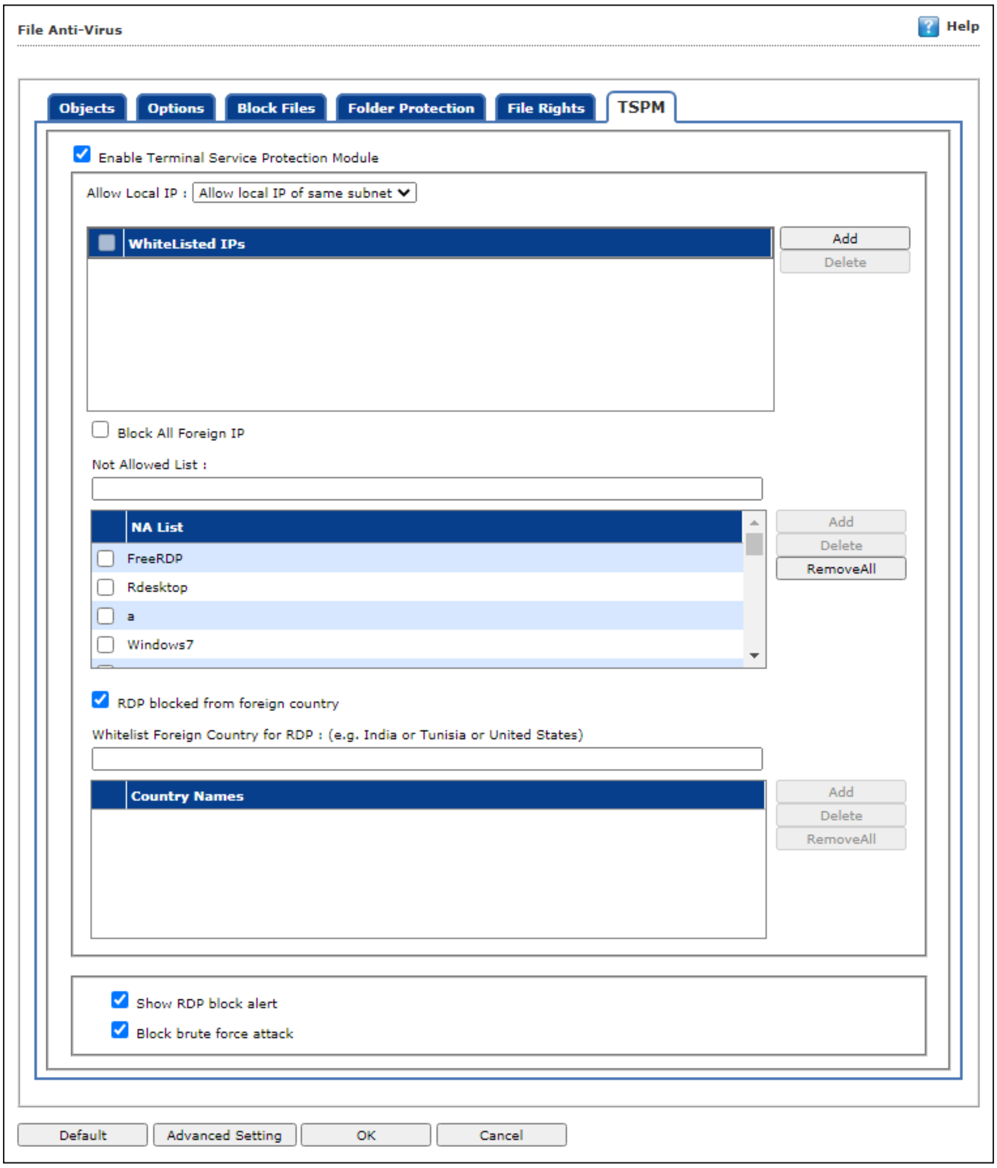
Enable eScan local file rights
Select this checkbox to allow/restrict the local users to make any modifications to the files/folders.

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

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

TSPM

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



☑ Enable Terminal Service Protection Module

Allow Local IP : Allow local IP of same subnet

□	WhiteListed IPs

□ Block All Foreign IP

Not Allowed List :

	NA List
□	FreeRDP
□	Rdesktop
□	a
□	Windows7

☑ RDP blocked from foreign country

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

	Country Names

☑ Show RDP block alert

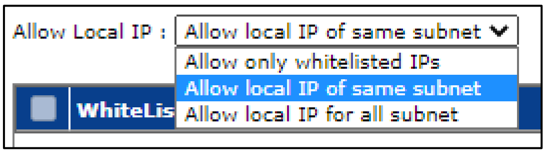
☑ Block brute force attack

Enable Terminal Service Protection Module

Select this checkbox to activate TSPM module.

Allow Local IP

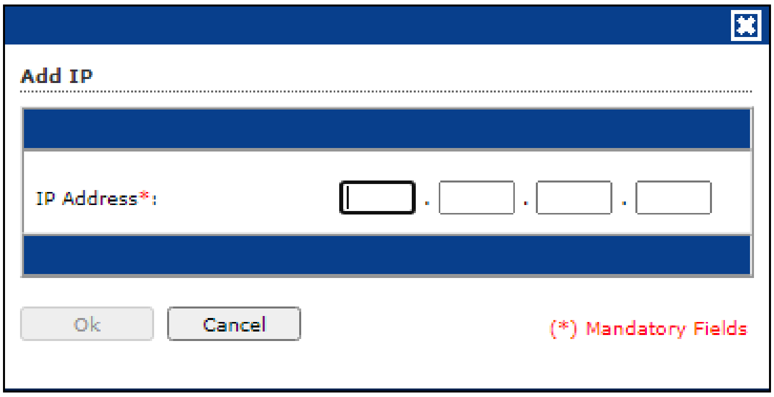
This dropdown menu has following options:



Allow Local IP : Allow local IP of same subnet

Allow only whitelisted IPs
Allow local IP of same subnet
Allow local IP for all subnet
WhiteLis

- **Allow only whitelisted IPs**: Select this option to allow only whitelisted IPs to connect to the endpoints.
  To add a list of IP addresses to be excluded from being blocked by TSPM, click **Add**. Add IP window appears.



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

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

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

To add custom-defined username, Enter the username and then click **Add**.
To delete the username from pre-defined list, select the name and click **Delete**.
To remove all the usernames from list, click **Remove All**.

RDP blocked from foreign country [Default]
This checkbox blocks all the RDP connection attempts from the foreign country.

Whitelist Foreign Country for RDP: (e.g. India or Tunisia or United States)
This option allows to whitelist the country names, so that RDP connections from those countries can be allowed.

Show RDP block alert [Default]

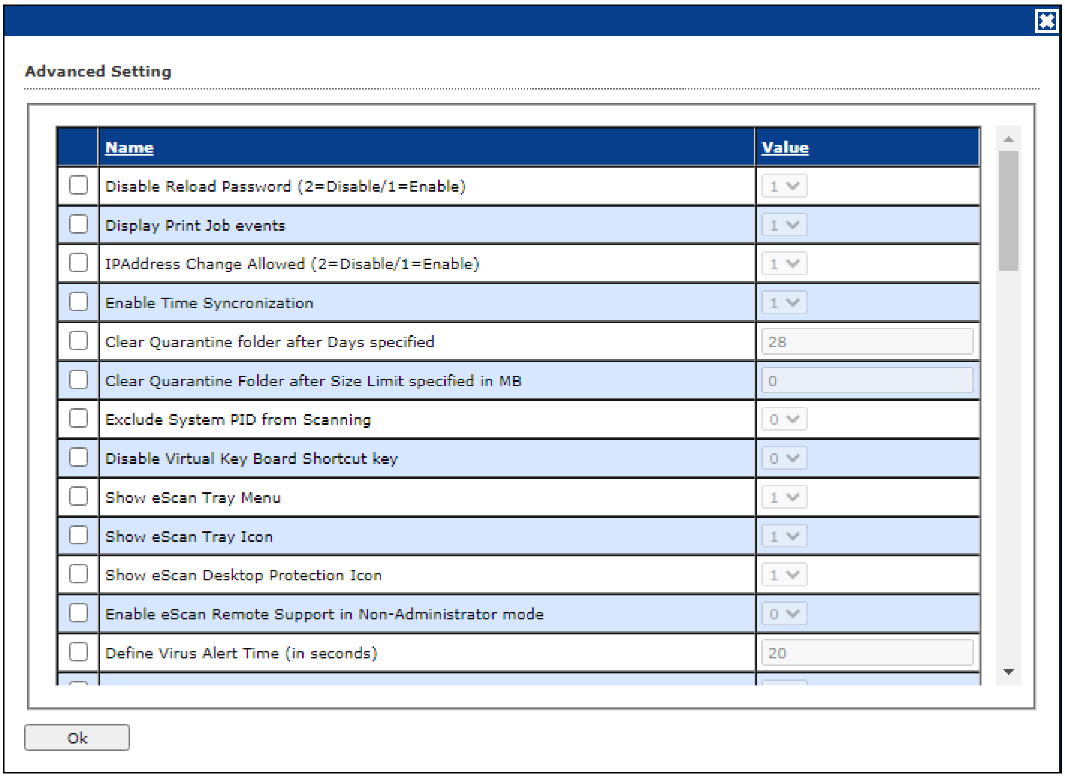
This checkbox allows eScan to alert the user in case of any RDP connection is blocked.

Block brute force attack [Default]
This checkbox allows to block the connection in case of any brute force attack.

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

Advanced Setting

Clicking **Advanced Setting** displays additional advanced settings.



Advanced Setting

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

Disable Reload Password (2=Disable/1=Enable)
This option lets you enable or disable password for reloading eScan. After enabling, the user will be asked to enter reload password if user attempts to reload eScan. This is the administrator password for eScan Protection Center.

Display Print Job events (1 = Enable/0 = Disable)
This option lets you capture events for the Print Jobs from Managed Computers.

IP Address Change Allowed (2 = Disable/1 = Enable)
This option lets you enable/disable IP Address Change by the user on their computer.

Enable Time Synchronization (1 = Enable/0 = Disable)
This option lets you enable/disable time synchronization with internet. Active internet connection is mandatory for this feature.

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

Clear Quarantine Folder after Size Limit specified in MB
This option lets you specify size limit for the Quarantine folder. If the defined size limit exceeds, the Quarantine folder will be cleared on Managed Computers.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Enable backup of DLL files (1 = Enable/0 = Disable)
This option lets you Enable/Disable backup of DLL files on Managed Computers.
Integrate Server Service dependency with Real-time monitor (1 = Enable/0 = Disable)
This option lets you Integrate Server Service dependency with real-time monitor.

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

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

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

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

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

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

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

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

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

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

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

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

Enable Share Access Control (1 = Enable/0 = Disable)
It enables Share Access Control. Network Shares ReadOnly Access and Network Shares NoAccess options will work only if this option is selected.

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

List of comma-separated servers and/or shares and/or wildcards which needs to be given NO ACCESS e.g. \\192.168.X.X\temp or \\192.168.X.X\temp\*.doc or *.doc (Work only when "Enable Share Access Control" is set)
Selecting this option lets you add the List of comma-separated servers and/or shares and/or wildcards that should not be accessible.

List of comma-separated servers and/or shares and/or wildcards which needs to be given READ ONLY ACCESS e.g. \\192.168.X.X\temp or \\192.168.X.X\temp\*.doc or *.doc (Work only when "Enable Share Access Control" is set)
Selecting this option lets you add the List of comma-separated servers and/or shares and/or wildcards that should be given only view access and not be editable.

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

Whitelist IP Address (Depends on IP Address Change Allowed) (E.G 192.168.X.* You can put comma-separated list)
Selecting this option lets you add the list of IP addresses separated by commas to whitelist them.

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

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

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

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

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

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

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

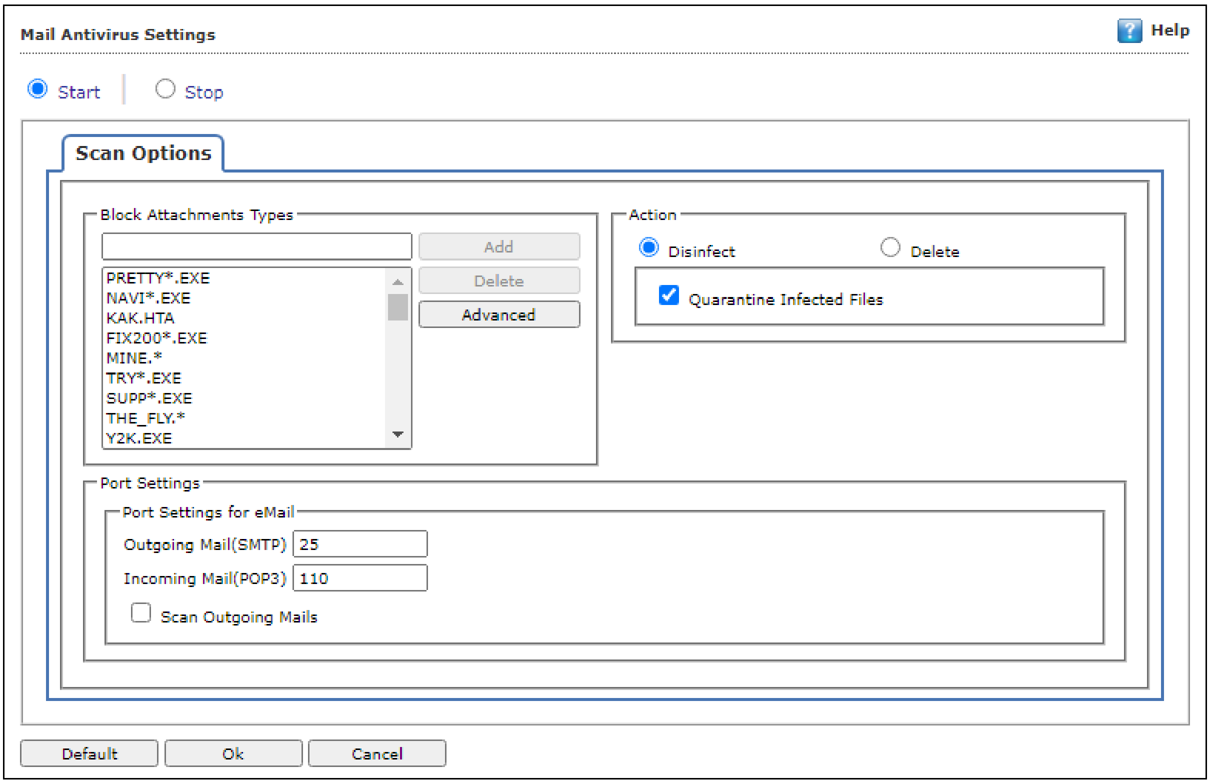
Block Renaming of Hostname (1 = Enable/0 = Disable)
Selecting this option lets you enable/disable block Hostname renaming.

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

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

Mail Antivirus

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



Mail Antivirus Settings

● Start ○ Stop

Scan Options

Block Attachments Types
- PRETTY*.EXE
- NAVI*.EXE
- KAK.HTA
- FIX200*.EXE
- MINE.*
- TRY*.EXE
- SUPP*.EXE
- THE_FLY.*
- Y2K.EXE

Action
● Disinfect ○ Delete
☑ Quarantine Infected Files

Port Settings
Port Settings for eMail
Outgoing Mail(SMTP): 25
Incoming Mail(POP3): 110
□ Scan Outgoing Mails

Scan Options

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

Block Attachments Types
This section provides you with a predefined list of file types that are often used by virus writers to embed viruses. Any email attachment having an extension included in this list will be blocked or deleted by eScan at the gateway level. You can add file extensions to this list as per your requirements.

As a best practice, you should avoid deleting the file extensions that are present in the **Block Attachments Types** list by default. You can also configure advanced settings required to scan emails for malicious code.

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

Disinfect [Default]
Select this option if you want Mail Anti-Virus to disinfect infected emails or attachments.
Delete
Select this option if you want Mail Anti-Virus to delete infected emails or attachments.

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

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

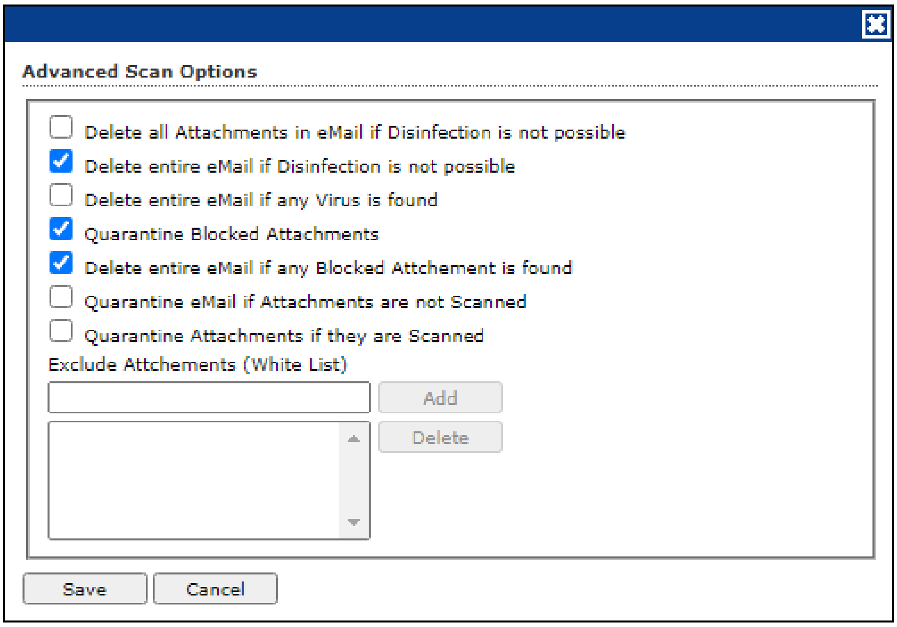
Outgoing Mail (SMTP) [Default: 25]
You need to specify a port number for SMTP.

Incoming Mail (POP3) [Default: 110]
You need to specify a port number for POP3.

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

Advanced

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



Advanced Scan Options

☐ Delete all Attachments in eMail if Disinfection is not possible
☑ Delete entire eMail if Disinfection is not possible
☐ Delete entire eMail if any Virus is found
☑ Quarantine Blocked Attachments
☑ Delete entire eMail if any Blocked Attchement is found
☐ Quarantine eMail if Attachments are not Scanned
☐ Quarantine Attachments if they are Scanned

Exclude Attchements (White List)

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

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

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

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

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

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

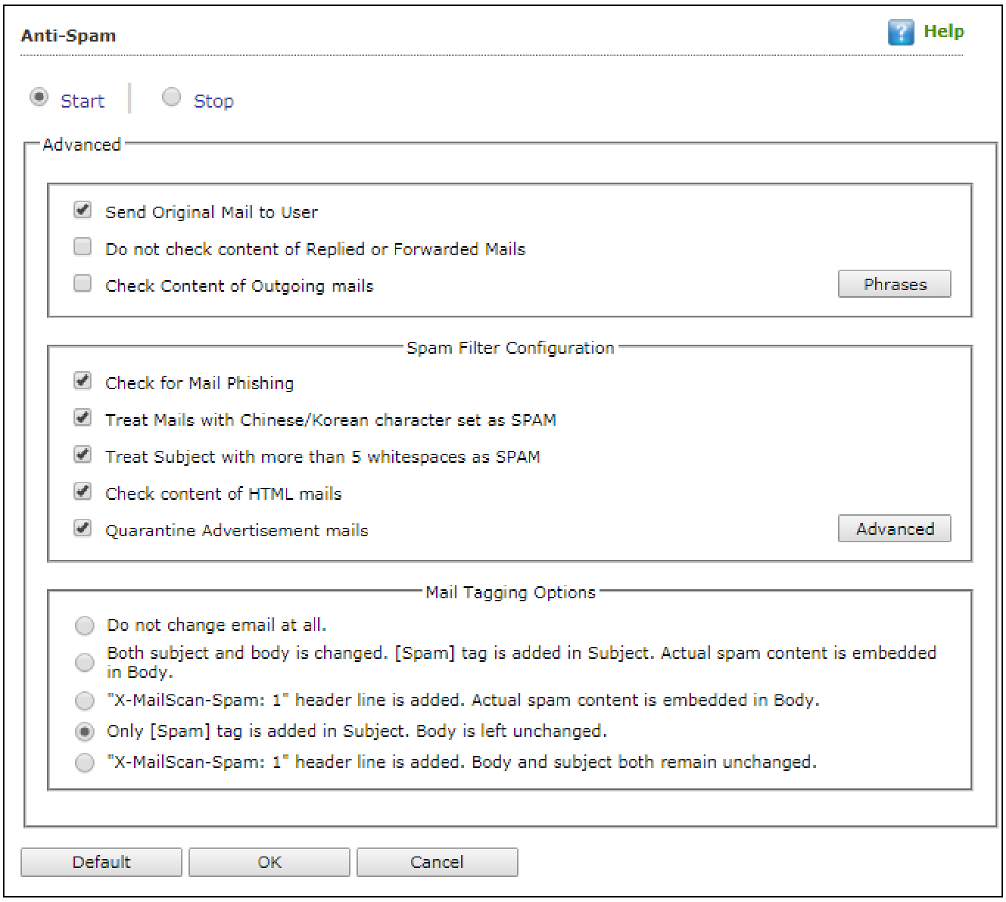
Quarantine Attachments if they are scanned
Select this checkbox if you want eScan to quarantine attachments that are scanned by Mail Anti-Virus.

Exclude Attachments (White List)

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

Anti-Spam

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



Anti-Spam

● Start ○ Stop

Advanced

☑ Send Original Mail to User
☐ Do not check content of Replied or Forwarded Mails
☐ Check Content of Outgoing mails

Spam Filter Configuration

☑ Check for Mail Phishing
☑ Treat Mails with Chinese/Korean character set as SPAM
☑ Treat Subject with more than 5 whitespaces as SPAM
☑ Check content of HTML mails
☑ Quarantine Advertisement mails

Mail Tagging Options

○ Do not change email at all.
○ Both subject and body is changed. [Spam] tag is added in Subject. Actual spam content is embedded in Body.
○ "X-MailScan-Spam: 1" header line is added. Actual spam content is embedded in Body.
● Only [Spam] tag is added in Subject. Body is left unchanged.
○ "X-MailScan-Spam: 1" header line is added. Body and subject both remain unchanged.

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

Send Original Mail to User [Default]
This checkbox is selected by default. eScan delivers spam mail to your inbox with a spam tag. When an email is tagged as SPAM, it is moved to this folder. Select this checkbox, if you want to send original email tagged as spam to the recipient as well.

Do not check content of Replied or Forwarded Mails
Select this checkbox, if you want to ensure that eScan does not check the contents of emails that you have either replied or forwarded to other recipients.

Check Content of Outgoing mails
Select this checkbox, if you want Anti-Spam to check outgoing emails for restricted content.

Phrases
Click **Phrases** to open the **Phrases** dialog box. This dialog box lets you configure additional email related options. In addition, it lets you specify a list of words that the user can either allow or block.
User specified whitelist of words/phrases (Color Code: **GREEN**)
This option indicates the list of words or phrases that are present in the whitelist. A phrase added to the whitelist cannot be edited, enabled, or disabled.

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

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

Action List

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

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

Check for Mail Phishing [Default]
Select this option if you want Anti-Spam to check for fraudulent emails and quarantine them.

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

Treat Subject with more than 5 whitespaces as SPAM [Default]
In its research, MicroWorld found that spam emails usually contain more than five consecutive white spaces. When this option is selected, Anti-Spam checks the spacing between characters or words in

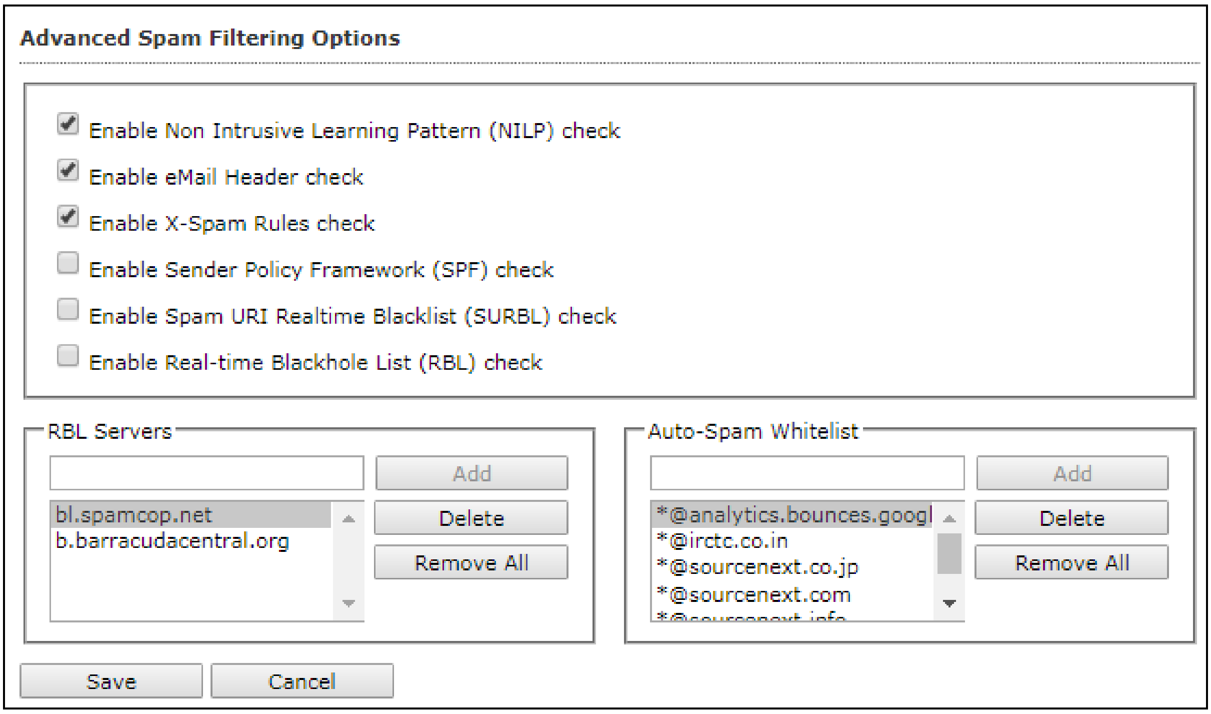
the subject line of emails and treats emails with more than five whitespaces in their subject lines as spam emails.

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

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

Advanced

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



Advanced Spam Filtering Options

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

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

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

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

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

Enable X Spam Rules check [Default]
X Spam Rules are rules that describe certain characteristics of an email. It checks whether the words in the content of emails are present in eScan's database. This database contains a list of words and phrases, each of which is assigned a particular score. The Spam Rules Check technology matches X

Spam Rules with the mail header, body, and attachments of each email to generate a score. If the score crosses a threshold value, the mail is considered as spam. Anti-Spam refers to this database to identify emails and takes action on them.

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

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

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

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

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

Mail Tagging Options

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

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

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

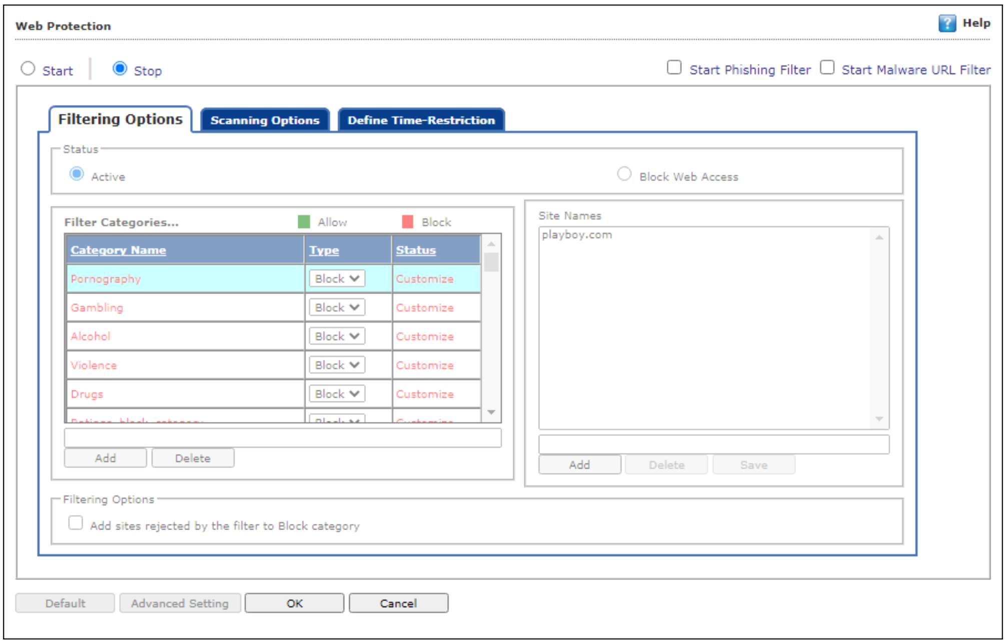
"X MailScan Spam: 1" header line is added: Actual spam content is embedded in Body
This option lets you add a [Spam] tag in the body of the email that has been identified as spam. In addition, it adds a line in the header line of the email.

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

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

Web Protection

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



○ Start | ● Stop   □ Start Phishing Filter □ Start Malware URL Filter

Status: ● Active ○ Block Web Access

Filter Categories... 🟩 Allow 🟥 Block

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

Site Names: playboy.com

Filtering Options: □ Add sites rejected by the filter to Block category

You can configure the following settings:

Filtering Options

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

Status

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

Filter Categories

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

Green

It represents an allowed websites category.

Red

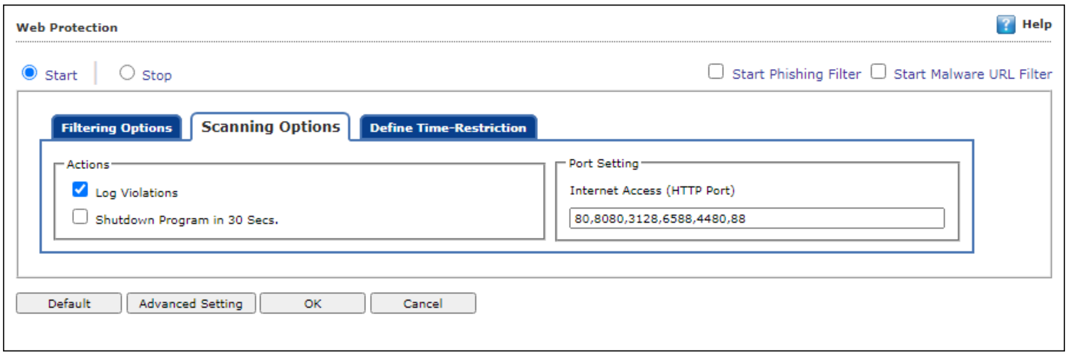
It represents a blocked websites category.
The filter categories used in this section include categories like Pornography, Gambling, Chat, Alcohol, Violence, Drugs, Ratings_block_category, Websites Allowed, etc. You can also add or delete filter categories depending on your requirement.

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

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

Scanning Options

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



Web Protection

Help

● Start | ○ Stop

□ Start Phishing Filter □ Start Malware URL Filter

Filtering Options | Scanning Options | Define Time-Restriction

Actions
☑ Log Violations
□ Shutdown Program in 30 Secs.

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

Default | Advanced Setting | OK | Cancel

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

Log Violations [Default]
This checkbox is selected by default. Select this option if you want Web Protection to log all security violations for your future reference.

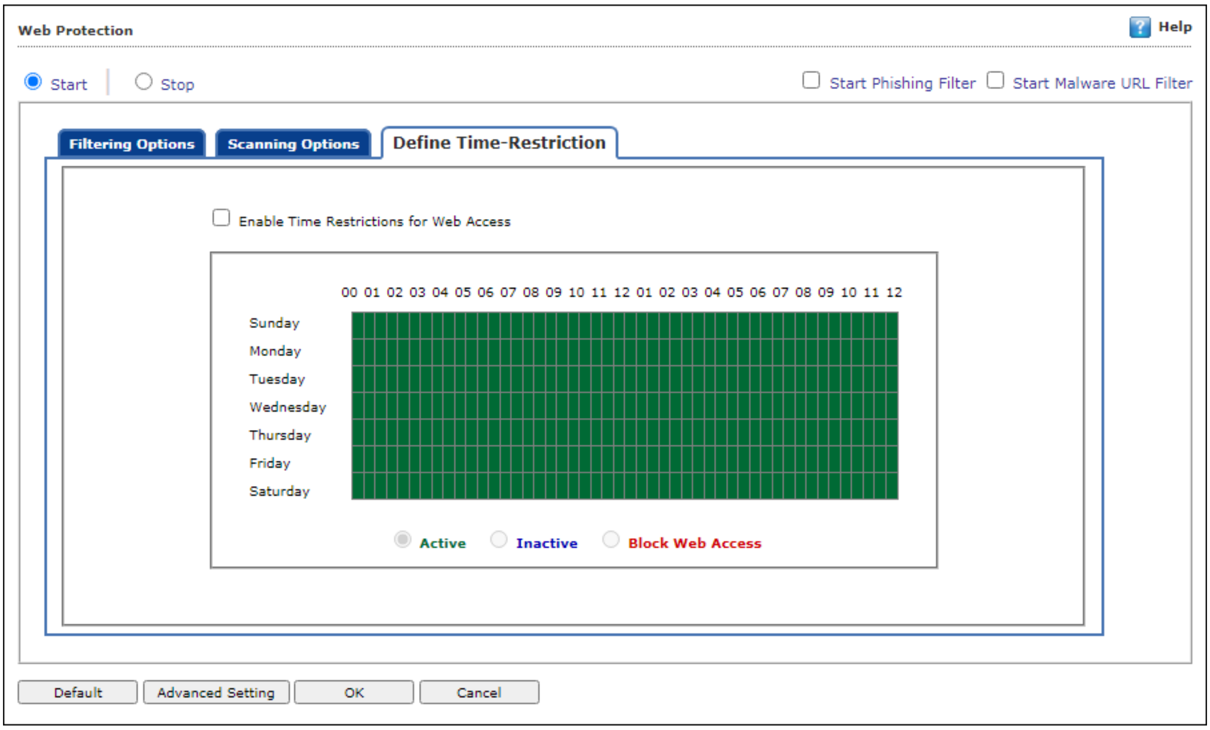
Shutdown Program in 30 Secs
Select this option if you want Web Protection to shut down the browser automatically in 30 seconds when any of the defined rules or policies is violated.

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

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

Define Time Restriction

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



Web Protection ? Help

● Start | ○ Stop ☐ Start Phishing Filter ☐ Start Malware URL Filter

Filtering Options | Scanning Options | Define Time-Restriction

☐ Enable Time Restrictions for Web Access

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

Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday

○ Active ○ Inactive ○ Block Web Access

Default | Advanced Setting | OK | Cancel

Enable Time Restrictions for Web Access

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

Active

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

Inactive

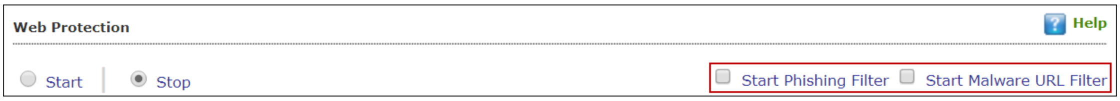
Select this option if you want to keep web access inactive on certain days for a specific interval.

Block Web Access

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

Phishing and Malware URL Filter

Under Web Protection, eScan also provides options to enable Phishing and Malware filters which will detect and prevent any phishing attempts on the system and block all malware attacks.
To enable the filters, select **Start** and then select the respective checkboxes.



Web Protection ? Help

○ Start | ● Stop ☐ Start Phishing Filter ☐ Start Malware URL Filter

Advanced Setting

Ignore IP address from Web-scanning

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

Enable Unknown Browser detection

Select this option to enable/disable unknown browser detection.

Enable allowing of WhiteListed Site during BlockTime
Select this option to enable/disable white listed site during block time.

Enable Online Web-Scanning Module
Select this option to enable/disable online web-scanning module.

Disable Web Warning Page
Select this option to enable/disable web warning page.

Enable HTTPS Popup
Select this option to enable/disable HTTPS Popup.
Show External Page for Web blocking (Page to be define under External Page)

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

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

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

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

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

Allow access to SubDomain for Whitelisted sites(Only HTTP Sites)
Select this option to enable/disable access to SubDomain for Whitelisted sites.

Allow access to SubDomain for Whitelisted sites(Only HTTPS Sites)
Select this option to enable/disable access to SubDomain for Whitelisted sites.

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

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

Block HTTP Traffic only on Web Browser
Select this option to enable/disable block HTTP Traffic on Web Browser.

Allow website list (Depends on "Block HTTP Traffic only on Web Browser")
Select this option to enter to block HTTP Traffic on Web Browser.

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

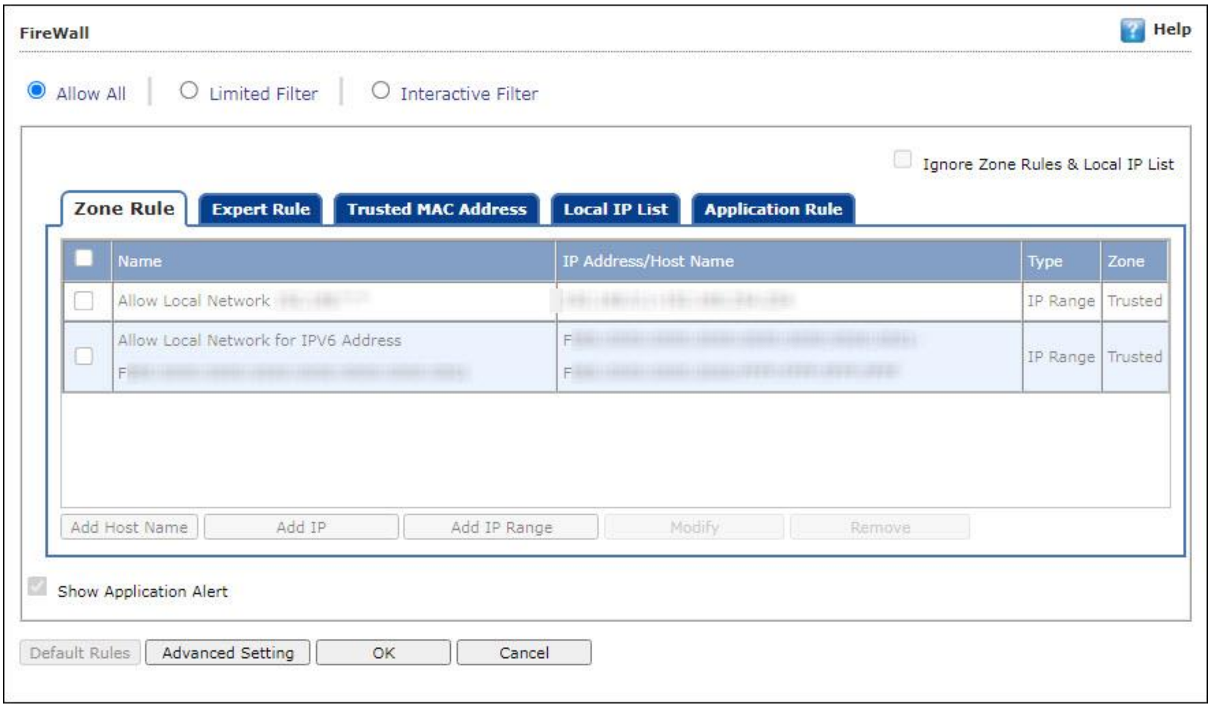
Enable Web Protection using Filter driver (1 = Enable/0 = Disable)
Select this option to enable/disable web protection using filter driver.

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

WFP Exclude IP List (1 = Enable/0 = Disable)
Select this option to enable/disable excluding IP list from Web Filter Protection.

Firewall

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



FireWall

● Allow All | ○ Limited Filter | ○ Interactive Filter

□ Ignore Zone Rules & Local IP List

□	Name	IP Address/Host Name	Type	Zone
□	Allow Local Network [redacted]	[redacted]	IP Range	Trusted
□	Allow Local Network for IPV6 Address F[redacted]	F[redacted] F[redacted]	IP Range	Trusted

☑ Show Application Alert

The Firewall feature of eScan protects your data when you:

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

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

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

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

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

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

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

Zone Rule

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

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

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

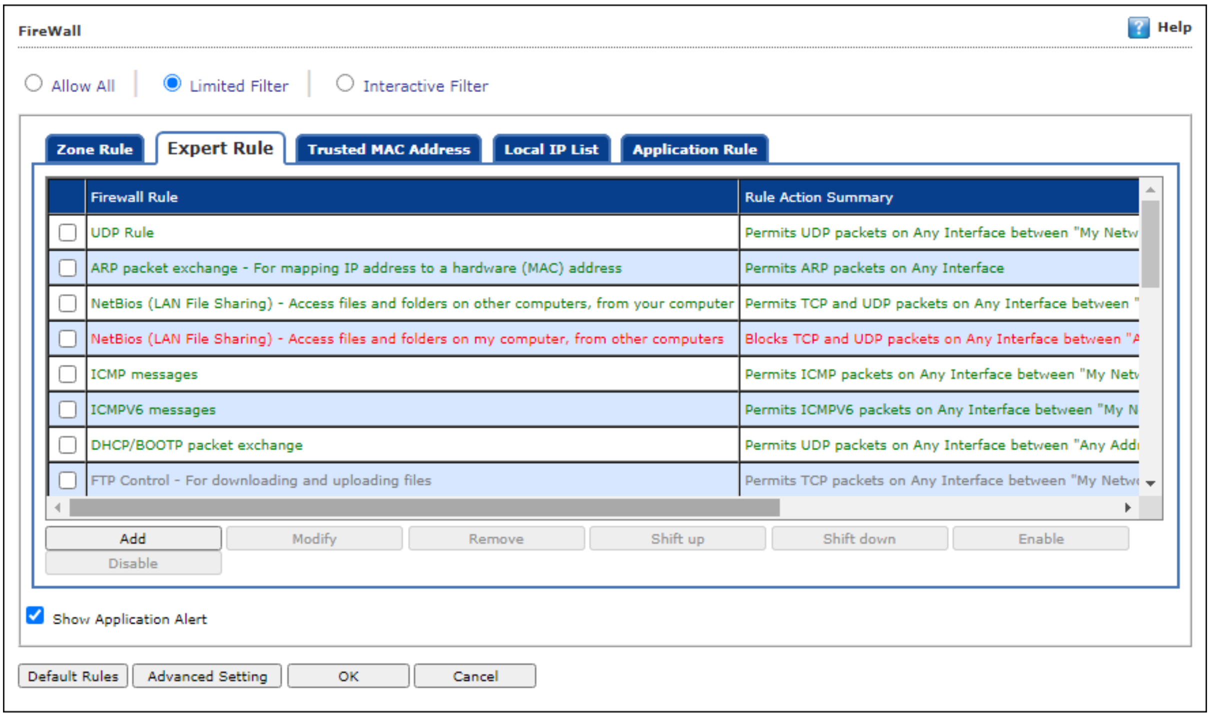
Add IP Range – This option lets you add an IP range to be added in the zone rule. After clicking **Add IP Range**, add the IP Range (i.e. a range of IP that the zone rules should be applied), select the zone (Trusted/Blocked) and enter a name for the zone rule. Click **OK** to create the zone rule.

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

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

Expert Rule

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



○ Allow All | ● Limited Filter | ○ Interactive Filter

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

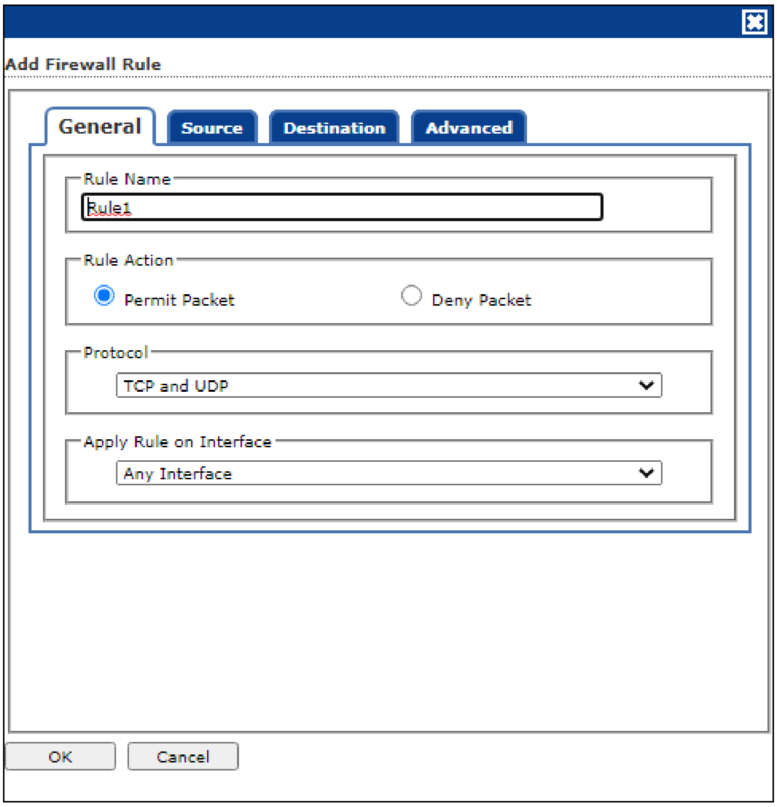
☑ Show Application Alert

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

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

Buttons to configure an Expert Rule:

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



Add Firewall Rule

Rule Name: Rule1

Rule Action: ● Permit Packet ○ Deny Packet

Protocol: TCP and UDP

Apply Rule on Interface: Any Interface

General tab
In this section, specify the Rule settings:

Rule Name – Provide a name to the Rule.

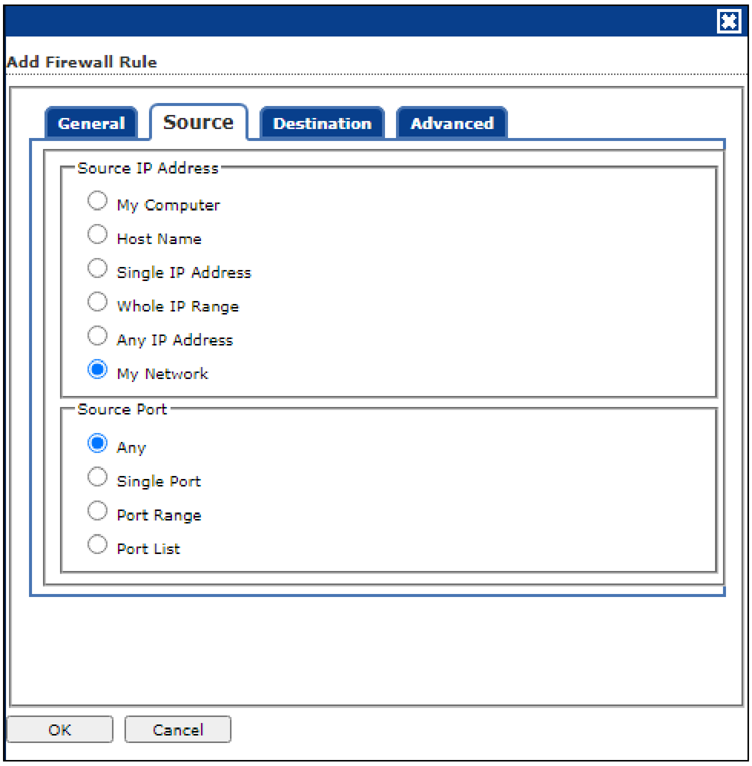
Rule Action – Action to be taken, whether to Permit Packet or Deny Packet.

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

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

Source tab

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



Add Firewall Rule

Source IP Address

○ My Computer

○ Host Name

○ Single IP Address

○ Whole IP Range

○ Any IP Address

● My Network

Source Port

● Any

○ Single Port

○ Port Range

○ Port List

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

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

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

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

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

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

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

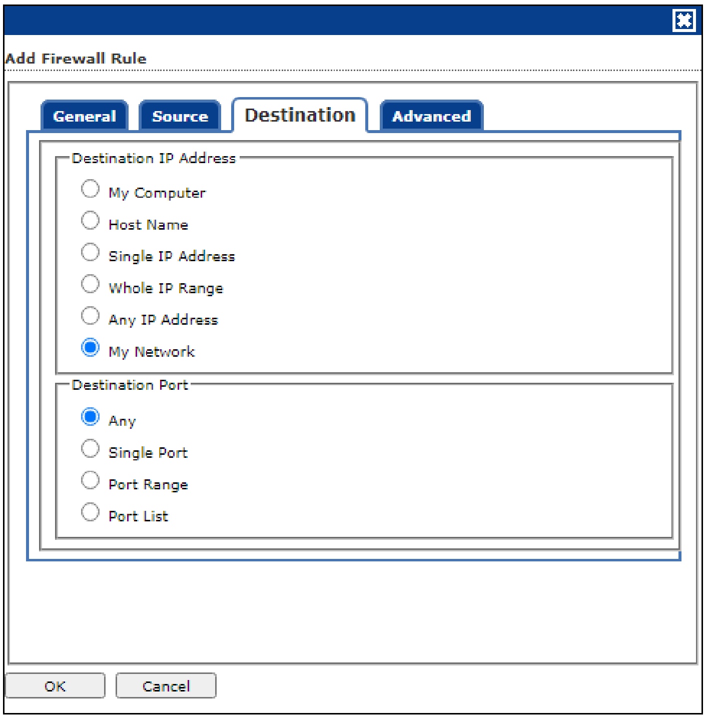
Port Range – To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the outgoing traffic originating from the port which is within the defined range of ports.

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

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

Destination tab

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



Add Firewall Rule

Destination IP Address

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

Destination Port

● Any
○ Single Port
○ Port Range
○ Port List

Destination IP Address

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

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

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

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

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

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

Destination Port

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

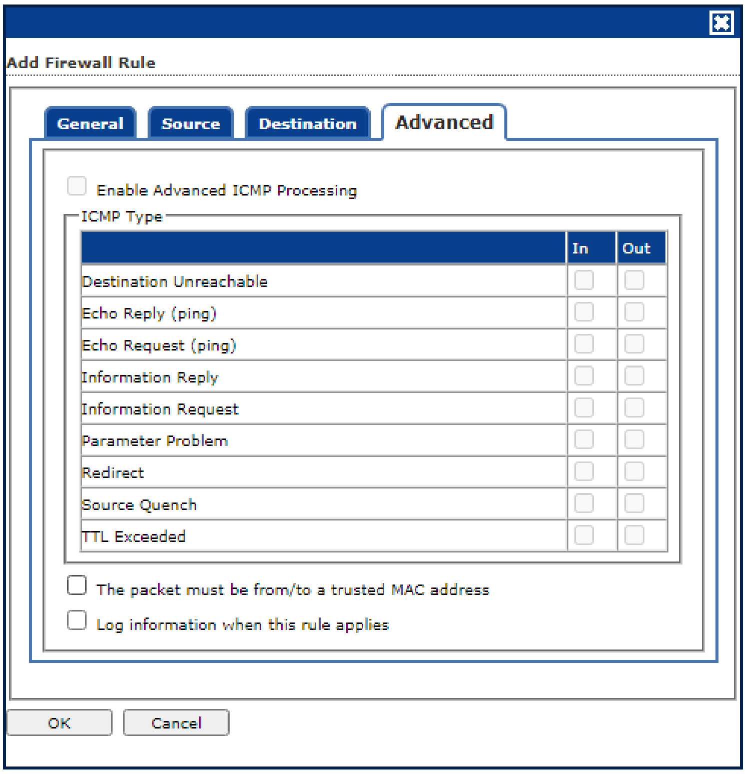
Single Port – After selecting this option, the rule will be applied for the incoming traffic to the specified/defined port.

Port Range – To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the incoming traffic to the port which is within the defined range of ports.
Port List – A list of port can be specified/added. The rule will be applied for incoming traffic originating from the ports as per specified in the list.

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

Advanced tab

This tab contains advance setting for Expert Rule.



Add Firewall Rule

□ Enable Advanced ICMP Processing

ICMP Type

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

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

□ Log information when this rule applies

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

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

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

Following are additional buttons the Expert Rule tab provides:

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

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

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

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

Trusted MAC Address

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

Buttons (to configure the Trusted MAC Address)
Add – To add a MAC address click on this button. Enter the MAC address to be added in the list for e.g. 00-13-[redacted]

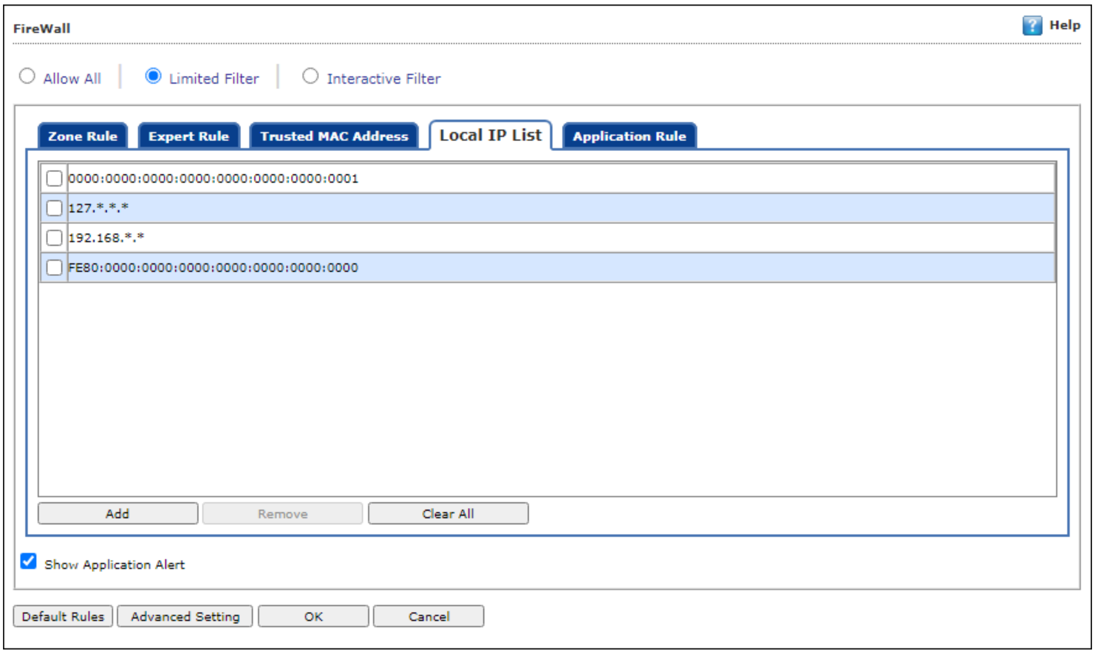
Edit – To modify/change the MAC Address, click **Edit**.

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

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

Local IP List

This section contains a list of Local IP addresses.



FireWall

○ Allow All | ● Limited Filter | ○ Interactive Filter

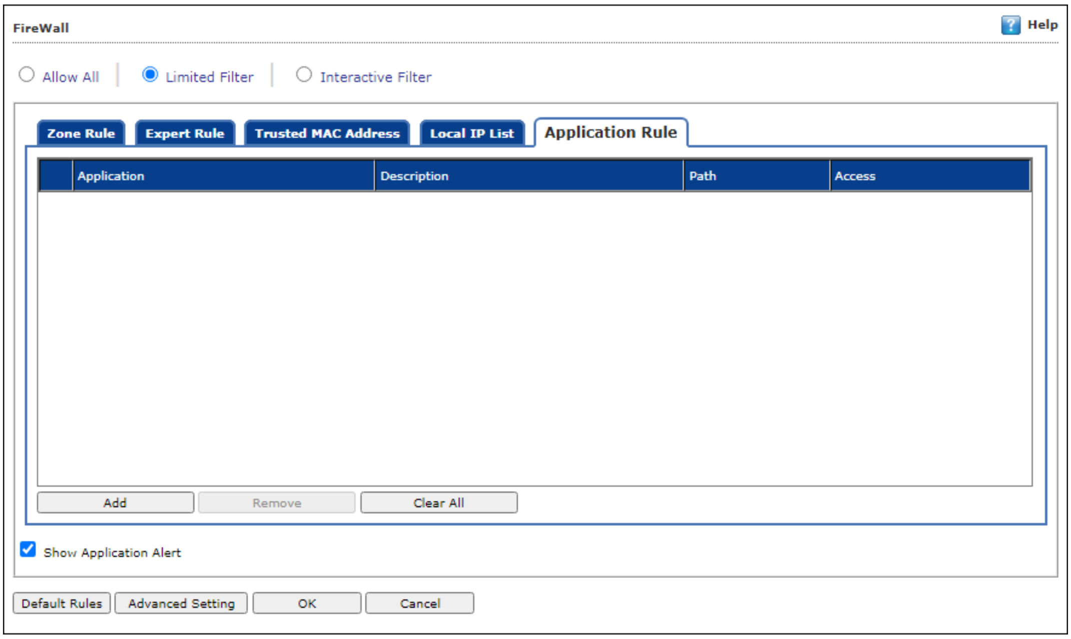
□ 0000:0000:0000:0000:0000:0000:0000:0001
□ 127.*.*.*
□ 192.168.*.*
□ FE80:0000:0000:0000:0000:0000:0000:0000

☑ Show Application Alert

Add – To add a local IP address, click **Add**.
Remove – To remove a local IP address, click **Remove**.
Clear All – To clear all local IP addresses, click **Clear All**.
Default List – To load the default list of IP addresses, click **Default List**.

Application Rule

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



○ Allow All | ● Limited Filter | ○ Interactive Filter

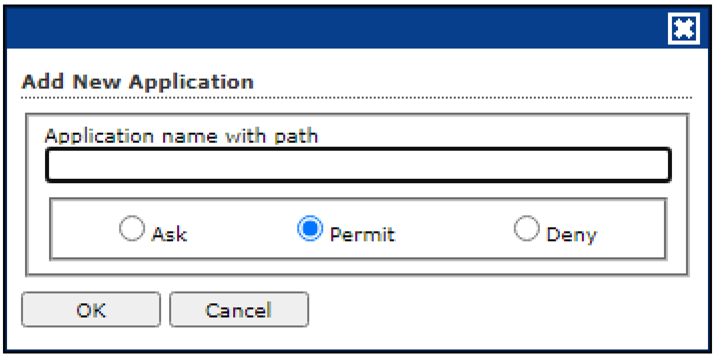
Application	Description	Path	Access

☑ Show Application Alert

Defining permission for an application

To define permission for an application:

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



Application name with path

○ Ask ● Permit ○ Deny

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

   The permission for the application will be defined.

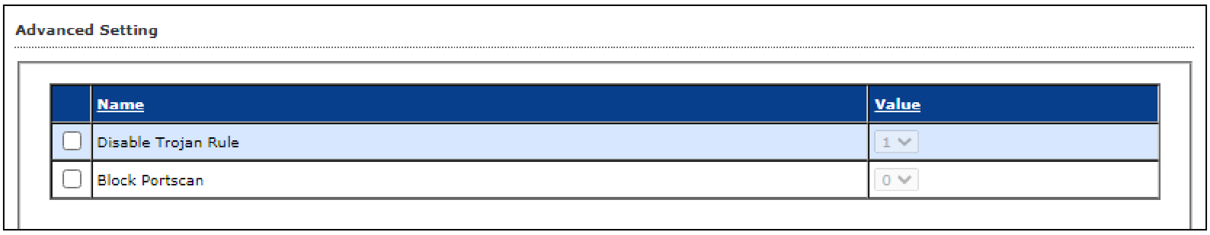
Removing permission of an application

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

Other Buttons:

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

- **Advanced Setting**: Clicking this button displays additional advanced settings:



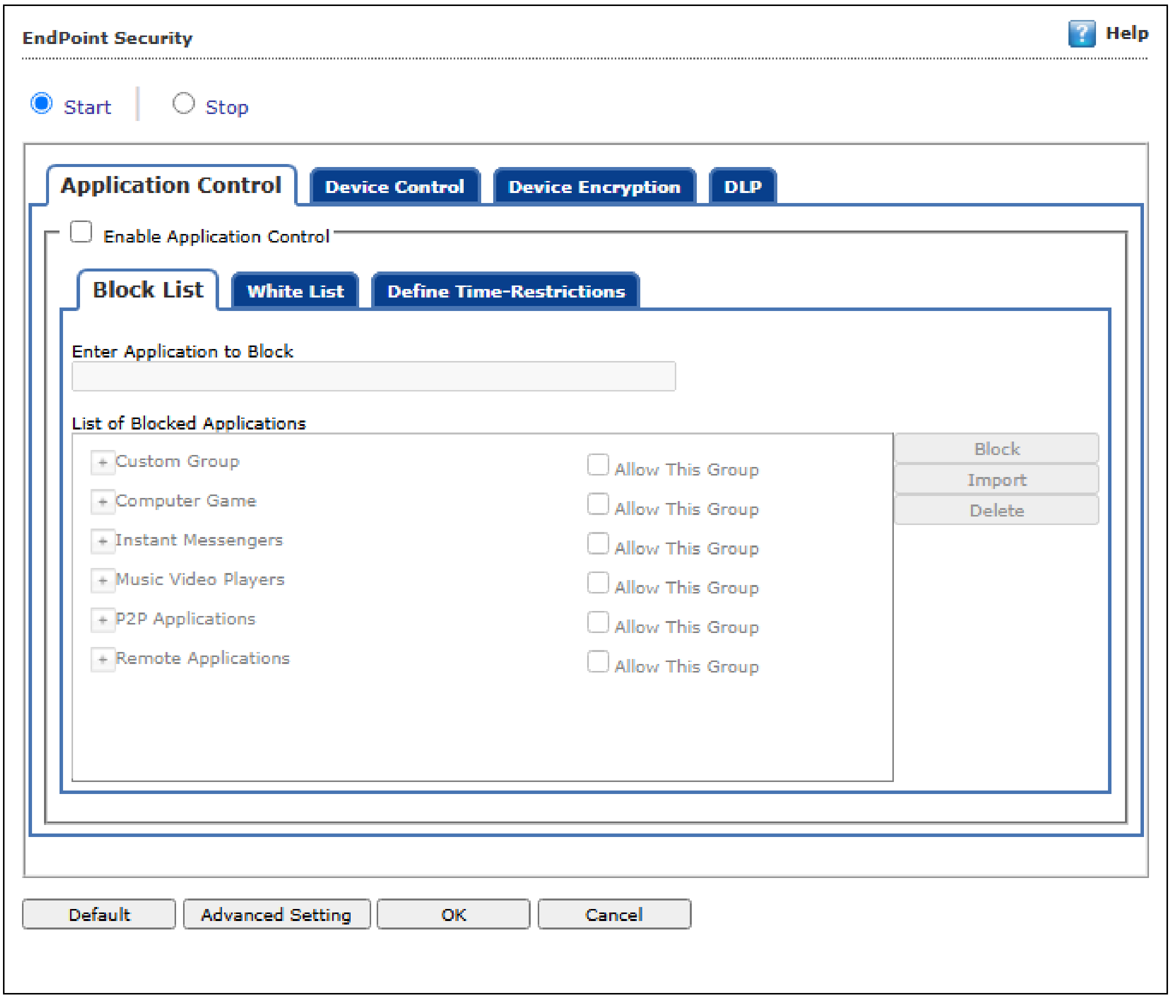
Advanced Setting

	Name	Value
□	Disable Trojan Rule	1 ⌄
□	Block Portscan	0 ⌄

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

Endpoint Security

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



EndPoint Security

● Start | ○ Stop

Application Control | Device Control | Device Encryption | DLP

□ Enable Application Control

Block List | White List | Define Time-Restrictions

Enter Application to Block

List of Blocked Applications

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

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

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

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

Application Control

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

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

Block List

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

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

White List

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

Enter Application to whitelist
Enter the name of the application to be whitelisted.

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

Define Time Restrictions

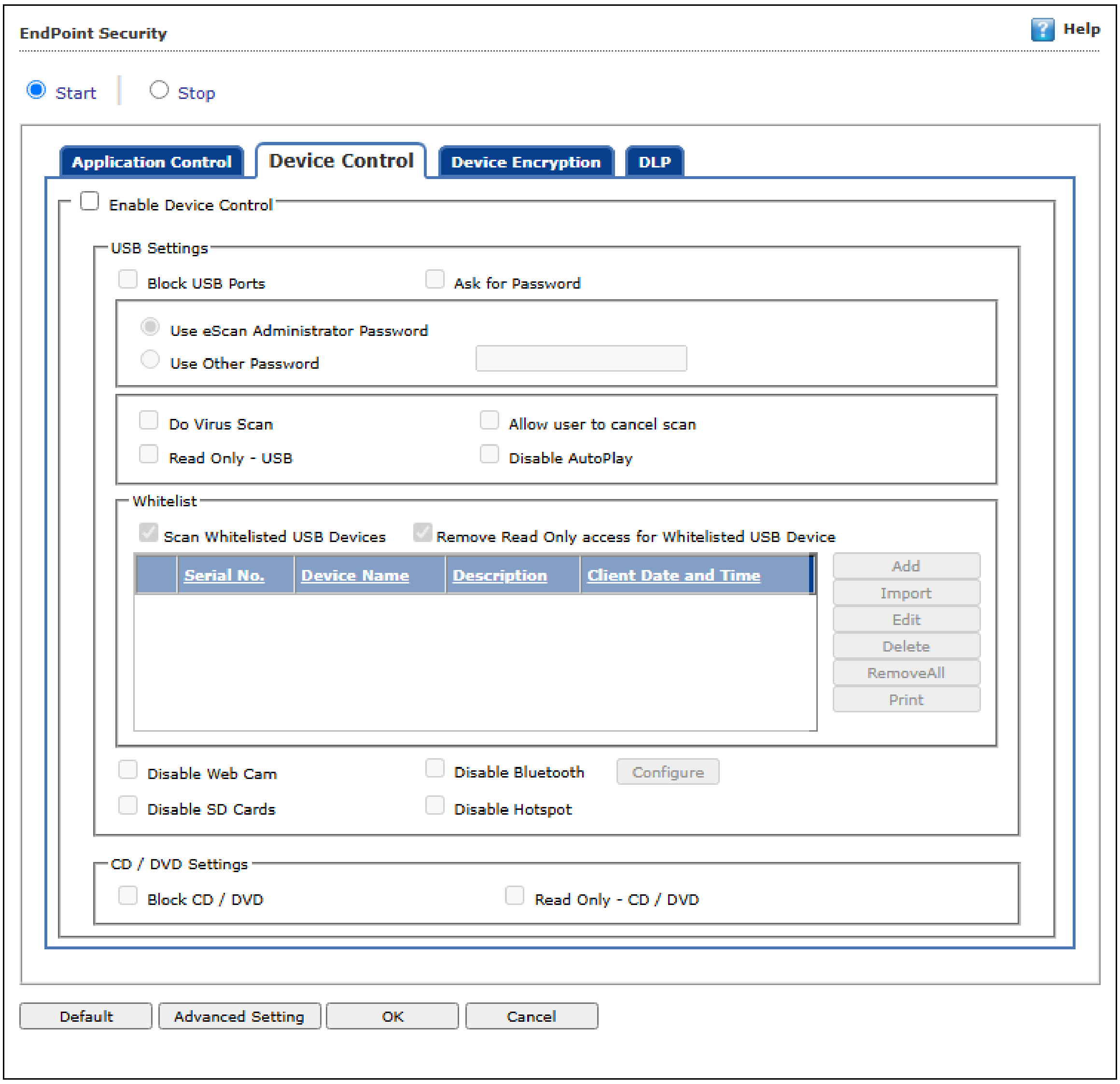
This option lets you enable/disable application control feature. This feature lets you define time restriction when you want to allow or block access to the applications based on specific days and between pre-defined hours during a day.

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

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

Device Control

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



EndPoint Security

● Start | ○ Stop

Device Control

□ Enable Device Control

USB Settings

□ Block USB Ports □ Ask for Password

● Use eScan Administrator Password

○ Use Other Password

□ Do Virus Scan □ Allow user to cancel scan

□ Read Only - USB □ Disable AutoPlay

Whitelist

☑ Scan Whitelisted USB Devices ☑ Remove Read Only access for Whitelisted USB Device

	Serial No.	Device Name	Description	Client Date and Time

□ Disable Web Cam □ Disable Bluetooth

□ Disable SD Cards □ Disable Hotspot

CD / DVD Settings

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

You can configure the following settings:

Enable Device Control [Default]
Select this option if you want to monitor all the USB storages devices connected to your endpoint. This will enable all the options in this tab.

USB Settings

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

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

Ask for Password

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

- **Use eScan Administrator**: This option is available only when you select the **Ask for Password** checkbox. Click this option if you want to assign eScan Administrator password for accessing USB storage device.
- **Use Other Password**: This option is available only when you select the **Ask for Password** checkbox. Click this option if you want assign a unique password for accessing USB storage device.

Do Virus Scan [Default]

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

Allow user to cancel scan

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

Read Only – USB

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

Disable AutoPlay [Default]

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

Whitelist

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

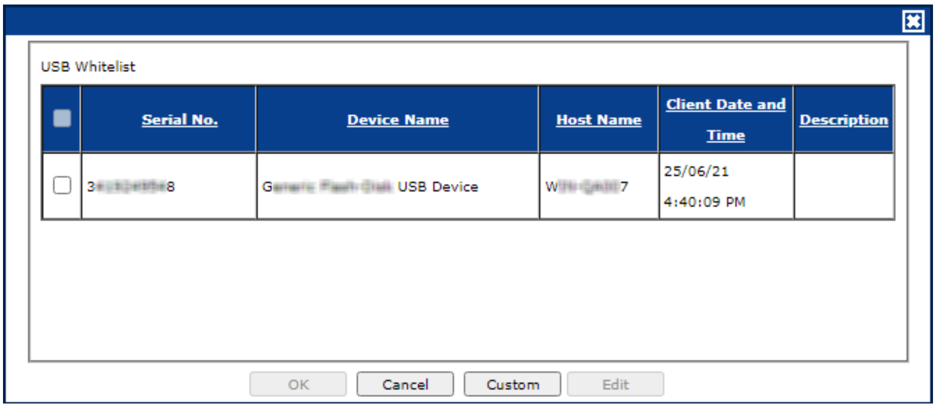
Scan Whitelisted USB Devices

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

Remove Read Only access for Whitelisted USB Device

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

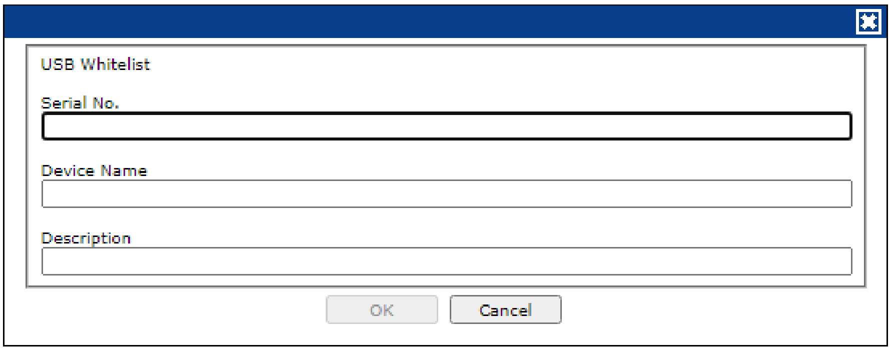
- **Add**
  Click **Add** to whitelist USB devices.
  USB Whitelist window appears.



USB Whitelist

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

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



USB Whitelist

Serial No.

Device Name

Description

Enter the USB details and then click **OK**.

The USB device will be added and whitelisted.

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

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

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

Disable Web Cam: Select this option to disable Webcams.

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

Disable Bluetooth: Select this option to disable Bluetooth.

CD / DVD Settings

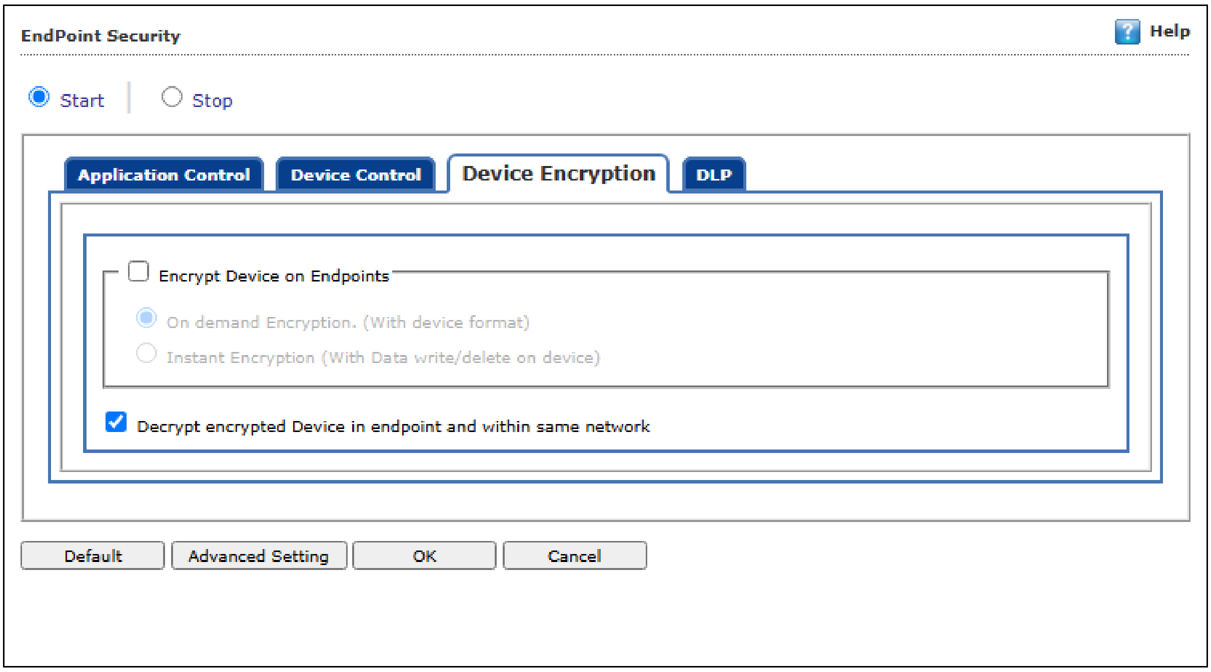
Block CD / DVD: Select this option to block all CD/DVD access.

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

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

Device Encryption (requires Enterprise DLP license)

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.



● Start ○ Stop

□ Encrypt Device on Endpoints

● On demand Encryption. (With device format)

○ Instant Encryption (With Data write/delete on device)

☑ Decrypt encrypted Device in endpoint and within same network

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.

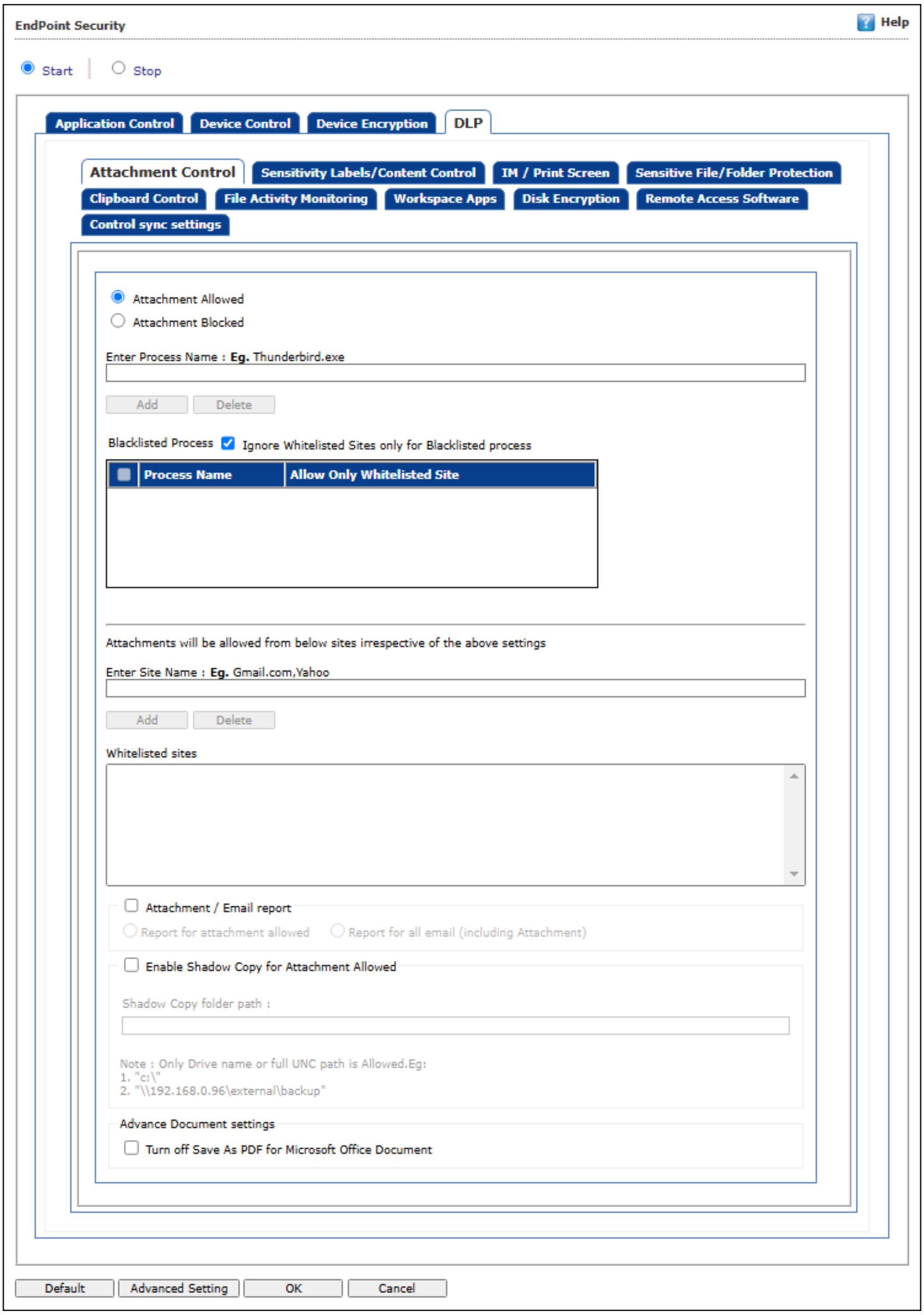
- **On demand Encryption (With device format):** This option formats the connected USB device and encrypts it for further use of storing data in encrypted format.
- **Instant Encryption (With Data write/delete on device):** This option instantly encrypts the device without formatting existing data.

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 (requires Enterprise DLP license)

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



EndPoint Security

● Start | ○ Stop

Attachment Control

● Attachment Allowed
○ Attachment Blocked

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

Blacklisted Process ☑ Ignore Whitelisted Sites only for Blacklisted process

□	Process Name	Allow Only Whitelisted Site

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

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

Whitelisted sites

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

□ Enable Shadow Copy for Attachment Allowed

Shadow Copy folder path :

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

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

Attachment Control

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

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

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

Configure Extension/Group based Whitelisting
This option allows you to select/add group wise 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

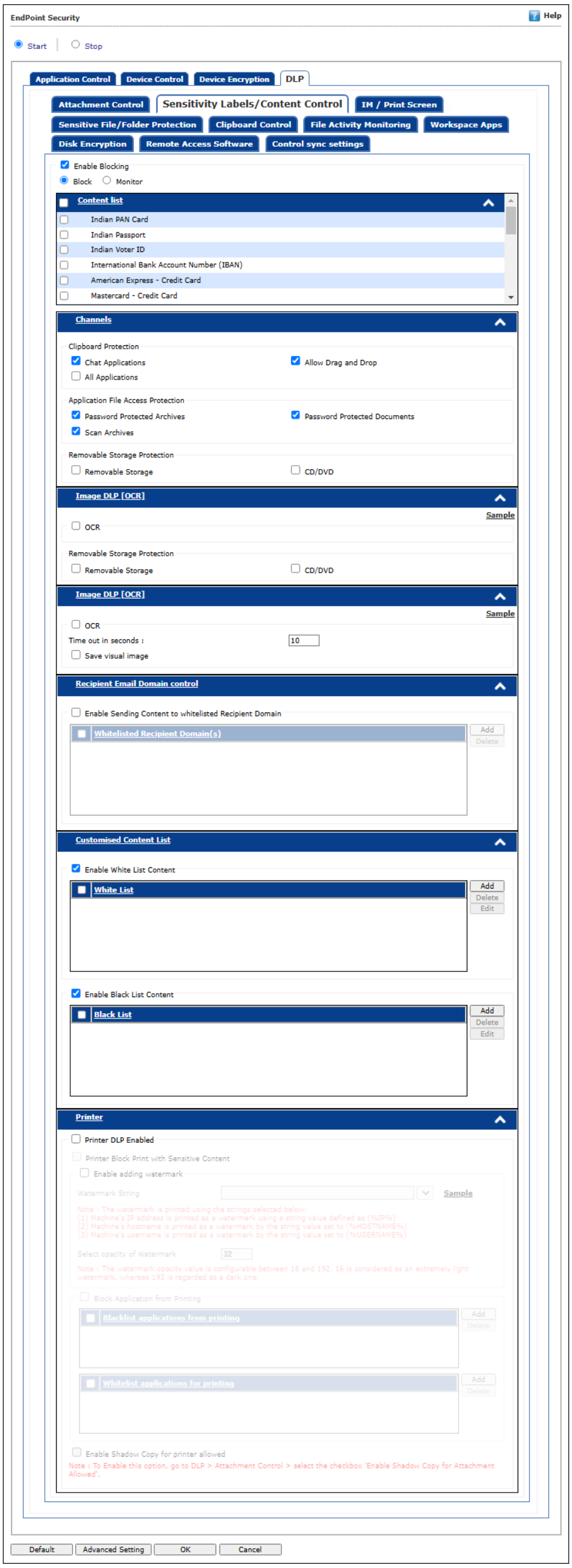
Select this checkbox to create shadow copies of outgoing attachments. Enter the drive name or complete UNC path in the provided field where these shadow copies need to be saved.

Advance Document setting

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

Sensitivity Labels/Content Control

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



EndPoint Security

● Start | ○ Stop

☑ Enable Blocking

● Block ○ Monitor

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

Channels

Clipboard Protection
- ☑ Chat Applications
- ☑ Allow Drag and Drop
- □ All Applications

Application File Access Protection
- ☑ Password Protected Archives
- ☑ Password Protected Documents
- ☑ Scan Archives

Removable Storage Protection
- □ Removable Storage
- □ CD/DVD

Image DLP [OCR]

Sample

□ OCR

Removable Storage Protection
- □ Removable Storage
- □ CD/DVD

Image DLP [OCR]

Sample

□ OCR

Time out in seconds : 10

□ Save visual image

Recipient Email Domain control

□ Enable Sending Content to whitelisted Recipient Domain

□ Whitelisted Recipient Domain(s)

Customised Content List

☑ Enable White List Content

□ White List

☑ Enable Black List Content

□ Black List

Printer

□ Printer DLP Enabled

□ Printer Block Print with Sensitive Content

□ Enable adding watermark

Watermark String

Sample

Note : The watermark is printed using the strings selected below:
(1) Machine's IP address is printed as a watermark using a string value defined as (%IP%)
(2) Machine's hostname is printed as a watermark by the string value set to (%HOSTNAME%)
(3) Machine's username is printed as a watermark by the string value set to (%USERNAME%)

Select opacity of Watermark 32

Note : The watermark opacity value is configurable between 16 and 192. 16 is considered as an extremely light watermark, whereas 192 is regarded as a dark one.

□ Block Application from Printing

□ Blacklist applications from printing

□ Whitelist applications for printing

□ Enable Shadow Copy for printer allowed

Note : To Enable this option, go to DLP > Attachment Control > select the checkbox 'Enable Shadow Copy for Attachment Allowed'.

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

Set the sensitivity labels (Data Classification) for your files based on its sensitivity and importance so that the DLP will treat each file accordingly. Follow the steps below to define sensitivity labels. By categorizing your files using these labels, you can apply appropriate security measures tailored to the data's classification labels and respond quickly to potential data leaks. Below are the three categories under which the data gets labelled:

- **Normal:** Select this label on files which you want to be accessible to external requests and sharable outside the network.
- **Internal:** Select this label on files which you want to be accessible and sharable only within the network.
- **Confidential:** Select this label on files which you don't want to be accessible for anyone except the host user. The DLP will also restrict this file from being shared outside the 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]

The text-based DLP monitors only text in the content in order to prevent data leak outside the network. However, the Image DLP prevents leakage of sensitive data from visuals files (images) 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.

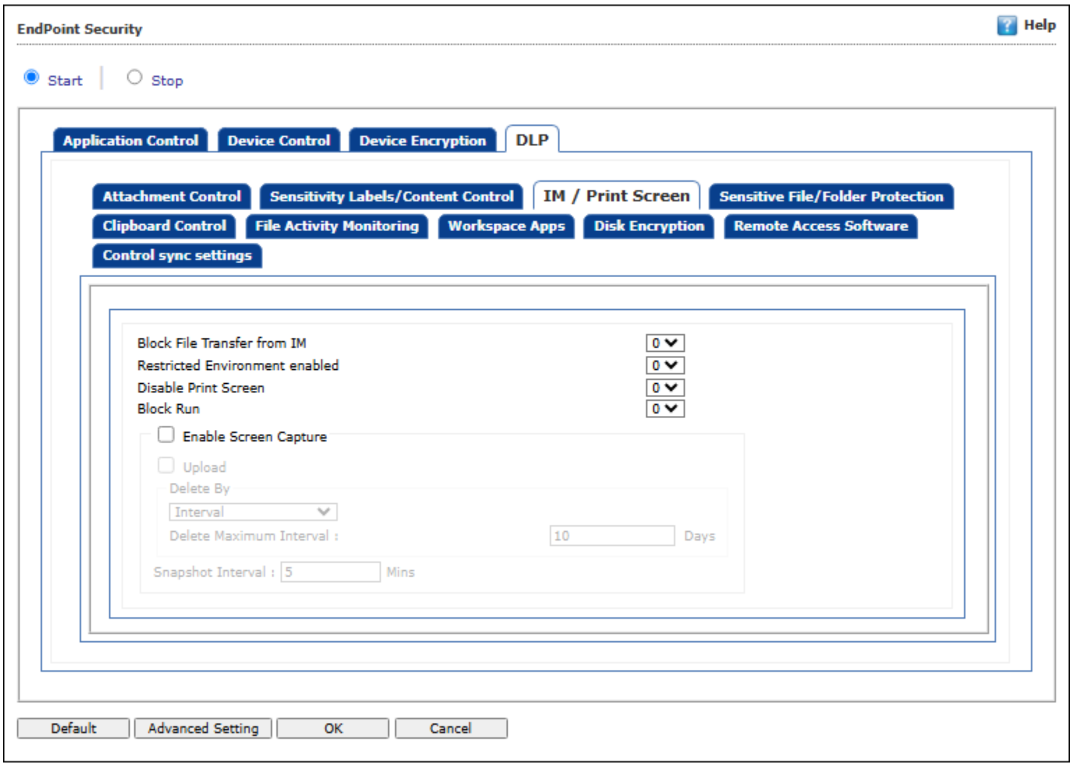
9. To whitelist the applications for printing, click on provided **Add** button.
   The 'Add Application name which will only be allowed to print' prompt appears

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.



● Start | ○ Stop

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

☐ Enable Screen Capture

☐ Upload

Delete By

Interval

Delete Maximum Interval : 10 Days

Snapshot Interval : 5 Mins

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.

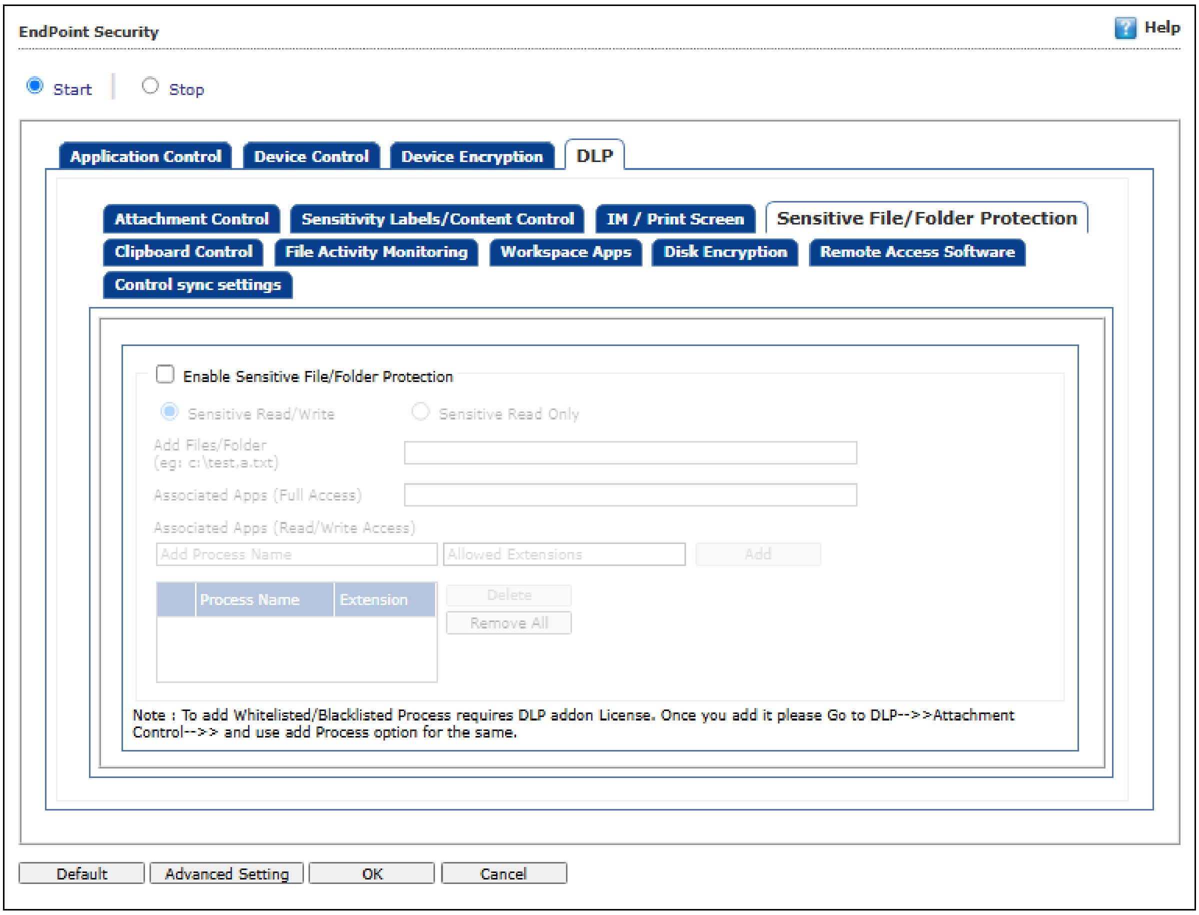
Enable Screen Capture
Selecting this checkbox allow endpoint users to take screenshot.

- **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.



EndPoint Security

Help

● Start | ○ Stop

Application Control | Device Control | Device Encryption | DLP

Attachment Control | Sensitivity Labels/Content Control | IM / Print Screen | Sensitive File/Folder Protection
Clipboard Control | File Activity Monitoring | Workspace Apps | Disk Encryption | Remote Access Software
Control sync settings

□ Enable Sensitive File/Folder Protection

● Sensitive Read/Write ○ Sensitive Read Only

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

Associated Apps (Full Access)

Associated Apps (Read/Write Access)

Add Process Name | Allowed Extensions | Add

	Process Name	Extension

Delete

Remove All

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

Default | Advanced Setting | OK | Cancel

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)

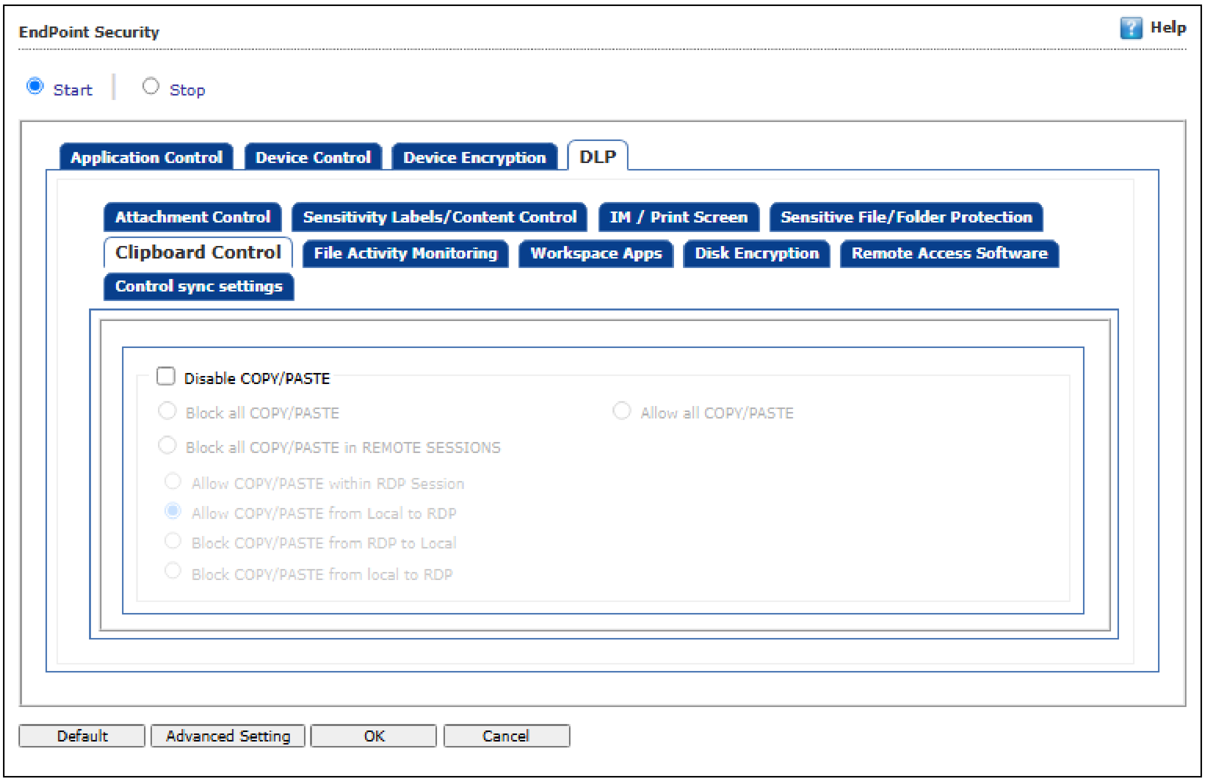
Enter the associated application name that has full access on sensitive files/folders.

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.



EndPoint Security

● Start | ○ Stop

□ Disable COPY/PASTE

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

○ Block all COPY/PASTE in REMOTE SESSIONS

○ Allow COPY/PASTE within RDP Session

● Allow COPY/PASTE from Local to RDP

○ Block COPY/PASTE from RDP to Local

○ Block COPY/PASTE from local to RDP

Disable COPY/PASTE

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

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

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

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

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

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

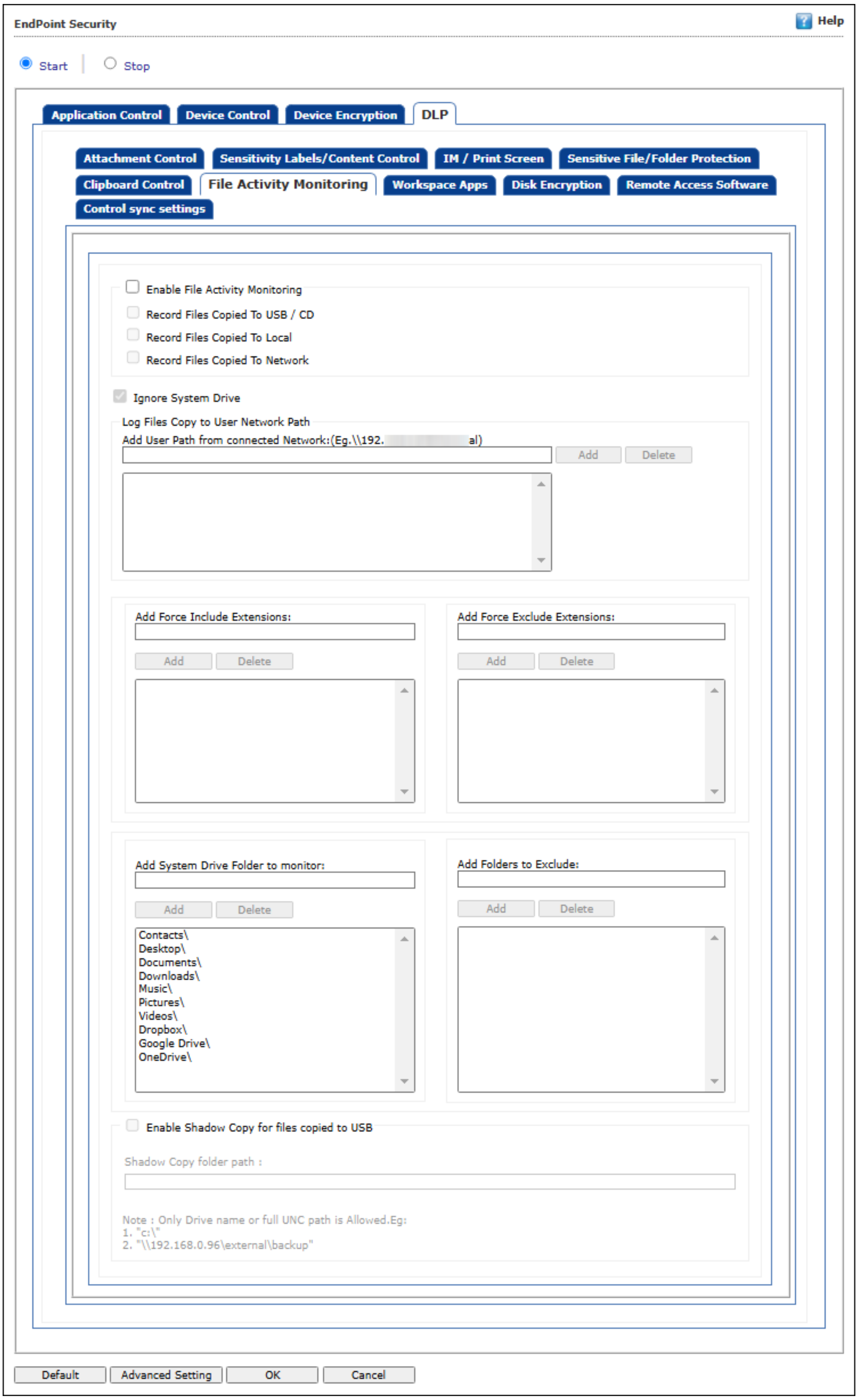
Block COPY/PASTE from RDP to local: Select this option to block copy/paste actions from RDP to local sessions.

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

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

File Activity Monitoring

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



EndPoint Security — Help

● Start | ○ Stop

Application Control | Device Control | Device Encryption | DLP

Attachment Control | Sensitivity Labels/Content Control | IM / Print Screen | Sensitive File/Folder Protection | Clipboard Control | File Activity Monitoring | Workspace Apps | Disk Encryption | Remote Access Software | Control sync settings

□ Enable File Activity Monitoring

□ Record Files Copied To USB / CD

□ Record Files Copied To Local

□ Record Files Copied To Network

☑ Ignore System Drive

Log Files Copy to User Network Path

Add User Path from connected Network:(Eg.\\192.[redacted]al) Add Delete

Add Force Include Extensions: Add Delete

Add Force Exclude Extensions: Add Delete

Add System Drive Folder to monitor: Add Delete

Contacts\
Desktop\
Documents\
Downloads\
Music\
Pictures\
Videos\
Dropbox\
Google Drive\
OneDrive\

Add Folders to Exclude: Add Delete

□ Enable Shadow Copy for files copied to USB

Shadow Copy folder path :

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

Default | Advanced Setting | OK | 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**.

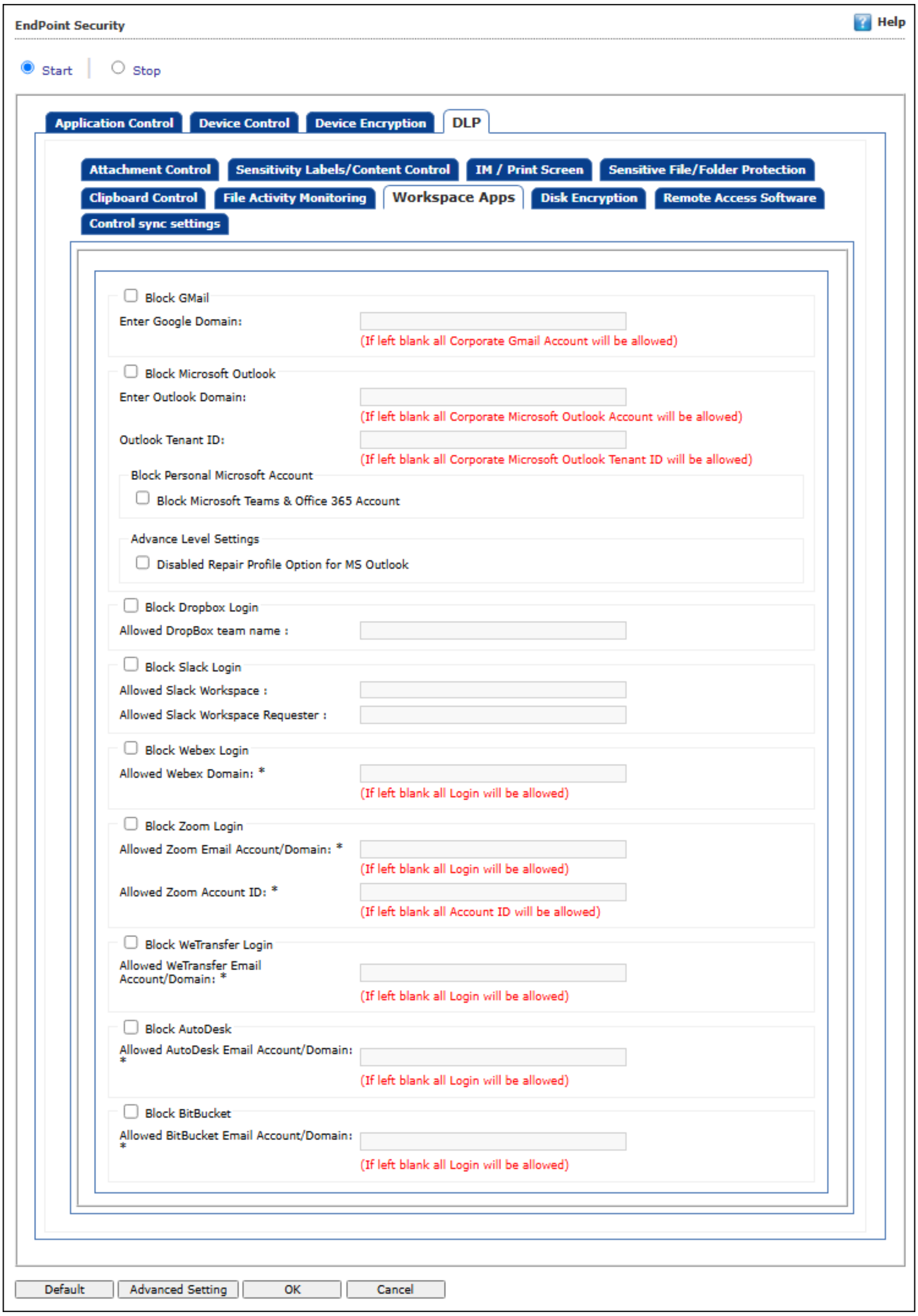
Add System Drive Folder to monitor
Select this option if you want eScan to monitor all the system drives installed on the computer. You can add or delete system drive folder from the list of by clicking **Add/Delete**.

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.



EndPoint Security

● Start | ○ Stop

□ Block GMail

Enter Google Domain: (If left blank all Corporate Gmail Account will be allowed)

□ Block Microsoft Outlook

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

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

Block Personal Microsoft Account

□ Block Microsoft Teams & Office 365 Account

Advance Level Settings

□ Disabled Repair Profile Option for MS Outlook

□ Block Dropbox Login

Allowed DropBox team name :

□ Block Slack Login

Allowed Slack Workspace :

Allowed Slack Workspace Requester :

□ Block Webex Login

Allowed Webex Domain: * (If left blank all Login will be allowed)

□ Block Zoom Login

Allowed Zoom Email Account/Domain: * (If left blank all Login will be allowed)

Allowed Zoom Account ID: * (If left blank all Account ID will be allowed)

□ Block WeTransfer Login

Allowed WeTransfer Email Account/Domain: * (If left blank all Login will be allowed)

□ Block AutoDesk

Allowed AutoDesk Email Account/Domain: * (If left blank all Login will be allowed)

□ Block BitBucket

Allowed BitBucket Email Account/Domain: * (If left blank all Login will be allowed)

Block GMail

Select this checkbox to block the personal Gmail account.

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

Block Microsoft 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 Personal Microsoft Account:** Select this checkbox to block personal Microsoft account.
- **Advance Level Settings:** Select this checkbox to disable repair profile option for MS Outlook.

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.

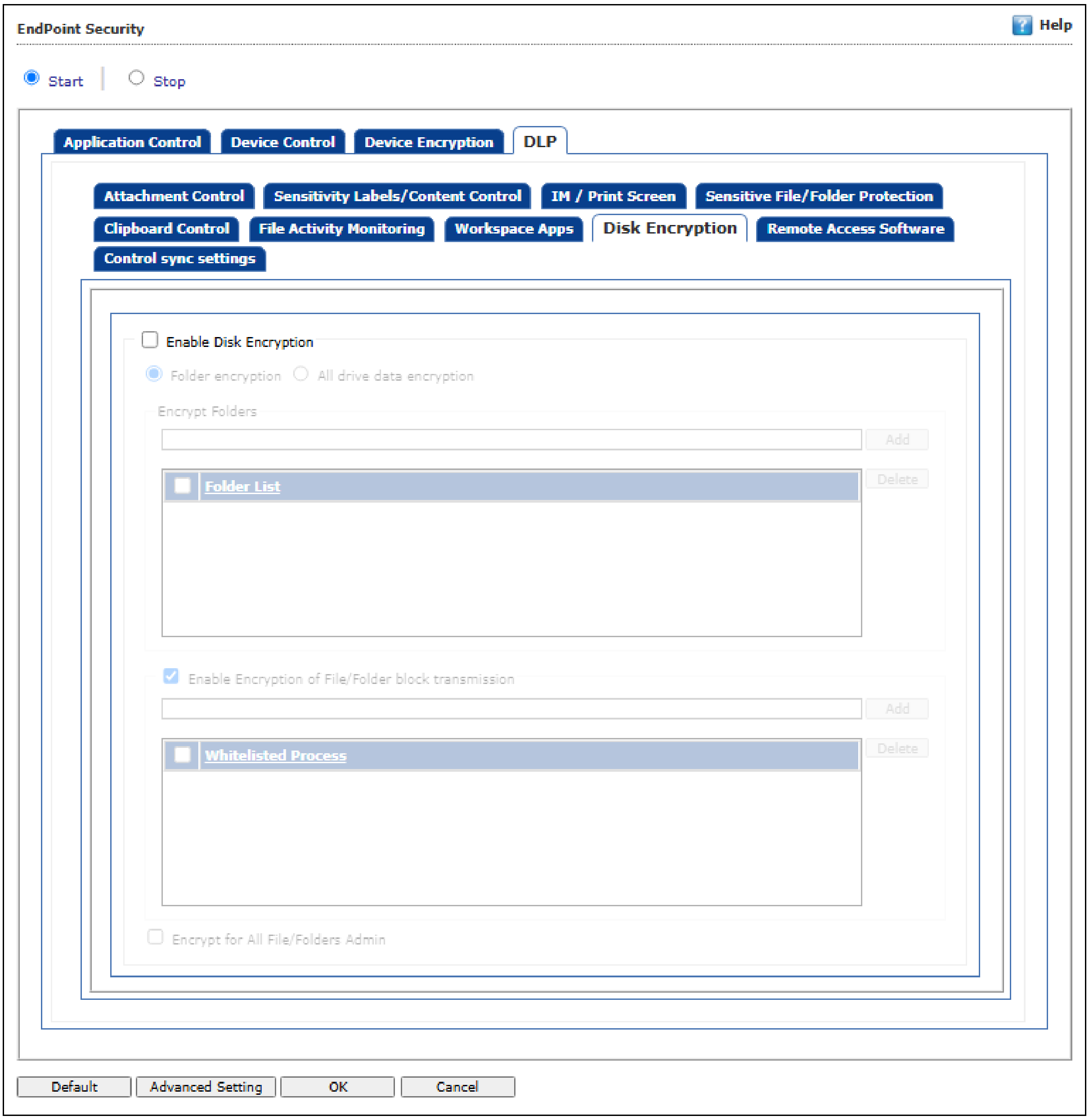
- **Allowed AutoDesk Email Account/Domain:** Enter the Autodesk email id to be allowed.

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.

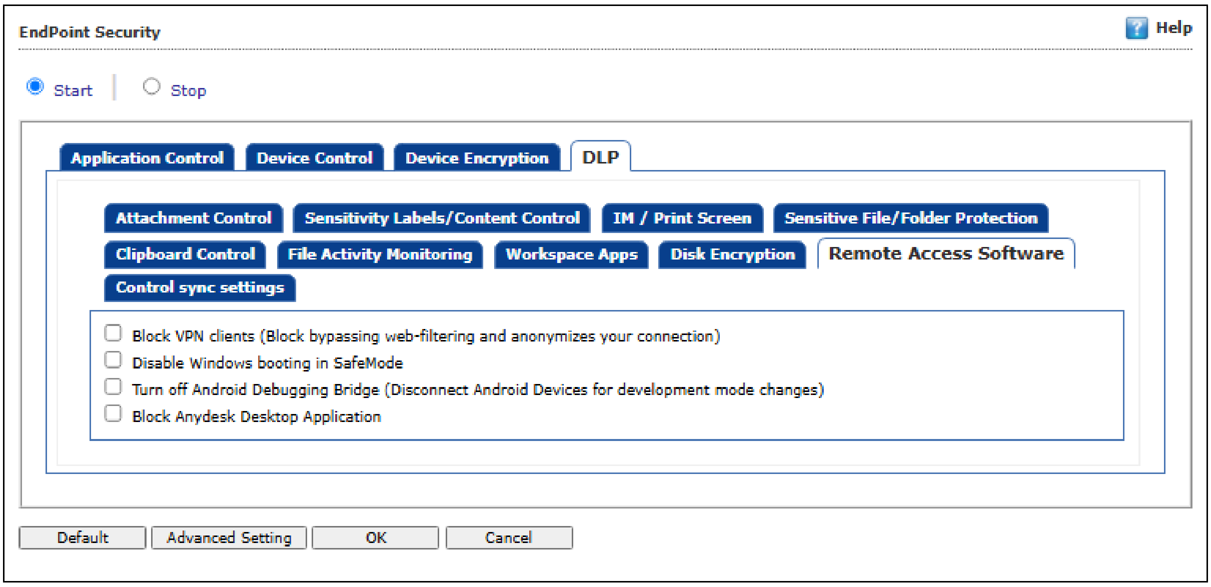
Encrypt for All File/Folders Admin

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

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

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.



□ Block VPN clients (Block bypassing web-filtering and anonymizes your connection)
□ Disable Windows booting in SafeMode
□ Turn off Android Debugging Bridge (Disconnect Android Devices for development mode changes)
□ Block Anydesk Desktop Application

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.

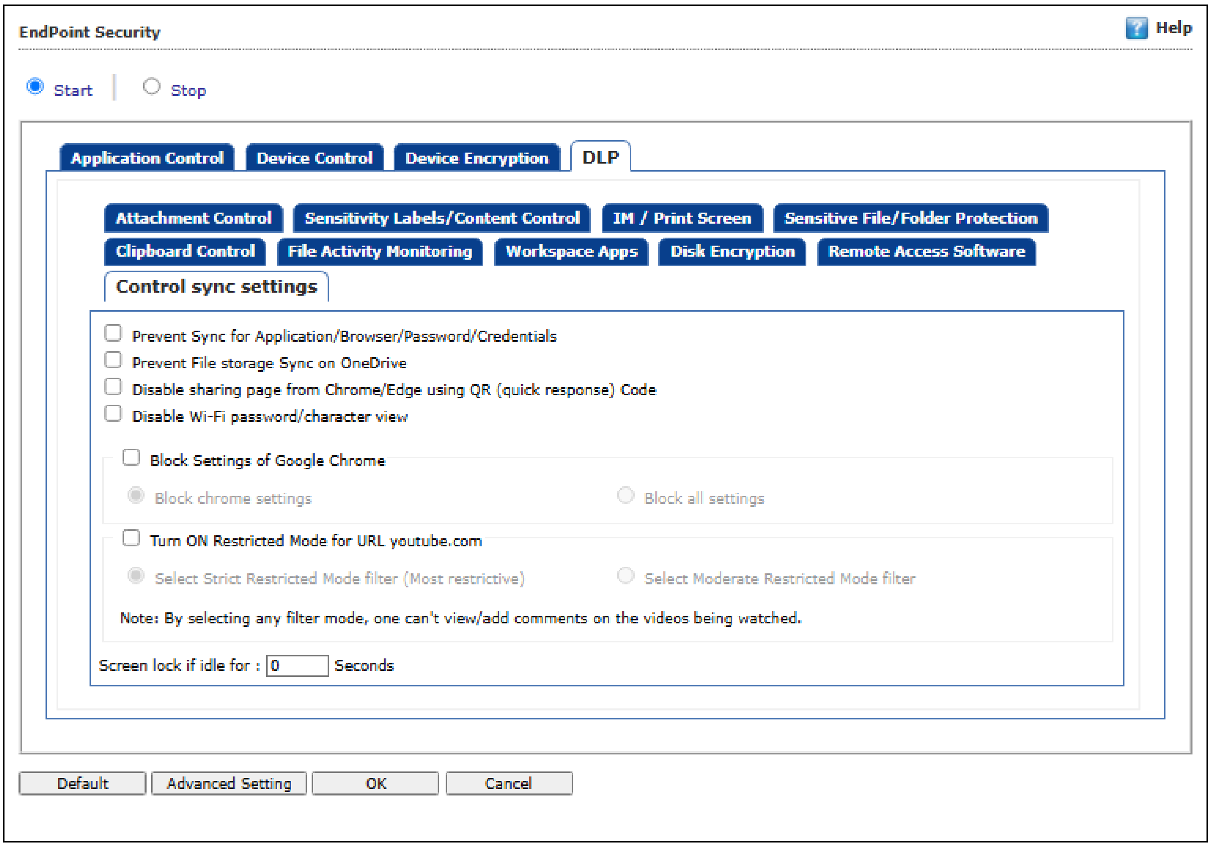
Disable Windows booting in SafeMode
It restricts booting of Windows in SafeMode on an endpoint via remote session.

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.



□ Prevent Sync for Application/Browser/Password/Credentials
□ Prevent File storage Sync on OneDrive
□ Disable sharing page from Chrome/Edge using QR (quick response) Code
□ Disable Wi-Fi password/character view

□ Block Settings of Google Chrome
● Block chrome settings ○ Block all settings

□ Turn ON Restricted Mode for URL youtube.com
● Select Strict Restricted Mode filter (Most restrictive) ○ Select Moderate Restricted Mode filter
Note: By selecting any filter mode, one can't view/add comments on the videos being watched.

Screen lock if idle for : 0 Seconds

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

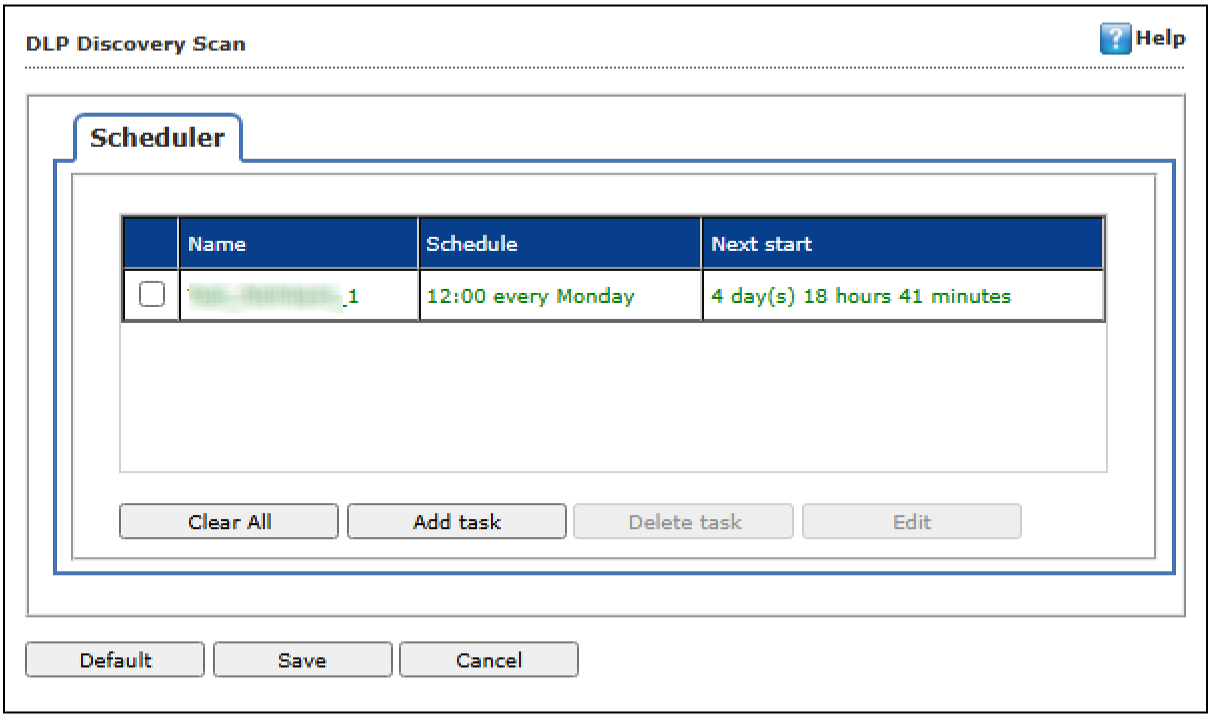
- **Select Strict Restricted Mode filter (Most restrictive):** It restricts adult videos that may contain pornography, violence, nudity, and other videos that are sensitive in nature. It is applicable for G Suite (corporate account) users.
- **Select Moderate Restricted Mode filter:** Select this option 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.

DLP Discovery (requires Enterprise DLP license)

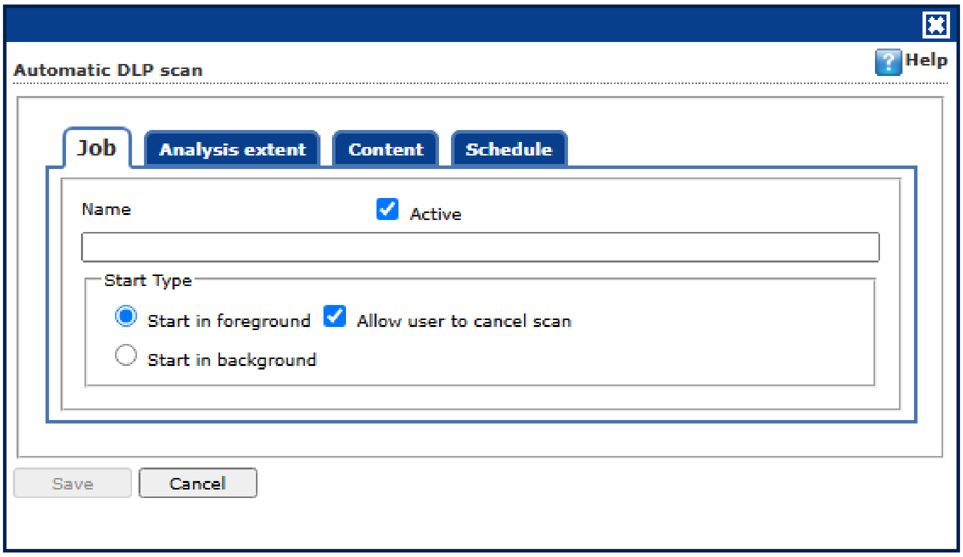
The policy Data Discovery allows you to locate and manage sensitive data across an organization's network and endpoints. It scans and generates a detailed report of your sensitive data present in the endpoints. This helps you take informed decisions regarding the same and ultimately mitigate risks associated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



	Name	Schedule	Next start
□	[redacted]_1	12:00 every Monday	4 day(s) 18 hours 41 minutes

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

   The Automatic DLP scan window opens



Automatic DLP scan

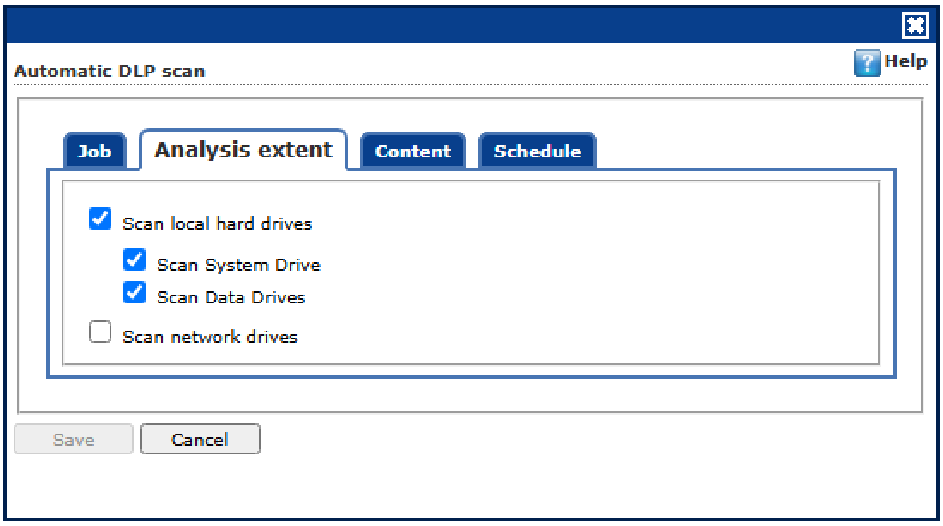
Name ☑ Active

Start Type

● Start in foreground ☑ Allow user to cancel scan

○ Start in background

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.



Automatic DLP scan

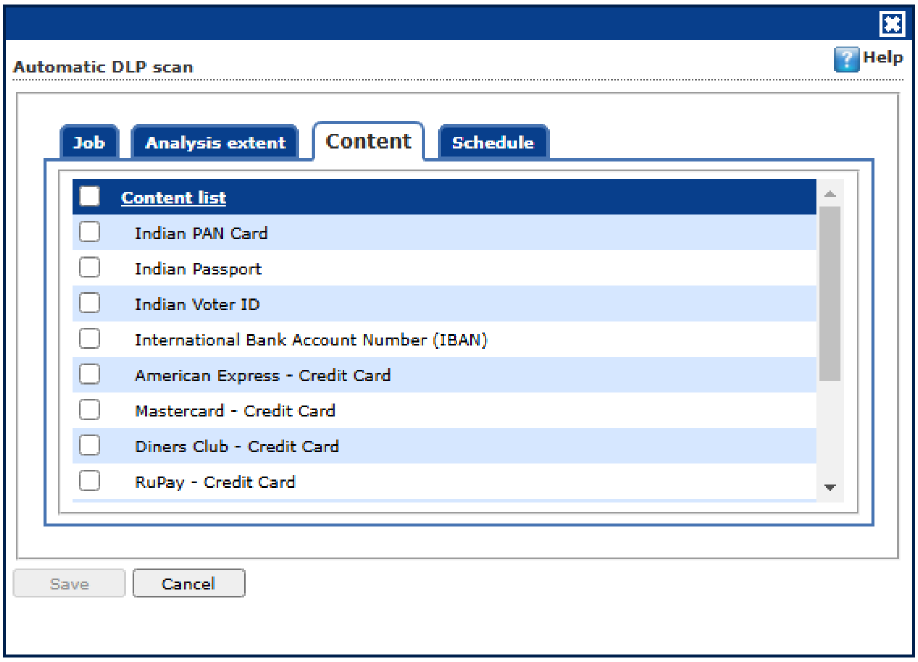
☑ Scan local hard drives

☑ Scan System Drive

☑ Scan Data Drives

☐ Scan network drives

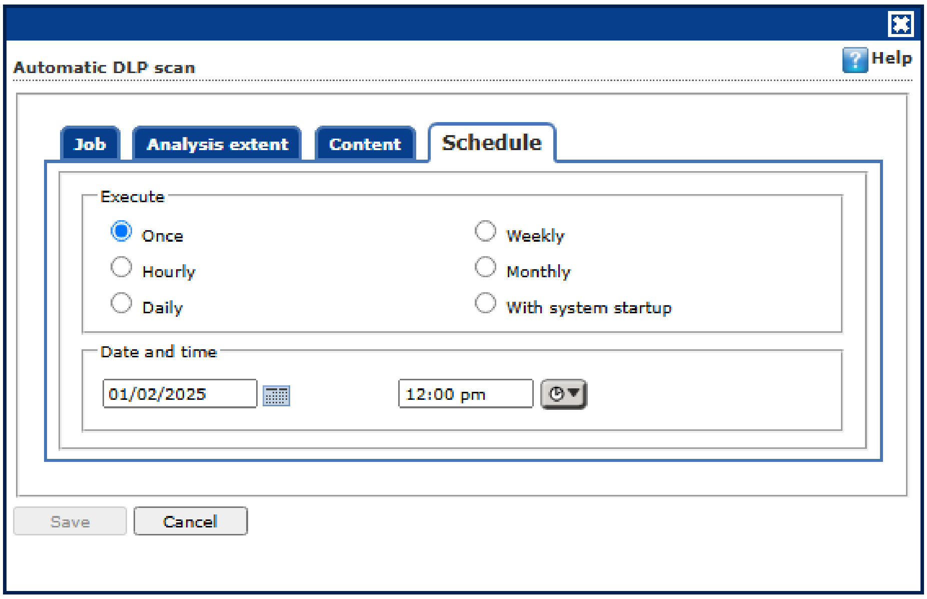
6. Under the Analysis extent tab, select target locations for scanning from system drive, data drives, or network drives.



Automatic DLP scan

- □ Content list
- □ Indian PAN Card
- □ Indian Passport
- □ Indian Voter ID
- □ International Bank Account Number (IBAN)
- □ American Express - Credit Card
- □ Mastercard - Credit Card
- □ Diners Club - Credit Card
- □ RuPay - Credit Card

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



Automatic DLP scan

Execute

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

Date and time

01/02/2025 12:00 pm

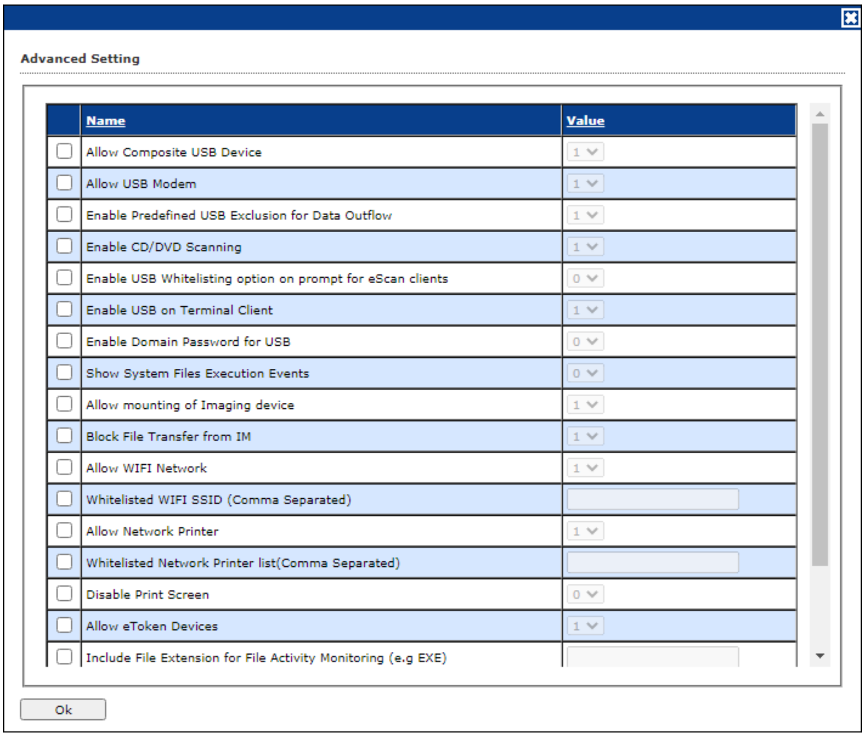
8. Under the Schedule tab, select the scan execution option from once, hourly, daily, weekly, monthly, or with system startup.
9. Define the date and time for scanning to initiate.
10. Click on **Save** to save the policy.

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.

Advanced Setting

Clicking **Advanced Setting** displays additional advanced settings.



Advanced Setting

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

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

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

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

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

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

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

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

Show System Files Execution Events (1 = Enable/0 = Disable)
Select this option 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).

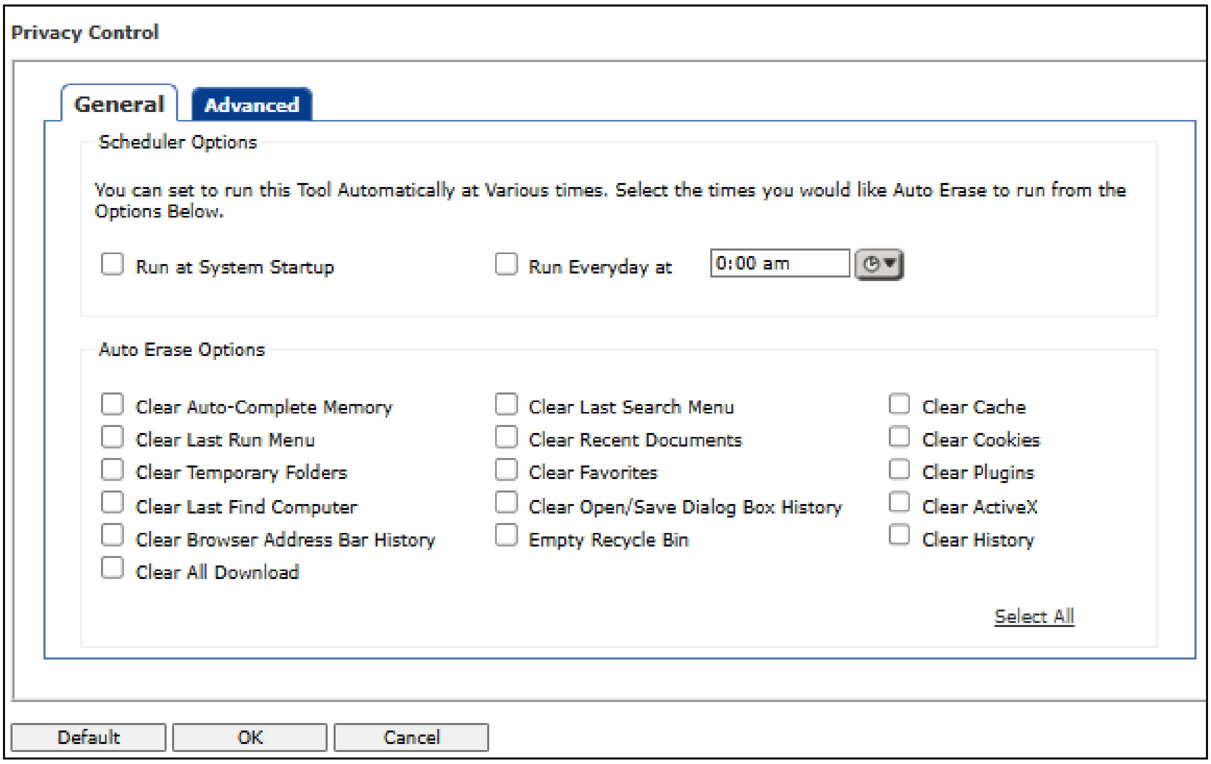
Auto Whitelist BitLocker encrypted USB Devices (1 = Enable/0 = Disable)
Select this option to allow/block auto whitelist BitLocker encrypted USB devices.

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

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

Privacy Control

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



Privacy Control

Scheduler Options

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

□ Run at System Startup
□ Run Everyday at 0:00 am

Auto Erase Options

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

It consists following tabs:

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

General tab

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

Scheduler Options

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

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

Auto Erase Options

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

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

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

Clear Temporary Folders
When you select this option, Privacy Control clears files in the Temporary folder. This folder contains temporary files installed or saved by software. Clearing this folder creates space on the hard drive 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 Files & Folders
When you select this checkbox, Privacy Control deletes selected Files and Folders. Use this option with caution as it permanently deletes unwanted files and folders from the computer to free space on the computer.

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

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

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

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

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

Clear Plugins

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

Clear ActiveX

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

Clear History

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

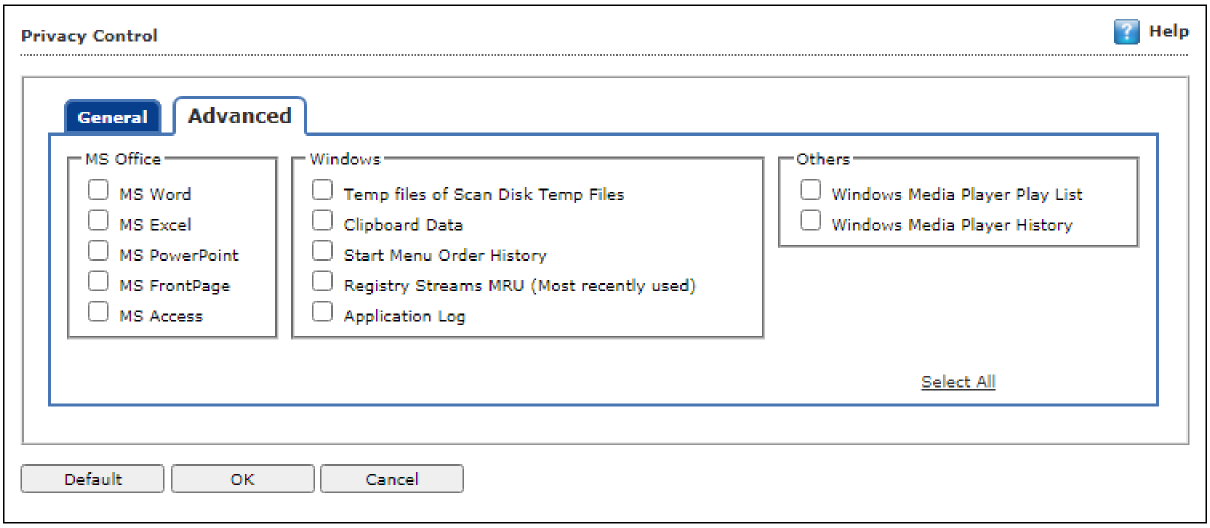
In addition to these options, the **Auto Erase Options** section has below option as well.

Select All/ Unselect All

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

Advanced tab

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



Privacy Control

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

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

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

MS Office

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

Windows

The respective unwanted files like temp files will be cleared.

Others

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

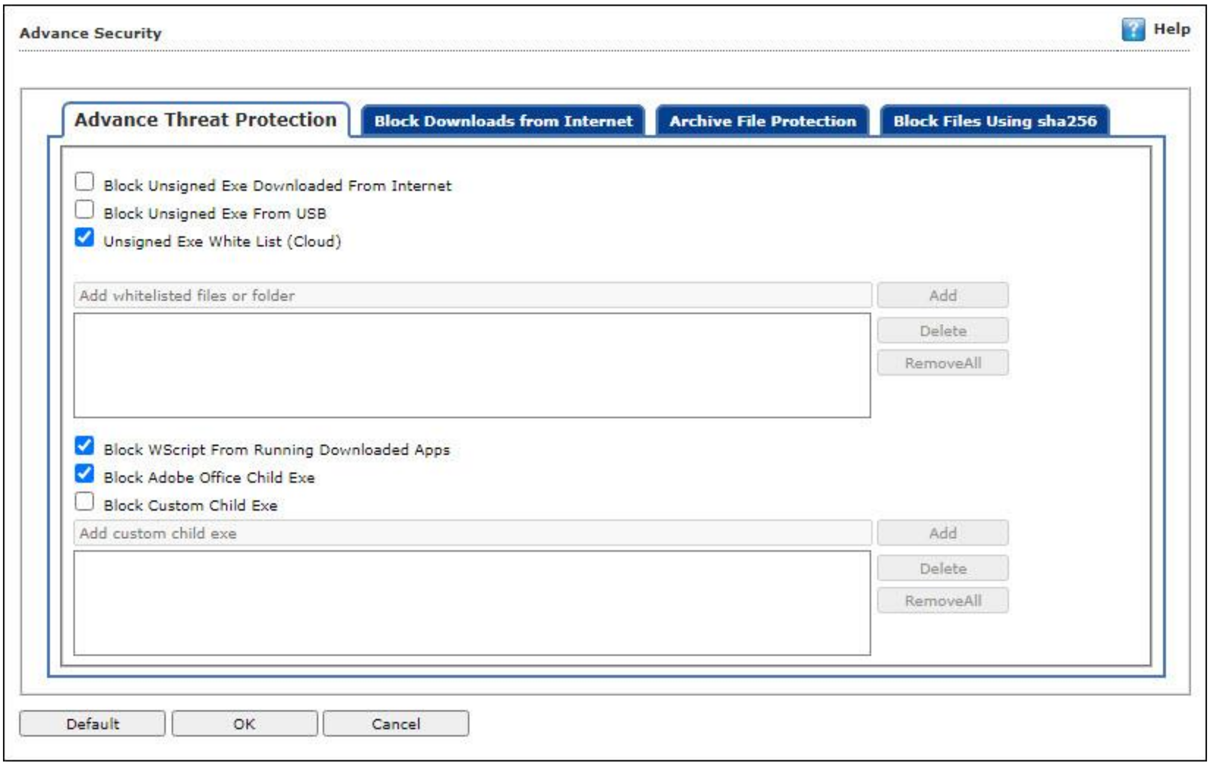
NOTE	Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.

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

Advance Security policy

As an advanced security measures, this policy provides you with multiple threat protection options. Through the Advance Security policy, you can safeguard the endpoints by blocking Unsigned Exe files, WScripts, Child Exe, Internet downloaded files, and Archive files. It also offers the SHA256 protection to the networked computers. This module consist of following tabs to configure:

- Advance Threat Protection
- Block Downloads from Internet
- Archive File Protection
- Block Files Using sha256



Advance Security

□ Block Unsigned Exe Downloaded From Internet
□ Block Unsigned Exe From USB
☑ Unsigned Exe White List (Cloud)

Add whitelisted files or folder

☑ Block WScript From Running Downloaded Apps
☑ Block Adobe Office Child Exe
□ Block Custom Child Exe

Add custom child exe

Advance Threat Protection

This tab allows you to block the execution of EXE files downloaded from Internet or present in the USB devices. Along with this, you can restrict the WScript and Adobe reader from the execution of child processes.

Block Unsigned Exe Downloaded from Internet

This option blocks the execution of untrusted/unknown executable files downloaded from the internet.

Block Unsigned Exe from USB

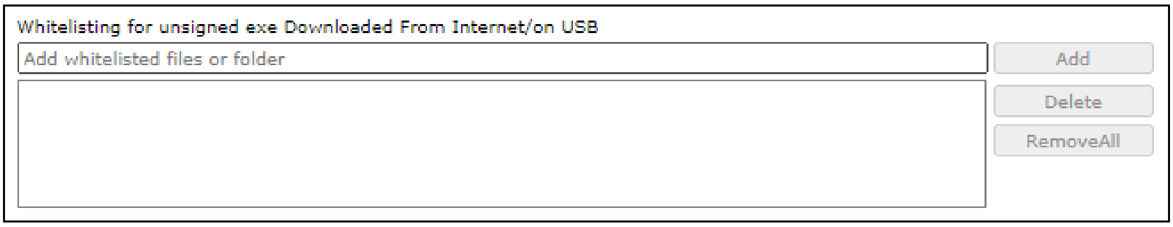
This option blocks the execution of untrusted/unknown executable files from portable storage devices like USB drives.

Unsigned Exe White list (Cloud)

This option allows the execution of whitelisted executable files based on the eScan Cloud database. It is enabled by default.

Whitelisting for unsigned exe Downloaded From Internet/on USB

This option allows the user to whitelist the unknown executable files. After enabling the above listed options, you can configure this option:



Whitelisting for unsigned exe Downloaded From Internet/on USB

Add whitelisted files or folder

- **Add**: To add an unknown executable file, enter the name of the file and click **Add.** The file will be added in the list.
- **Delete:** To delete an executable file, select the particular file from the list and click **Delete**.
- **Remove All**: To remove all the files from the list, click **Remove All**.

Block WScript From Running Downloaded Apps

This option allows you to blocks the execution of any potentially malicious scripts (.js, PowerShell) that running from the downloaded apps.

Block Adobe Office Child Exe

This option allows you to block the generation of any child process (VB macros, exploit code, PowerShell commands) by Adobe Reader and Office apps.

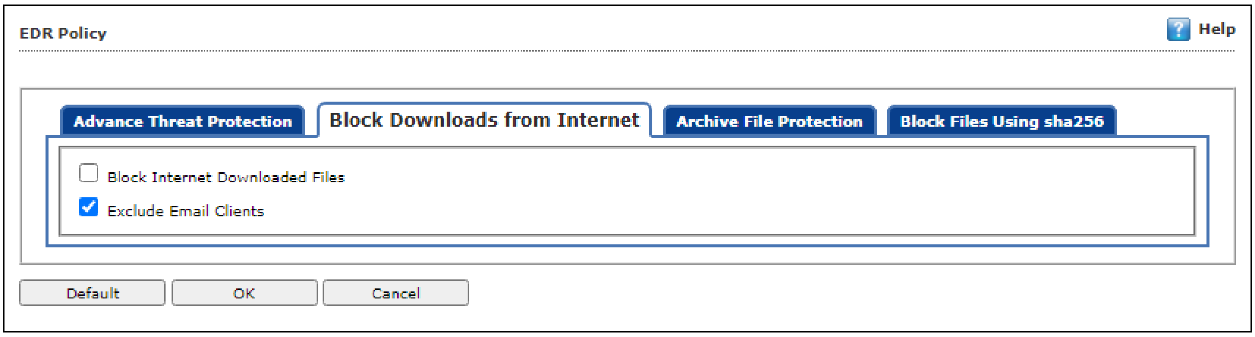
Block Custom Child Exe

This option lets you to add or delete the custom child EXE.
After enabling this option, you can configure the following options:

- **Add**: To add custom child EXE, enter the name and click **Add**.
- **Delete**: To delete any child EXE, select the file and click **Delete**.
- **Remove All**: To remove all the file at once, click **Remove All**.

Block Downloads From Internet

This tab allows you to block or restrict the internet downloaded files and files downloaded from email clients.



EDR Policy

□ Block Internet Downloaded Files

☑ Exclude Email Clients

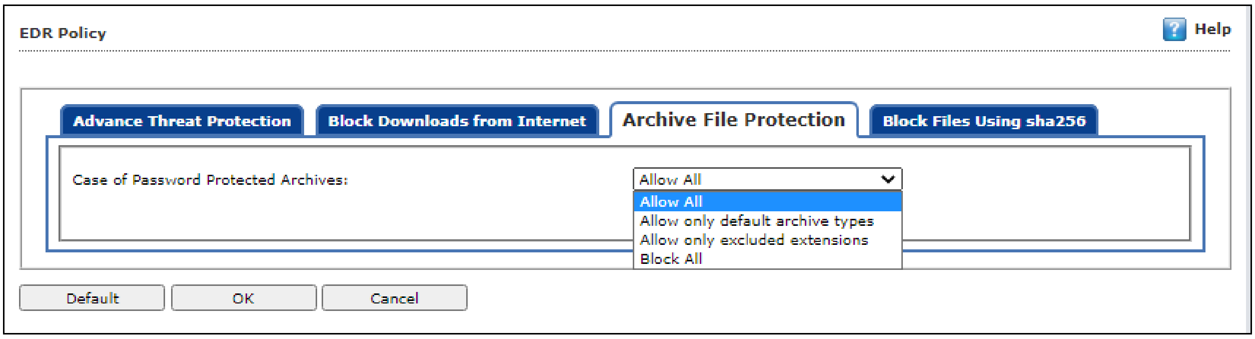
Block Internet Downloaded Files

This option allows you to directly block the files while downloading from internet.

Exclude Email Clients
This option allows the execution of attachment and auto-run executable files that are downloaded via email clients (Outlook, Thunderbird, and more). It is enabled by default.

Archive File Protection

This tab allows or blocks the running of password-protected archive files (zip, rar, 7zip, and more).


EDR Policy
Help
Advance Threat Protection
Block Downloads from Internet
Archive File Protection
Block Files Using sha256
Allow All
Allow only default archive types
Allow only excluded extensions
Block All
Default
OK
Cancel

Case of Password Protected Archives: Allow All

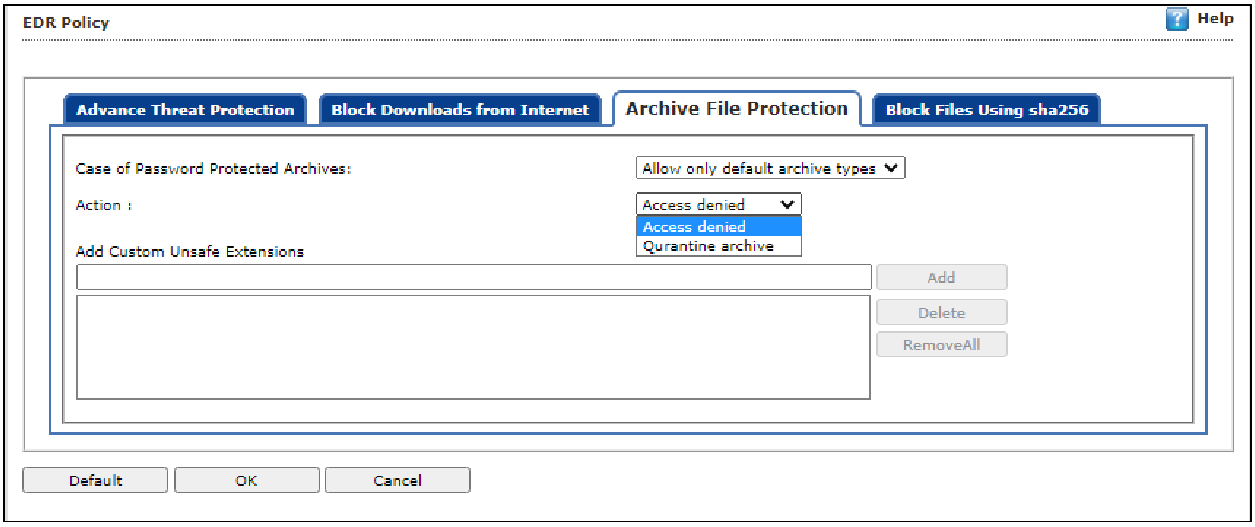
Following options can be configured:

Allow All

This option is enabled by default and allows running of all the password-protected archive files.

Allow only default archive types

This option allows the access of only default archive types and file name with extensions that are added in the list.



Case of Password Protected Archives: Allow only default archive types

Action : Access denied

Action

This drop-down option allows you to select the action to be taken in case of password protected archive file that does not belong to default type or whitelisted file extensions.

- **Access Denied:** This option will deny the access to the archive files that are not default type or whitelisted file extensions.
- **Quarantine archive:** This option will quarantine all the archive files other than default types or whitelisted file extensions.

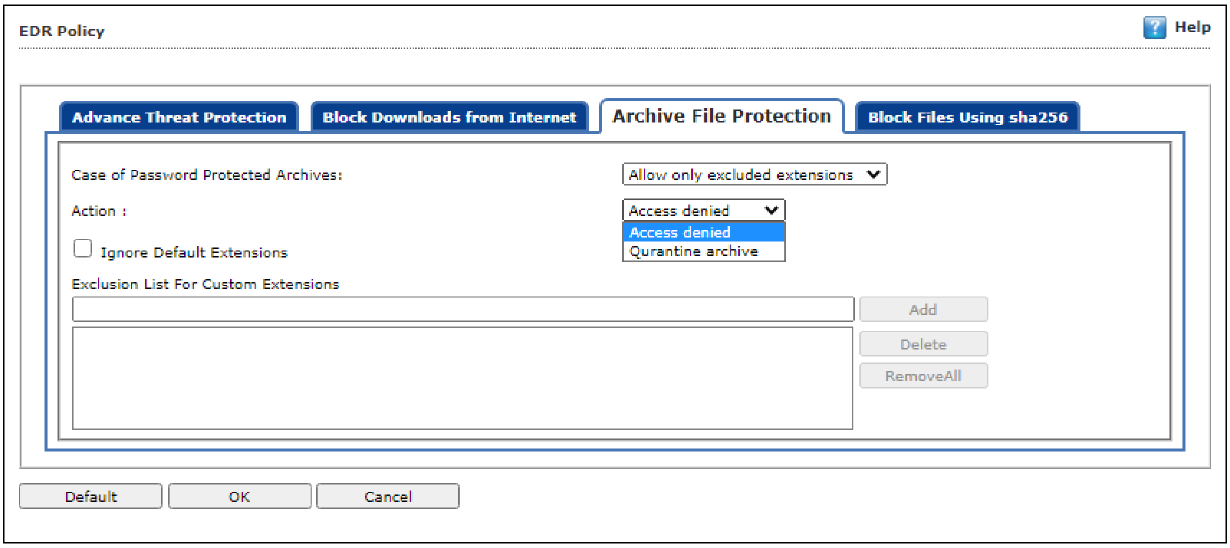
Add Custom Unsafe Extensions

This option allows you to add custom unsafe archive in the list.

- **Add**: To add custom unsafe extension, enter the extension and click **Add**.
- **Delete**: To delete any custom extension, select the extension and click **Delete**.
- **Remove All**: To remove all the extension at once, click **Remove All**.

Allow only excluded extensions

This option allows the access of only the archive files extensions that are added in the excluded list.



Case of Password Protected Archives: Allow only excluded extensions

Action : Access denied

Access denied
Qurantine archive

☐ Ignore Default Extensions

Exclusion List For Custom Extensions

Action

This drop-down option allows you to select the action to be taken in case of password-protected archive file that does not belong to excluded file extensions.

- **Access Denied:** This option will deny the access to the archive files that are not added in the exclusion list.
- **Quarantine archive:** This option will quarantine all the archive files that are not added in the exclusion list.

Ignore Default Extensions

This checkbox will allow the access of default archive extensions by including them in the blacklist.

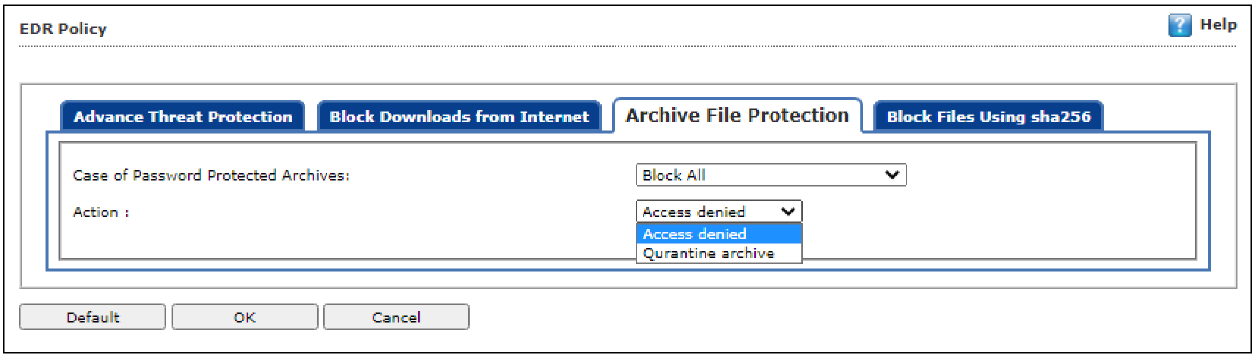
Exclusion List for Custom Extensions

This option allows you to add custom extension file type in the list.

- **Add**: To add custom extension, enter the extension and click **Add**.
- **Delete**: To delete any custom extension, select the extension and click **Delete**.
- **Remove All**: To remove all the extension at once, click **Remove All**.

Block All

This option blocks the access of all the password-protected archive files types.



EDR Policy

Case of Password Protected Archives: Block All

Action : Access denied

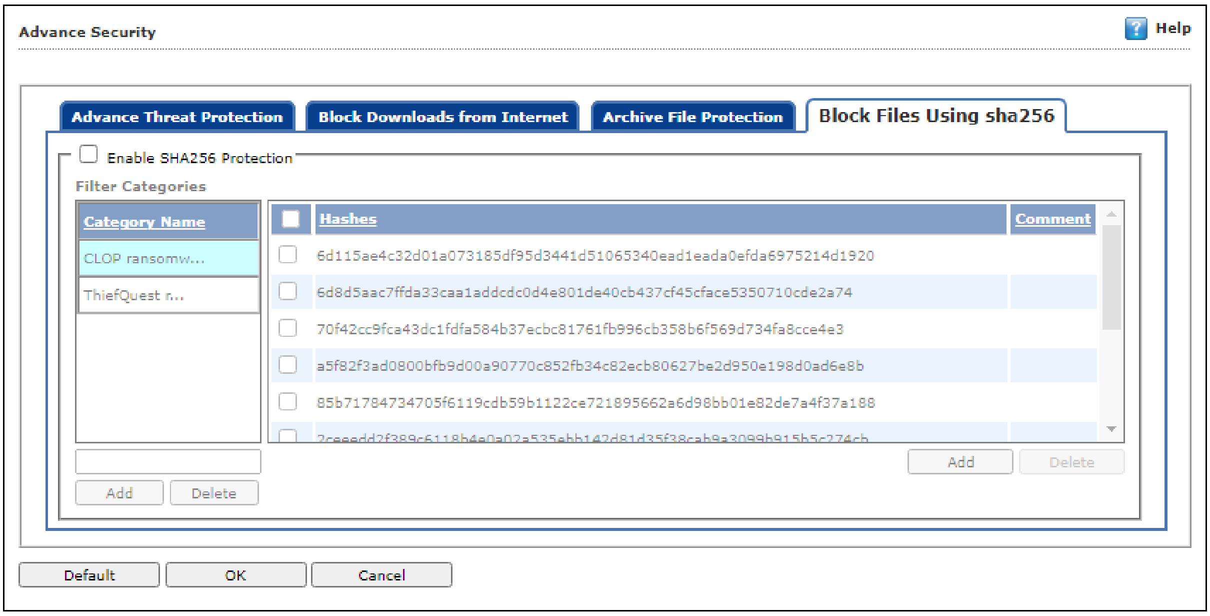
Action

This drop-down option allows you to select the action to be taken on the password-protected archive file types.

- **Access Denied:** This option will deny the access to all the password-protected archive files.
- **Quarantine archive:** This option will quarantine all the password-protected archive files.

Block Files Using sha256

This tab allows you to block the files that are encrypted using SHA256 encryption based on the hash value of it.



Advance Security

☐ Enable SHA256 Protection

Filter Categories

Category Name
CLOP ransomw...
ThiefQuest r...

☐	Hashes	Comment
☐	6d115ae4c32d01a073185df95d3441d51065340ead1eada0efda6975214d1920	
☐	6d8d5aac7ffda33caa1addcdc0d4e801de40cb437cf45cface5350710cde2a74	
☐	70f42cc9fca43dc1fdfa584b37ecbc81761fb996cb358b6f569d734fa8cce4e3	
☐	a5f82f3ad0800bfb9d00a90770c852fb34c82ecb80627be2d950e198d0ad6e8b	
☐	85b71784734705f6119cdb59b1122ce721895662a6d98bb01e82de7a4f37a188	
☐	2ceeedd2f389c6118b4e0a02a535ebb142d81d35f38cab9a3099b915b5c274cb	

Enable SHA256 Protection

This option lets you enable the SHA256 protection to block the files having identical hash key.

Filter Categories

This option will be enabled after selecting the **Enable SHA256 Protection** option. You can use this option to add or remove SHA256 categories and the hash values that has been added to the particular category.

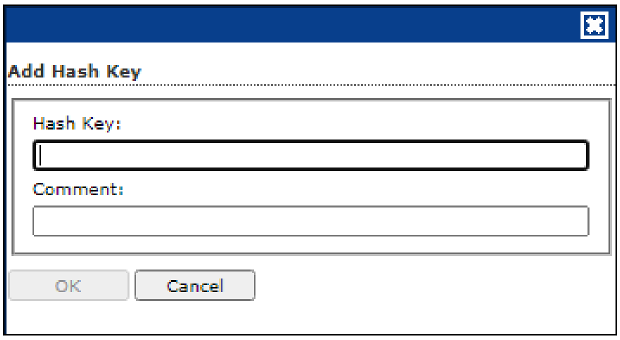
Category Name

- **Add**: To add a filter category, enter the category name and click **Add**.
- **Delete**: To remove filter category, select the category name and click **Delete**.

Hash files

To add/remove the hash file in particular category, select the category and then add or delete the file.

- **Add**: To add a hash value, select the category in the **Category Name** column. Enter the hash value and comment (optional) and click **OK**.



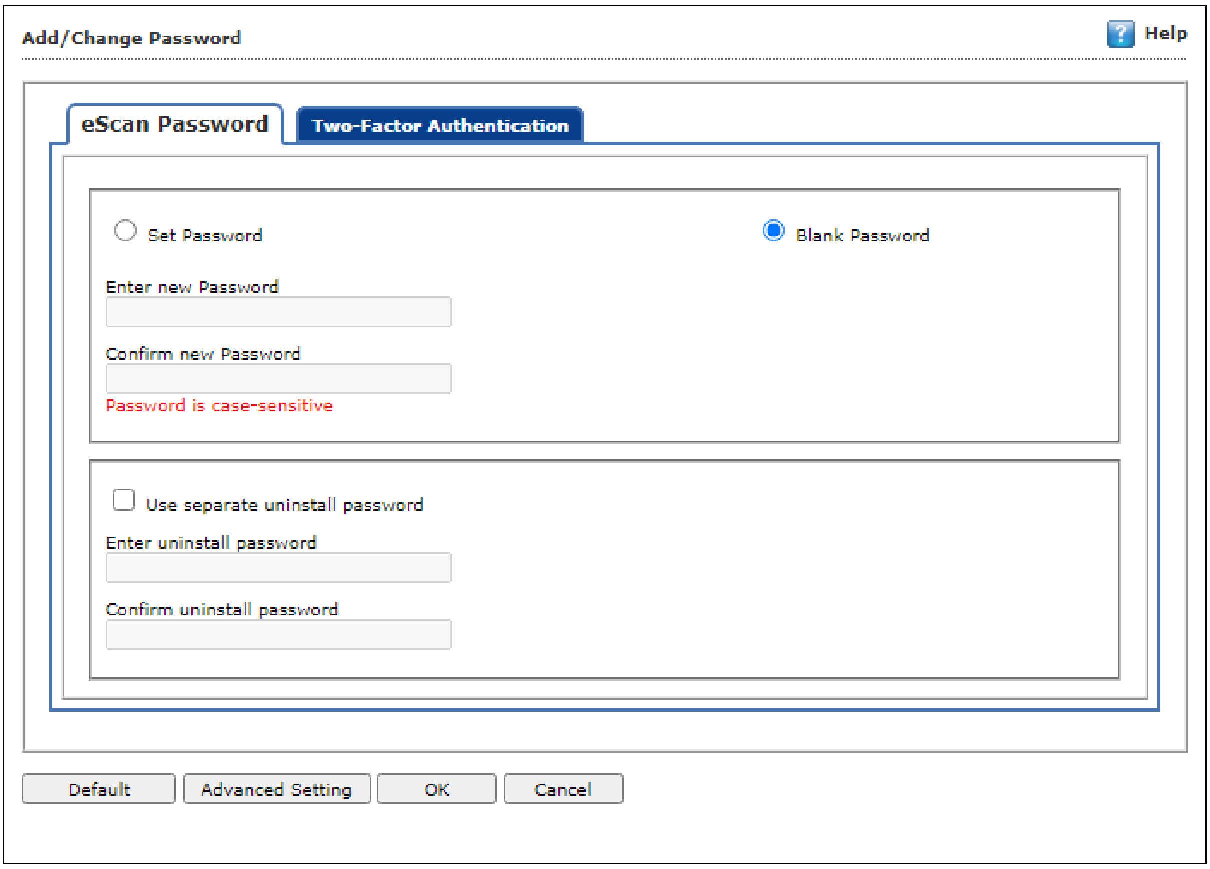
- **Delete**: To remove a hash file, select the category in the **Category Name** column. Select the hash file and click **Delete**.

Administrator Password

Administrator Password policy in eScan Vision Core XDR lets you create and change password for administrative login of eScan Protection Center and Two-Factor Authentication.

eScan Password

Select the option **Set Password** and define a password as per your choice. It also lets you keep the password as blank, wherein you can login to eScan Protection Center without entering any password for read-only access.



Add/Change Password

○ Set Password ● Blank Password

Enter new Password

Confirm new Password

Password is case-sensitive

□ Use separate uninstall password

Enter uninstall password

Confirm uninstall password

Below are the mandatory criteria for strong password creation:

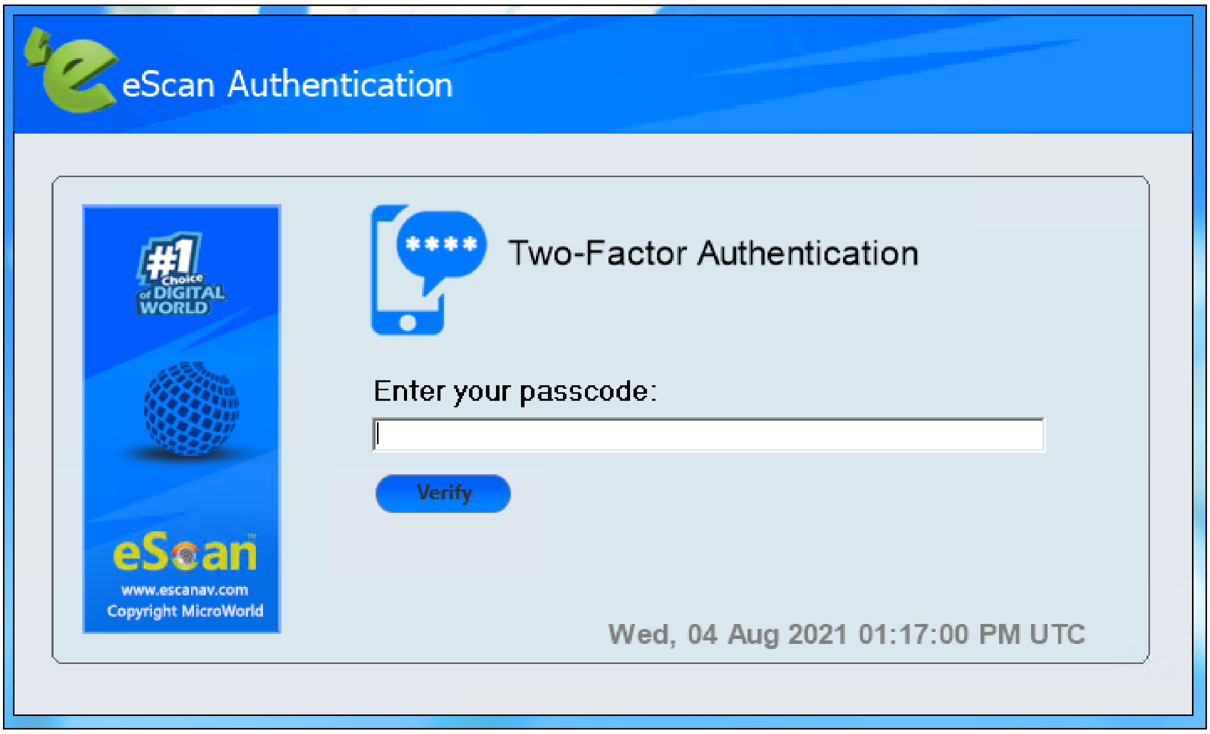
Password length: The password length should be of minimum 8 characters.
Lowercase: The password must contain at least 1 letter in Lowercase (a-z).
Uppercase: The password must contain at least 1 letter in Uppercase (A-Z).
Numeric: The password must contain at least 1 digit (0-9).
Special character: The password must contain at least 1 special character ($ @ ! % * # ? _ &).
Password match: Both the entered passwords should be matching.

Additionally, there is an option to set an uninstall password. An uninstall password prevents unauthorized uninstallation of eScan client from the endpoint. Upon selecting Uninstall option, eScan asks for uninstall password before proceeding further. To set an uninstall password, select checkbox **Use separate uninstall password**.

Two-Factor Authentication (2FA) (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.

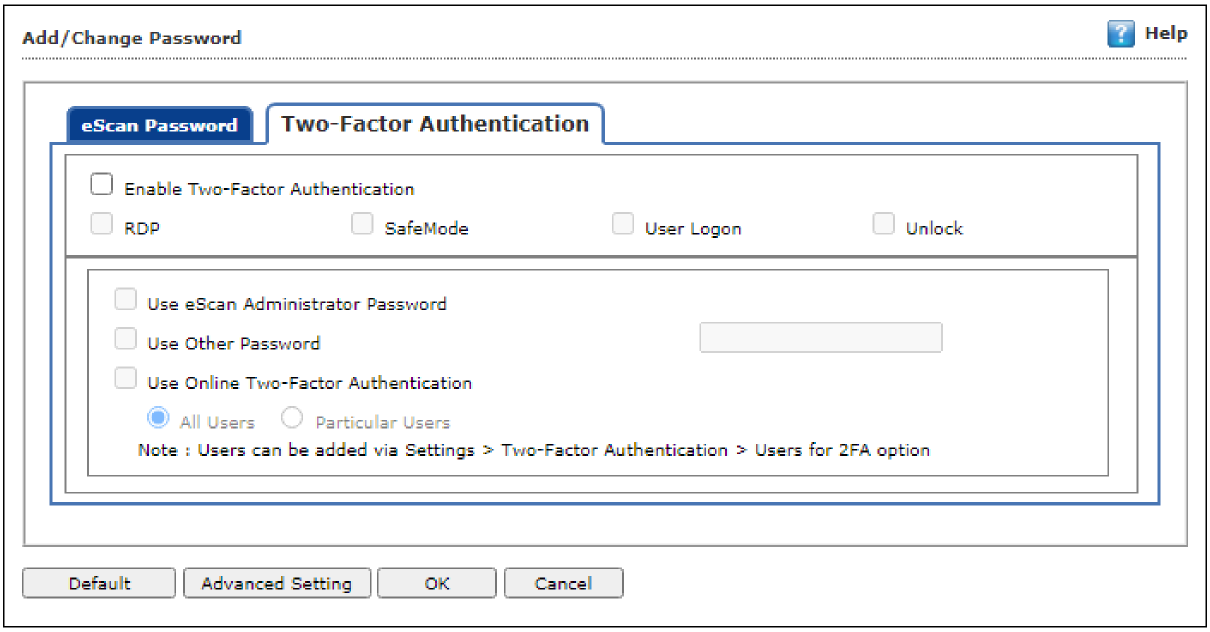


To enable the Two-Factor Authentication feature, follow the steps given below:

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

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

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



Add/Change Password

eScan Password | Two-Factor Authentication

□ Enable Two-Factor Authentication

□ RDP □ SafeMode □ User Logon □ Unlock

□ Use eScan Administrator Password

□ Use Other Password

□ Use Online Two-Factor Authentication

● All Users ○ Particular Users

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

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

Login Scenarios

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

RDP

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

Safe Mode

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

Local Logon

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

Unlock

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

Password Types

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

Use eScan Administrator Password

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

Use Other Password

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

Use Online Two-Factor Authentication

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

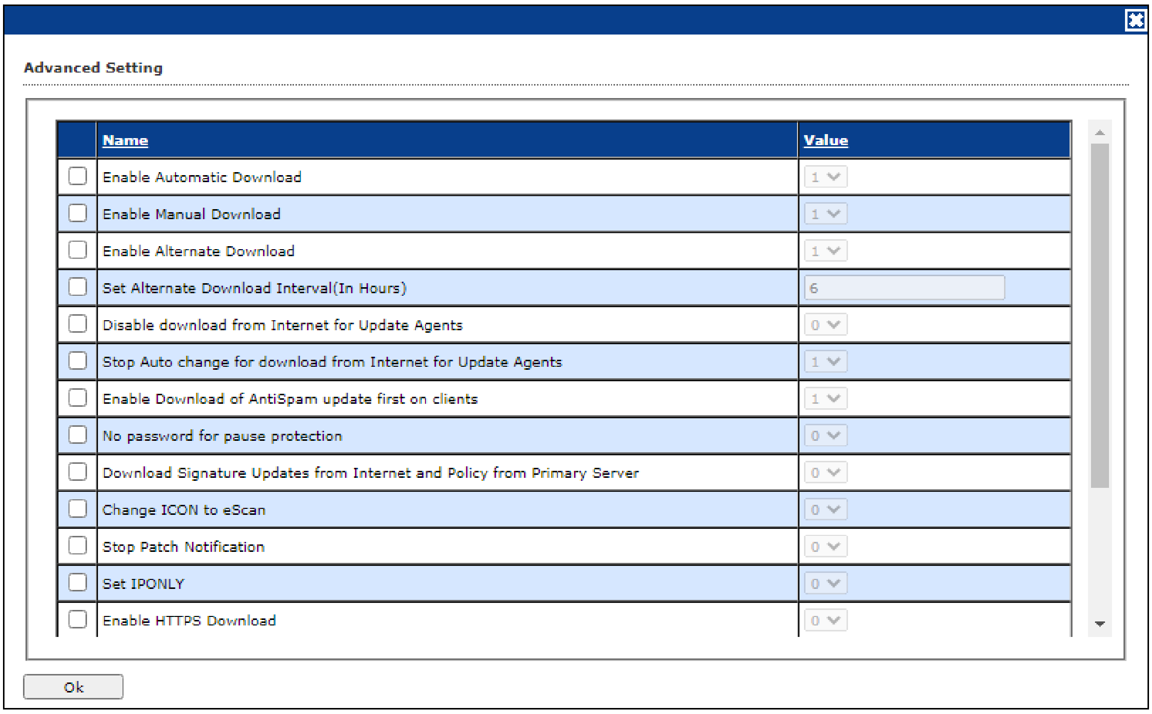
NOTE	Users can be added via **Settings** > **Two-Factor Authentication** > **Users for 2FA** option.

To use this feature, follow the steps given below:

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

Advanced Setting

Clicking **Advanced Setting** displays additional advanced settings.



Advanced Setting

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

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

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

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

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

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

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

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

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

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

No password for pause protection
Selecting this option lets you pause the eScan protection without entering password.

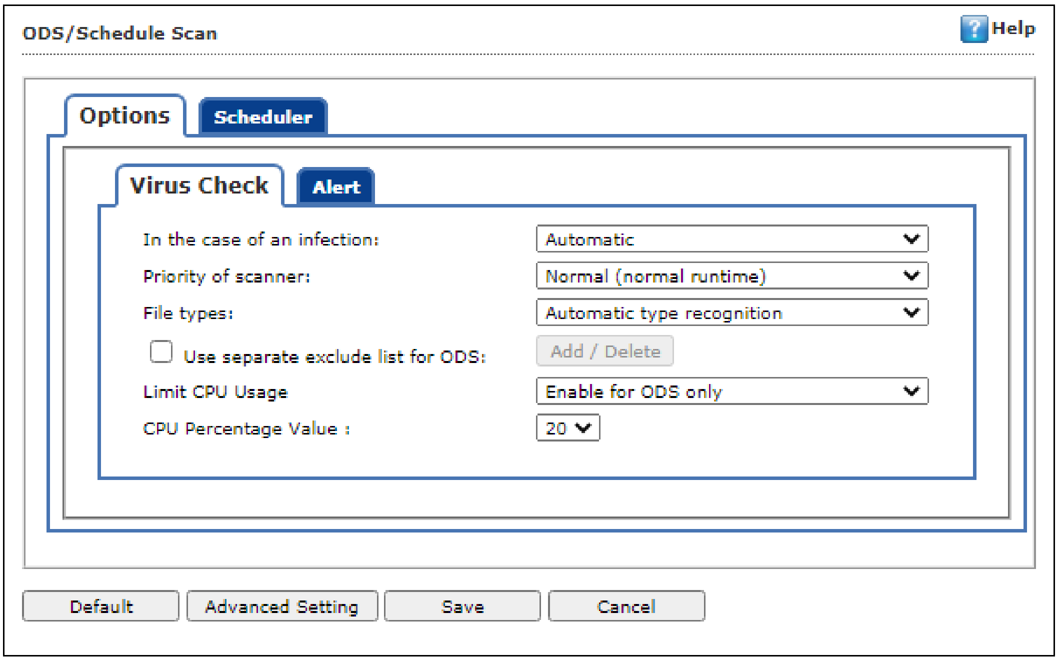
ODS/Schedule Scan

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

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

It consists following tabs:

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



In the case of an infection: Automatic
Priority of scanner: Normal (normal runtime)
File types: Automatic type recognition
☐ Use separate exclude list for ODS:
Limit CPU Usage: Enable for ODS only
CPU Percentage Value : 20

Options

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

- Virus Check
- Alerts

Virus Check

It lets you configure the settings for checking viruses.

To set Virus Check:

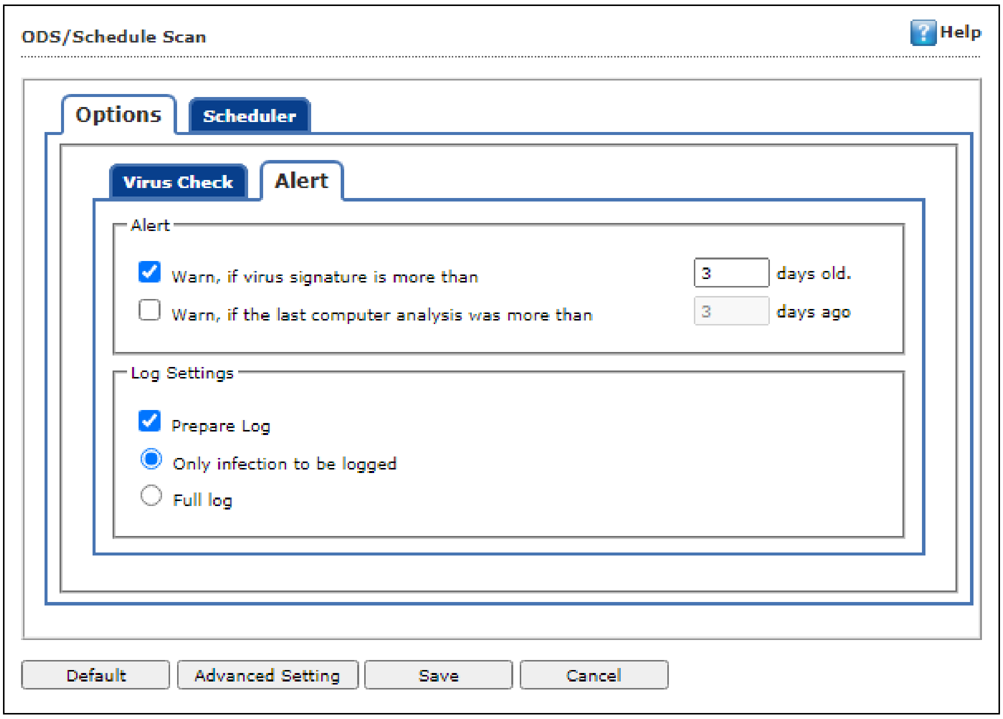
1. Specify the following field details:
    - **In the case of an infection**: Select an appropriate option from the drop-down list. For example, Log only, Delete infected file, and Automatic [Default]. If the option Automatic is selected, eScan will quarantine the infected file. In this case, if the action Delete object is selected in File Anti-Virus module, the object will be deleted.
    - **Priority of scanner**: Select an appropriate option from the drop-down list. For example,
        - High (short runtime)

  - ○ Normal (normal runtime) [Default]
  - ○ Low (long runtime)
- **File types**: Select an appropriate option from the drop-down list. For example, \[Default\] Automatic type recognition and only program files.
- **Use separate exclude list for ODS**: Select this option to add a list of file/folders that should be excluded from scan.

2. Click **Save**.

Alerts tab

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



Alert

☑ Warn, if virus signature is more than 3 days old.

□ Warn, if the last computer analysis was more than 3 days ago

Log Settings

☑ Prepare Log

● Only infection to be logged

○ Full log

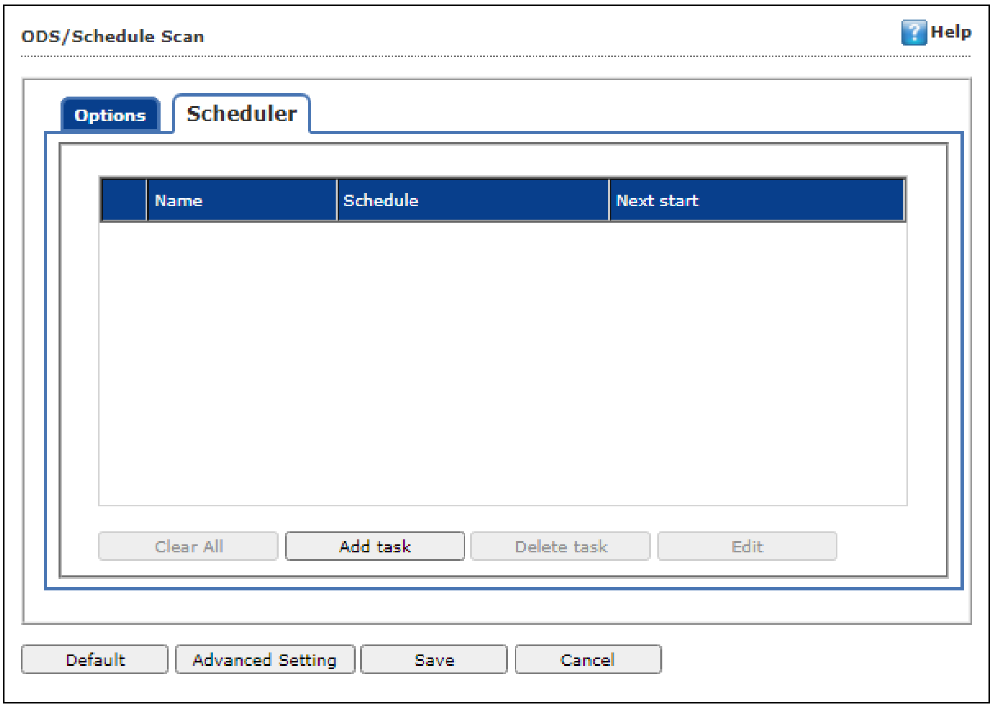
To set alerts,

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

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

Scheduler

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



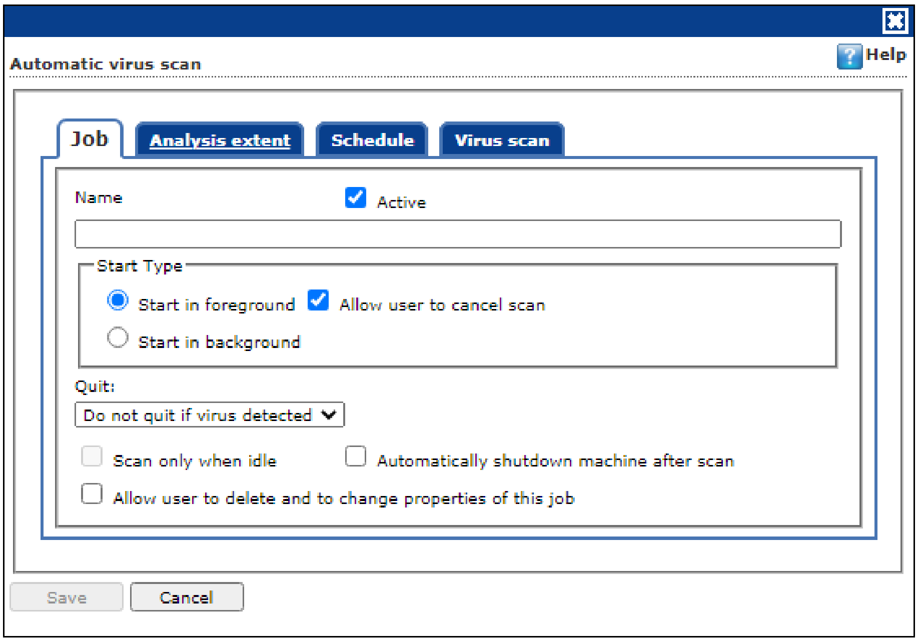
ODS/Schedule Scan

	Name	Schedule	Next start

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

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

Add Task



Automatic virus scan

Name ☑ Active

Start Type

● Start in foreground ☑ Allow user to cancel scan

○ Start in background

Quit: Do not quit if virus detected

□ Scan only when idle □ Automatically shutdown machine after scan

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

Automatic Virus Scan window lets you do following activities:

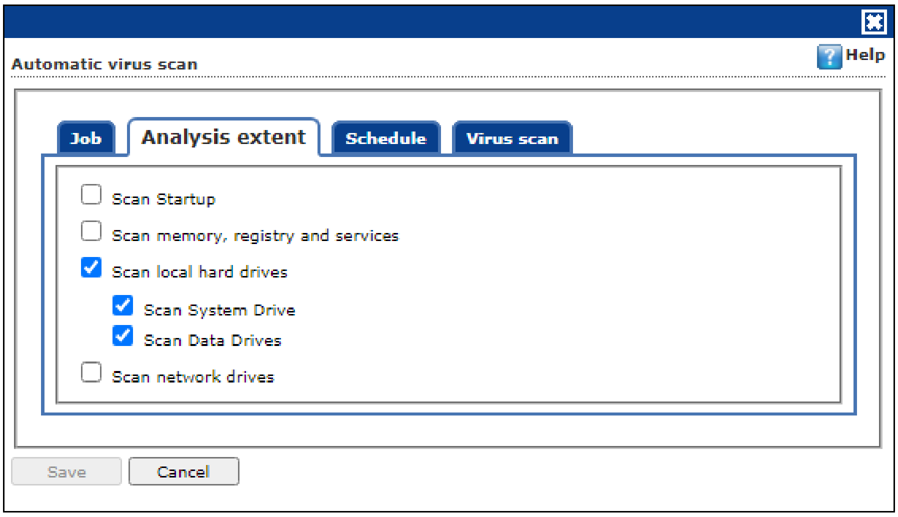
a) Creating job

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

a) Job
It lets you create the job details for virus scanning.

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

b) Analysis Extent
It lets you configure analysis extent settings for virus scanning.

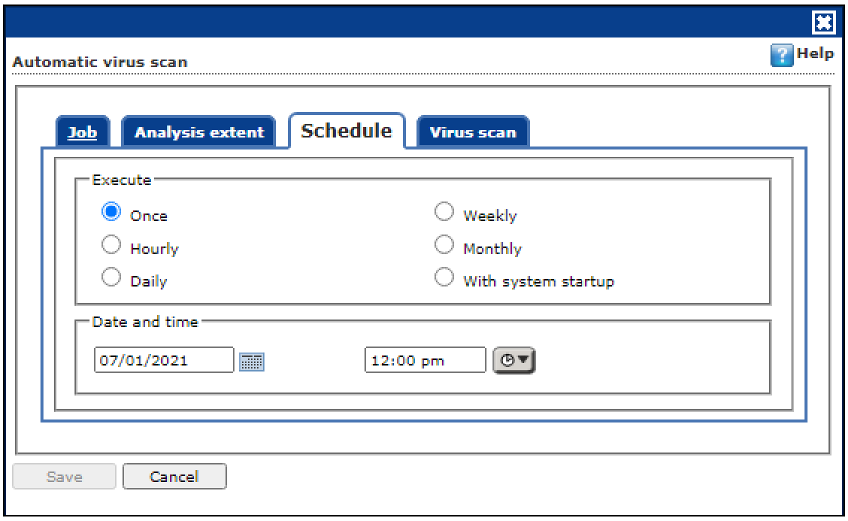


Automatic virus scan

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

1. Click the **Analysis Extent** tab.
2. Select the **Scan Startup** option, if you want to scan all startup entries.
3. Select the **Scan memory, registry** and **services** option, if you want to scan memory, registry and services.
4. Select the [Default] **Scan local hard drives** option, if you want to scan local hard drives.
5. Select Scan network drives option, if you want to scan network drives. Users should note that scanning a network drive may affect system performance.
6. Click **Save**.

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



Automatic virus scan

Execute

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

Date and time

07/01/2021 12:00 pm

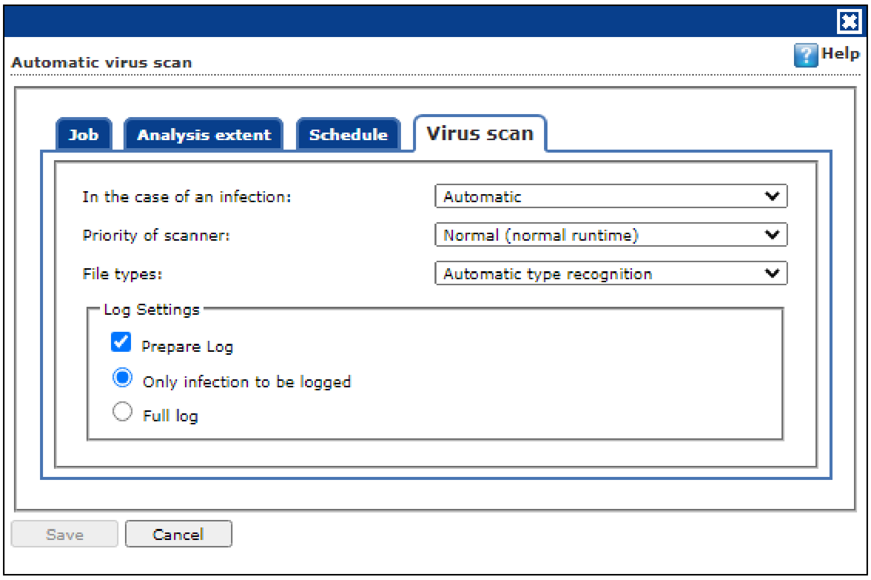
1. Click **Schedule** tab.
2. Under Execute section, select an appropriate option. For example, [Default] Once, weekly, hourly, and so on.
3. Under Date and time section, click the calendar icon. The calendar appears.
4. Select an appropriate date from the calendar.

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

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

d) Virus Scan

It lets you schedule virus scanning.



Automatic virus scan

In the case of an infection: Automatic

Priority of scanner: Normal (normal runtime)

File types: Automatic type recognition

Log Settings

☑ Prepare Log

● Only infection to be logged

○ Full log

1. Click the **Virus Scan** tab.

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

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

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

Advanced Setting

Autorun System Scanning if System not scanned for days defined
This option let you define days for autorun system scanning if system is not scanned.

Ignore Battery Status
Select this option to Ignore Battery Status.

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

Remove LNK
This option lets you Enable/Disable Removal of LNK.

Start Background Scan in System Mode
Select this option to start background scan in system mode**.**

Enable Scan Caching
This option lets you Enable/Disable scanning of cache.

Check for Corrupted Files
Select this option to check for corrupted files.

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

Enable Unhiding of USB Files & Folder
This option let you enable/disable unhiding USB files & folders.

Enable Missed schedule scan JOB’s to run
This option let you enable/disable missed schedule scan JOB’s to run.

MWL (MicroWorld WinSock Layer)

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

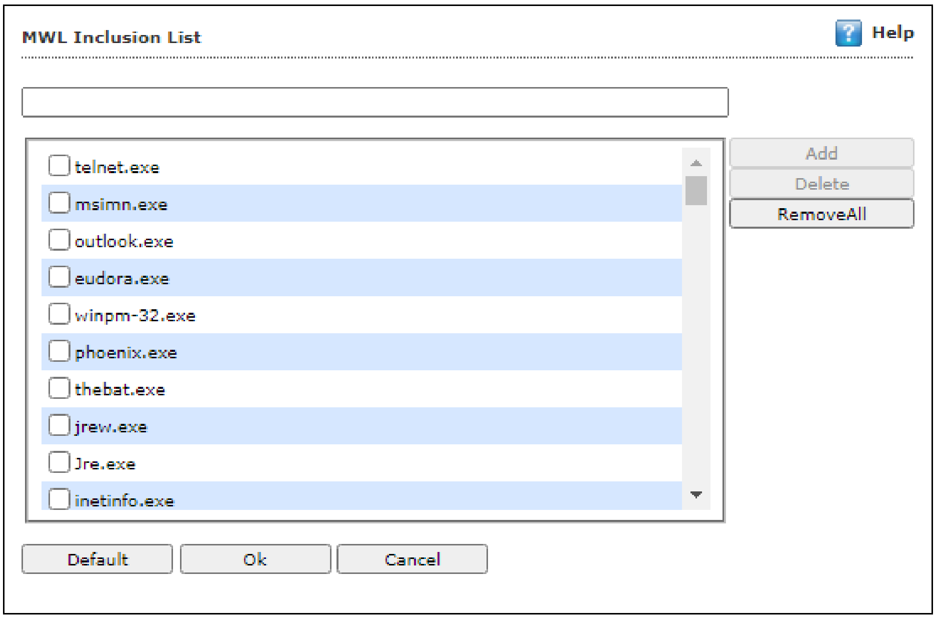
MWL Inclusion List

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

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

You can do the following activities.

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



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

Add files to Inclusion List

To add executable files to the Inclusion List,

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

Delete files from Inclusion List

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

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

Remove all files from Inclusion List

To remove all executable files from the Inclusion List,

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

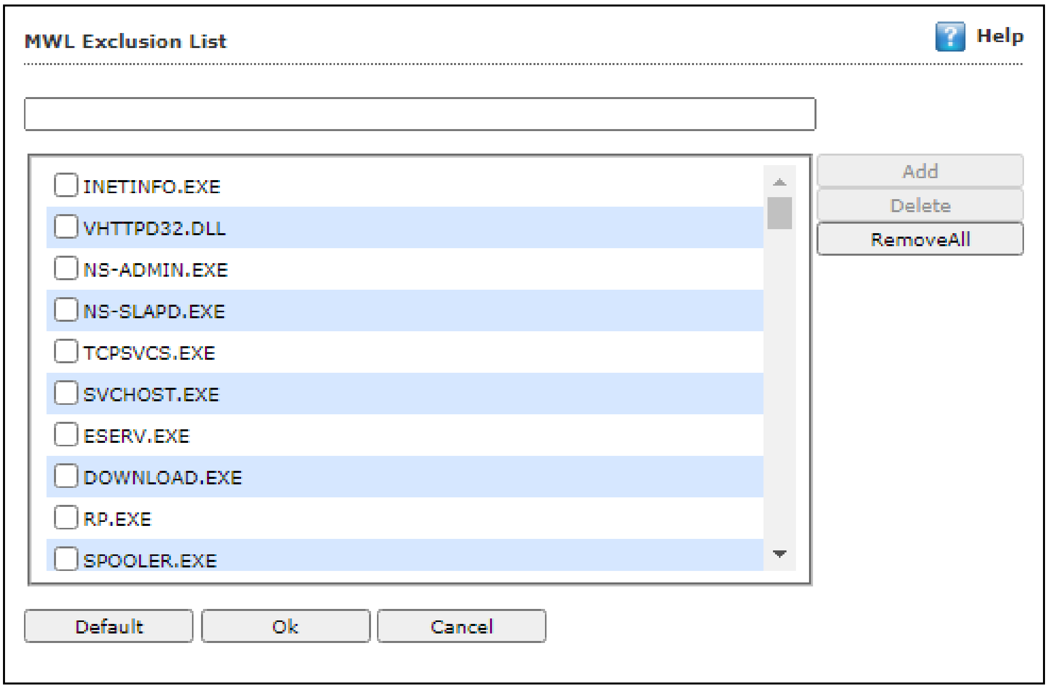
MWL Exclusion List

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

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

You can do the following activities:

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



MWL Exclusion List

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

Adding files to Exclusion List

To add executable files to the Exclusion List:

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

Deleting files from Exclusion List

To delete executable files from the Exclusion List:

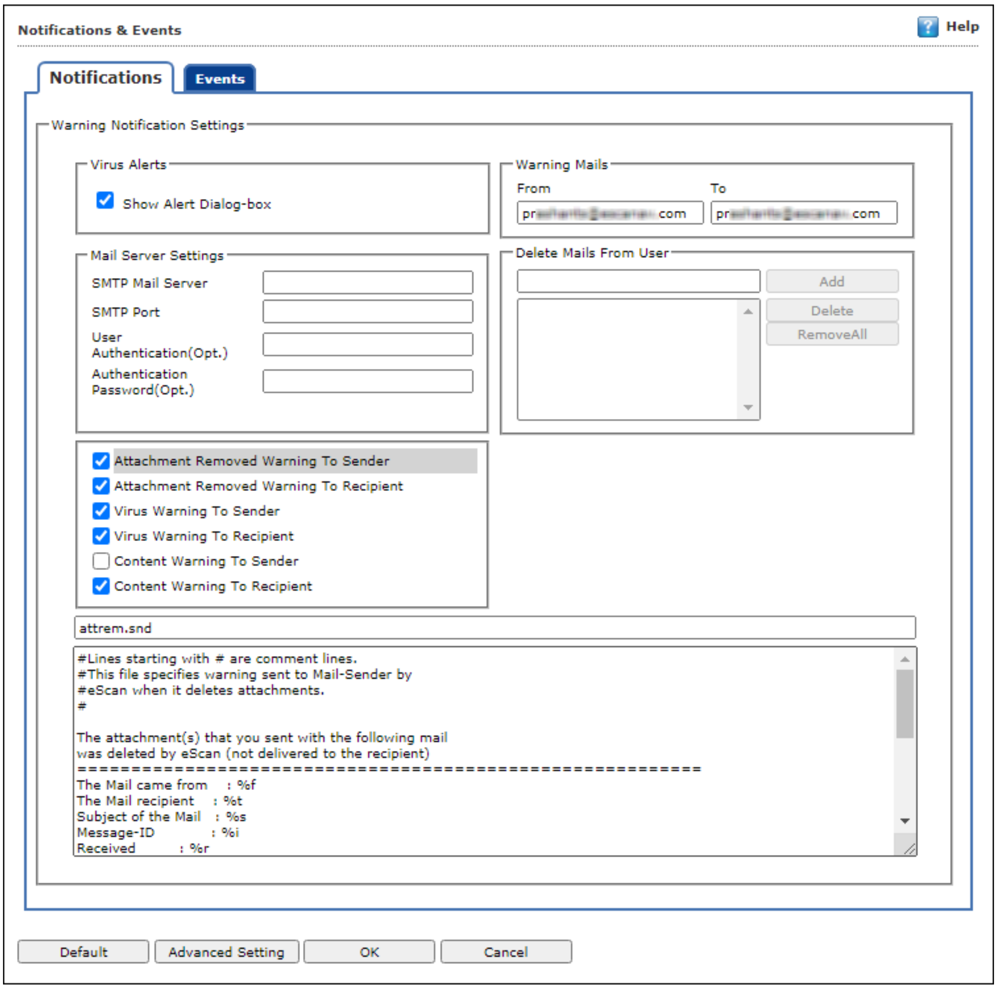
1. Select the appropriate file checkbox, and then click **Delete**.
   A confirmation prompt appears.
2. Click **OK**.
   The executable file gets deleted from the Exclusion List.

Removing all files from Exclusion List

To remove all executable files from the Exclusion List:

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

Notifications and Events



Notifications & Events

Warning Notification Settings

Virus Alerts

☑ Show Alert Dialog-box

Warning Mails

From: pr[redacted].com

To: pr[redacted].com

Mail Server Settings

SMTP Mail Server:

SMTP Port:

User Authentication(Opt.):

Authentication Password(Opt.):

Delete Mails From User

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

attrem.snd

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

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

Notifications

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

Virus Alerts [Default]

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

Warning Mails

Configure this setting if you want Mail Anti-Virus to send warning emails and alerts to a given sender or recipient. The default sender is **postmaster** and the default recipient is **postmaster**.

Attachment Removed Warning to Sender [Default]

Select this checkbox if you want Mail Anti-Virus to send a warning message to the sender of an infected attachment. Mail Anti-Virus sends this email when it encounters a virus infected attachment in an email. The email content is displayed in the preview box.

Attachment Removed Warning to Recipient [Default]
Select this checkbox if you want Mail Anti-Virus to send a warning message to the recipient when it removes an infected attachment. The email content is displayed in the preview box.

Virus Warning to Sender [Default]
Select this checkbox if you want Mail Anti-Virus to send a virus warning message to the sender. The email content is displayed in the preview box.

Virus Warning to Recipient [Default]
Select this checkbox if you want Mail Anti-Virus to send a virus warning message to the recipient. The email content is displayed in the preview box.

Content Warning to Sender
Select this checkbox if you want Mail scanner to send a content warning message to the sender. The email content is displayed in the preview box.

Content Warning to Recipient [Default]
Select this checkbox if you want Mail scanner to send a content warning message to the recipient. The email content is displayed in the preview box.

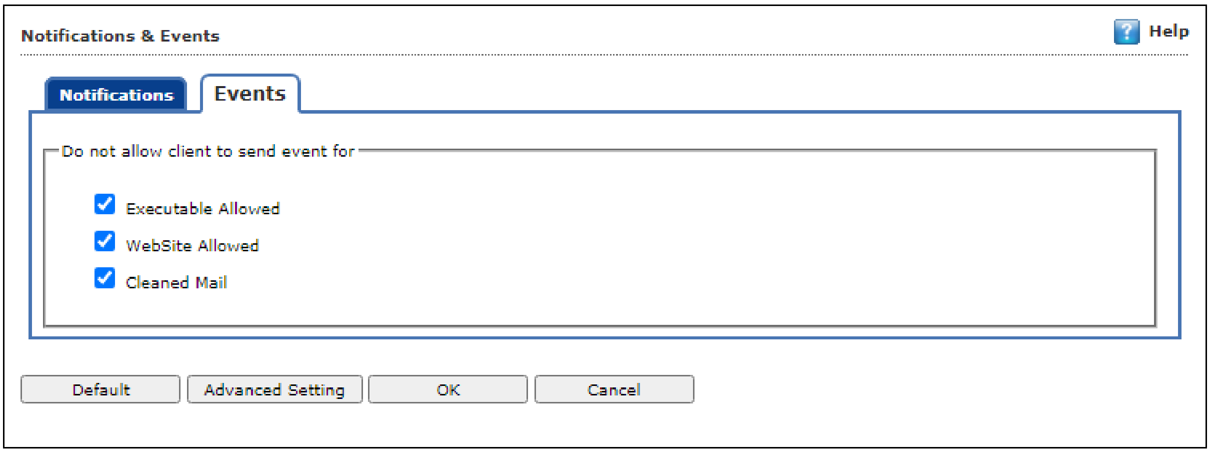
Delete Mails from User
You can configure eScan to automatically delete emails that have been sent by specific users. For this, you need to add the email addresses of such users to the **Delete Mails From User** field. The **Add**, **Delete**, and **Remove All** buttons appear as dimmed. After you enter text in the **Delete Mails From User** field, the buttons get enabled.

Events

Events tab lets you define the settings to allow/restrict clients from sending alert for following events:

- Executable Allowed
- Website Allowed
- Cleaned Mail

By default, all events are selected.

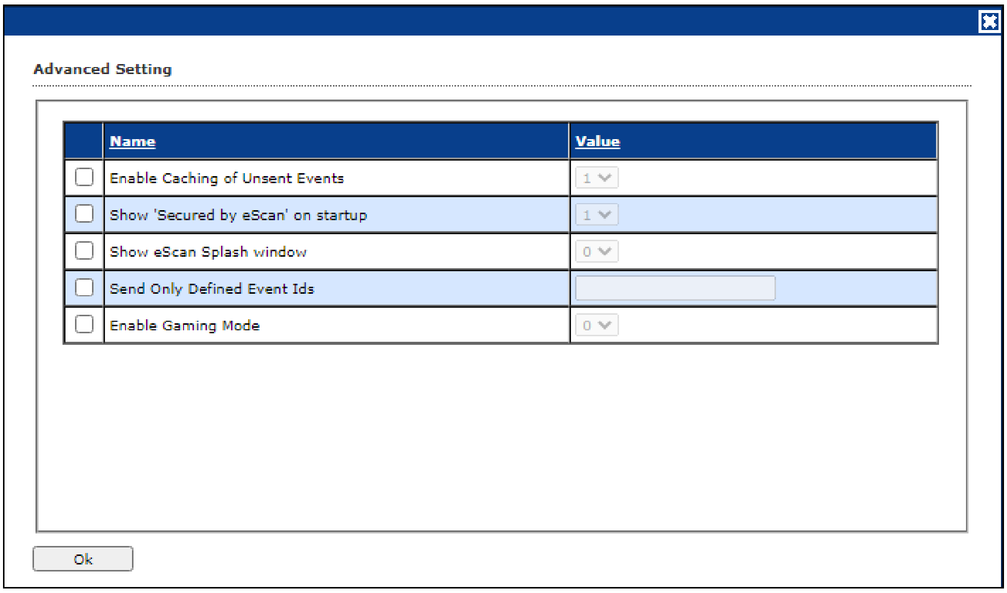


Notifications & Events

Do not allow client to send event for

☑ Executable Allowed
☑ WebSite Allowed
☑ Cleaned Mail

Advanced Setting



Advanced Setting

	Name	Value
□	Enable Caching of Unsent Events	1
□	Show 'Secured by eScan' on startup	1
□	Show eScan Splash window	0
□	Send Only Defined Event Ids	
□	Enable Gaming Mode	0

Enable Caching of Unseen Events (1 = Enable/0= Disable)
It lets you Enable/Disable automatic caching of unseen events.

Show 'Secured by eScan' on startup (1 = Enable/0= Disable)
It lets you Enable/Disable the display of 'Secured by eScan' at the startup of the computers.

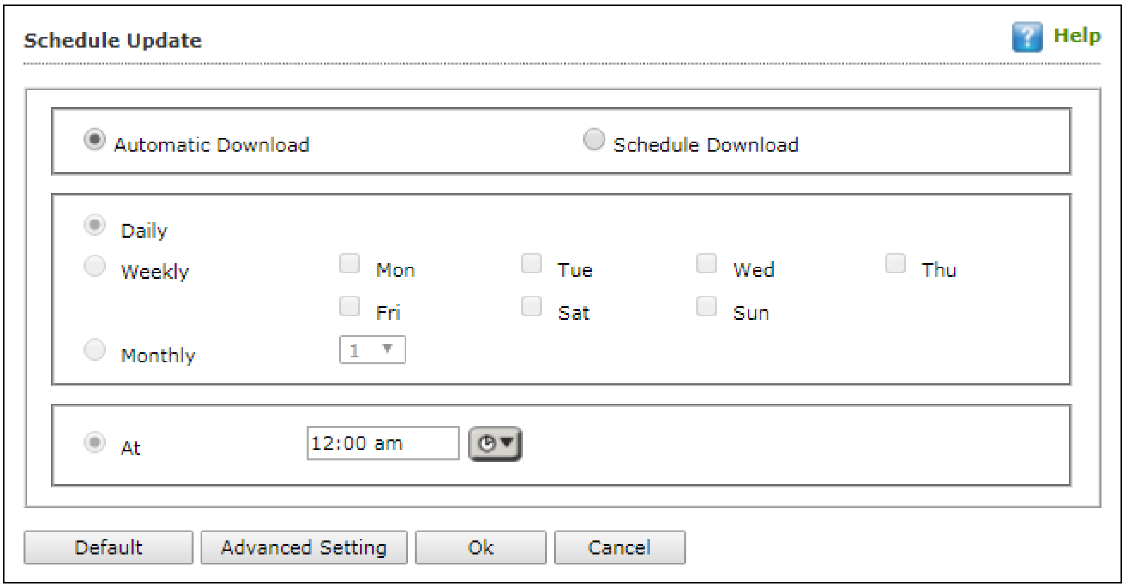
Show eScan Splash window (1 = Enable/0= Disable)
It lets you Enable/Disable display of eScan Splash Window.

Send Only Defined Event Ids
It lets you send only the defined events such as File Antivirus IDs, Mail Antivirus IDs, and more.

Enable Gaming Mode (1 = Enable/0 = Disable)
It lets you Enable/Disable the gaming mode on the computer.

Schedule Update

The Schedule Update lets you schedule eScan database updates.



Schedule Update

Help

● Automatic Download ○ Schedule Download

● Daily
○ Weekly □ Mon □ Tue □ Wed □ Thu
□ Fri □ Sat □ Sun
○ Monthly 1

● At 12:00 am

The updates can be downloaded automatically with **Automatic Download** option.

-OR-

The updates can be downloaded on a schedule basis with **Schedule Download** option. Select intervals and time basis as per your preferences.

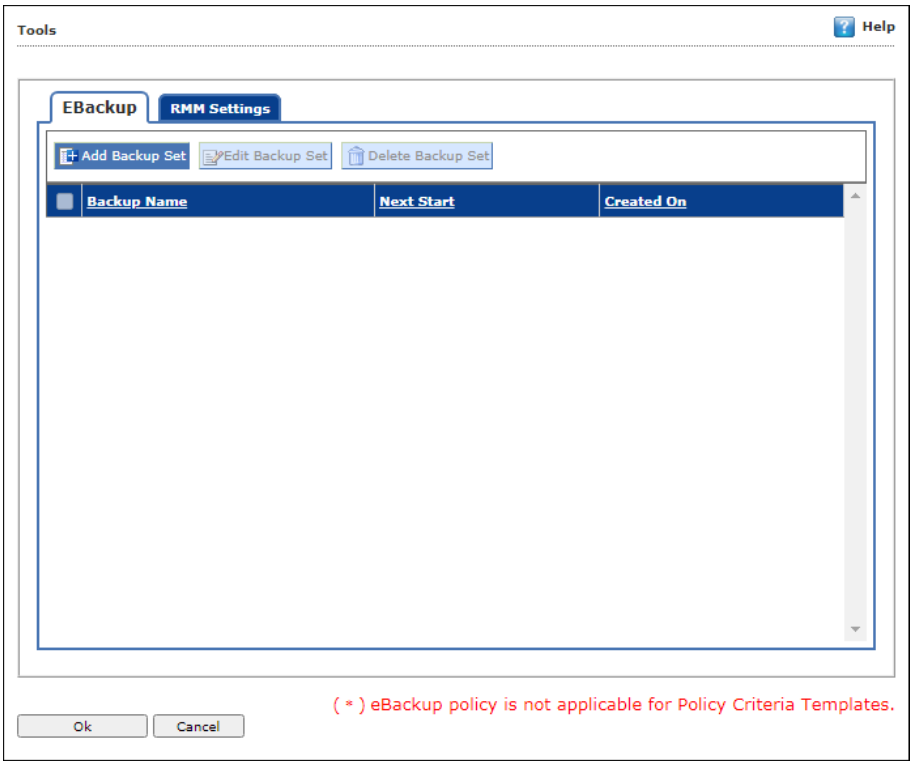
Advanced Setting

Set bandwidth limit for download (in kb/sec)
It lets you define bandwidth limit for download on managed computers, if you have limited internet connection or other network issues.

Retry schedule download (Default retry interval is 15 minutes)
It lets you define time to retry for download updates (Default retry interval is 15 minutes) on managed computers.

Tools

The Tools lets you configure eBackup and Remote Monitoring Management (RMM) Settings.



(*) eBackup policy is not applicable for Policy Criteria Templates.

EBackup (requires additional license for Network and Cloud backup)

Taking regular backup of your critical files stored on your computer is very important, as files may get misplaced or damaged due to issues such as virus outbreak, modification by a ransomware or another user. This feature of eScan allows you to take backup of your important files stored on your computer such as documents, photos, media files, music files, contacts, and so on. It allows you to schedule the backup process by creating tasks. The backed up data is stored in an encrypted format in a folder secured by eScan's real-time protection. You can create Backup jobs by adding files, folders to take a backup either manually or schedule the backup at a defined time or day.

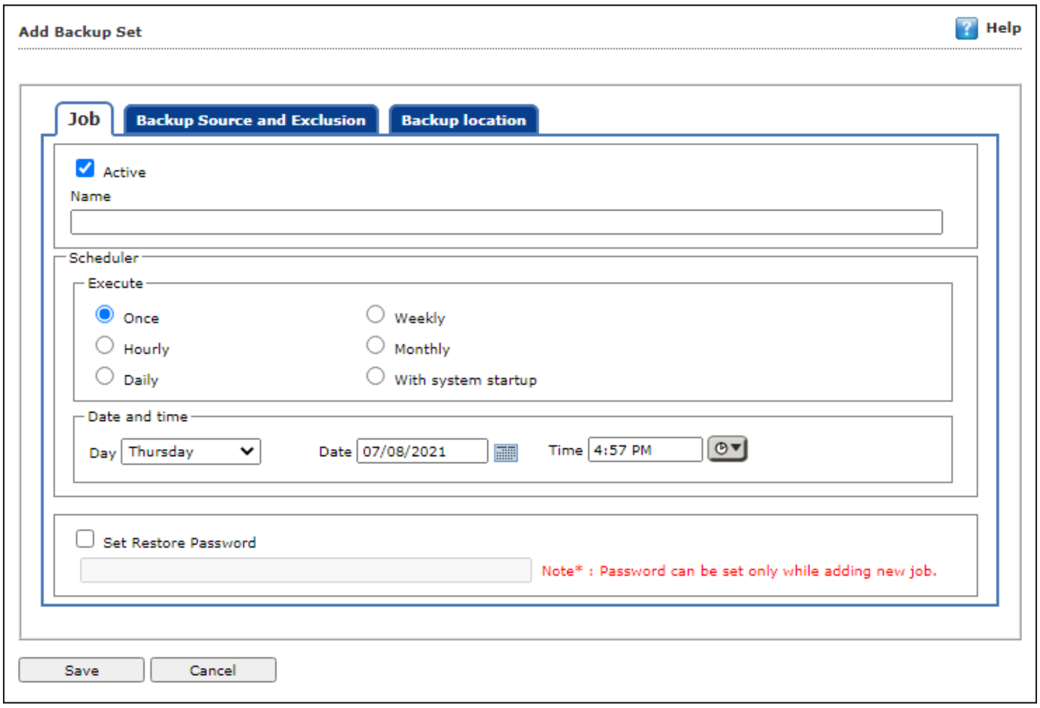
With eBackup feature you can:

- Create, schedule, edit, and delete backup jobs as per requirement.
- Take a backup of specific folder(s)/file extension(s) on local endpoint, external drives or network drive.
- Exclude specific folder(s)/file extension(s) from being backed up.
- Add specific file extensions to be backed up along with regular backup as per requirement.
- Save the backup data in external hard drive or local drive.

The eBackup option has following tabs to configure:

Job

Using this tab you can schedule the eBackup task.



Add Backup Set

☑ Active

Name

Scheduler

Execute

● Once ○ Weekly
○ Hourly ○ Monthly
○ Daily ○ With system startup

Date and time

Day Thursday Date 07/08/2021 Time 4:57 PM

□ Set Restore Password

Note* : Password can be set only while adding new job.

Active

Select this option to set the configuring eBackup option as active.

Scheduler

This option allows you to schedule the eBackup to repeat the process such as Once, Hourly, Daily, Weekly, Monthly, or with system startup.

Date and time

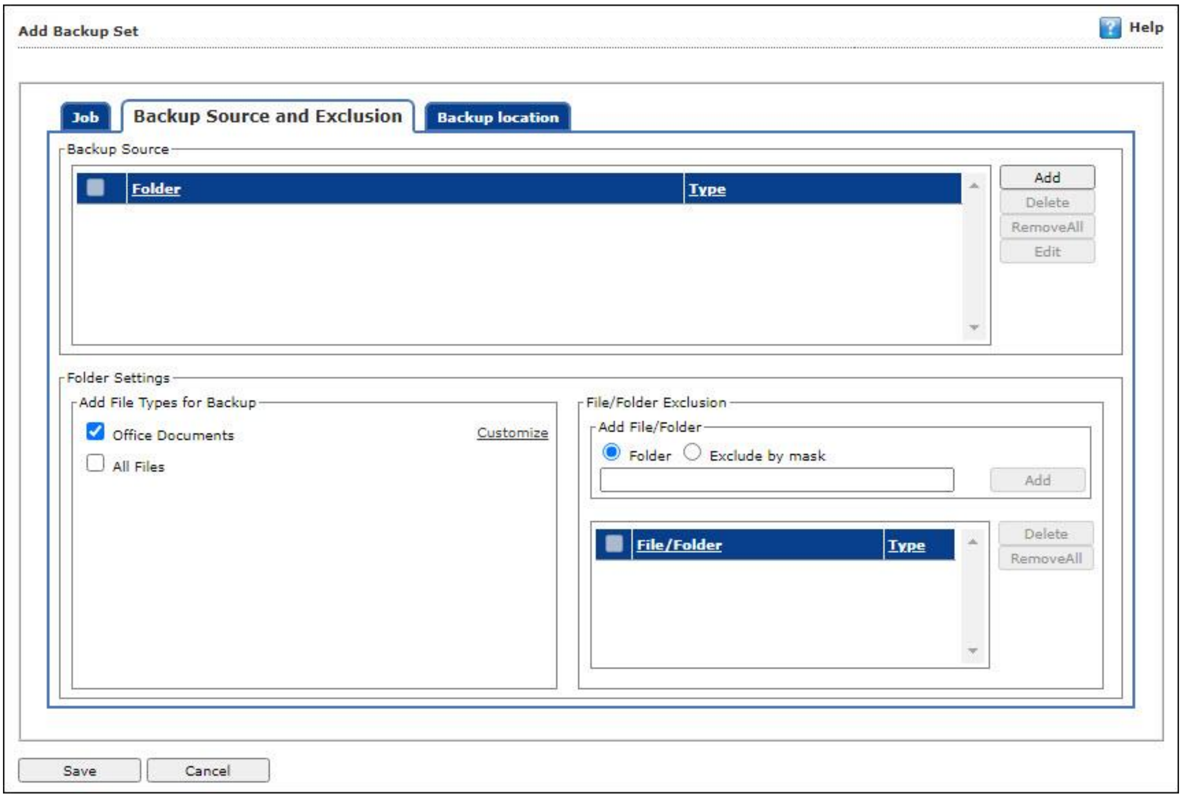
This option allows you select the day, time, and date for running the scheduled eBackup task.

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.



☑ Office Documents

☐ All Files

● Folder ○ Exclude by mask

Backup Source

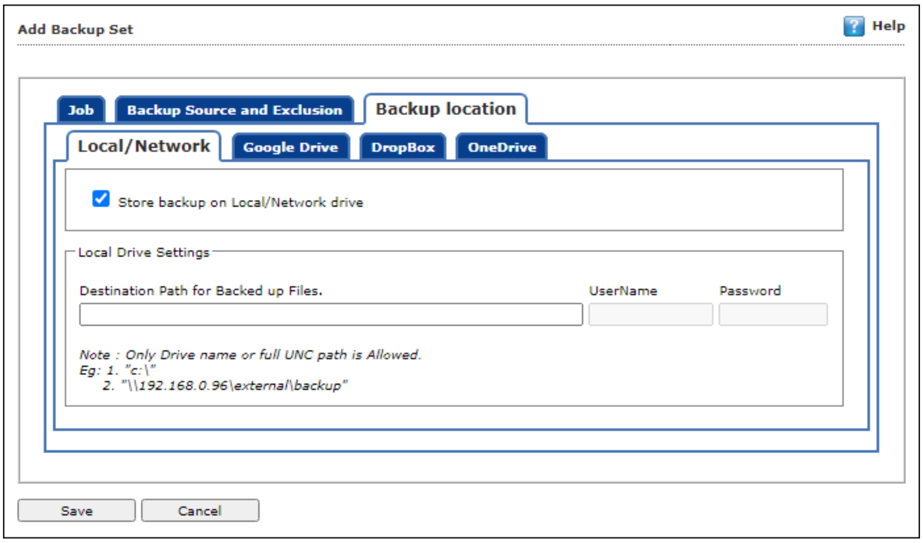
This option allows to add the folder path(s) on which the backup has to be performed. Apart from that you can select the document types to be backed up from these particular folders.

Folder Settings

- **Add File Type for Backup**: Select the type of files for backup. By default, Office Documents option is selected.
- **File/Folder Exclusion**: In this section, you can exclude a specific folder or a file format from getting backed up. You can add, delete, and remove the files for the same.

Backup Location

This tab allows to define the storage location for the backup created.



☑ Store backup on Local/Network drive

Local Drive Settings

Destination Path for Backed up Files.

UserName

Password

Note : Only Drive name or full UNC path is Allowed.
Eg: 1. "c:\"
2. "\\192.168.0.96\external\backup"

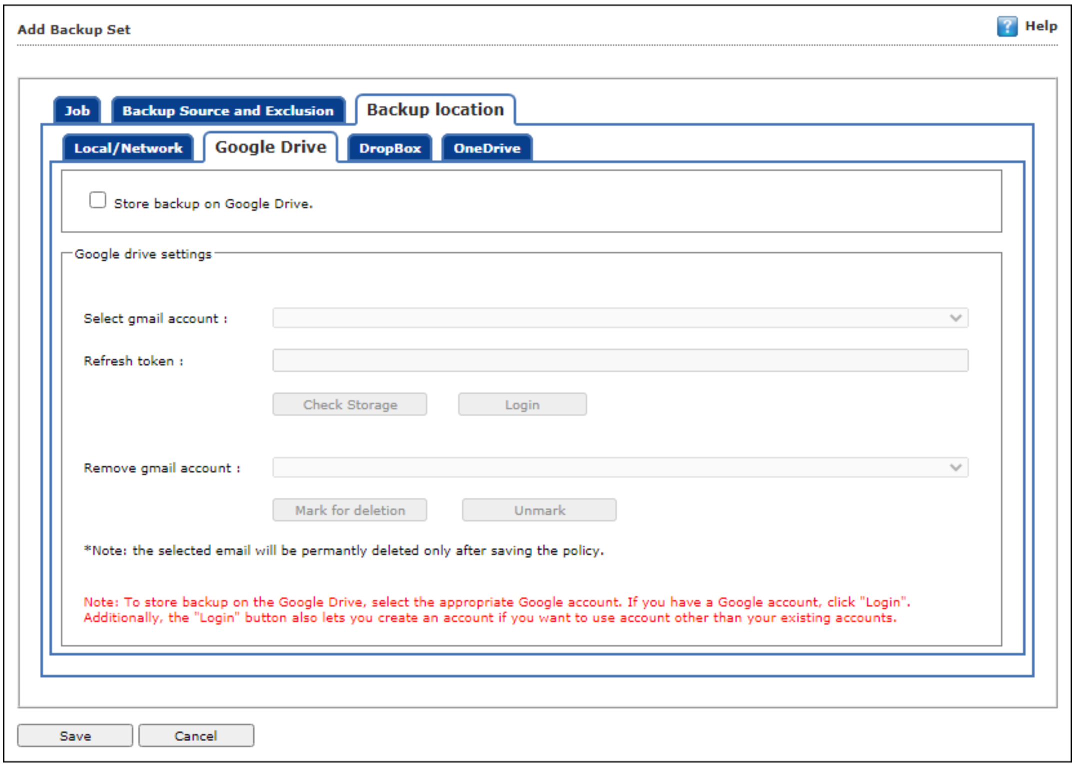
Local/Network

Administrator can save the backup set in the Local/Network Drive by providing the path of the drive and Username and password for the network drive.

NOTE	Network storage of backup set will be available in the trial period. To continue the use of this feature user need to avail the license for the same. In case of system crash or hardware failure, user can recover the created data backup, so storing the backup in the network drive, mapped drive, or NAS drive would be useful in such scenarios.

Google Drive

Administrator can save the backup set in the Google Drive by selecting the appropriate Gmail account and password for the same.



□ Store backup on Google Drive.

Google drive settings

Select gmail account :

Refresh token :

Remove gmail account :

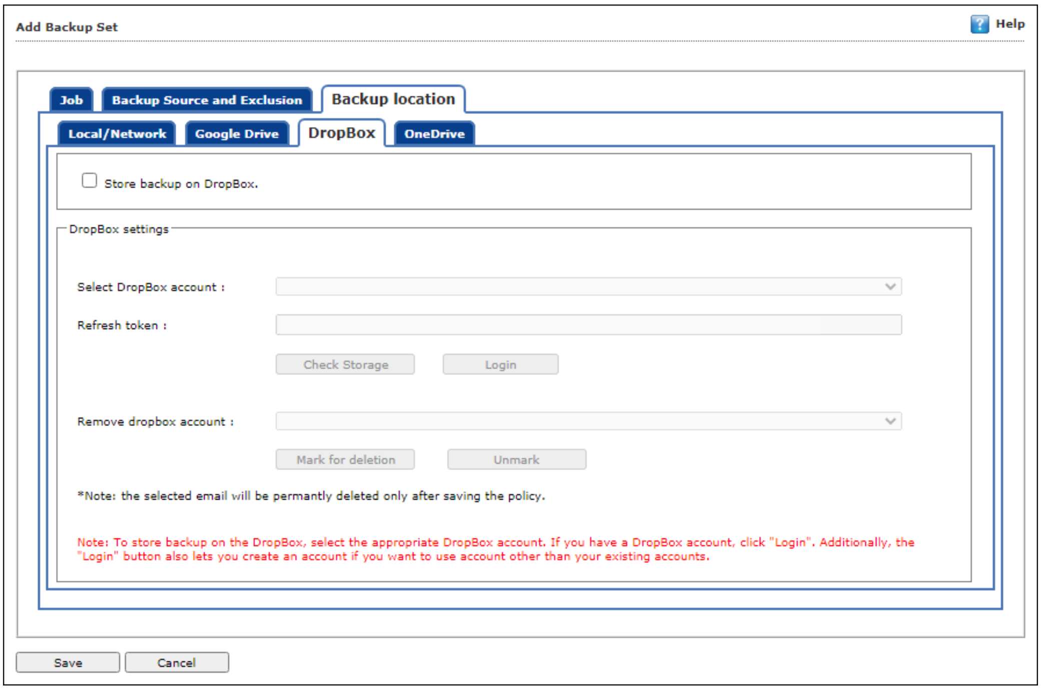
*Note: the selected email will be permantly deleted only after saving the policy.

Note: To store backup on the Google Drive, select the appropriate Google account. If you have a Google account, click "Login". Additionally, the "Login" button also lets you create an account if you want to use account other than your existing accounts.

NOTE	To store backup on the Google Drive, select the appropriate Google account. If you have a Google account, click "**Login**". Additionally, the "**Login**" button also lets you create an account if you want to use account other than your existing accounts.

DropBox

Administrator can save the backup set in the DropBox by selecting the appropriate DropBox account and password for the same.



□ Store backup on DropBox.

DropBox settings

Select DropBox account :

Refresh token :

Remove dropbox account :

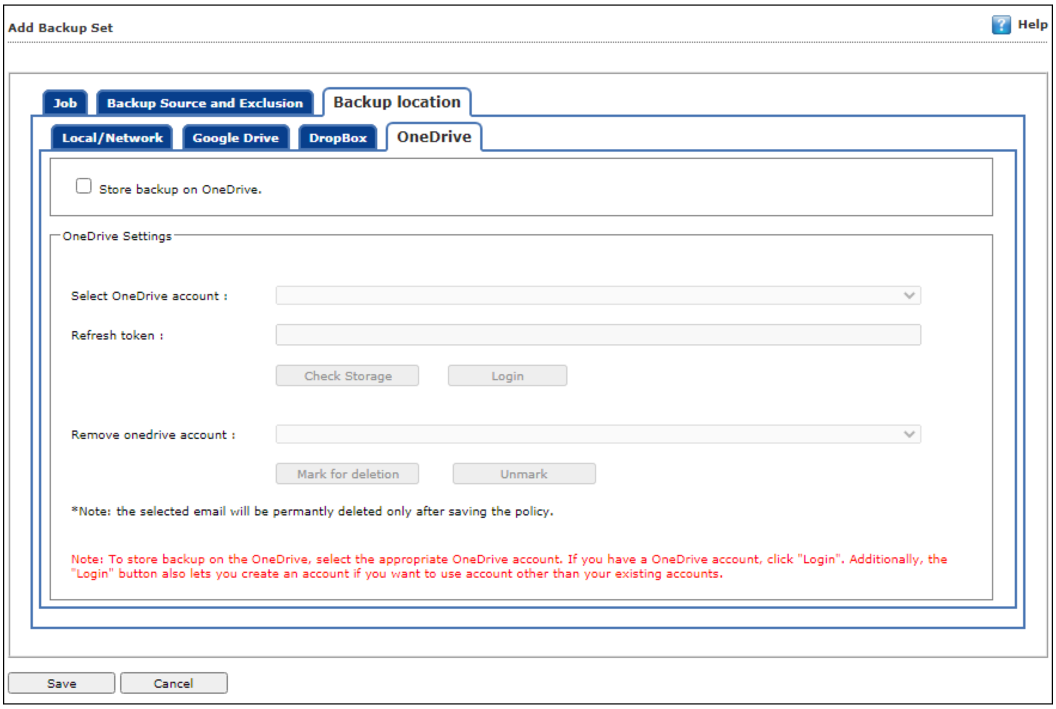
*Note: the selected email will be permantly deleted only after saving the policy.

Note: To store backup on the DropBox, select the appropriate DropBox account. If you have a DropBox account, click "Login". Additionally, the "Login" button also lets you create an account if you want to use account other than your existing accounts.

NOTE	To store backup on the DropBox, select the appropriate DropBox account. If you have a DropBox account, click "**Login**". Additionally, the "**Login**" button also lets you create an account if you want to use account other than your existing accounts.

OneDrive

Administrator can save the backup set in the OneDrive by selecting the appropriate OneDrive account and password for the same.



□ Store backup on OneDrive.

OneDrive Settings

Select OneDrive account :

Refresh token :

Remove onedrive account :

*Note: the selected email will be permantly deleted only after saving the policy.

Note: To store backup on the OneDrive, select the appropriate OneDrive account. If you have a OneDrive account, click "Login". Additionally, the "Login" button also lets you create an account if you want to use account other than your existing accounts.

NOTE	To store backup on the OneDrive, select the appropriate OneDrive account. If you have 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.

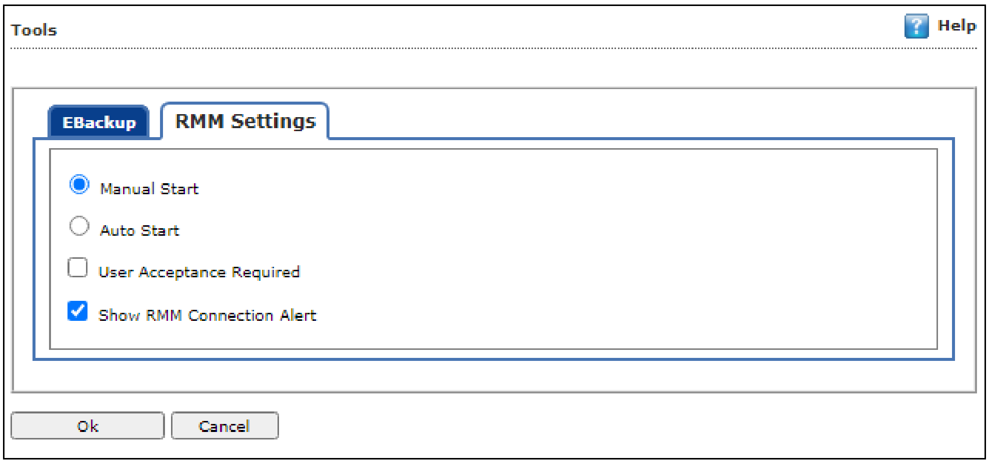
Delete Backup Set

To delete a Backup Set:

2. Select a Backup Set.
3. Click **Delete Backup Set**.
   A confirmation prompt appears.
4. 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. You will get the following configuration options:



Tools
Help

EBackup | RMM Settings

● Manual Start
○ Auto Start
□ User Acceptance Required
☑ Show RMM Connection Alert

Ok | Cancel

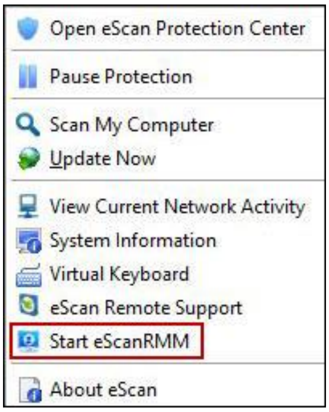
- **Manual Start**: If this option is selected, client endpoint users have to manually start the RMM service to establish a RMM connection.
- **Auto Start**: If this option is selected, RMM service will be started automatically and all client endpoints will be connected to your main eScan server.
- **User Acceptance Required**: If this 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**: 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.

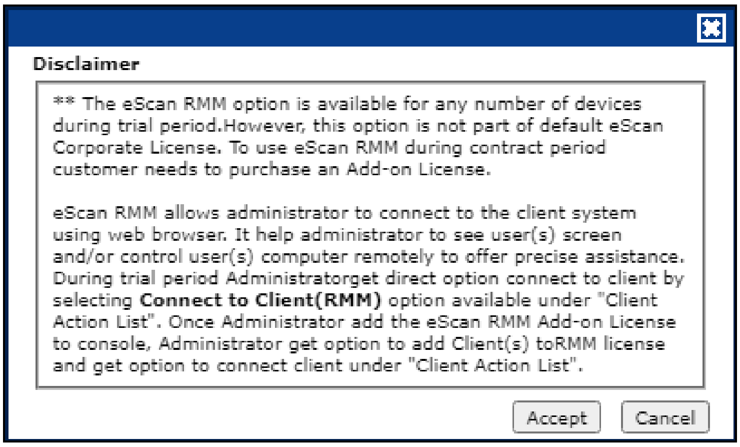
RMM - Manual Start

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.



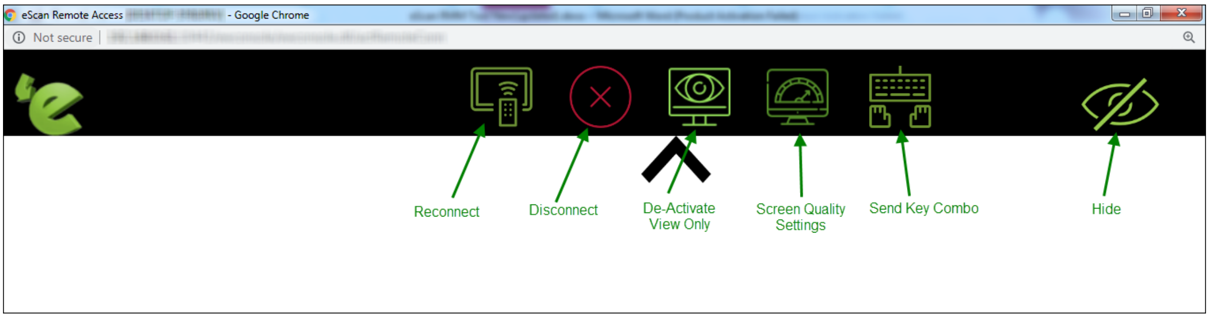
Disclaimer

** The eScan RMM option is available for any number of devices during trial period.However, this option is not part of default eScan Corporate License. To use eScan RMM during contract period customer needs to purchase an Add-on License.

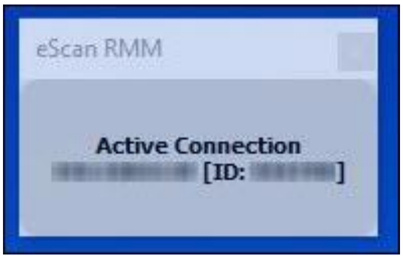
eScan RMM allows administrator to connect to the client system using web browser. It help administrator to see user(s) screen and/or control user(s) computer remotely to offer precise assistance. During trial period Administratorget direct option connect to client by selecting **Connect to Client(RMM)** option available under "Client Action List". Once Administrator add the eScan RMM Add-on License to console, Administrator get option to add Client(s) toRMM license and get option to connect client under "Client Action List".

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).



eScan RMM

Active Connection
[redacted] [ID: [redacted]]

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.)

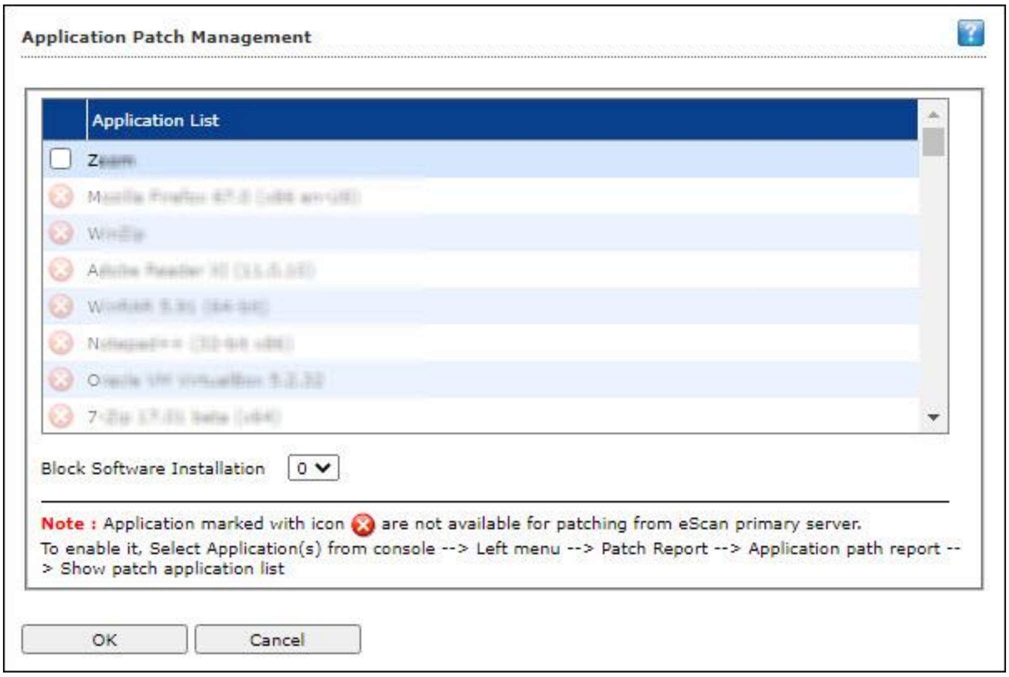
After you are done performing an activity, click the **Disconnect** icon to end remote connection.

NOTE	To get detailed information about RMM feature, **click here**.

Application Patch Management (requires additional license)

The Application Patch Management helps in patching the applications in the client machines from eScan primary server.

NOTE	To enable the patching of unavailable applications, open Patch Report from navigation panel > Application Patch Report > Show patch application list. Select the required applications and click **Save**.



Application Patch Management

	Application List
□	Zoom
☒	Mozilla Firefox 67.0 (x64 en-US)
☒	WinZip
☒	Adobe Reader XI (11.0.10)
☒	WinRAR 5.31 (64-bit)
☒	Notepad++ (32-bit x86)
☒	Oracle VM VirtualBox 5.2.32
☒	7-Zip 17.01 beta (x64)

Block Software Installation 0

Note : Application marked with icon ☒ are not available for patching from eScan primary server.
To enable it, Select Application(s) from console --> Left menu --> Patch Report --> Application path report --> Show patch application list

Patching the Applications

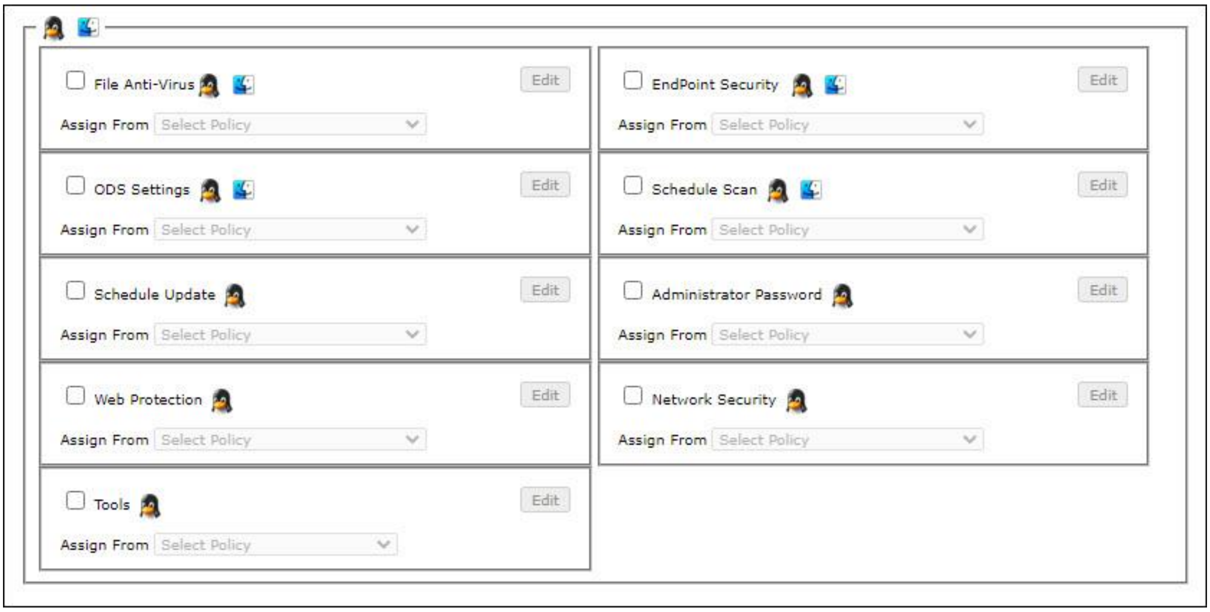
To use this function, select the applications to be patched and click on **OK**. After the policy gets applied, the selected applications will automatically get updated in the client systems.

Block Software Installation

This option allows you to block the software installations in the client systems. To block the installations, select **1** from the provided drop-down.

Configuring eScan Policies for Linux and Mac Computers

eScan lets you define settings for File Anti-Virus, Endpoint Security, On Demand scanning and Schedule Scan module for Linux and Mac computers connected to the network. Click **Edit** to configure the eScan module settings for computers with respective operating systems.



□ File Anti-Virus Edit
Assign From Select Policy

□ EndPoint Security Edit
Assign From Select Policy

□ ODS Settings Edit
Assign From Select Policy

□ Schedule Scan Edit
Assign From Select Policy

□ Schedule Update Edit
Assign From Select Policy

□ Administrator Password Edit
Assign From Select Policy

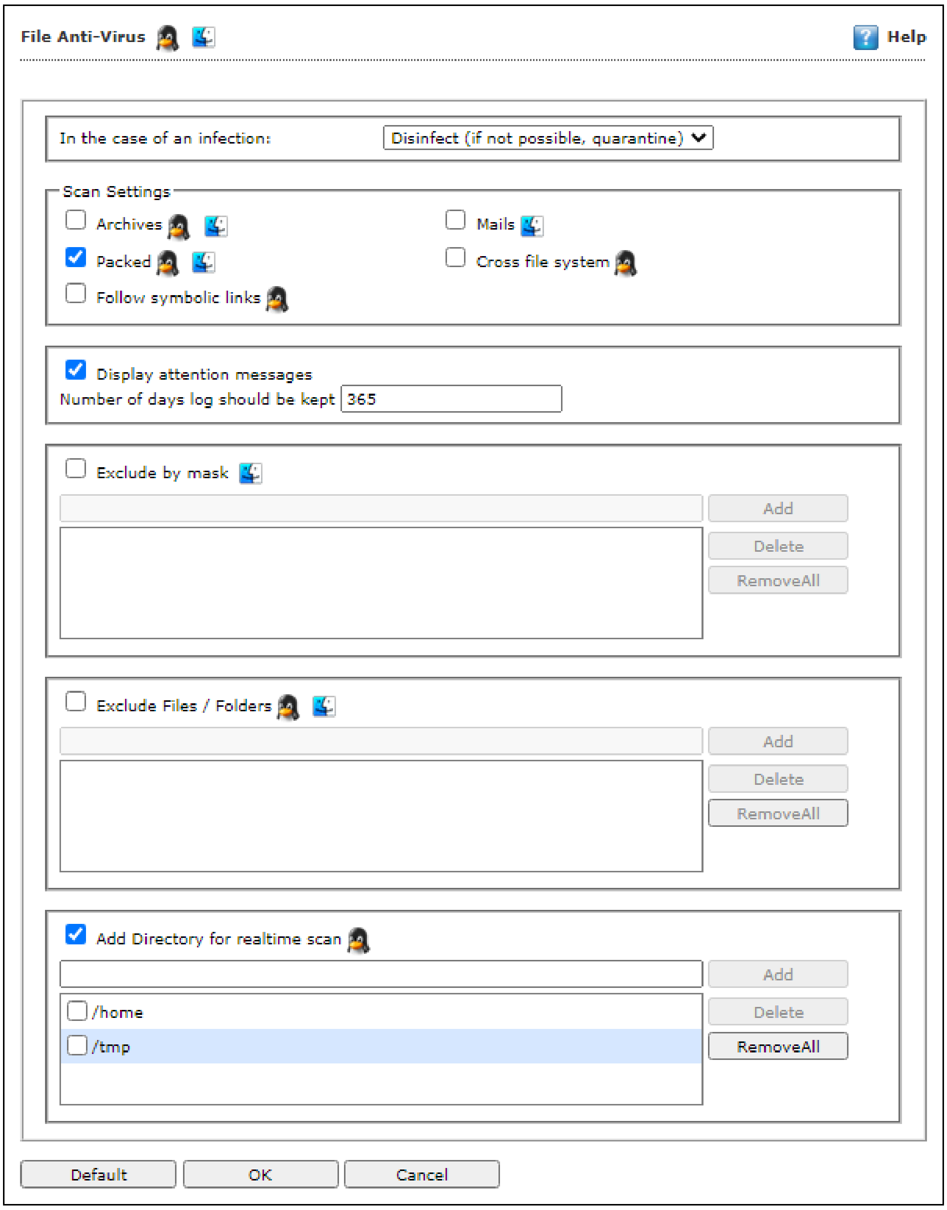
□ Web Protection Edit
Assign From Select Policy

□ Network Security Edit
Assign From Select Policy

□ Tools Edit
Assign From Select Policy

NOTE	Icons next to every module displays that the settings are valid for the respective operating systems only. It lets you define settings for Scanning; you can also define action to be taken in case of an infection. It also lets you define the number of days for which the logs should be kept as well as create list for Masks, Files or Folders to be excluded from scanning.

File Anti-Virus



File Anti-Virus

Help

In the case of an infection: Disinfect (if not possible, quarantine)

Scan Settings

☐ Archives

☐ Mails

☑ Packed

☐ Cross file system

☐ Follow symbolic links

☑ Display attention messages

Number of days log should be kept 365

☐ Exclude by mask

☐ Exclude Files / Folders

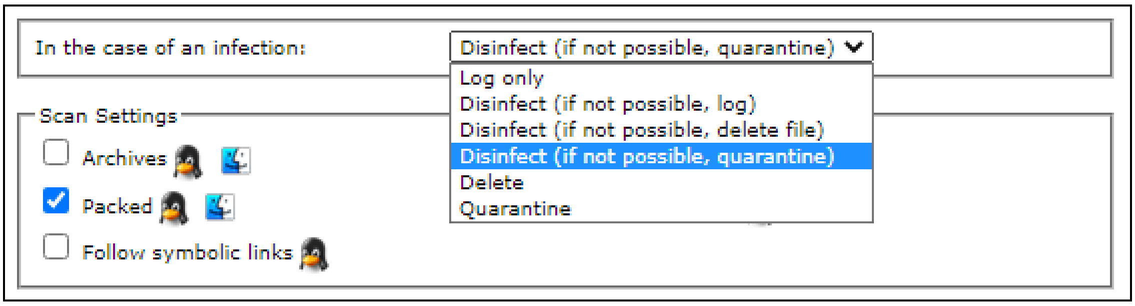
☑ Add Directory for realtime scan

☐ /home

☐ /tmp

Actions in case of infection [Drop-down]

It displays a list of actions eScan should take, in case of virus detection.



In the case of an infection: Disinfect (if not possible, quarantine)

Log only
Disinfect (if not possible, log)
Disinfect (if not possible, delete file)
Disinfect (if not possible, quarantine)
Delete
Quarantine

Scan Settings

☐ Archives

☑ Packed

☐ Follow symbolic links

By default, Disinfect (if not possible, quarantine file) option is selected. Following are the types of actions:

- **Log Only:** This option indicates or alerts the user about the infection detected (No Action is taken; only logs are maintained).
- **Disinfect (if not possible, log):** This option tries to disinfect and if disinfection is not possible it logs the information of only the infected object.
- **Disinfect (if not possible, delete file):** This option tries to disinfect and if disinfection is not possible it deletes the infected object.
- **Disinfect (if not possible, quarantine file):** This option tries to disinfect and if disinfection is not possible it quarantines the infected object.
- **Delete:** This option deletes the infected object.
- **Quarantine:** This option quarantines the infected object.

Scan Settings

- **Mails -** It indicates scanning the mail files. By default, it is selected. Select this checkbox if you want eScan real-time protection to scan mails.
- **Archives -** It indicates the archived files, such as zip, rar, and so on. Select this checkbox if you want eScan real-time protection to scan archived files.
- **Packed -** It indicates the compressed executable. Select this checkbox if you want eScan real-time protection to scan packed files.
- **Cross File System** that facilitates scanning of files over cross-file systems.
- **Follow Symbolic Links:** scans the files following the symbolic links.

Exclude by Mask (file types) - Select this option if you want eScan real-time protection to exclude specific file extensions.

Exclude Folders and files - Select this option if you want eScan real-time protection to exclude Folders and files from scanning. eScan lets you add; Remove any or all Added Files or Folders whenever required.

Add Directory for Real-Time Scan - If you want eScan to perform real-time scan on any of the directories add them in this list.

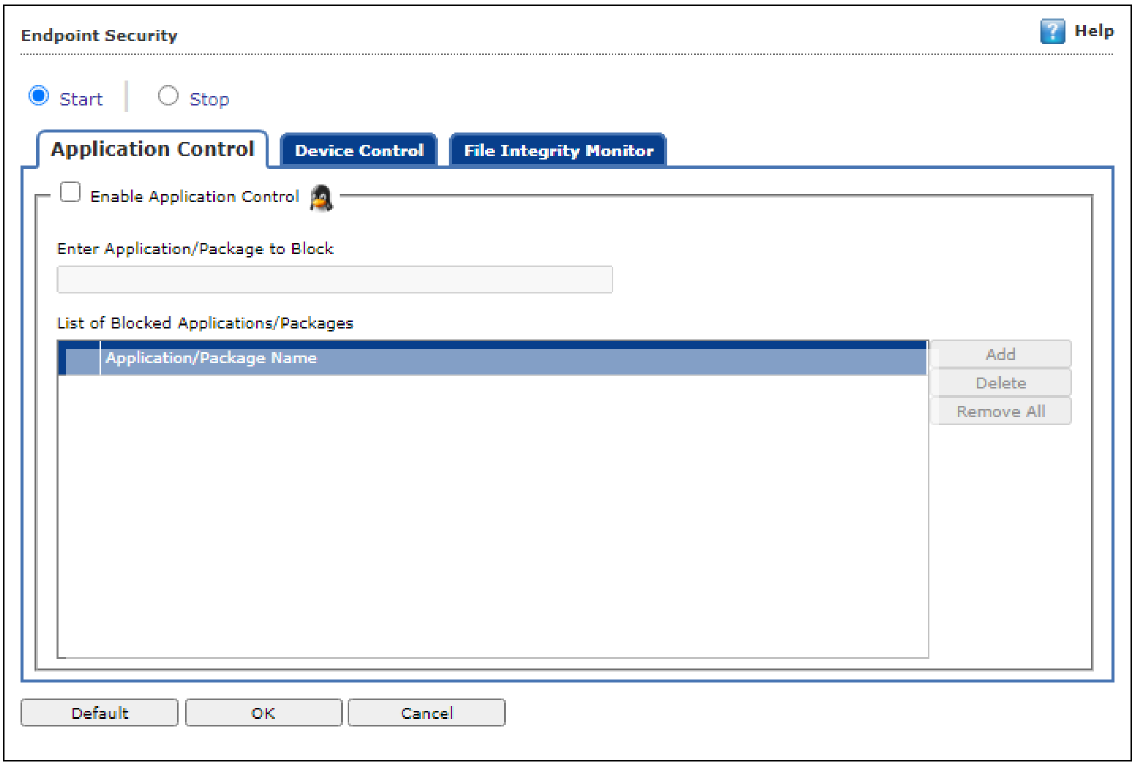
You can restore default eScan settings by clicking **Default**.

Endpoint Security

The Endpoint Security module lets you centrally manage all endpoints on your network and closely monitor all USB activities in real-time. With eScan USB control, you can prevent data theft by blocking all except your trusted USB storage devices and Stop your files from being taken away on thumb drives, iPod, mp3 players and portable USB hard drives.

Application Control

The Application Control tab allows to block the execution of application or package.

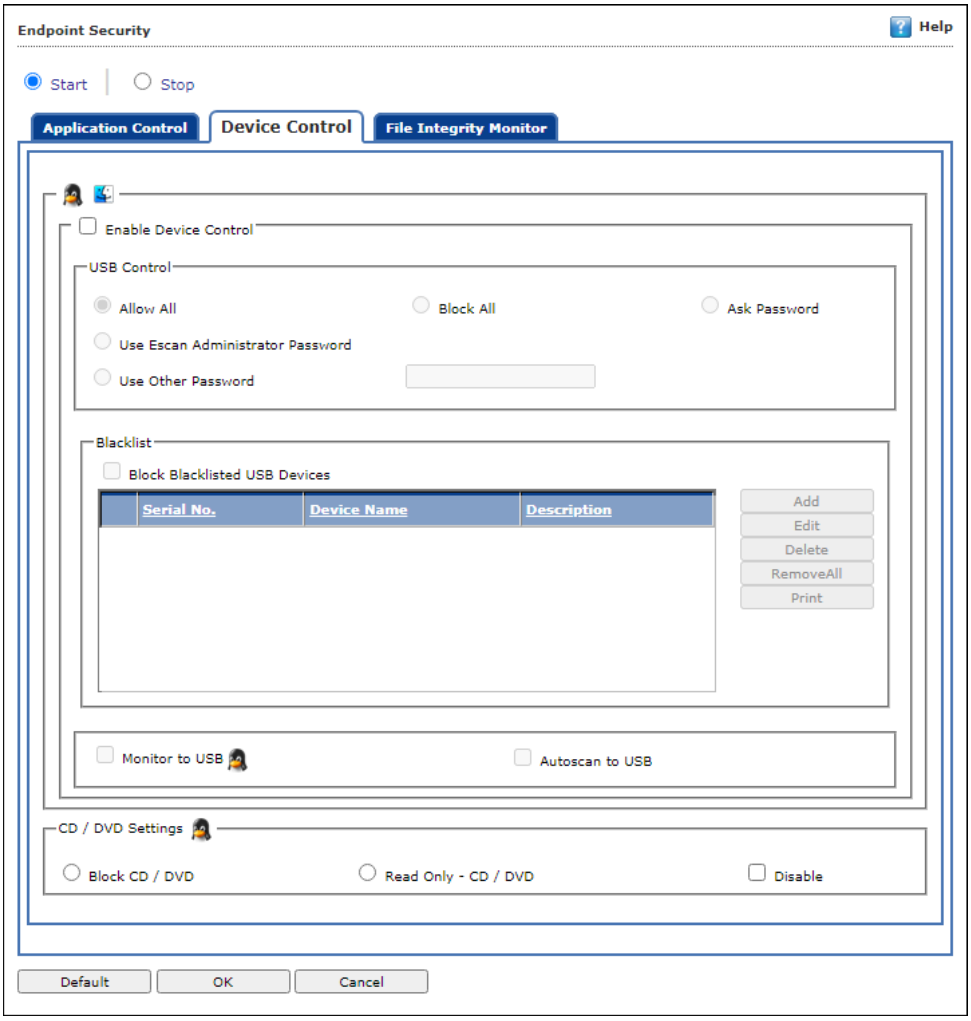


Enable Application Control
Select the checkbox to enable the application control feature.

Enter Application/Package to block
Enter the application or package name to add them in the list of application/packages blocked.
To delete the application/package, select the specific app/package and click **Delete**.
To delete all the application from the list, click **Remove All**.

Device Control

The Device Control tab enables you to allow/block the access to the USB devices and the CD/DVD in client computers.



Endpoint Security

● Start | ○ Stop

□ Enable Device Control

USB Control

● Allow All ○ Block All ○ Ask Password

○ Use Escan Administrator Password

○ Use Other Password

Blacklist

□ Block Blacklisted USB Devices

Serial No.	Device Name	Description

□ Monitor to USB □ Autoscan to USB

CD / DVD Settings

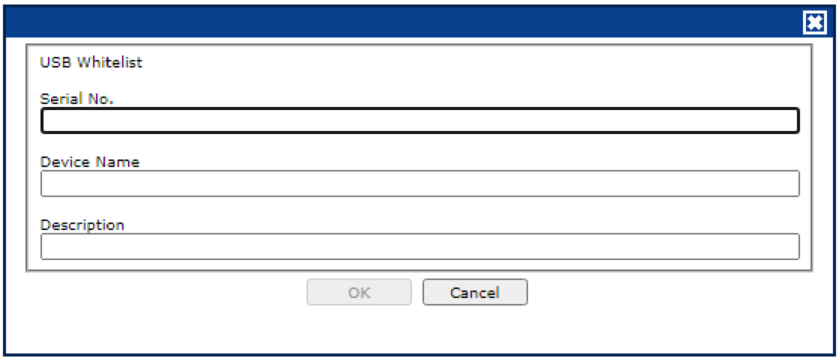
○ Block CD / DVD ○ Read Only - CD / DVD □ Disable

Enable Device Control: Select this checkbox to configure the Device Control settings.

- **USB Control**: This option lets you allow, block, or set password for the USB device connected to the endpoint. It has following options:
    - **Allow All:** Select this option to allow all the connected USB devices.
    - **Block All:** Select this option to block all the connected USB devices.
    - **Ask Password:** Select this option to set password for the connected USB devices. This will ask password before allowing USB devices to connect to the system. You can either set a password or use the administrator password using the options **Use Other Password** and **Use Escan Administrator Password** respectively.

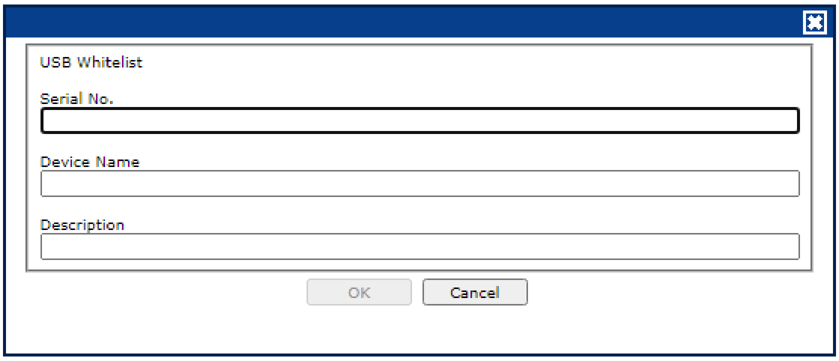
- **Blacklist:** This option lets you add USB devices to the blacklist. You can add, delete, modify USB devices using the following options:

- **Add:** Use this button to enter USB serial number, name, and description of the USB devices in order to blacklist it.


USB Whitelist
Serial No.
Device Name
Description

- **Import:** It allows you to blacklist multiple USB devices at once using CSV file.
- **Edit:** It allows you to edit the details of the USB devices.
- **Delete**: It allows you to remove the USB device from the list.
- **Remove All**: It allows you to remove all the USB devices from the list.
- **Print**: It allows you to print the USB device list along with their details.

- **Whitelist:** This option lets you add USB devices to the whitelist. You can add, delete, modify USB devices using the following options:
  - **Add:** Use this button to enter USB serial number, name, and description of the USB devices in order to whitelist it.


USB Whitelist
Serial No.
Device Name
Description

  - **Import:** It allows you to whitelist multiple USB devices at once using CSV file.
  - **Edit:** It allows you to edit the details of the USB devices.
  - **Delete**: It allows you to remove the USB device from the list.
  - **Remove All**: It allows you to remove all the USB devices from the list.
  - **Print**: It allows you to print the USB device list along with their details.

- **Monitor to USB:** Select this checkbox to monitor all the USB devices connected to the endpoints.

- **Autoscan to USB**: Select this option to auto-scan all the USB devices connected to the endpoints.

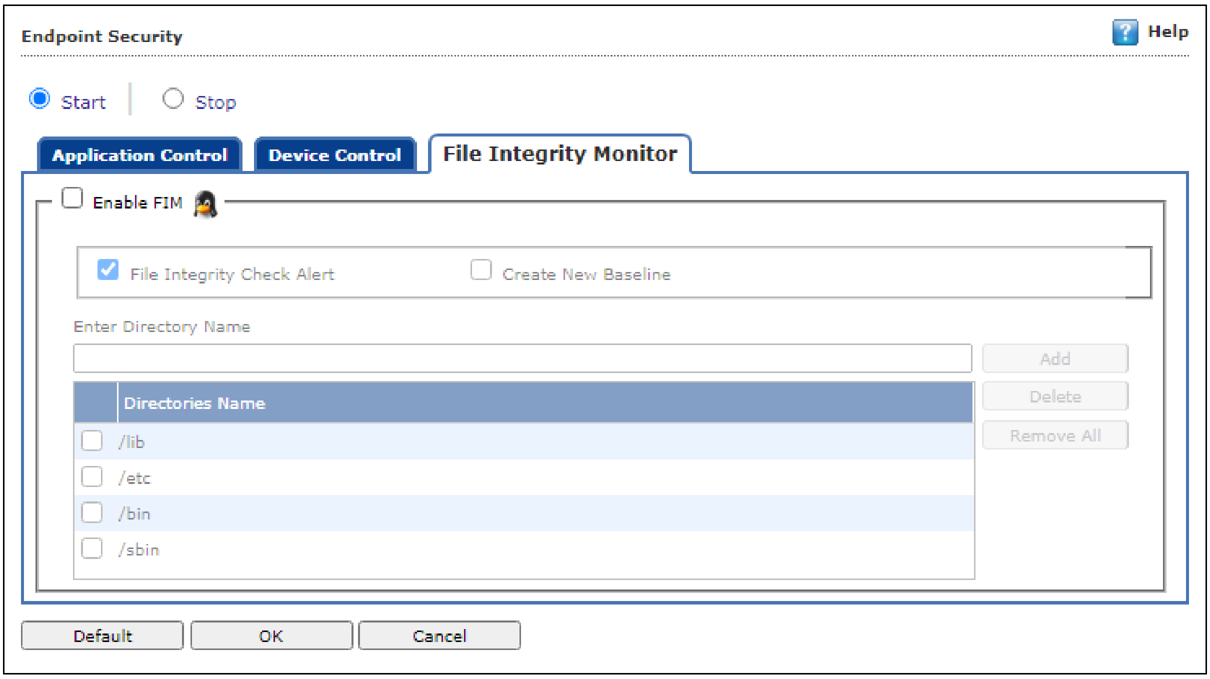
CD/DVD Settings

This option lets administrator to block, allow, and disable the CD/DVD settings. You have following options to configure:

- **Block CD/DVD:** This option blocks CD/DVD inserted in the computer.

- **Read Only CD/DVD:** This option allows limited (only reading) access to the user for the data stored in inserted CD/DVD.
- **Disable:** This option disables the configured settings for CD/DVD.

File Integrity Monitor



● Start ○ Stop

☐ Enable FIM

☑ File Integrity Check Alert ☐ Create New Baseline

Enter Directory Name

	Directories Name
☐	/lib
☐	/etc
☐	/bin
☐	/sbin

Enable FIM
Select this checkbox to enable the File Integrity Monitor option.

- **File Integrity Check Alert**: This checkbox will check the file integrity and alert the admin accordingly.
- **Create baseline**: This checkbox will create a baseline for the selected directories and the FIM will begin monitoring changes for the selected directories.

Enter Directory Name
Enter the directory name to add it to the integrity monitoring.

You can also select the directory name from the pre-defined list in the below table to add them to monitoring.

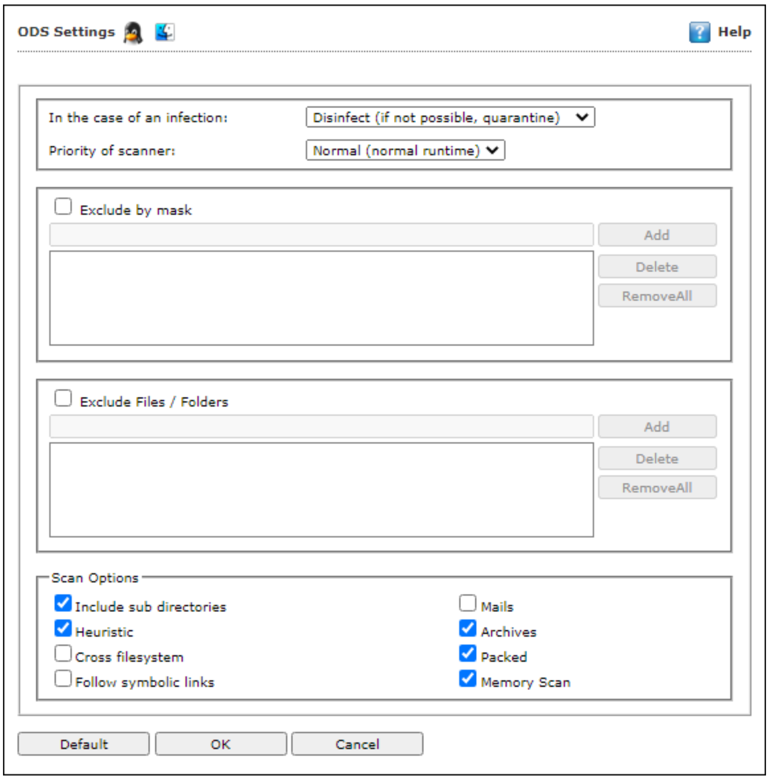
To delete a specific directory from monitoring, select the directory, and click **Delete**.

To remove all the directory from monitoring, click **Remove All**.

Default
This button will reset all the settings of the window to their default values.

ODS Settings

With ODS Settings you can define actions in case of infection, you can also define list of files by mask, Files or Folders to be excluded from Scanning. It also lets you configure settings for various other Scan options like Include Sub directories, Mails, Archives Heuristic Scanning etc. by selecting respective options.



ODS Settings

Help

In the case of an infection: Disinfect (if not possible, quarantine)

Priority of scanner: Normal (normal runtime)

□ Exclude by mask

Add | Delete | RemoveAll

□ Exclude Files / Folders

Add | Delete | RemoveAll

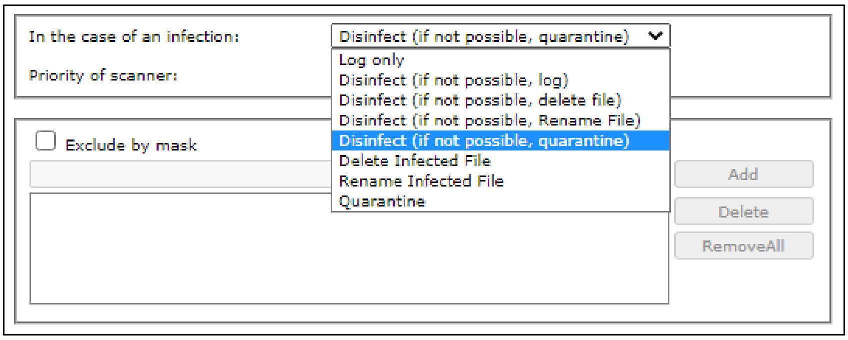
Scan Options

☑ Include sub directories
☑ Heuristic
□ Cross filesystem
□ Follow symbolic links
□ Mails
☑ Archives
☑ Packed
☑ Memory Scan

Default | OK | Cancel

Actions in case of infection [Drop-down]

It indicates a type of action which you want eScan real-time protection to take, in case of virus detection.



In the case of an infection: Disinfect (if not possible, quarantine)

Priority of scanner:

- Log only
- Disinfect (if not possible, log)
- Disinfect (if not possible, delete file)
- Disinfect (if not possible, Rename File)
- Disinfect (if not possible, quarantine)
- Delete Infected File
- Rename Infected File
- Quarantine

□ Exclude by mask

Add | Delete | RemoveAll

By default, Disinfect (if not possible, quarantine file) option is selected. Following actions can be taken:

- **Log Only:** It indicates or alerts the user about the infection detected.
- **Disinfect (if not possible, log):** It tries to disinfect and if disinfection is not possible it logs the information of only the infected object.

- **Disinfect (if not possible, delete file):** It tries to disinfect and if disinfection is not possible it deletes the infected object.
- **Disinfect (if not possible, Rename file):** It tries to disinfect and if disinfection is not possible it renames the infected object.
- **Disinfect (if not possible, quarantine):** It tries to disinfect and if disinfection is not possible it quarantines the infected object.
- **Delete Infected File:** It deletes the infected object.
- **Rename Infected File:** It renames the infected object.
- **Quarantine:** It quarantines the infected object.

Priority of Scanner – You can select the priority of scanning as **High (short runtime)**, **Normal (normal runtime)**, or **Low (long runtime)**.

- **High (short runtime)** – Has a short runtime.
- **Normal (normal runtime)** – Has a normal runtime.
- **Low (long runtime)** – Has a long runtime.

Exclude by Mask – Select this checkbox if you want eScan real-time protection to exclude specific files, and Remove any or all Added Files whenever required.

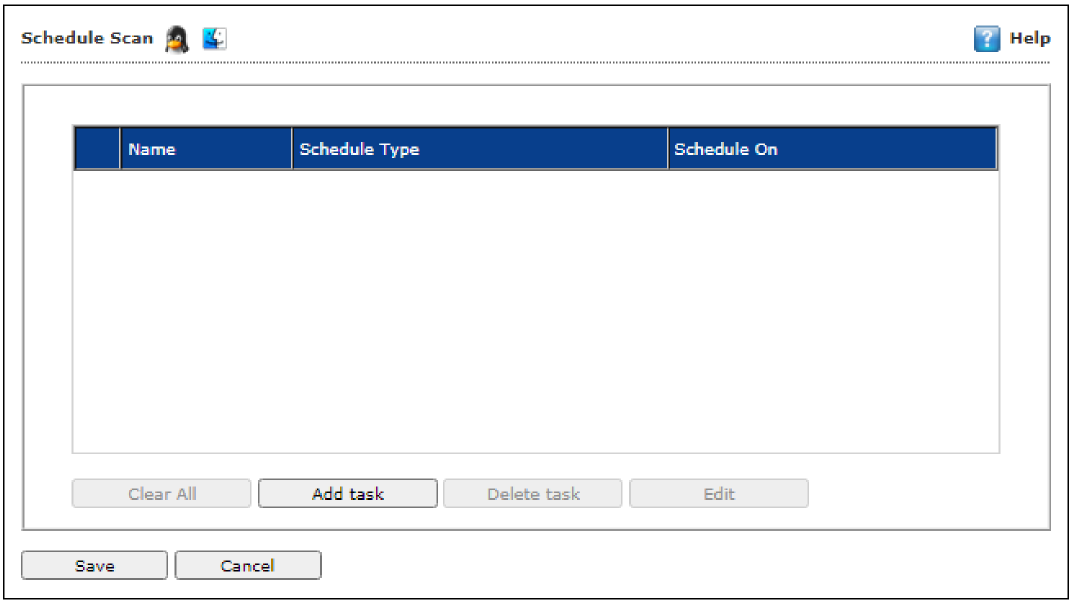
Exclude Folders and Files – Select this checkbox if you want eScan real-time protection to exclude Folders and files from scanning. eScan lets you add; Remove any or all Added Files or Folders whenever required during On Demand Scanning.

Scan options

- **Mails** – It indicates scanning the mail files. By default, it is selected. Select this checkbox if you want eScan real-time protection to scan mails.
- **Archives** – It indicates the archived files, such as zip, rar, and so on. Select this checkbox if you want eScan real-time protection to scan archived files.
- **Packed** – It indicates the compressed executable.
- **Memory Scan** – This option ensures eScan scans the system's memory for any infection from malwares.
- **Include Sub Directories** – This option ensures eScan scans all the sub directories recursively under every directory and not only the first level of directories.
- **Heuristic** – Heuristic scanning is almost identical to signature scanning, which instead of looking for specific signatures looks for certain instructions or commands within a program/application. This results in the detection of potentially malicious function in program/application.
- **Cross File System** – that facilitates scanning of files over cross-file systems.
- **Follow Symbolic Links** – scans the files following the symbolic links.
- **Memory Scan** – This will scan the memory of the system.

You can restore default eScan settings by clicking **Default**.

Schedule Scan

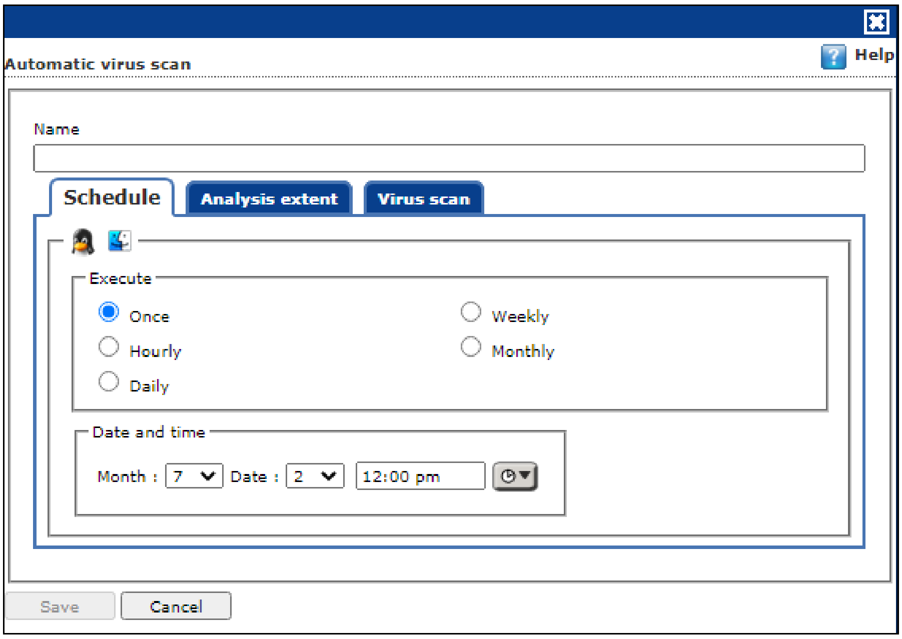


It lets you add a task for scheduling a scan.

Adding a task - It lets you schedule and define options for Analysis extent and the files or folders to be scanned.

Automatic Virus Scan

Schedule



Name

Execute

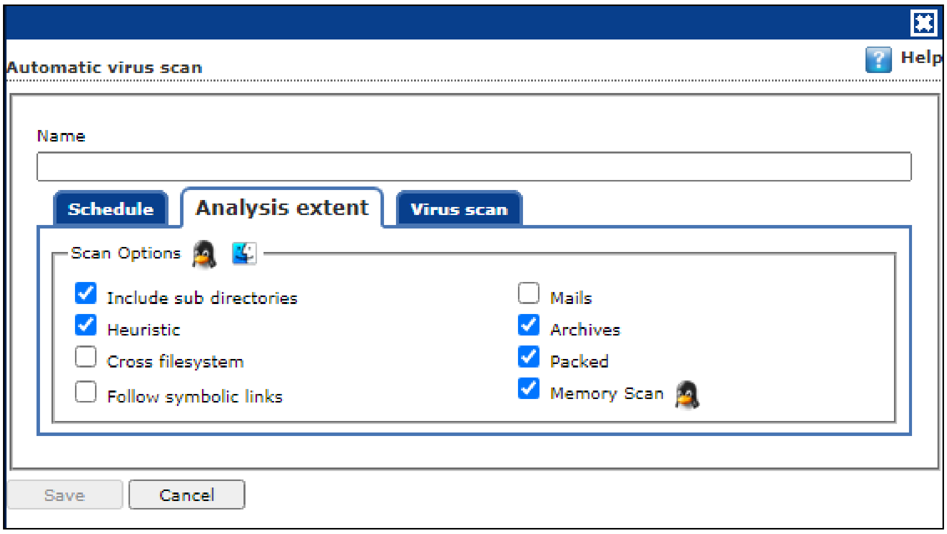
● Once
○ Hourly
○ Daily
○ Weekly
○ Monthly

Date and time

Month : 7 Date : 2 12:00 pm

Using this tab you can define the task name and schedule it as desired. You can schedule the scan once, weekly basis, every hour, monthly or daily. It also lets you schedule virus scan at desired date and time.

Analysis Extent



Automatic virus scan

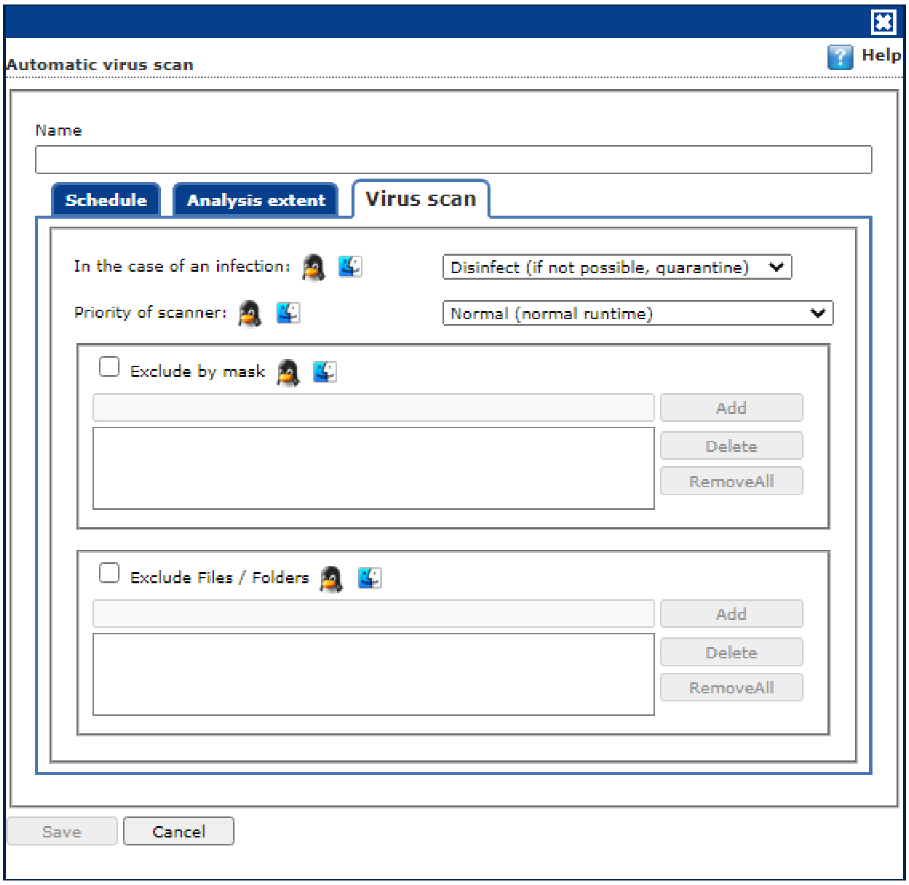
Scan Options

☑ Include sub directories
☑ Heuristic
□ Cross filesystem
□ Follow symbolic links
□ Mails
☑ Archives
☑ Packed
☑ Memory Scan

Using this tab you can define the scan options for Linux and Mac computers connected to the network.

- **Include sub Directories** – This option lets you include sub directories while conducting an automatic scan.
- **Heuristic Scan** – Heuristic scanning is almost identical to signature scanning, which instead of looking for specific signatures looks for certain instructions or commands within a program/application. This results in the detection of potentially malicious function in program/application.
- **Cross File System** facilitates scanning of files over cross-file systems.
- **Symbolic Link Scanning** scans the files following the symbolic links.
- **Mails -** It indicates scanning the mail files. By default, it is selected. Select this checkbox if you want eScan real-time protection to scan mails.
- **Archives -** It indicates the archived files, such as zip, rar, and so on. Select this checkbox if you want eScan real-time protection to scan archived files.
- **Packed -** It indicates the compressed executable. Select this checkbox if you want eScan real-time protection to scan packed files.
- **Memory Scan -** This option will only scan the memory of the system.

Virus Scan



Name

In the case of an infection: Disinfect (if not possible, quarantine)

Priority of scanner: Normal (normal runtime)

□ Exclude by mask

□ Exclude Files / Folders

Actions in case of Infection [Drop-down]
It displays a list of actions eScan should take, in case of virus detection. By default, Disinfect (if not possible, quarantine file) option is selected. Following are the types of actions:

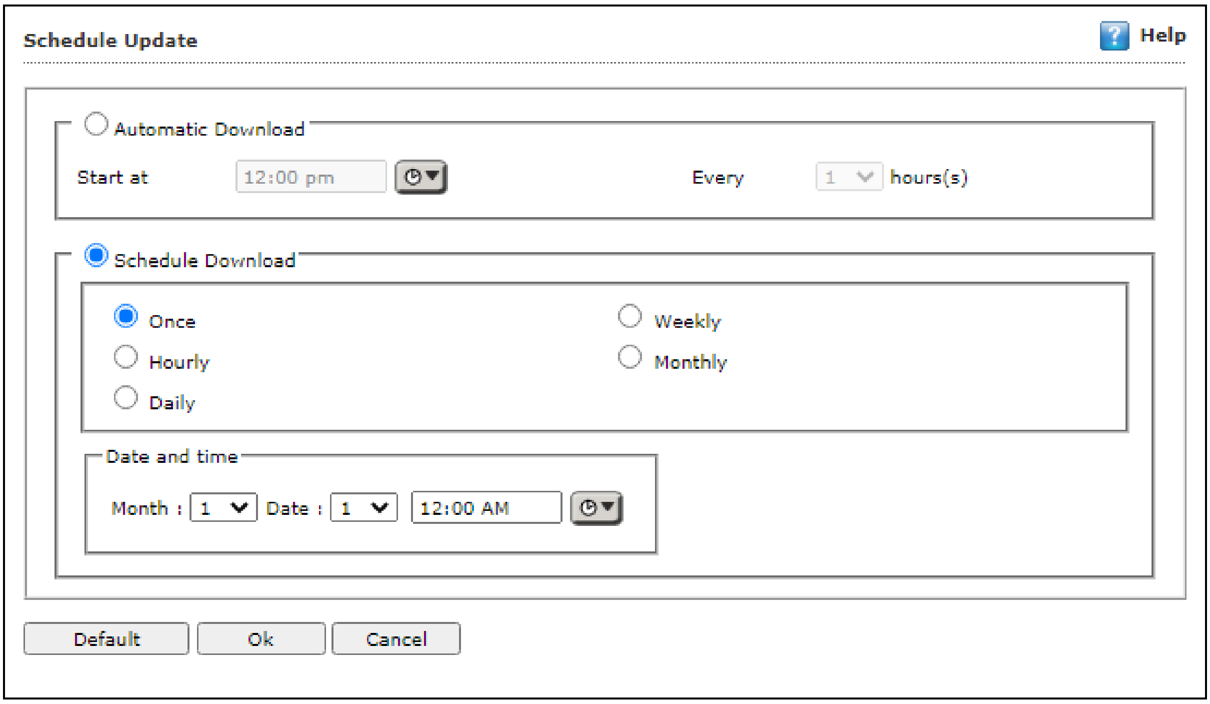
- **Log Only:** It indicates or alerts the user about the infection detected.
- **Disinfect (if not possible, log):** It tries to disinfect and if disinfection is not possible it logs the information of only the infected object.
- **Disinfect (if not possible, delete file):** It tries to disinfect and if disinfection is not possible it deletes the infected object.
- **Disinfect (if not possible, quarantine file):** It tries to disinfect and if disinfection is not possible it quarantines the infected object.
- **Delete:** Infected objects are deleted with this option.
- **Quarantine:** Infected objects are quarantined with this option.

Exclude file types (Mask) - Select this checkbox if you want eScan real-time protection to exclude specific files, and then add the directories and files that you want to exclude by clicking **Add**. eScan lets you Remove any or all Added Files whenever required.

Exclude Folders and files - Select this checkbox if you want eScan real-time protection to exclude Folders and files from scanning. eScan lets you add; Remove any or all Added Files or Folders whenever required.

Schedule Update

This module lets you schedule the updates for Linux computers.



Schedule Update

○ Automatic Download

Start at 12:00 pm Every 1 hours(s)

● Schedule Download

● Once ○ Weekly
○ Hourly ○ Monthly
○ Daily

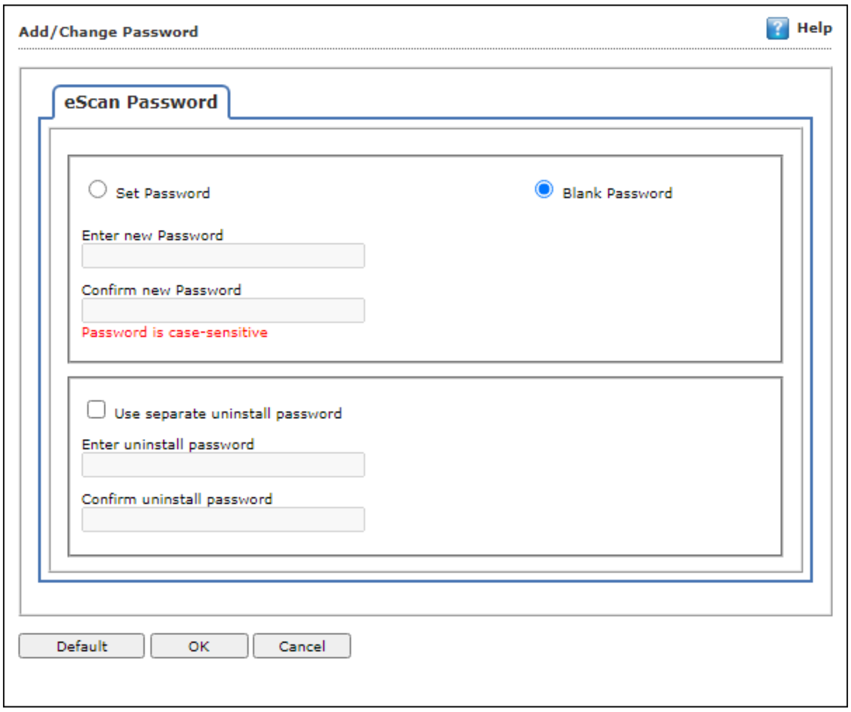
Date and time

Month : 1 Date : 1 12:00 AM

- The updates can be downloaded automatically with **Automatic Download** option.
- The updates can be downloaded on a schedule basis with **Schedule Download** option. Select intervals and time basis as per your preferences.

Administrator Password

Administrator Password lets you create and change password for administrative login of eScan protection center for Linux computers. It also lets you keep the password as blank, wherein you can login to eScan protection center without entering any password. It also lets you define uninstallation password which will be required before uninstalling eScan Client from managed computers manually. The user will not be able to uninstall eScan Client without entering uninstallation password.



Add/Change Password

eScan Password

○ Set Password ● Blank Password

Enter new Password

Confirm new Password

Password is case-sensitive

□ Use separate uninstall password

Enter uninstall password

Confirm uninstall password

To Add/Change eScan administrator password:

Set Password
Click this option, if you want to set password.

Blank Password
Click this option, if you do not want to set any password for login.
When you click this option, the **Enter new Password** and **Confirm new Password** fields become unavailable.

Enter new Password
Enter the new password.

Confirm new Password
Re-enter the new password for confirmation.

Use separate uninstall password
Click this option, if you want to set password before uninstallation of eScan Client.

Enter uninstall Password
Enter the uninstallation password.

Confirm uninstall Password
Re-enter the uninstallation password for confirmation.

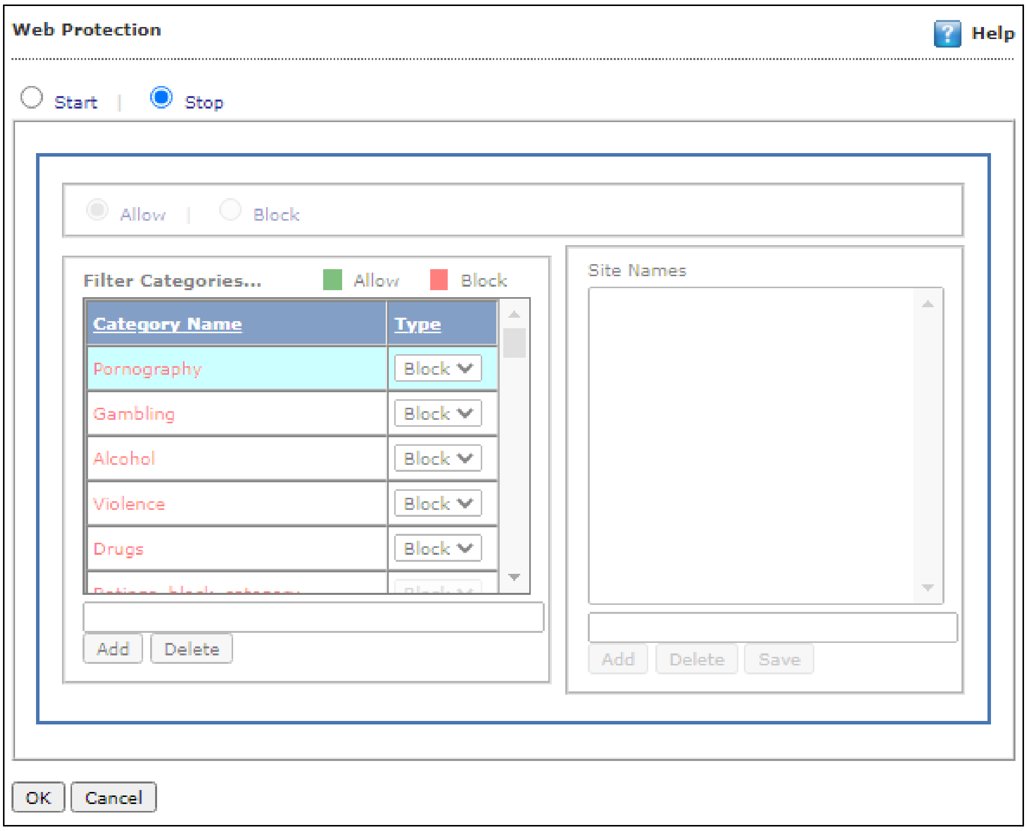
After filling all fields, click **OK**. The Password will be saved.

Web Protection

Web Protection module lets you block websites containing pornographic or offensive material for Linux computers. This feature is extremely beneficial to parents because it prevents kids from accessing websites containing harmful or restricted content. Administrators can also use this feature to prevent employees from accessing non-work-related websites during work hours. You can configure the following settings:

Start/Stop

It lets you enable/disable **Web-Protection** module. Click the appropriate option.



Web Protection

○ Start | ● Stop

● Allow | ○ Block

Filter Categories... 🟩 Allow 🟥 Block

Category Name	Type
Pornography	Block
Gambling	Block
Alcohol	Block
Violence	Block
Drugs	Block

You can configure the following settings.

Filtering Options

This tab has predefined categories that help you control access to the Internet.

Status

This section lets you allow or block access to specific websites based on Filter Categories. You can set the status as **Active** or **Block** web access. Select the **Block Web Access** option if you want to block all the websites except the ones that have been listed in the **Filter Categories**. When you select this option, only **Filtering Options** and **Pop-up Filter** tabs are available.

Filter Categories

This section uses the following color codes for allowed and blocked websites.

- **Green**: It represents an allowed websites category.
- **Red**: It represents a blocked websites category.

The filter categories used in this section include categories like Pornography, Gambling, Chat, Alcohol, Violence, Drugs, Ratings block category, Websites Allowed, etc. You can also add or delete filter categories depending on your requirement.

Category Name

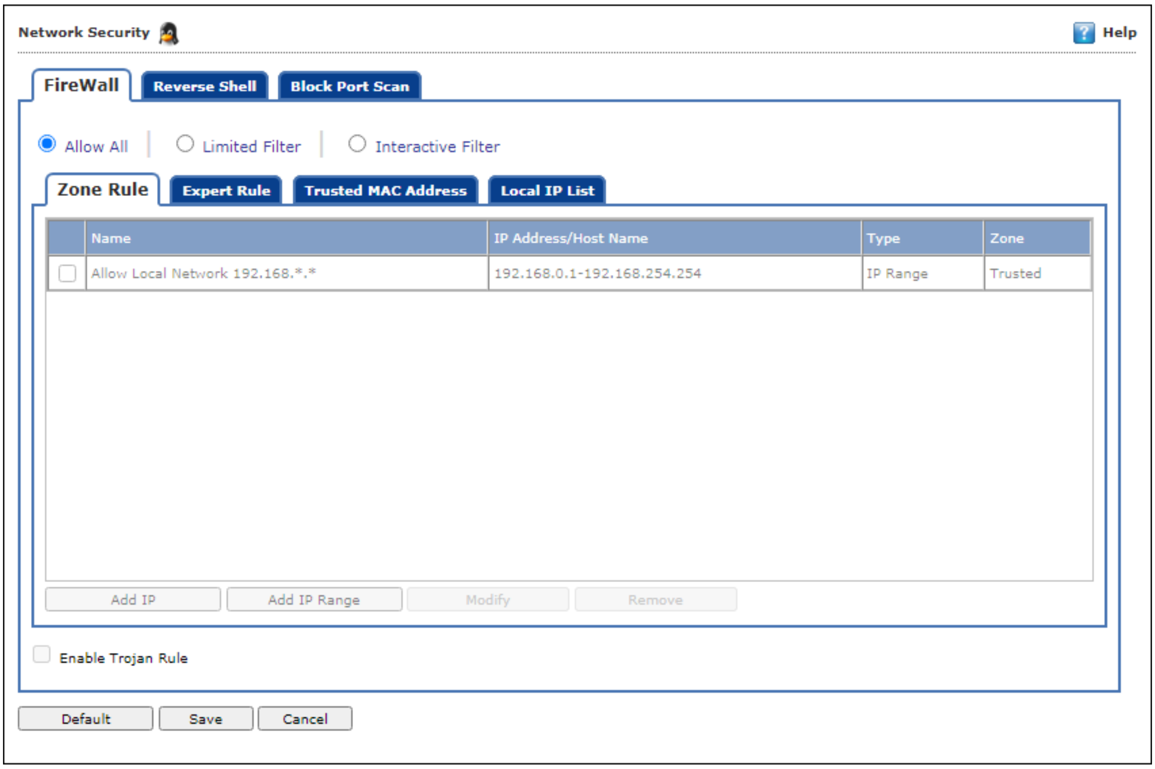
This section shows the **Words/Phrases** list. It lists the words or phrases present in the selected category. In addition, the section displays the **Site Names** list, which lists the websites belonging to the selected category. You can also add or delete filter categories depending on your requirement.

Filter Options

This section includes the **Add sites rejected by the filter to Block category checkbox**. Select this option if you want eScan to add websites that are denied access to the Block category database automatically.

Network Security

Network Security module helps to 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.



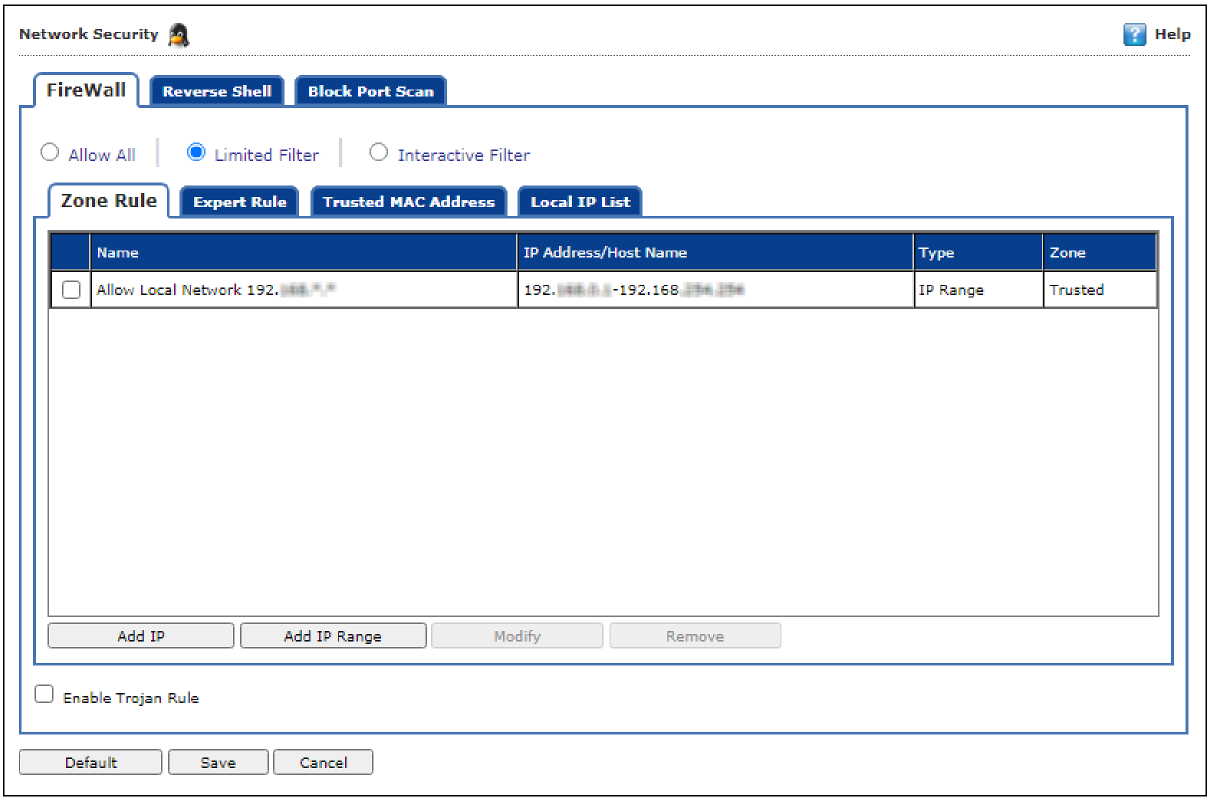
● Allow All | ○ Limited Filter | ○ Interactive Filter

	Name	IP Address/Host Name	Type	Zone
□	Allow Local Network 192.168.*.*	192.168.0.1-192.168.254.254	IP Range	Trusted

□ Enable Trojan Rule

Firewall

This tab is designed to monitor all incoming and outgoing network traffic and protect your endpoint from all types of network based attacks. eScan includes a set of predefined access control rules that you can remove or customize as per your requirements. These rules enforce a boundary between your computer and the network. These rules include Zone Rules, Expert Rules, Trusted Media Access Control (MAC) Address, and Local IP list.



Network Security

○ Allow All | ● Limited Filter | ○ Interactive Filter

	Name	IP Address/Host Name	Type	Zone
□	Allow Local Network 192.[redacted]	192.[redacted]-192.168[redacted]	IP Range	Trusted

□ Enable Trojan Rule

You can configure the following settings to be deployed to the eScan client systems.
Allow All – Clicking **Allow All** disables the eScan Firewall i.e. all the incoming and outgoing network traffic will not be monitored/filtered.

Limited Filter – Clicking **Limited Filter** enables eScan Firewall in limited mode which will monitor all incoming traffic only and will be allowed or blocked as per the conditions or rules defined in the Firewall.

Interactive – Clicking **Interactive** enables eScan Firewall to monitor all the incoming and outgoing network traffic and will be allowed or blocked as per the conditions or rules defined in the Firewall.

Following tabs are available:

- **Zone Rule**
- **Expert Rule**
- **Trusted MAC Address**
- **Local IP List**

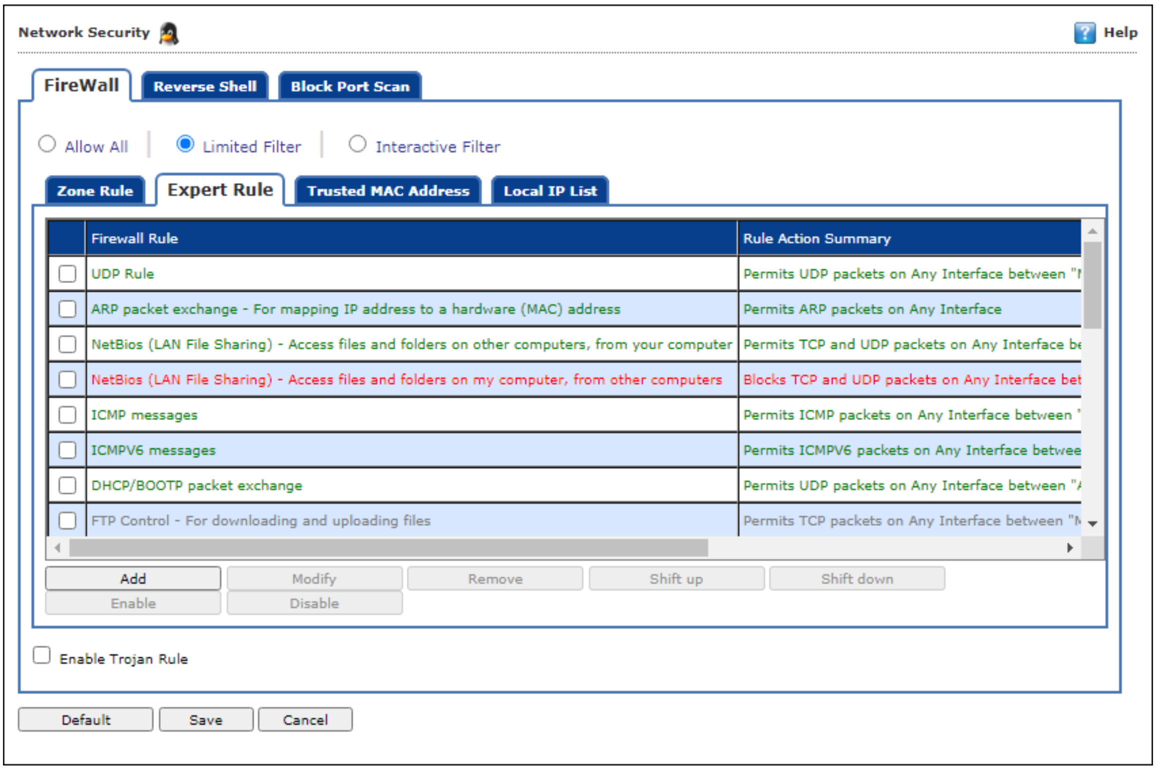
Zone Rule

This is a set of network access rules to make the decision of allowing/blocking of the access to the system. This will contain the source IP address or source Host name or IP range either to be allowed or blocked. The following buttons are available for configuring zone rule:

- **Add 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.



○ Allow All | ● Limited Filter | ○ Interactive Filter

	Firewall Rule	Rule Action Summary
□	UDP Rule	Permits UDP packets on Any Interface between "
□	ARP packet exchange - For mapping IP address to a hardware (MAC) address	Permits ARP packets on Any Interface
□	NetBios (LAN File Sharing) - Access files and folders on other computers, from your computer	Permits TCP and UDP packets on Any Interface be
□	NetBios (LAN File Sharing) - Access files and folders on my computer, from other computers	Blocks TCP and UDP packets on Any Interface bet
□	ICMP messages	Permits ICMP packets on Any Interface between '
□	ICMPV6 messages	Permits ICMPV6 packets on Any Interface betwee
□	DHCP/BOOTP packet exchange	Permits UDP packets on Any Interface between "
□	FTP Control - For downloading and uploading files	Permits TCP packets on Any Interface between "

□ Enable Trojan Rule

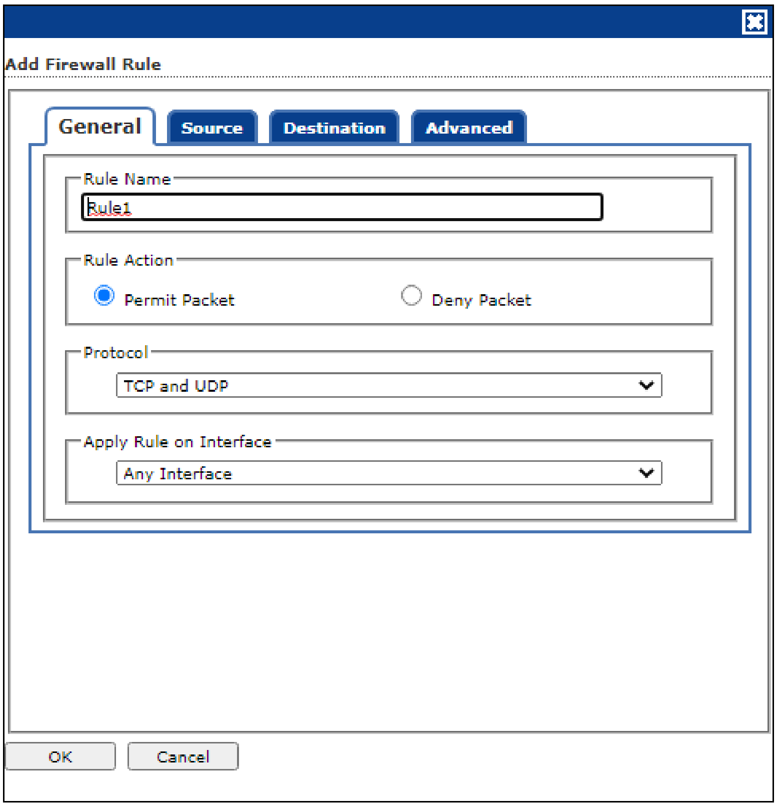
However, configure these rules only if you are familiar with firewalls and networking protocols.

- Source IP Address/Host Name
- Source Port Number

- Destination IP Address/Host Name
- Destination Port Number

The following buttons are available to configure an Expert Rule:

1. **Add** – Click **Add** to create a new Expert Rule. In the Add Firewall Rule Window:



Add Firewall Rule

Rule Name: Rule1

Rule Action: ● Permit Packet ○ Deny Packet

Protocol: TCP and UDP

Apply Rule on Interface: Any Interface

General tab

In this section, specify the Rule settings:

Rule Name – Provide a name to the Rule.

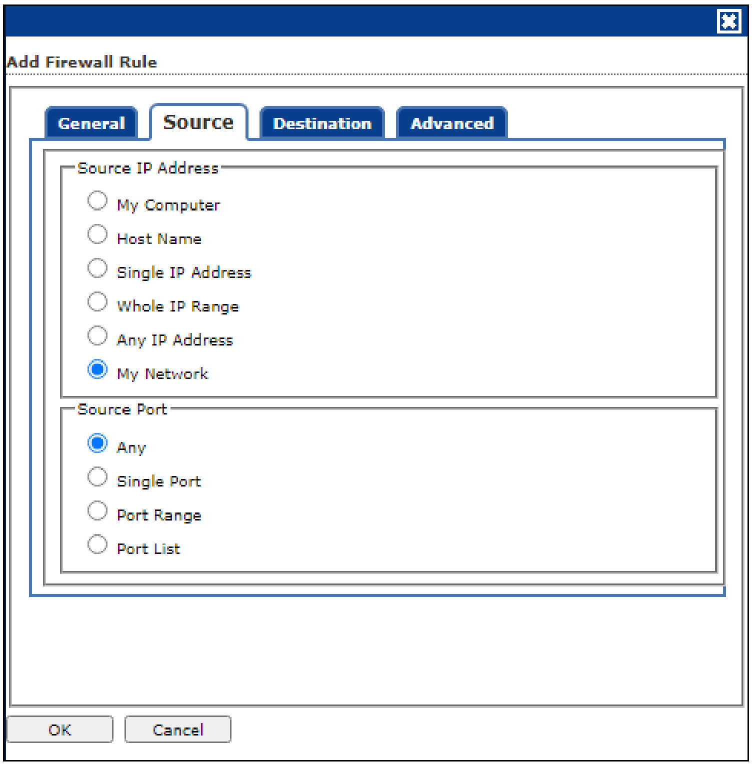
Rule Action – Action to be taken, whether to Permit Packet or Deny Packet.

Protocol – Select the network protocol (e.g. TCP, UDP, ARP) on which the Rule will be applied.

Apply rule on Interface – Select the Network Interface on which the Rule will be applied.

Source tab

In this section, specify/select the location from where the outgoing network traffic originates.



Add Firewall Rule

Source IP Address

○ My Computer
○ Host Name
○ Single IP Address
○ Whole IP Range
○ Any IP Address
● My Network

Source Port

● Any
○ Single Port
○ Port Range
○ Port List

Source IP Address:

My Computer – The rule will be applied for the outgoing traffic originating from your computer.

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.

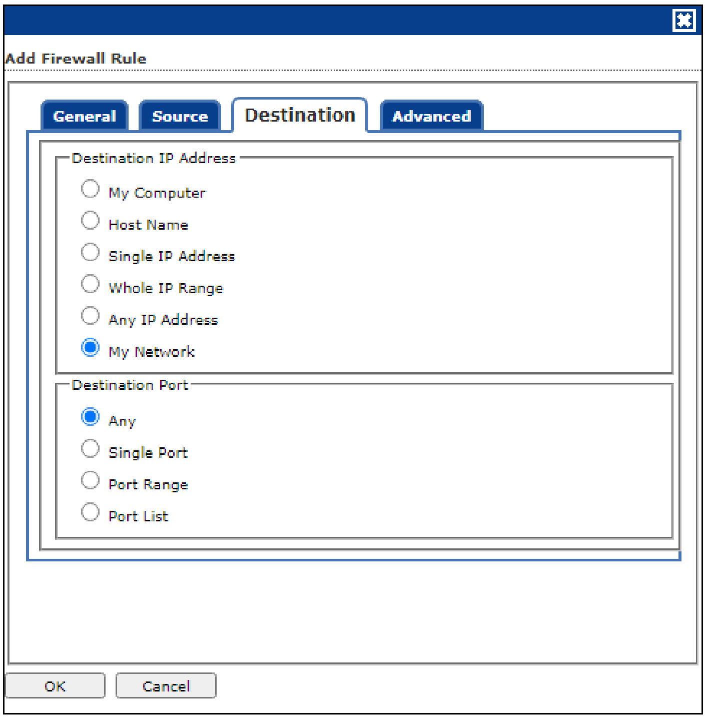
Port Range – To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the outgoing traffic originating from the port which is within the defined range of ports.

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.


Add Firewall Rule

Destination IP Address

○ My Computer
○ Host Name
○ Single IP Address
○ Whole IP Range
○ Any IP Address
● My Network

Destination Port

● Any
○ Single Port
○ Port Range
○ Port List

Destination IP Address:

My Computer – The rule will be applied for the incoming traffic to your computer.

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.

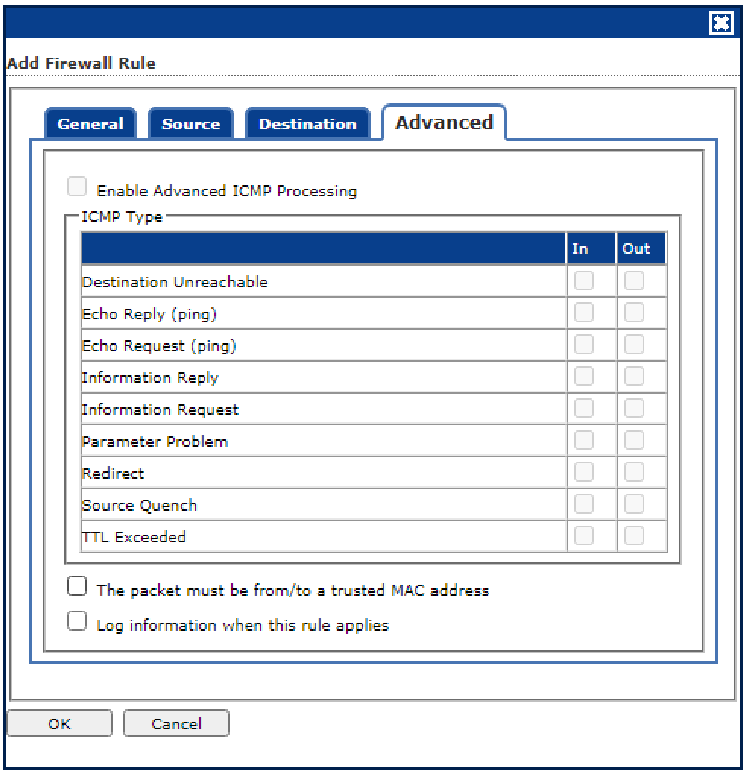
Single Port – After selecting this option, the rule will be applied for the incoming traffic to the specified/defined port.

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

ICMP Type

	In	Out
Destination Unreachable	□	□
Echo Reply (ping)	□	□
Echo Request (ping)	□	□
Information Reply	□	□
Information Request	□	□
Parameter Problem	□	□
Redirect	□	□
Source Quench	□	□
TTL Exceeded	□	□

□ The packet must be from/to a trusted MAC address

□ Log information when this rule applies

Enable Advanced ICMP Processing - This is activated when the ICMP protocol is selected in the General tab.

The packet must be from/to a trusted MAC address – When this option is selected, the rule will only be applied on the MAC address defined/listed in the Trusted MAC Address tab.

Log information when this rule applies – This will enable to log information of the Rule when it is implied.

Use the following buttons in this tab as and when required:

Modify – Clicking **Modify** lets you modify any Expert Rule.

Remove – Clicking **Remove** lets you delete a rule from the Expert Rule.

Shift Up and Shift Down– The UP and DOWN arrow button will enable to move the rules up or down as required and will take precedence over the rule listed below it.

Enable Rule/Disable Rule – These buttons lets you enable or disable a particular selected rule from the list.

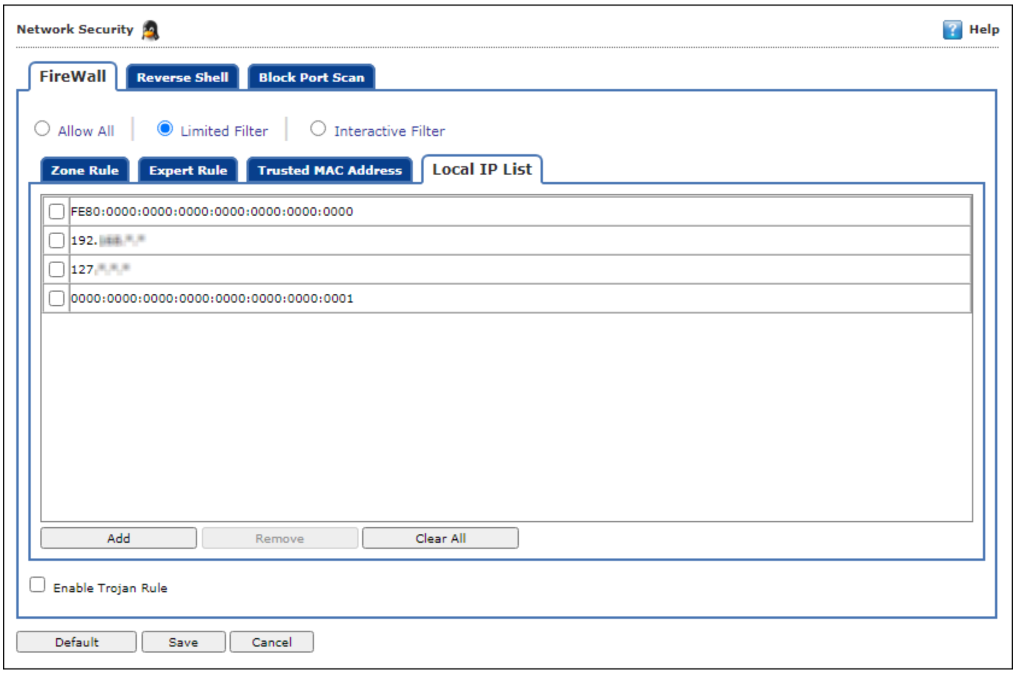
Trusted MAC Address

This section contains the information of the MAC address of the system. A MAC address is a hardware address that uniquely identifies each node of a network. The Trusted MAC address list will be checked along with the Expert Rule only when "The packet must be from/to a trusted MAC address" option is checked and the action will be as per specified in the rule. (Refer to the *Advance Tab* of the Expert Rule). The following buttons are available to configure the Trusted Mac Address:

- **Add –** To add a MAC address click on this button. Enter the MAC address to be added in the list for e.g. 00-13-[redacted]
- **Edit –** To modify/change the MAC Address, click **Edit**.
- **Remove –** To delete the MAC Address, click **Remove**.
- **Clear All –** To delete the entire listed MAC Address, click **Clear All**.

Local IP List

This section contains a list of Local IP addresses.



□ FE80:0000:0000:0000:0000:0000:0000:0000
□ 192.[redacted]
□ 127[redacted]
□ 0000:0000:0000:0000:0000:0000:0000:0001

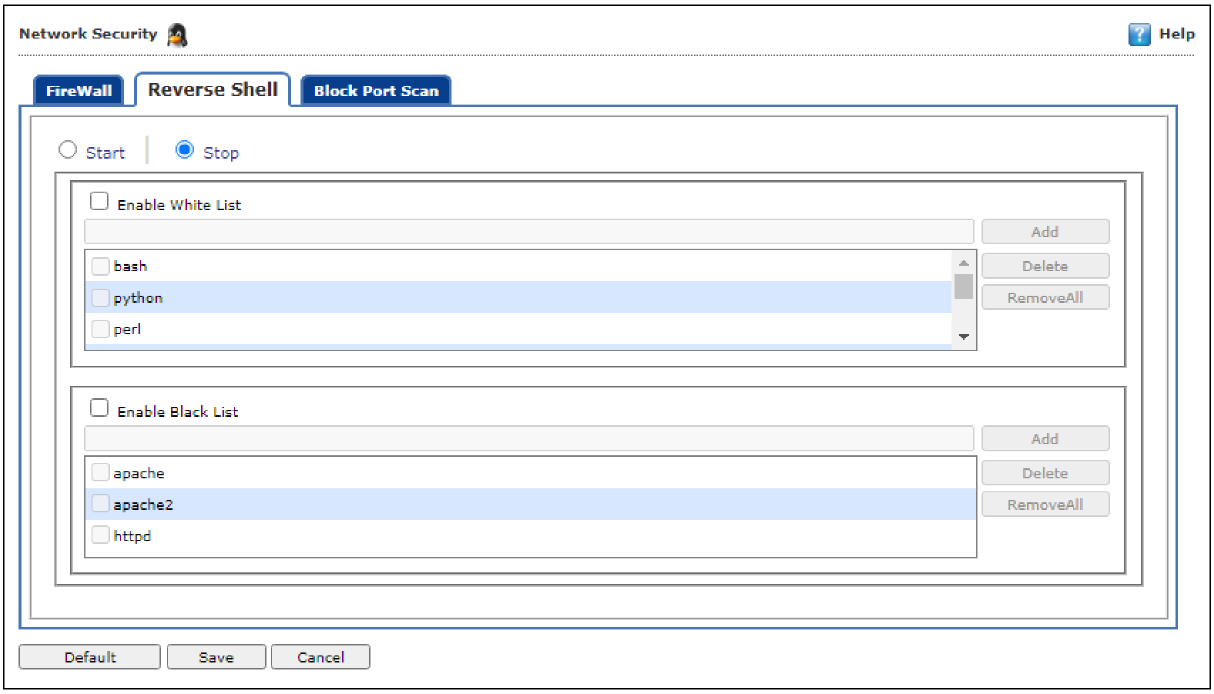
Add – To add a local IP address, click **Add**.
Remove – To remove a local IP address, click **Remove**.
Clear All – To clear all local IP addresses, click **Clear All**.

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.



Network Security

Help

FireWall | Reverse Shell | Block Port Scan

○ Start | ● Stop

□ Enable White List

- □ bash
- □ python
- □ perl

□ Enable Black List

- □ apache
- □ apache2
- □ httpd

Start/Stop

It allows you enable/disable **Network Security** module.

After enabling this, you can configure the following settings:

Enable White List

Select this checkbox to whitelist the trusted script languages, such as bash, Python, Perl, and more. You can add and delete the script languages from whitelisting.

- **Add**: To add a script language, select the language and click **Add**.
- **Delete**: To delete a script language, select a language and click **Delete**.
- **Remove All**: To remove all the whitelisted script language, click **Remove All**.

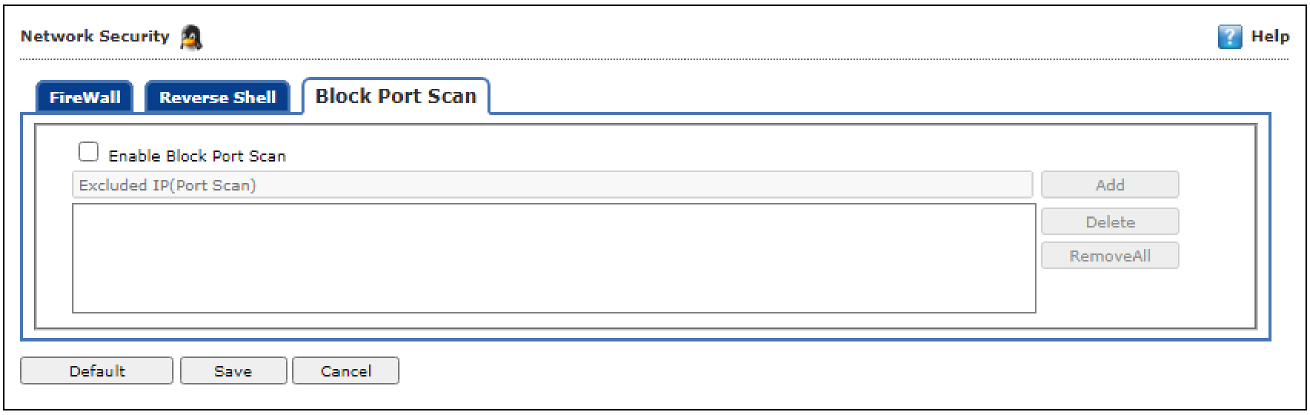
Enable Black List

Select this checkbox to blacklist the untrusted and risky script languages.

- **Add**: To add a script language, select the language and click **Add**.
- **Delete**: To delete a script language, select a language and click **Delete**.
- **Remove All**: To remove all the blacklisted script language, click **Remove All**.

Block Port Scan

This tab allows admin to configure the port scan option.



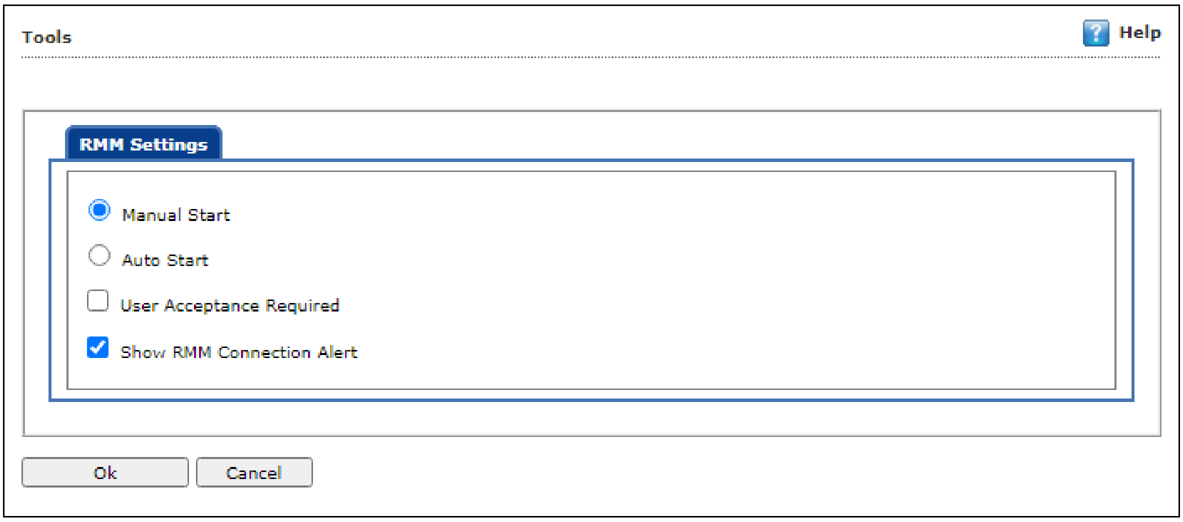
Enable Block Port Scan

Select this checkbox to enable the port scan option. You can add and delete the IP addresses that need to exclude from the port scan.

- **Add**: To add an IP, enter the IP address and click **Add**.
- **Delete**: To delete an IP, select the IP address and click **Delete**.
- **Remove All**: To remove all the excluded IP addresses, click **Remove All**.

Tools

The RMM settings let you configure default connection settings for connecting to client computers. You will get the following configuration options:



Tools

RMM Settings

● Manual Start

○ Auto Start

□ User Acceptance Required

☑ Show RMM Connection Alert

- **Manual Start**: If this option is selected, client endpoint users have to manually start the RMM service to establish a RMM connection.
- **Auto Start**: If this option is selected, RMM service will be started automatically and all client endpoints will be connected to your main eScan server.
- **User Acceptance Required**: If this 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**: 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.

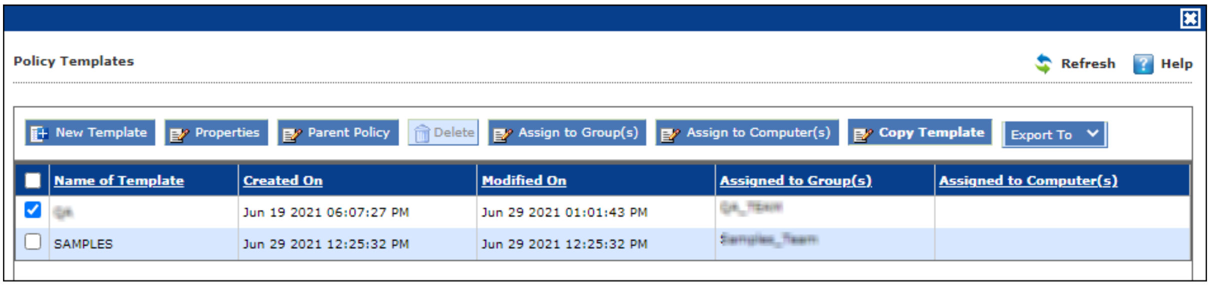
Assigning Policy Template to a group

There are two ways to assign the policy template to group:

Method 1

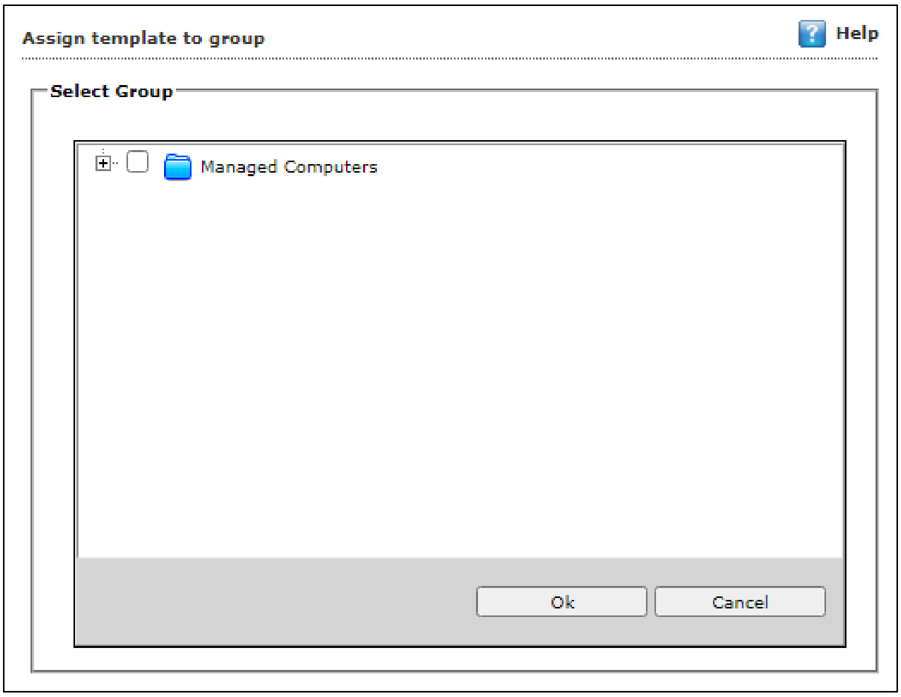
To assign a Policy to a group:

1. In the Managed Computers screen, click **Policy Templates**.
   Policy Templates window appears.
2. In the **Policy Templates** window, select a policy template.



	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
☑	[redacted]	Jun 19 2021 06:07:27 PM	Jun 29 2021 01:01:43 PM	[redacted]	
□	SAMPLES	Jun 29 2021 12:25:32 PM	Jun 29 2021 12:25:32 PM	[redacted]	

3. Click **Assign to Group(s)**.
   Select Group window appears.

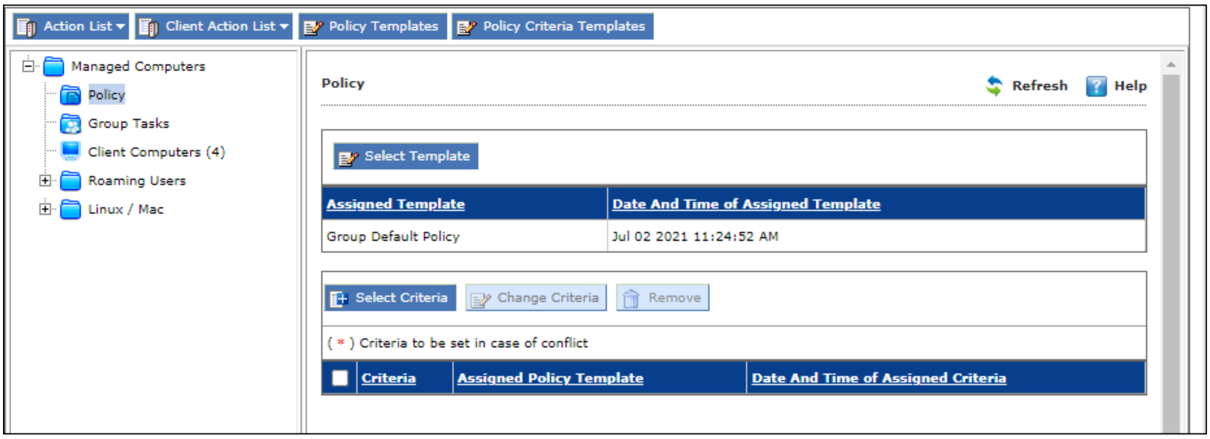


4. Select the group(s) and then click **OK**.
   The policy will be assigned to the selected group(s).

Method 2

To assign a Policy to the group:

1. In the Managed Computers folder tree, select a group.
2. Under the group, click **Policy**.
   Policy pane appears on the right side.

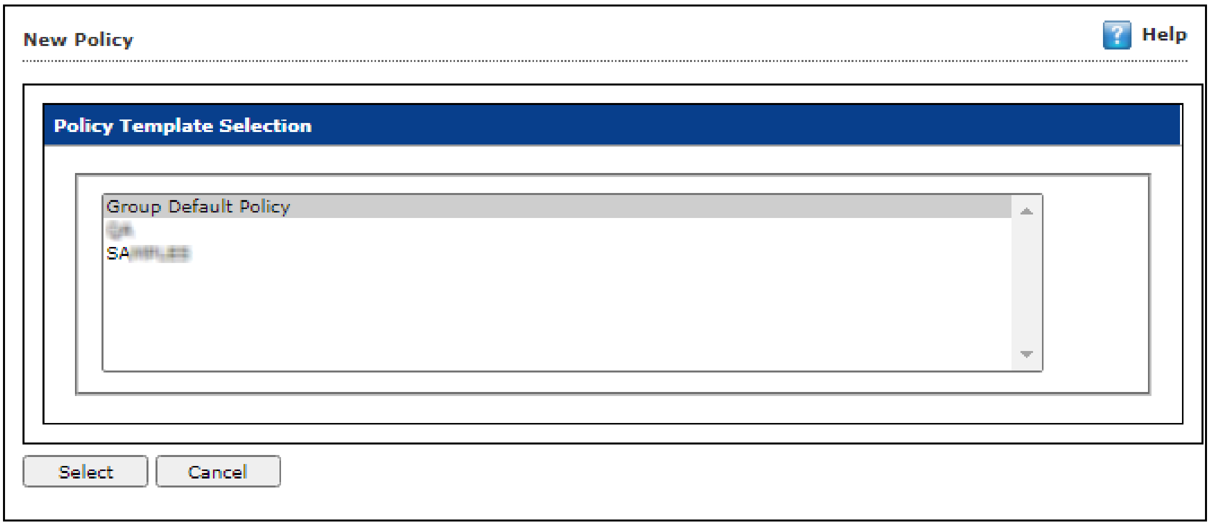


Assigned Template	Date And Time of Assigned Template
Group Default Policy	Jul 02 2021 11:24:52 AM

(*) Criteria to be set in case of conflict

□	Criteria	Assigned Policy Template	Date And Time of Assigned Criteria

3. In the right pane, click **Select Template**.
   New Policy window appears.

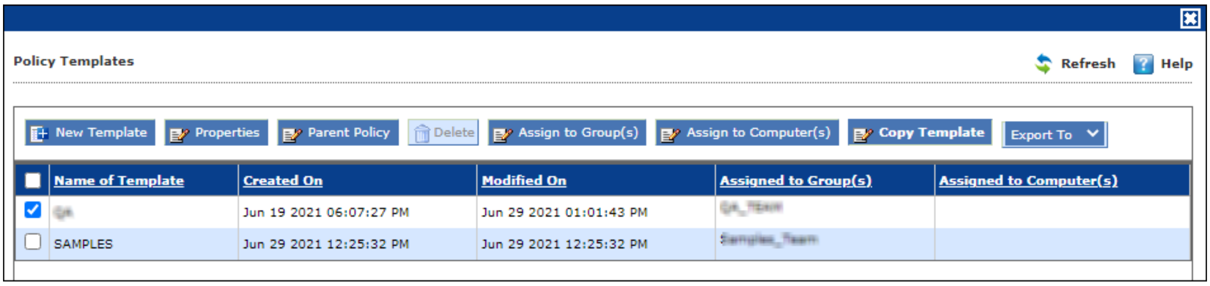


4. Select a policy template and then click **Select**.
   The default Policy Template for group will be saved and updated.

Assigning Policy Template to Computer(s)

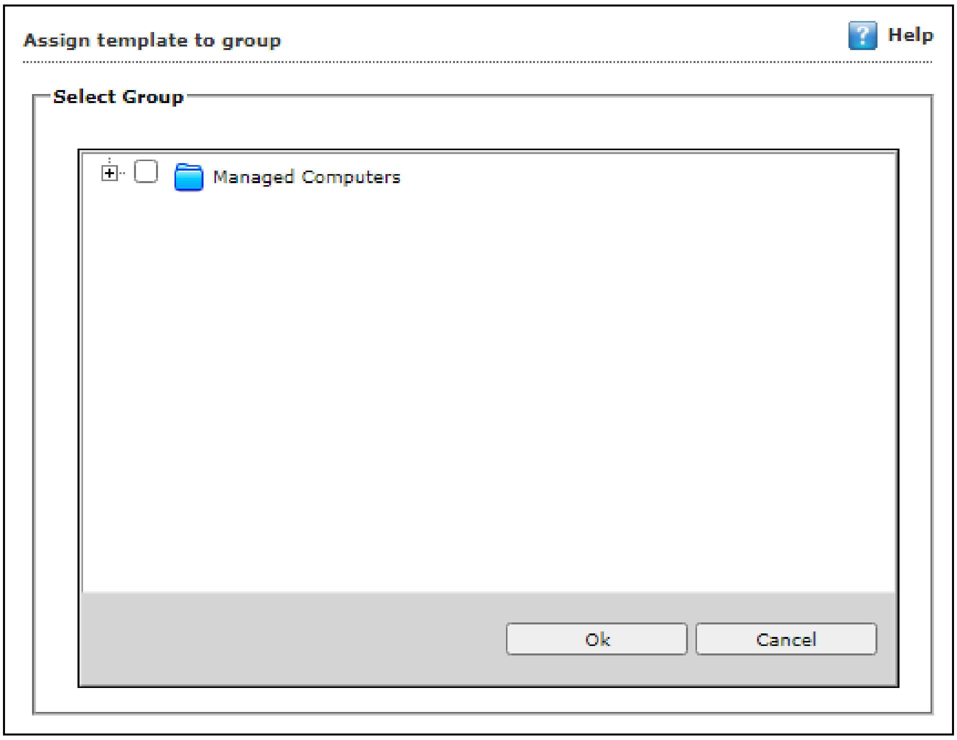
To assign a policy template to computers:

1. In the **Policy Templates** window, select a policy.



□	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
☑	[redacted]	Jun 19 2021 06:07:27 PM	Jun 29 2021 01:01:43 PM	[redacted]	
□	SAMPLES	Jun 29 2021 12:25:32 PM	Jun 29 2021 12:25:32 PM	[redacted]	

2. Click **Assign to Computer(s)**.
3. Assign Template to computer window appears.

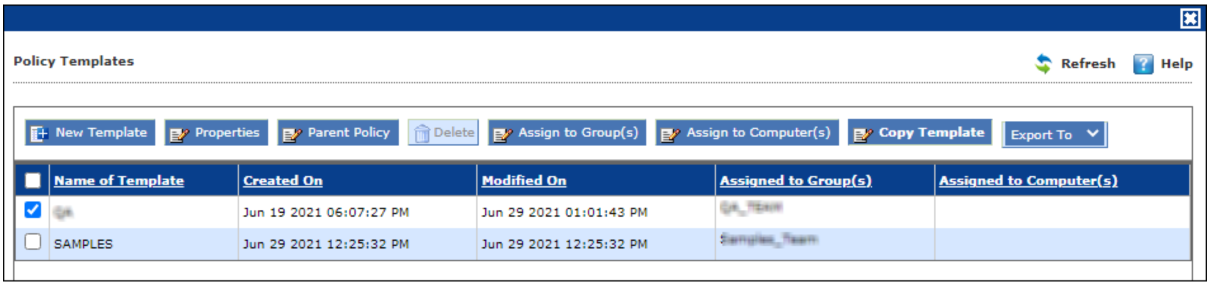


4. Click **Managed Computers**.
5. Select the computer(s) and then click **OK**.
   The policy template will be assigned to the selected computers.

Copying a Policy Template

To copy a Policy Template:

1. In the Policy Templates window, select a policy.



Policy Templates

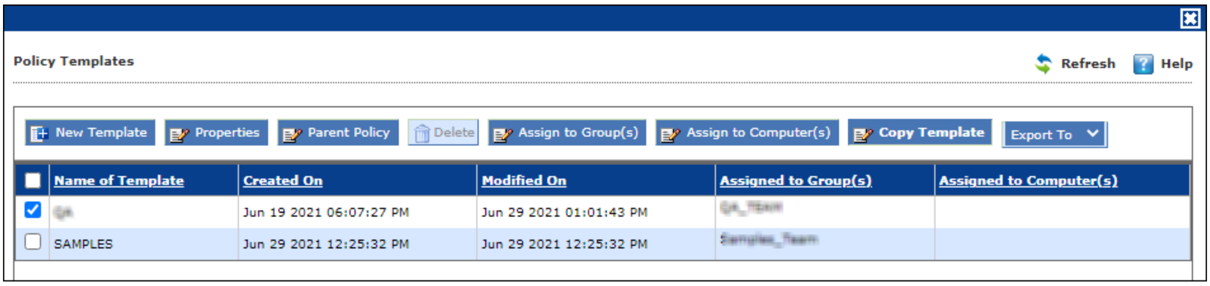
☐	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
☑	[redacted]	Jun 19 2021 06:07:27 PM	Jun 29 2021 01:01:43 PM	[redacted]	
☐	SAMPLES	Jun 29 2021 12:25:32 PM	Jun 29 2021 12:25:32 PM	[redacted]	

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:

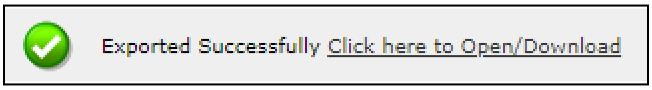
1. In the Policy Templates window, select a policy.



Policy Templates

☐	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
☑	[redacted]	Jun 19 2021 06:07:27 PM	Jun 29 2021 01:01:43 PM	[redacted]	
☐	SAMPLES	Jun 29 2021 12:25:32 PM	Jun 29 2021 12:25:32 PM	[redacted]	

2. Click **Export To**.
3. Select the file format from the drop-down menu (HTML, PDF, and Excel).
4. The Policy template report will be generated.

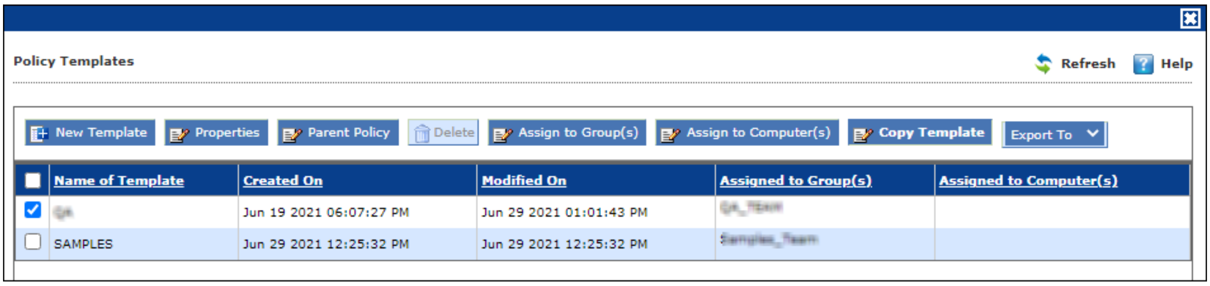

Exported Successfully Click here to Open/Download

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.

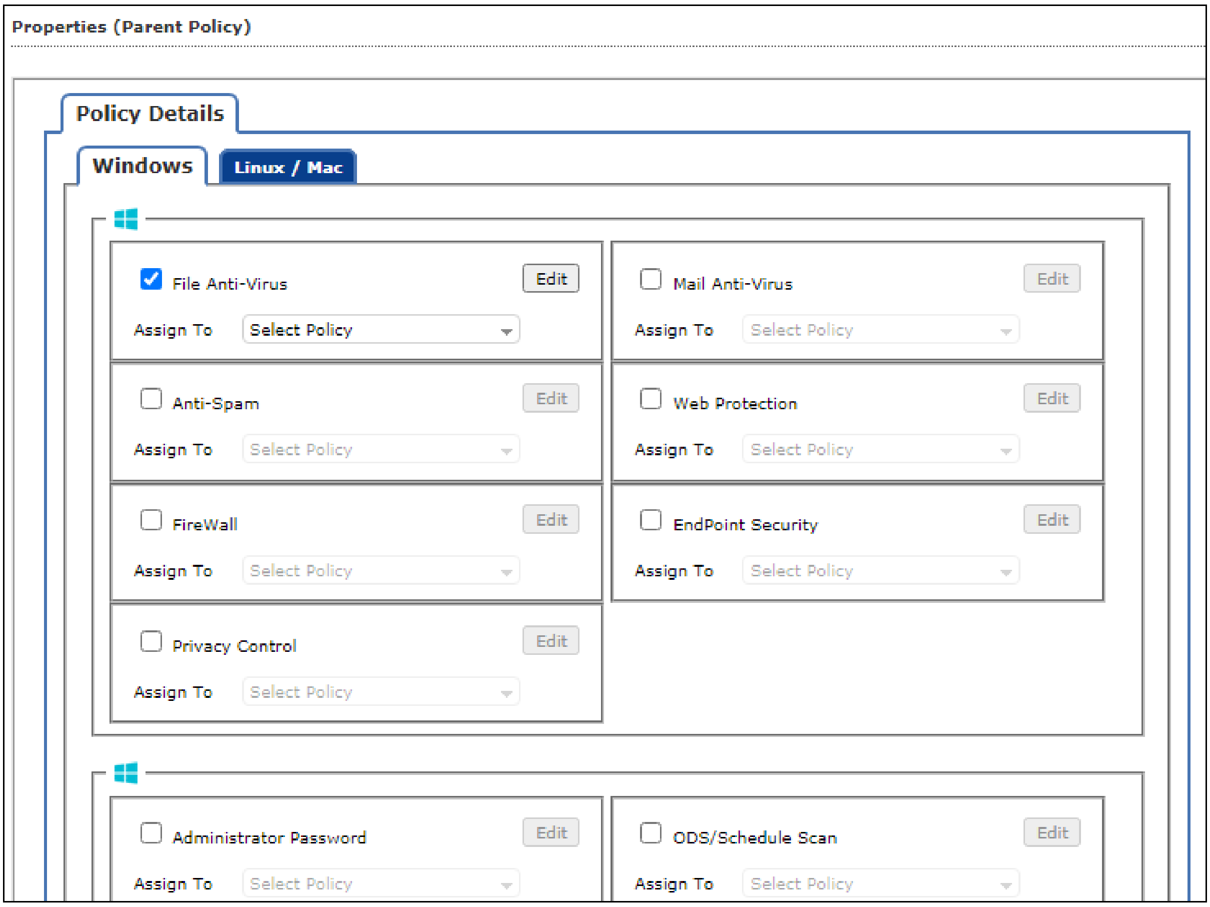
To configure Parent Policy, follow the steps given below:

1. In the Managed Computers screen, click **Policy Templates**.
   Policy Templates window appears.
2. In the Policy Template window, click **Parent Policy**.



□	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
☑	[redacted]	Jun 19 2021 06:07:27 PM	Jun 29 2021 01:01:43 PM	[redacted]	
□	SAMPLES	Jun 29 2021 12:25:32 PM	Jun 29 2021 12:25:32 PM	[redacted]	

Properties (Parent Policy) window appears displaying all the policies.



☑ File Anti-Virus
Assign To: Select Policy

□ Mail Anti-Virus
Assign To: Select Policy

□ Anti-Spam
Assign To: Select Policy

□ Web Protection
Assign To: Select Policy

□ FireWall
Assign To: Select Policy

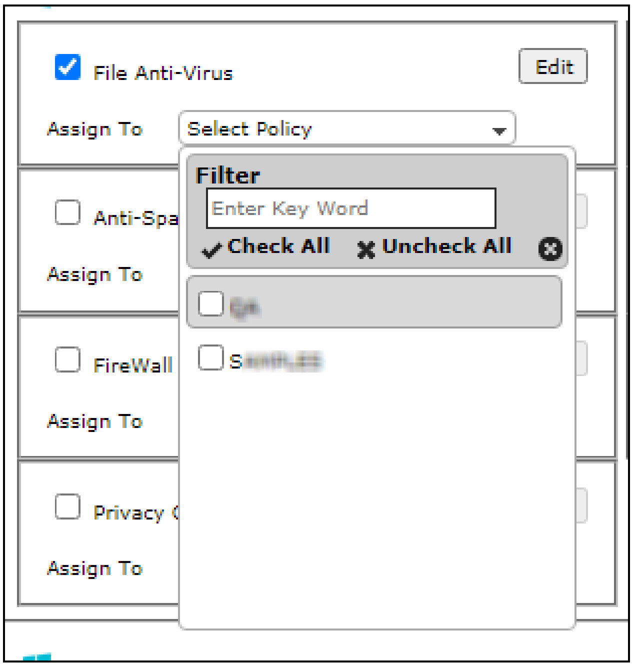
□ EndPoint Security
Assign To: Select Policy

□ Privacy Control
Assign To: Select Policy

□ Administrator Password
Assign To: Select Policy

□ ODS/Schedule Scan
Assign To: Select Policy

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.



☑ File Anti-Virus Edit

Assign To Select Policy

Filter

Enter Key Word

✓ Check All ✖ Uncheck All

□ [redacted]

□ [redacted]

□ Anti-Spa

Assign To

□ FireWall

Assign To

□ Privacy C

Assign To

5. Click **OK**. The Parent policy will be updated and changes will be applied to all the policies selected.

NOTE	Before disabling a module in Parent Policy, ensure that policies are unchecked from **Assign To** drop-down.

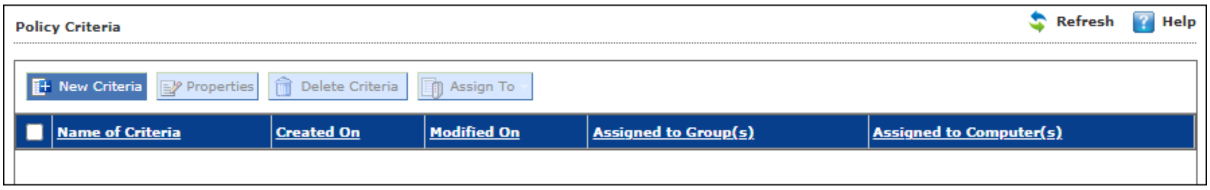
Policy Criteria Templates

This button allows to add criteria template based on the endpoints conditions.

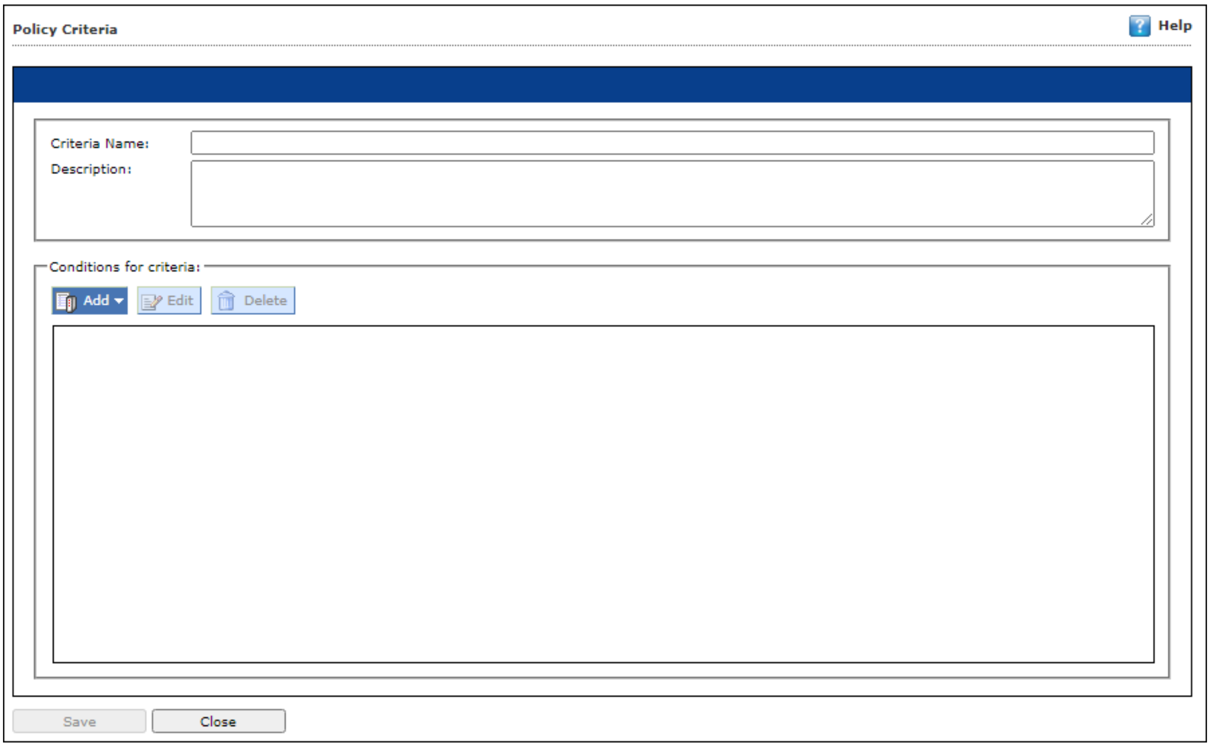
Adding a Policy Criteria Template

To define Policy Criteria Template, follow the steps given below:

1. In the Managed Computers screen, click **Policy Criteria Templates**.
   Policy Criteria screen appears.

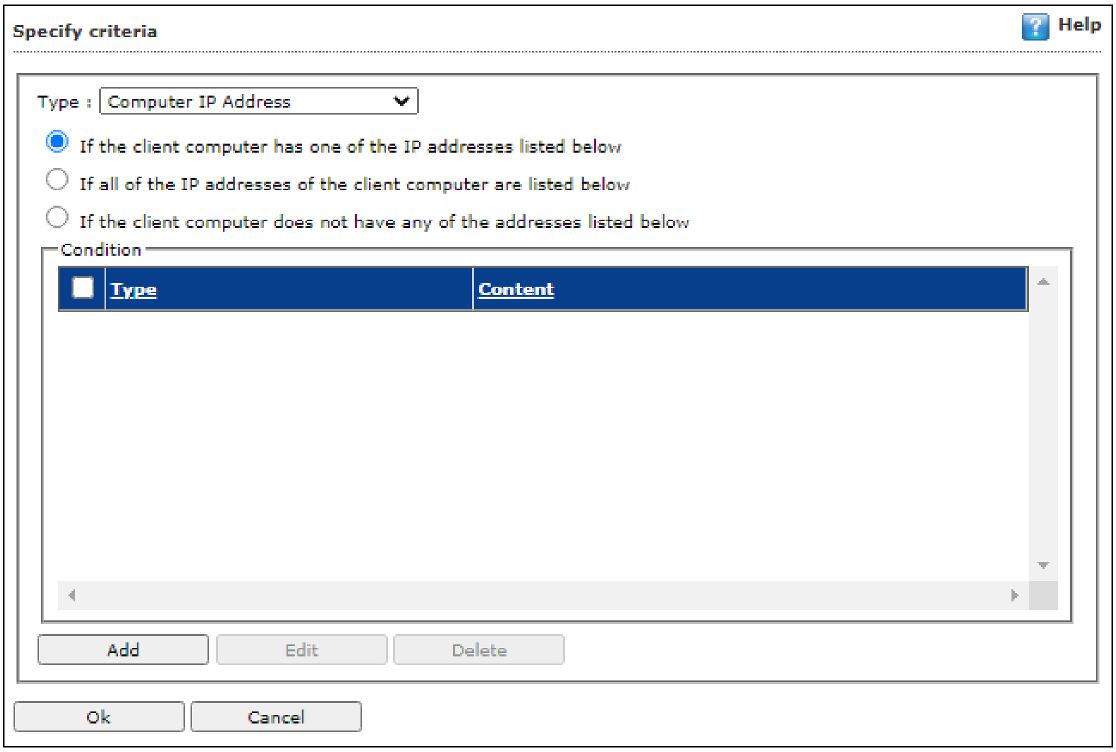


2. Click **New Criteria**.
   Policy Criteria screen displays parameter for creation.



3. Enter **Name** and **Description**.
4. Click **Add** drop-down.
5. Click **Add AND Condition**.

Specify Criteria screen appears.


Specify criteria

Type : Computer IP Address

● If the client computer has one of the IP addresses listed below

○ If all of the IP addresses of the client computer are listed below

○ If the client computer does not have any of the addresses listed below

Condition

□	Type	Content

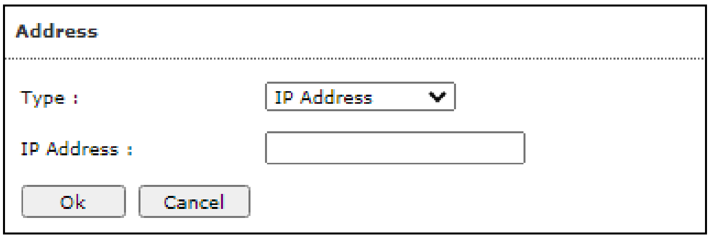
6. Click the **Type** drop-down. It displays following options:
    - Computer IP Address
    - Management Server Connection
    - Users
    - Machine Name

Depending upon the option, the conditions and settings vary.

Computer IP Address

1. Select the appropriate condition.
2. Click **Add**.

    Address window appears.


Address

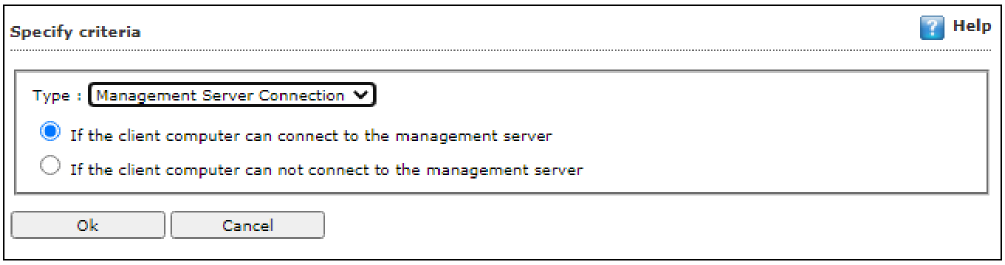
Type : IP Address

IP Address :

3. Enter the IP address.
4. Click **OK**.

    The Policy Criteria Template for an IP Address will be saved.

Management Server Connection



Specify criteria

Help

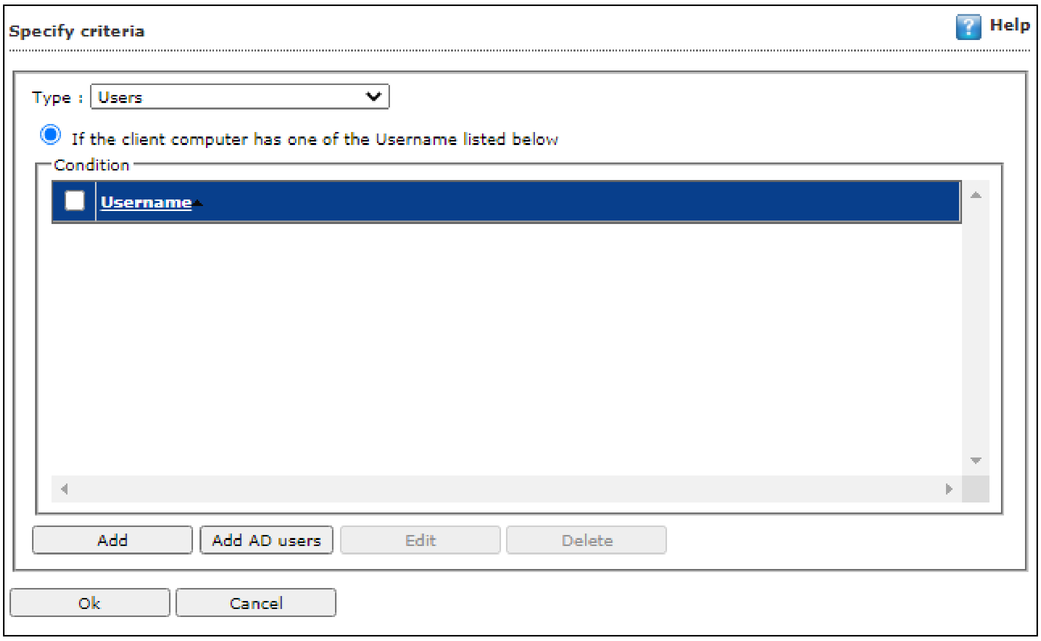
Type : Management Server Connection

● If the client computer can connect to the management server

○ If the client computer can not 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



Specify criteria

Help

Type : Users

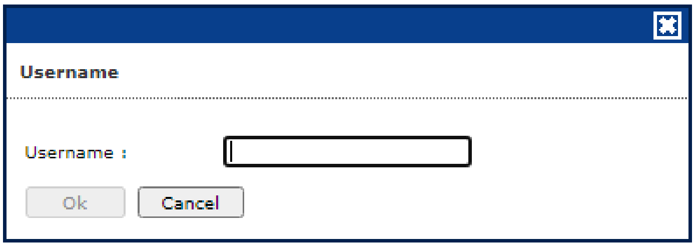
● If the client computer has one of the Username listed below

Condition

□	Username

Adding Local Users

1. To add local users, click **Add**.
   Username window appears.



Username

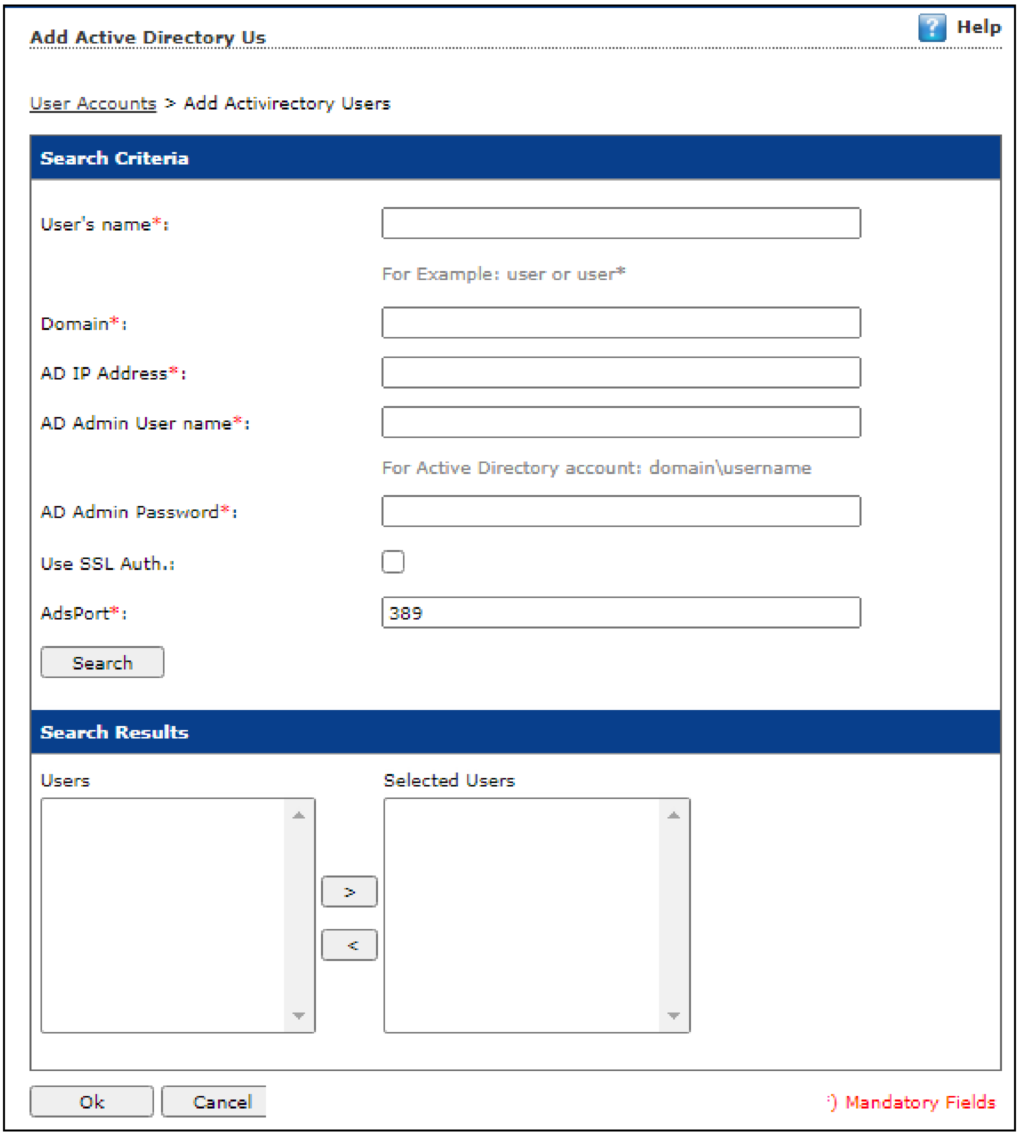
Username :

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.



Add Active Directory Us

Help

User Accounts > Add Activirectory 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*: 389

Search

Search Results

Users

Selected Users

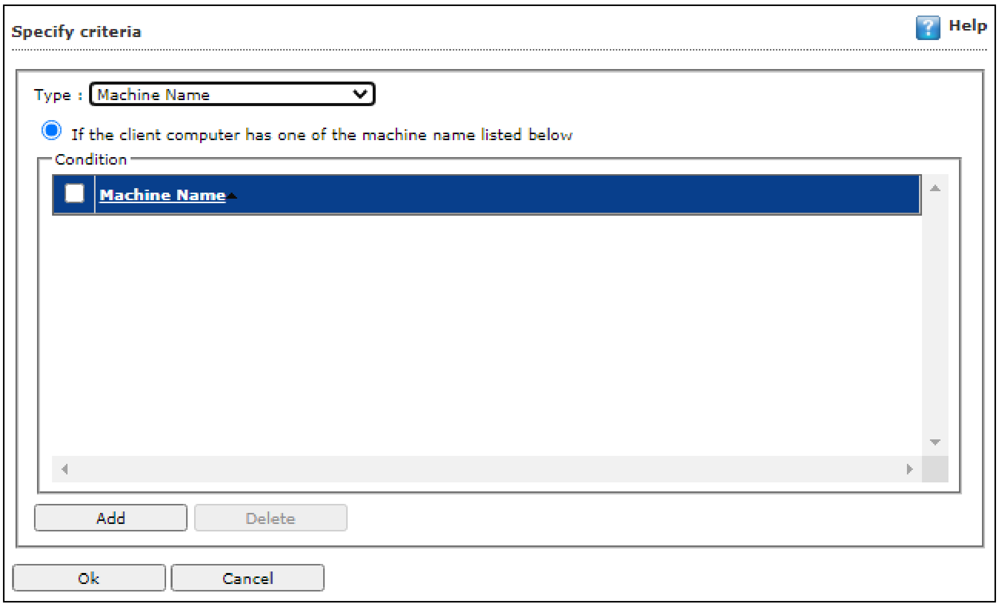
Ok

Cancel

*) 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.

Machine Name



Specify criteria

Help

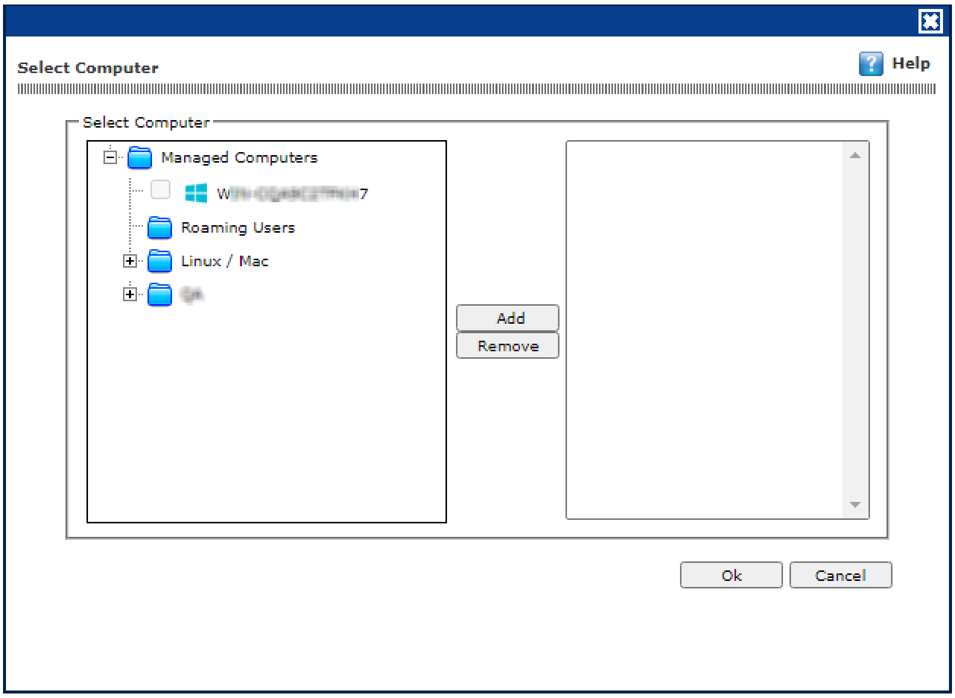
Type : Machine Name

● If the client computer has one of the machine name listed below

Condition

□	Machine Name

1. Click **Add**. Select Computer screen appears displaying all managed computers.



Select Computer

Help

Select Computer

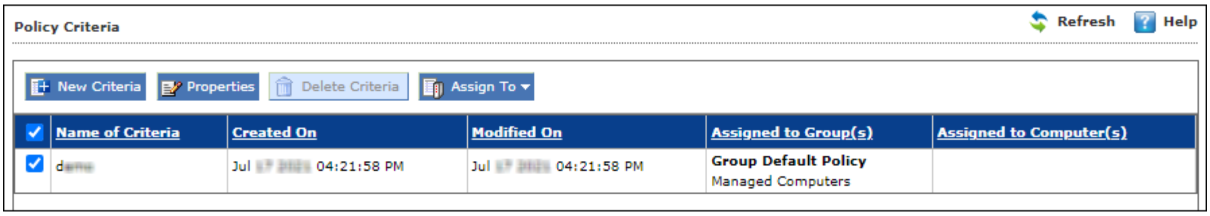
- Managed Computers
  - □ W[redacted]7
  - Roaming Users
  - Linux / Mac
  - [redacted]

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.

Viewing Properties of a Policy Criteria template

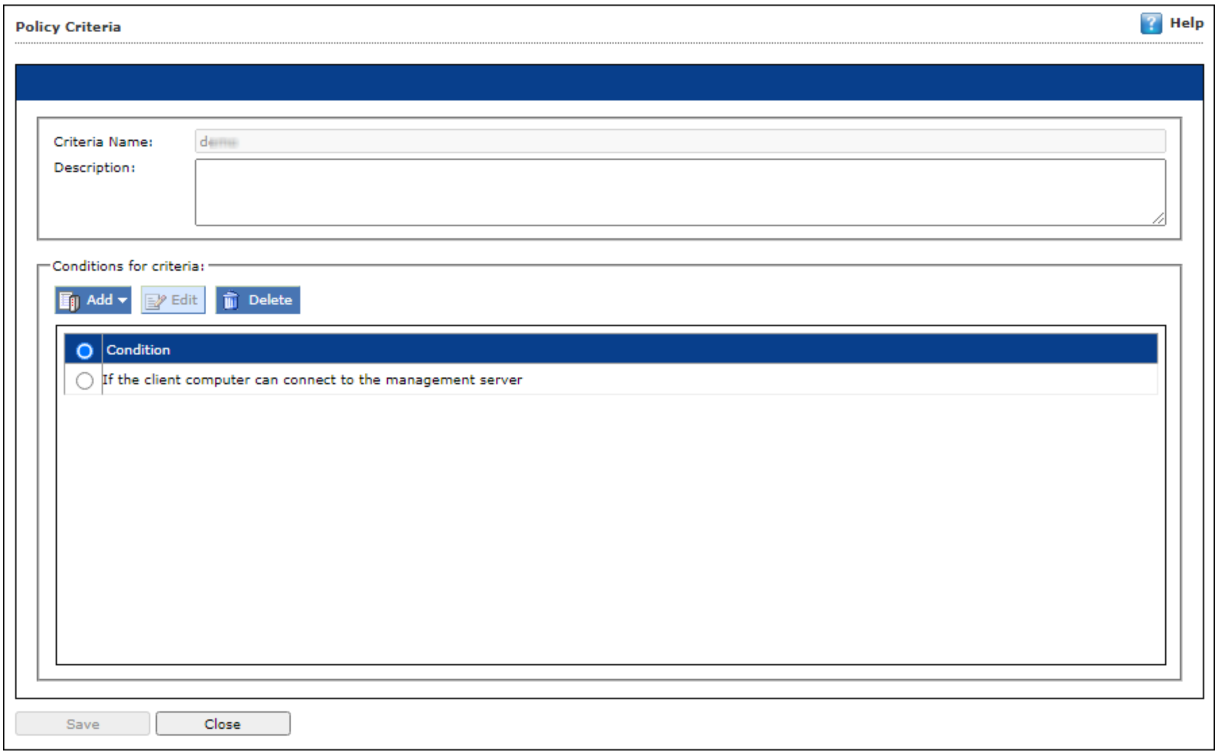
To view the properties of a Policy Criteria Template, follow the steps given below:

1. Select a policy criteria template.
2. Click **Properties**.



☑	Name of Criteria	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
☑	[redacted]	Jul [redacted] 04:21:58 PM	Jul [redacted] 04:21:58 PM	**Group Default Policy** Managed Computers	

Policy Criteria window appears.



Criteria Name: [redacted]

Description:

Conditions for criteria:

○	Condition
○	If the client computer can connect to the management server

3. Make the necessary changes and click **Save**.
   The Policy Criteria template will be saved and updated.

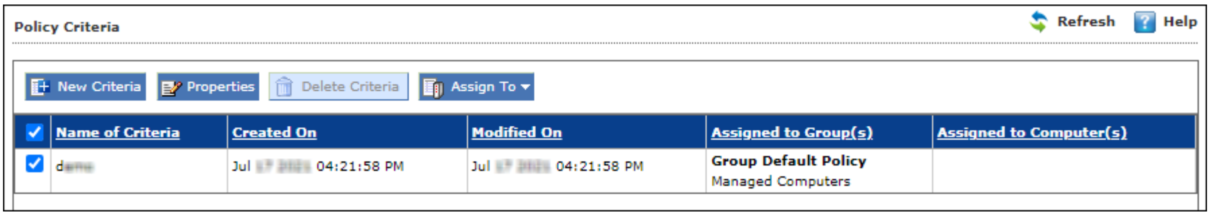
Deleting a Policy Criteria template

To delete assigned policy criteria template, follow the steps given below:

The Policy Criteria window displays to which group or computer the template is assigned in Assigned to Group(s) or Assigned to Computer(s) column.

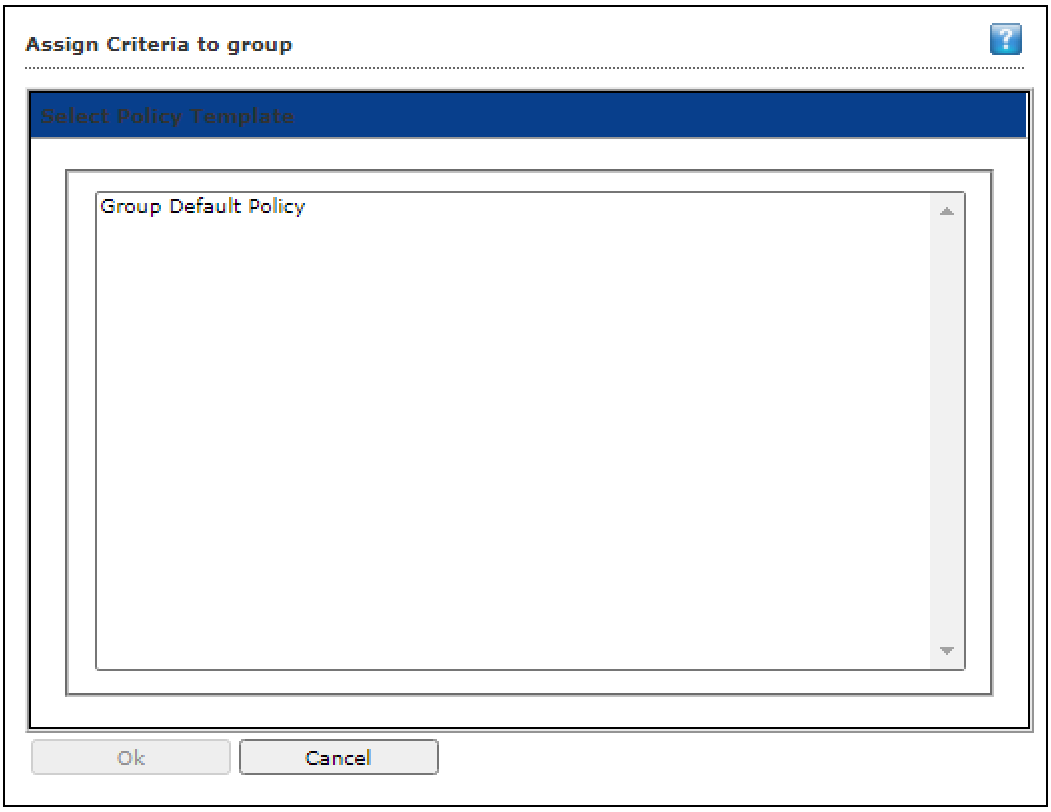
For explanation, we are following the procedure as per the screenshots below:

1. Select a policy criteria template.
2. Click **Assign To** > **Groups**.



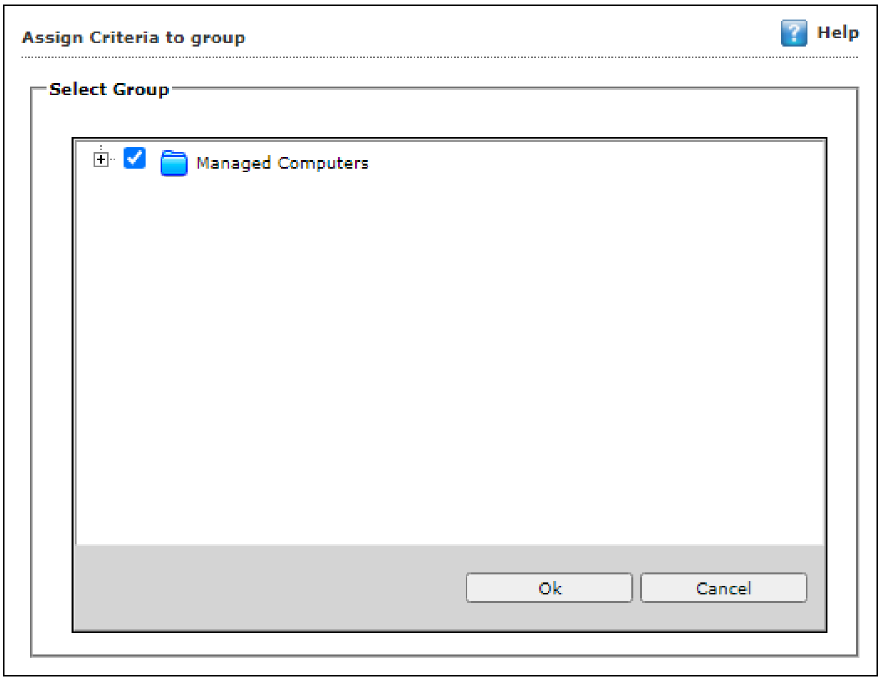
☑	Name of Criteria	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
☑	[redacted]	Jul [redacted] 04:21:58 PM	Jul [redacted] 04:21:58 PM	Group Default Policy Managed Computers	

Assign Criteria to Group window appears.



3. Click **Group Policy Template** > **OK**.

Assign Criteria to group window displays Managed Computers folder tree.

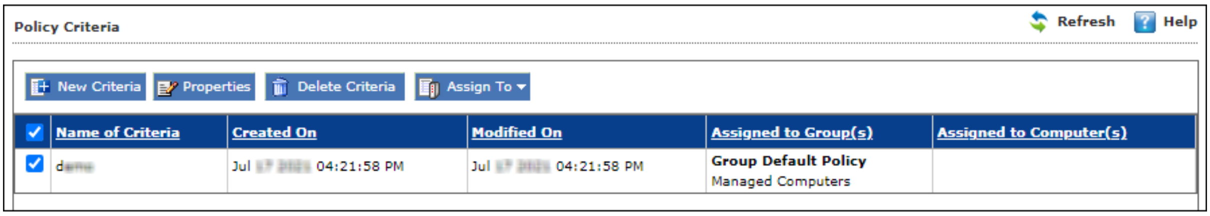


Assign Criteria to group

Select Group

☑ Managed Computers

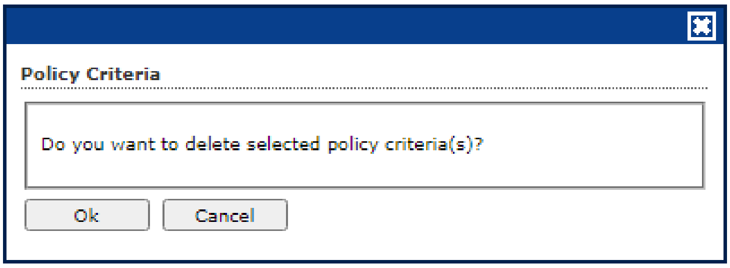
4. Uncheck the selected group.
5. Click **OK**.
   The Policy Criteria Template will no longer be assigned to any group. This enables **Delete Criteria** button.



Policy Criteria

☑	Name of Criteria	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
☑	[redacted]	Jul [redacted] 04:21:58 PM	Jul [redacted] 04:21:58 PM	**Group Default Policy** Managed Computers	

6. Select the template.
7. Click **Delete Criteria**.
   A confirmation window appears.



Policy Criteria

Do you want to delete selected policy criteria(s)?

8. Click **Ok**.
   The Policy Criteria Template will be deleted.

eScan Remediation Console

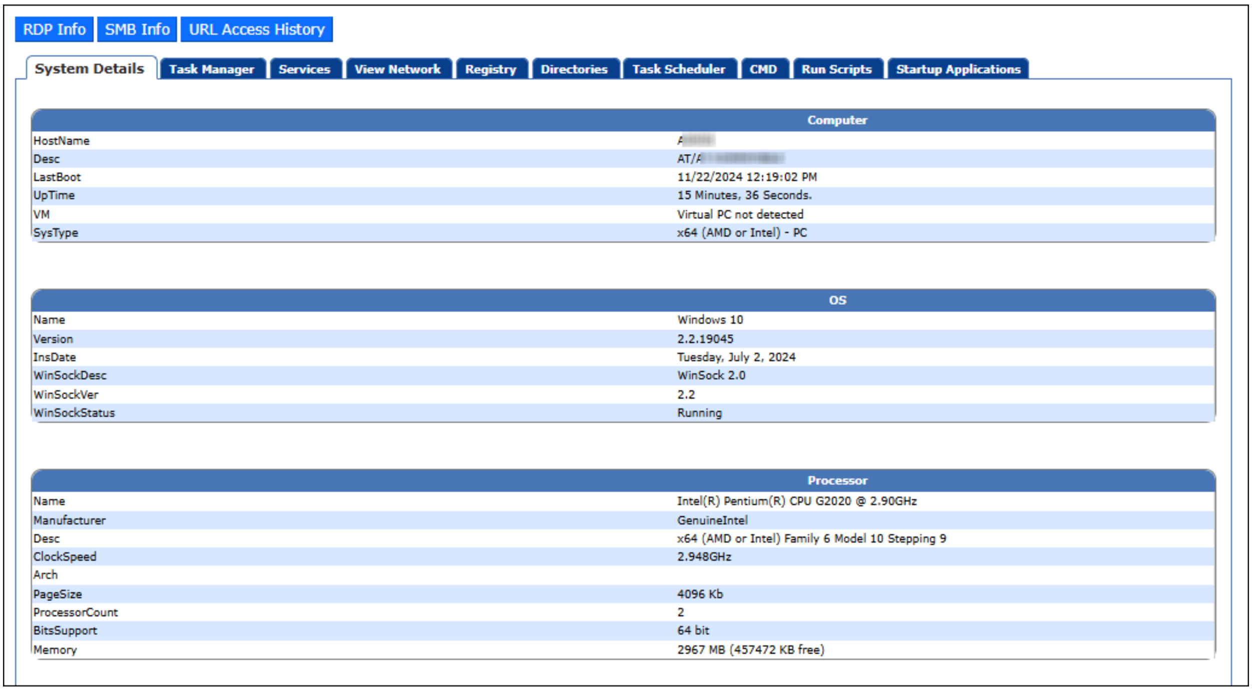
eScan Remediation Console offers unified dashboard for visibility across all endpoints in the network. It helps security team view real-time information and events about a particular client endpoint from a network. This includes system hardware and OS details, task manager activities, task scheduler, network connection activities, and a bunch of other components as well.

This console allows security team or administrators to perform certain remediation actions to manage the activities which are running on particular endpoints. E.g., under the 'Services' tab, admin can start, pause, restart, and stop particular service as and when required. Additionally, the console allows exporting the displayed information in common document formats. It consists following submodules:

- **System Details**
- **Task Manager**
- **Services**
- **View Network**
- **Registry**
- **Directories**
- **Task Scheduler**
- **CMD**
- **Run Scripts**
- **Startup Application**

System Details

The submodule displays endpoint's system details such as user profile, OS, and hardware configuration.



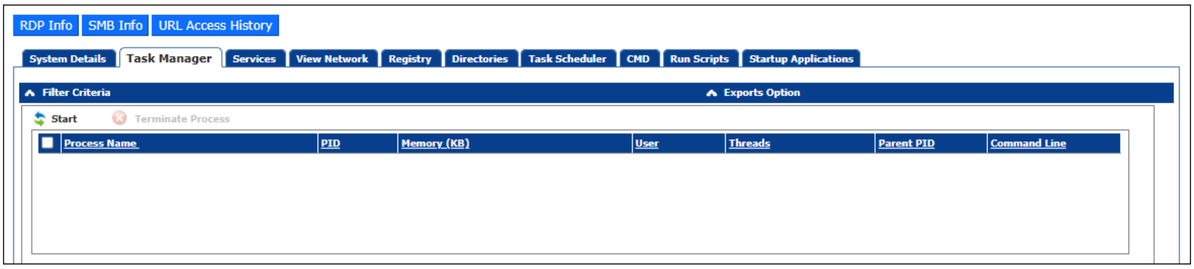
Computer	
HostName	A[redacted]
Desc	AT/A[redacted]
LastBoot	11/22/2024 12:19:02 PM
UpTime	15 Minutes, 36 Seconds.
VM	Virtual PC not detected
SysType	x64 (AMD or Intel) - PC

OS	
Name	Windows 10
Version	2.2.19045
InsDate	Tuesday, July 2, 2024
WinSockDesc	WinSock 2.0
WinSockVer	2.2
WinSockStatus	Running

Processor	
Name	Intel(R) Pentium(R) CPU G2020 @ 2.90GHz
Manufacturer	GenuineIntel
Desc	x64 (AMD or Intel) Family 6 Model 10 Stepping 9
ClockSpeed	2.948GHz
Arch	
PageSize	4096 Kb
ProcessorCount	2
BitsSupport	64 bit
Memory	2967 MB (457472 KB free)

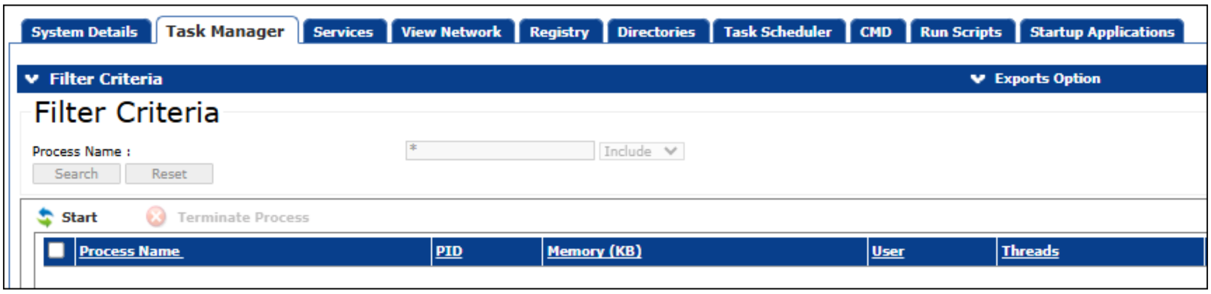
Task Manager

This module displays live task manager of client's computer. It includes Process Name, PID, memory (KB), users, threads, parent PID, and command line. The security team monitors these activities when required.



Filtering Task Manager

To filter the Task Manager as per your requirements, click **Filter Criteria** field.
Filter Criteria field expands.



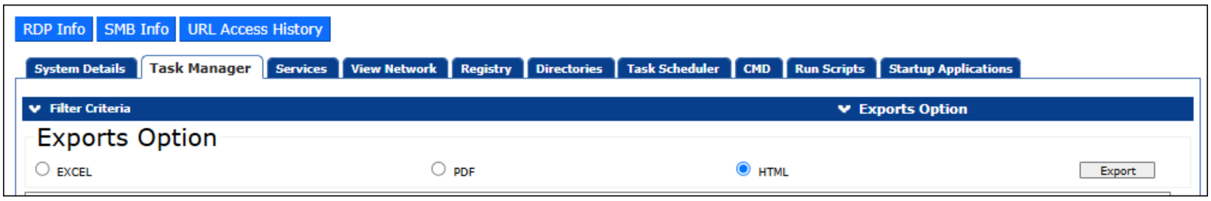
Process Name : * Include

Enter the Process Name to be included in the filtered report.

Include/Exclude
Selecting Include/Exclude for a parameter lets you include or exclude it from the report. After making the necessary selections, click **Search.**

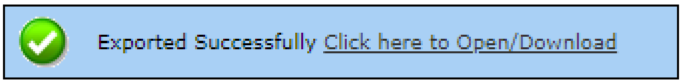
Exporting Task Manager

To export the Application Patch Report, click **Export Option**. Export Option field expands.



○ EXCEL ○ PDF ● HTML

Select the preferred option and then click **Export**.
A success message appears.

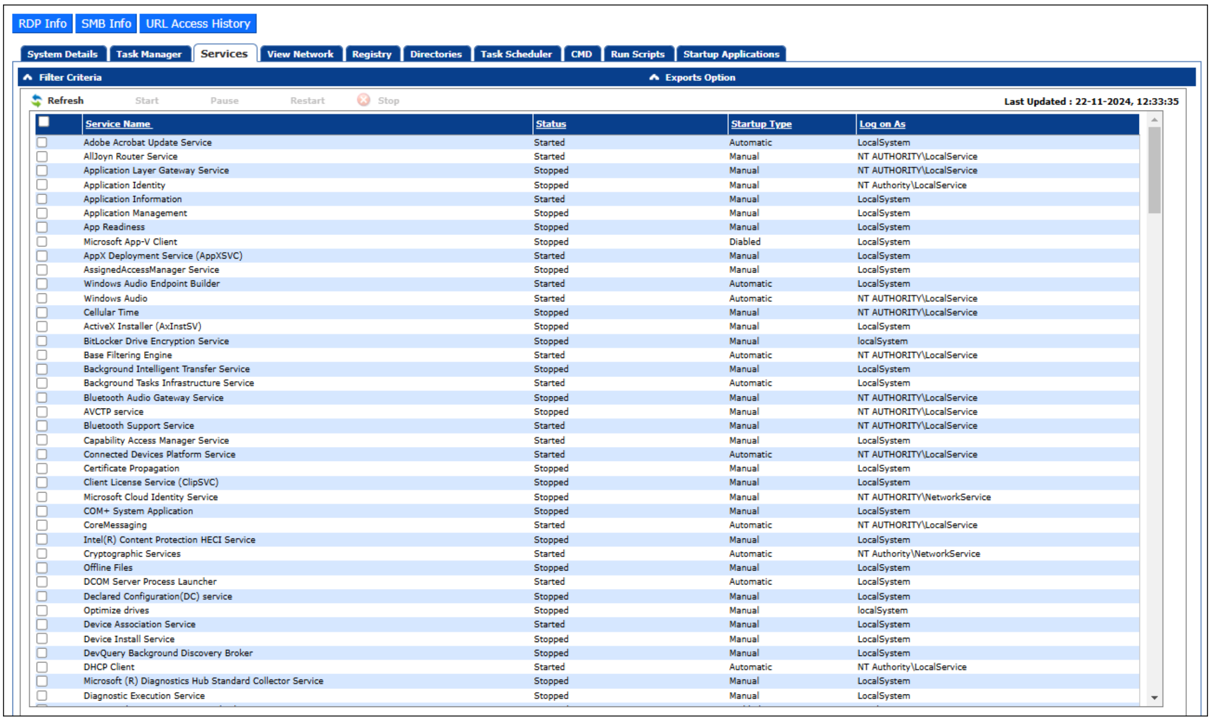


Exported Successfully Click here to Open/Download

Click the link to open/download the report file.

Services

The Services module allows security team keep track of the programs that are currently running on the endpoint. If required, the team can start, pause, restart, or stop any particular service.

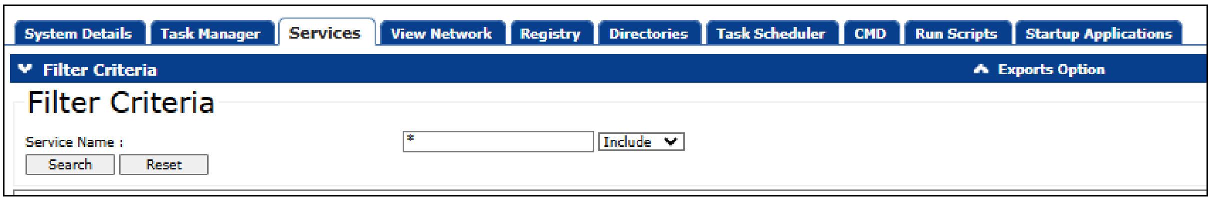


Last Updated : 22-11-2024, 12:33:35

□	Service Name	Status	Startup Type	Log on As
□	Adobe Acrobat Update Service	Started	Automatic	LocalSystem
□	AllJoyn Router Service	Started	Manual	NT AUTHORITY\LocalService
□	Application Layer Gateway Service	Stopped	Manual	NT AUTHORITY\LocalService
□	Application Identity	Stopped	Manual	NT Authority\LocalService
□	Application Information	Started	Manual	LocalSystem
□	Application Management	Stopped	Manual	LocalSystem
□	App Readiness	Stopped	Manual	LocalSystem
□	Microsoft App-V Client	Stopped	Diabled	LocalSystem
□	AppX Deployment Service (AppXSVC)	Started	Manual	LocalSystem
□	AssignedAccessManager Service	Stopped	Manual	LocalSystem
□	Windows Audio Endpoint Builder	Started	Automatic	LocalSystem
□	Windows Audio	Started	Automatic	NT AUTHORITY\LocalService
□	Cellular Time	Stopped	Manual	NT AUTHORITY\LocalService
□	ActiveX Installer (AxInstSV)	Stopped	Manual	LocalSystem
□	BitLocker Drive Encryption Service	Stopped	Manual	localSystem
□	Base Filtering Engine	Started	Automatic	NT AUTHORITY\LocalService
□	Background Intelligent Transfer Service	Stopped	Manual	LocalSystem
□	Background Tasks Infrastructure Service	Started	Automatic	LocalSystem
□	Bluetooth Audio Gateway Service	Stopped	Manual	NT AUTHORITY\LocalService
□	AVCTP service	Stopped	Manual	NT AUTHORITY\LocalService
□	Bluetooth Support Service	Started	Manual	NT AUTHORITY\LocalService
□	Capability Access Manager Service	Started	Manual	LocalSystem
□	Connected Devices Platform Service	Started	Automatic	NT AUTHORITY\LocalService
□	Certificate Propagation	Stopped	Manual	LocalSystem
□	Client License Service (ClipSVC)	Stopped	Manual	LocalSystem
□	Microsoft Cloud Identity Service	Stopped	Manual	NT AUTHORITY\NetworkService
□	COM+ System Application	Stopped	Manual	LocalSystem
□	CoreMessaging	Started	Automatic	NT AUTHORITY\LocalService
□	Intel(R) Content Protection HECI Service	Stopped	Manual	LocalSystem
□	Cryptographic Services	Started	Automatic	NT Authority\NetworkService
□	Offline Files	Stopped	Manual	LocalSystem
□	DCOM Server Process Launcher	Started	Automatic	LocalSystem
□	Declared Configuration(DC) service	Stopped	Manual	LocalSystem
□	Optimize drives	Stopped	Manual	localSystem
□	Device Association Service	Started	Manual	LocalSystem
□	Device Install Service	Stopped	Manual	LocalSystem
□	DevQuery Background Discovery Broker	Stopped	Manual	LocalSystem
□	DHCP Client	Started	Automatic	NT Authority\LocalService
□	Microsoft (R) Diagnostics Hub Standard Collector Service	Stopped	Manual	LocalSystem
□	Diagnostic Execution Service	Stopped	Manual	LocalSystem

Filtering Services

To filter the Services as per your requirements, click **Filter Criteria** field.
Filter Criteria field expands.



Filter Criteria

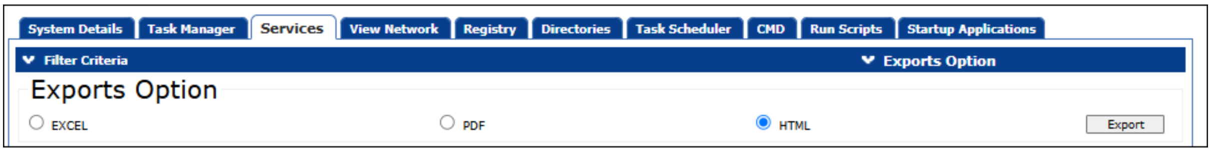
Service Name : * Include

Enter the Process Name to be included in the filtered report.

Include/Exclude
Selecting Include/Exclude for a parameter lets you include or exclude it from the report. After making the necessary selections, click **Search.**

Exporting Services

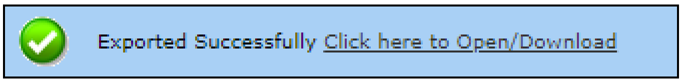
To export the Application Patch Report, click **Export Option**. Export Option field expands.



Exports Option

○ EXCEL ○ PDF ● HTML

Select the preferred option and then click **Export**.
A success message appears.



Exported Successfully Click here to Open/Download

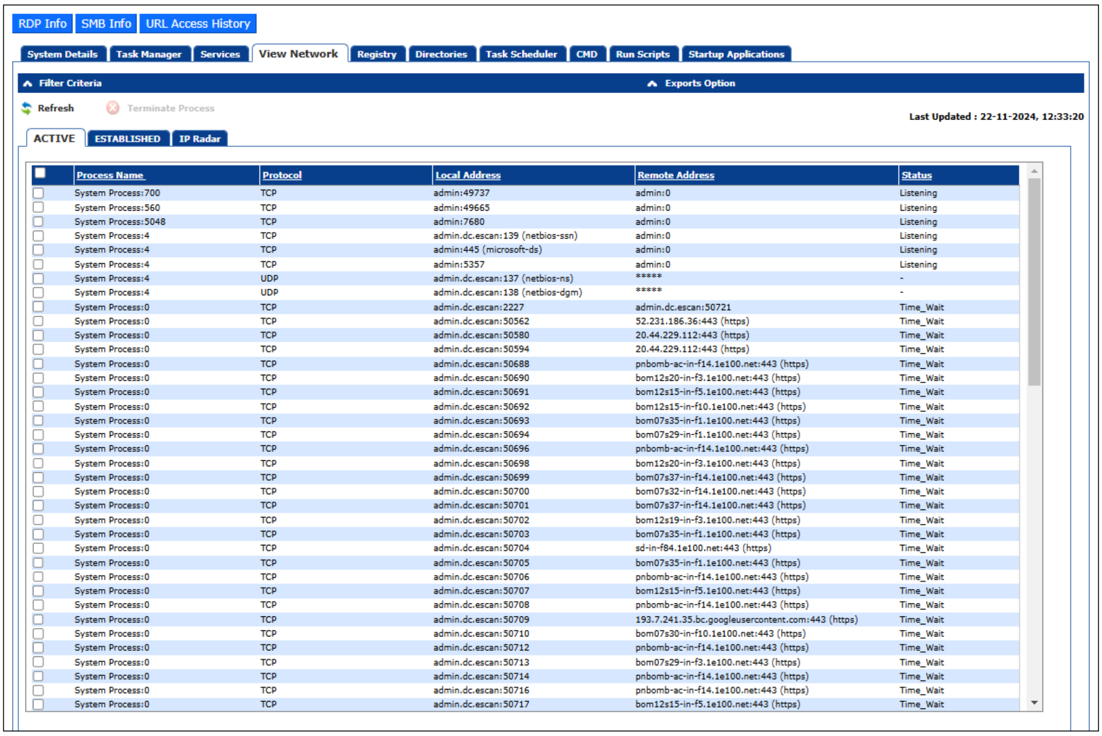
Click the link to open/download the report file.

View Network

View Network displays the processes and their details running via active and established connections on an endpoint. Apart from this, it also shows IP Radar map to trace the locations of the connection on a geographical map.

Active

This tab displays processes and their details running via active connections on an endpoint. Select particular process and click on **Terminate Process** to end it.

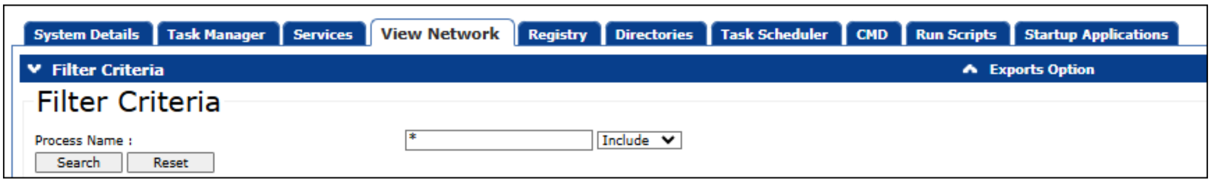


Last Updated : 22-11-2024, 12:33:20

□	Process Name	Protocol	Local Address	Remote Address	Status
□	System Process:700	TCP	admin:49737	admin:0	Listening
□	System Process:560	TCP	admin:49665	admin:0	Listening
□	System Process:5048	TCP	admin:7680	admin:0	Listening
□	System Process:4	TCP	admin.dc.escan:139 (netbios-ssn)	admin:0	Listening
□	System Process:4	TCP	admin:445 (microsoft-ds)	admin:0	Listening
□	System Process:4	TCP	admin:5357	admin:0	Listening
□	System Process:4	UDP	admin.dc.escan:137 (netbios-ns)	*****	-
□	System Process:4	UDP	admin.dc.escan:138 (netbios-dgm)	*****	-
□	System Process:0	TCP	admin.dc.escan:2227	admin.dc.escan:50721	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50562	52.231.186.36:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50580	20.44.229.112:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50594	20.44.229.112:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50688	pnbomb-ac-in-f14.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50690	bom12s20-in-f3.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50691	bom12s15-in-f5.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50692	bom12s15-in-f10.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50693	bom07s35-in-f1.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50694	bom07s29-in-f1.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50696	pnbomb-ac-in-f14.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50698	bom12s20-in-f3.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50699	bom07s37-in-f14.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50700	bom07s32-in-f14.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50701	bom07s37-in-f14.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50702	bom12s19-in-f3.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50703	bom07s35-in-f1.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50704	sd-in-f84.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50705	bom07s35-in-f1.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50706	pnbomb-ac-in-f14.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50707	bom12s15-in-f5.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50708	pnbomb-ac-in-f14.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50709	193.7.241.35.bc.googleusercontent.com:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50710	bom07s30-in-f10.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50712	pnbomb-ac-in-f14.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50713	bom07s29-in-f3.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50714	pnbomb-ac-in-f14.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50716	pnbomb-ac-in-f14.1e100.net:443 (https)	Time_Wait
□	System Process:0	TCP	admin.dc.escan:50717	bom12s15-in-f5.1e100.net:443 (https)	Time_Wait

Filtering View Network from Active Connections

To filter the View Network from all active connections, click on **Filter Criteria**.
The Filter Criteria field expands.



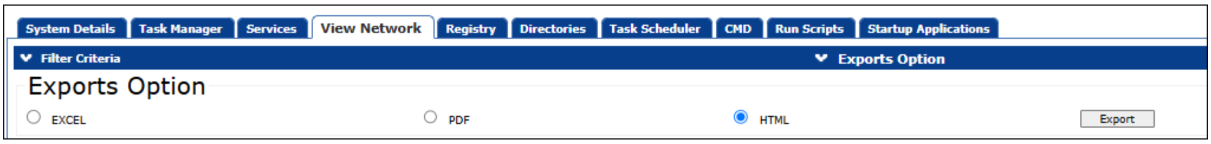
Process Name : * Include

Enter the Process Name to be included in the filtered report.

Include/Exclude
Select Include/Exclude from the provided drop-down to include or exclude the parameter from the report. After making the selections, click **Search**. The report will be filtered and displayed to you.

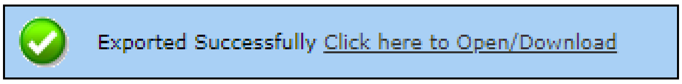
Exporting Active View Network

To export the report, click **Export Option**.



○ EXCEL ○ PDF ● HTML

From the expanded field, select the preferred file format and then click **Export**.
A success message appears.

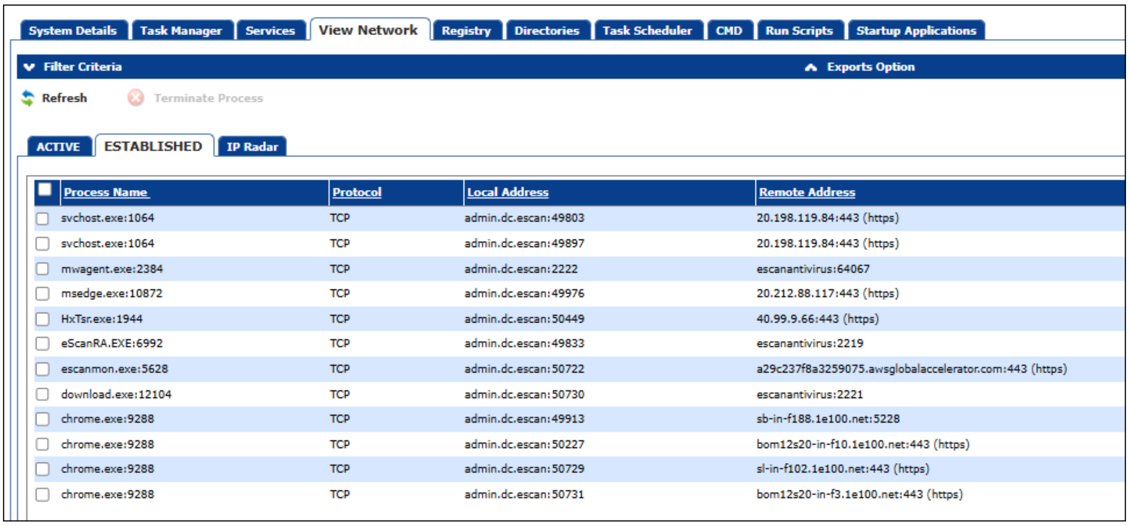


Exported Successfully Click here to Open/Download

Click the link to open and download the report file.

Established

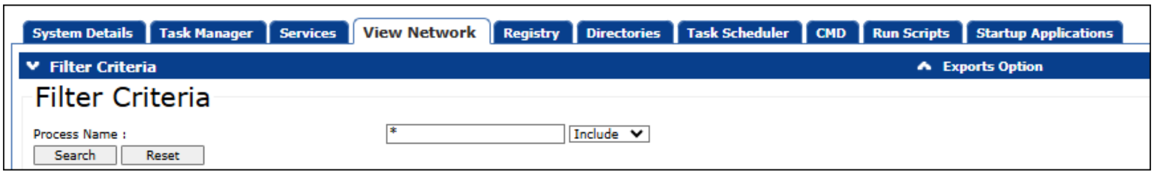
This tab displays processes and their details running via established connections on an endpoint. Select particular process and click on **Terminate Process** to end it.



□	Process Name	Protocol	Local Address	Remote Address
□	svchost.exe:1064	TCP	admin.dc.escan:49803	20.198.119.84:443 (https)
□	svchost.exe:1064	TCP	admin.dc.escan:49897	20.198.119.84:443 (https)
□	mwagent.exe:2384	TCP	admin.dc.escan:2222	escanantivirus:64067
□	msedge.exe:10872	TCP	admin.dc.escan:49976	20.212.88.117:443 (https)
□	HxTsr.exe:1944	TCP	admin.dc.escan:50449	40.99.9.66:443 (https)
□	eScanRA.EXE:6992	TCP	admin.dc.escan:49833	escanantivirus:2219
□	escanmon.exe:5628	TCP	admin.dc.escan:50722	a29c237f8a3259075.awsglobalaccelerator.com:443 (https)
□	download.exe:12104	TCP	admin.dc.escan:50730	escanantivirus:2221
□	chrome.exe:9288	TCP	admin.dc.escan:49913	sb-in-f188.1e100.net:5228
□	chrome.exe:9288	TCP	admin.dc.escan:50227	bom12s20-in-f10.1e100.net:443 (https)
□	chrome.exe:9288	TCP	admin.dc.escan:50729	sl-in-f102.1e100.net:443 (https)
□	chrome.exe:9288	TCP	admin.dc.escan:50731	bom12s20-in-f3.1e100.net:443 (https)

Filtering Established View Network

To filter the Established View Network as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.



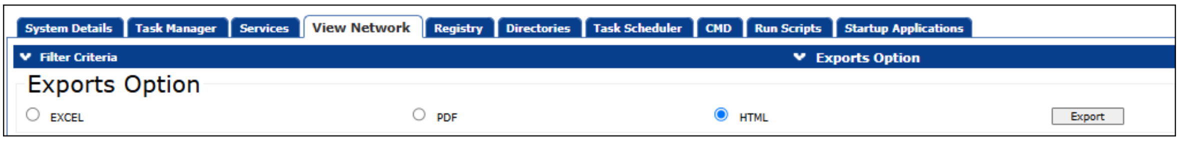
Process Name : * Include

Enter the Process Name to be included in the filtered report.

Include/Exclude
Selecting Include/Exclude for a parameter lets you include or exclude it from the report. After making the necessary selections, click **Search**.

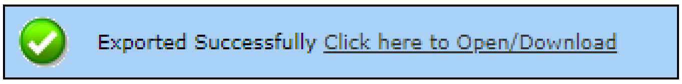
Exporting Established View Network

To export the Established View Network, click **Export Option**. Export Option field expands.



○ EXCEL ○ PDF ● HTML

Select the preferred option and then click **Export**.
A success message appears.

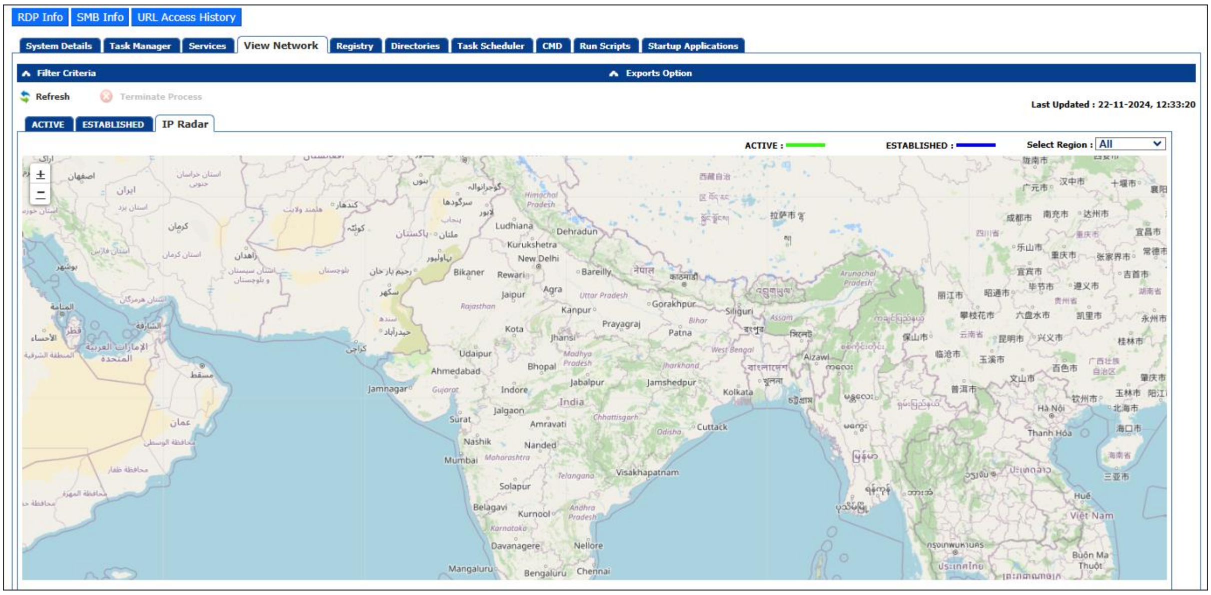


Exported Successfully Click here to Open/Download

Click the link to open/download the report file.

IP Radar

IP Radar’s geographical map helps trace the locations of the current connections running on an endpoint.

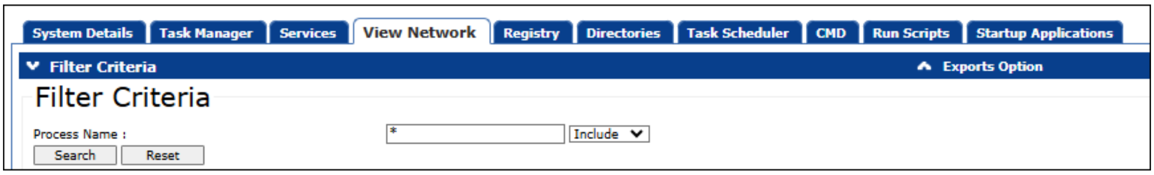


Last Updated : 22-11-2024, 12:33:20

Select Region : All

Filtering IP Radar View Network

To filter the IP radar View Network as per your requirements, click **Filter Criteria** field.
Filter Criteria field expands.



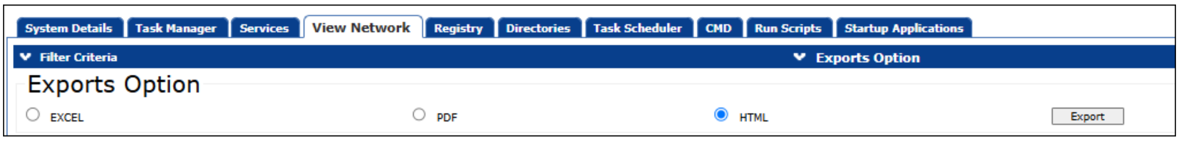
Process Name : * Include

Enter the Process Name to be included in the filtered report.

Include/Exclude
Selecting Include/Exclude for a parameter lets you include or exclude it from the report. After making the necessary selections, click **Search**.

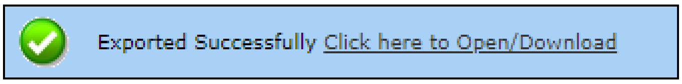
Exporting IP radar View Network

To export the IP radar View Network, click **Export Option**. Export Option field expands.



○ EXCEL ○ PDF ● HTML

Select the preferred option and then click **Export**.
A success message appears.

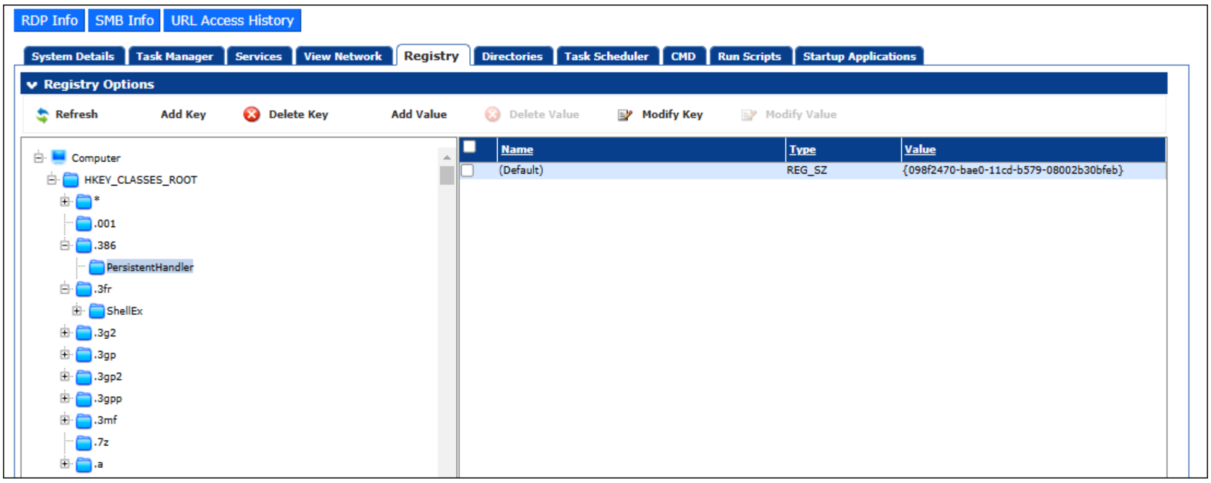


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Registry

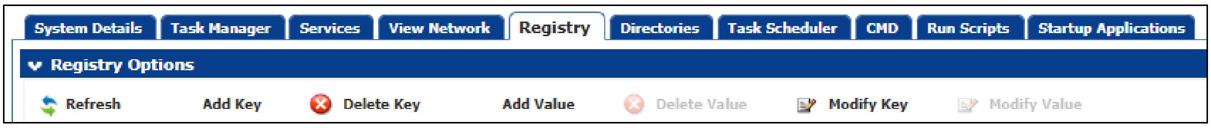
This tab displays the registry key holdings, a set of registry values that stores configurations and settings running on an endpoint. If required, the team can manage particular registered key(s) to customize or troubleshoot the operating system or software.



□	Name	Type	Value
□	(Default)	REG_SZ	{098f2470-bae0-11cd-b579-08002b30bfeb}

Registry Options

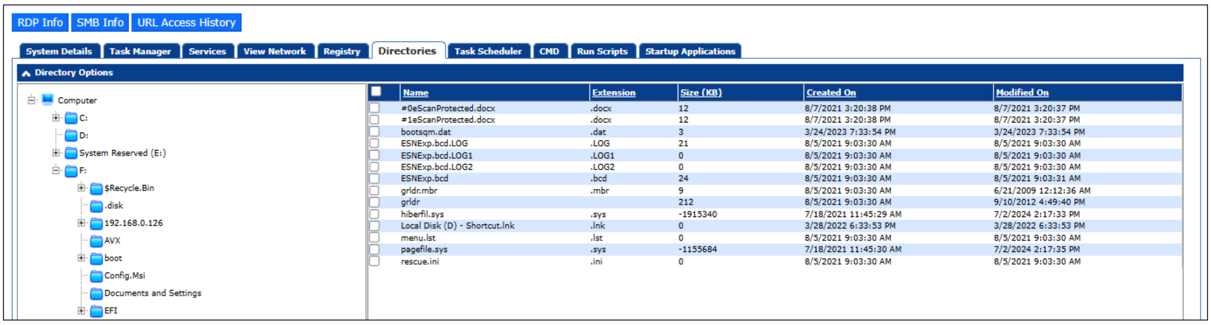
Click on **Registry Options** drop-down, to filter the settings as per your requirements.
The field expands.



You can select any registry from the computer and perform required activities available such as Add, delete, and more.

Directories

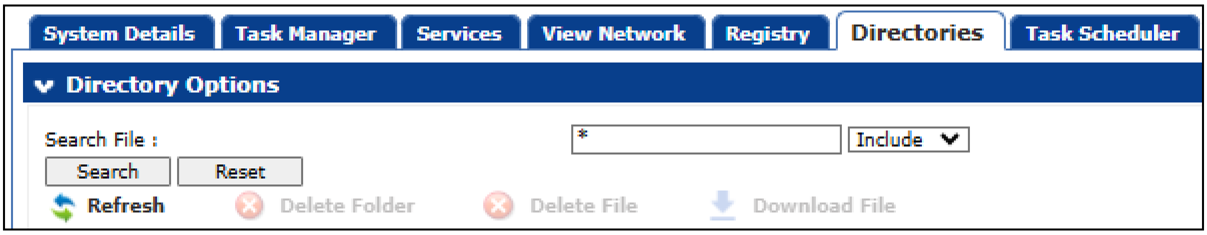
The Directories module allows the security team to keep track of files that are organized, easily accessible and manageable within a system currently running on the endpoint. If required, the team can delete directories folder or file. It also allows downloading of the file.



□	Name	Extension	Size (KB)	Created On	Modified On
□	#0eScanProtected.docx	.docx	12	8/7/2021 3:20:38 PM	8/7/2021 3:20:37 PM
□	#1eScanProtected.docx	.docx	12	8/7/2021 3:20:38 PM	8/7/2021 3:20:37 PM
□	bootsqm.dat	.dat	3	3/24/2023 7:33:54 PM	3/24/2023 7:33:54 PM
□	ESNExp.bcd.LOG	.LOG	21	8/5/2021 9:03:30 AM	8/5/2021 9:03:30 AM
□	ESNExp.bcd.LOG1	.LOG1	0	8/5/2021 9:03:30 AM	8/5/2021 9:03:30 AM
□	ESNExp.bcd.LOG2	.LOG2	0	8/5/2021 9:03:30 AM	8/5/2021 9:03:30 AM
□	ESNExp.bcd	.bcd	24	8/5/2021 9:03:30 AM	8/5/2021 9:03:31 AM
□	grldr.mbr	.mbr	9	8/5/2021 9:03:30 AM	6/21/2009 12:12:36 AM
□	grldr		212	8/5/2021 9:03:30 AM	9/10/2012 4:49:40 PM
□	hiberfil.sys	.sys	-1915340	7/18/2021 11:45:29 AM	7/2/2024 2:17:33 PM
□	Local Disk (D) - Shortcut.lnk	.lnk	0	3/28/2022 6:33:53 PM	3/28/2022 6:33:53 PM
□	menu.lst	.lst	0	8/5/2021 9:03:30 AM	8/5/2021 9:03:30 AM
□	pagefile.sys	.sys	-1155684	7/18/2021 11:45:30 AM	7/2/2024 2:17:35 PM
□	rescue.ini	.ini	0	8/5/2021 9:03:30 AM	8/5/2021 9:03:30 AM

Directories Options

Click on **Directories Option**, to filter the settings as per your requirements.
The Directory Option field expands.



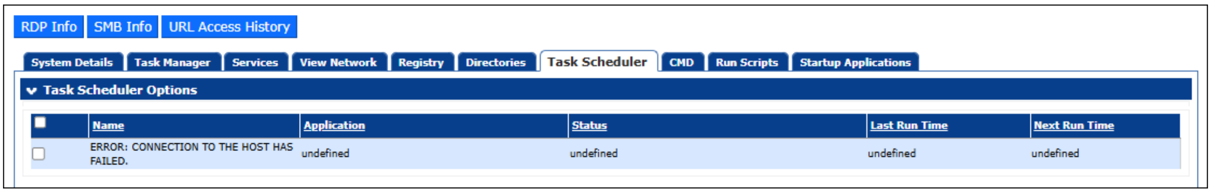
Search File : * Include

Enter the Process Name to be included in the filtered report.

Include/Exclude
Selecting Include/Exclude for a parameter lets you include or exclude it from the report. After making the necessary selections, click **Search**.
The Directories list will appear.

Task Scheduler

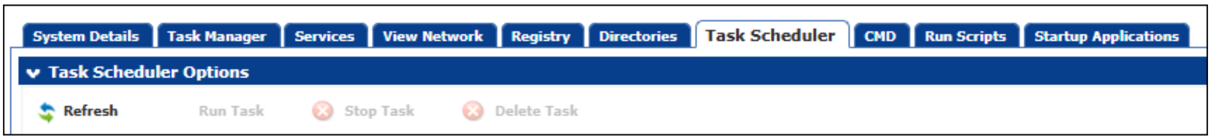
A Task Scheduler is a tool in operating systems used to automate the execution of tasks on a specific schedule or in response to certain events. The Task Scheduler tab displays Name, application, status, last run time, and next run time of a particular endpoint.



☐	Name	Application	Status	Last Run Time	Next Run Time
☐	ERROR: CONNECTION TO THE HOST HAS FAILED.	undefined	undefined	undefined	undefined

Task Scheduler Options

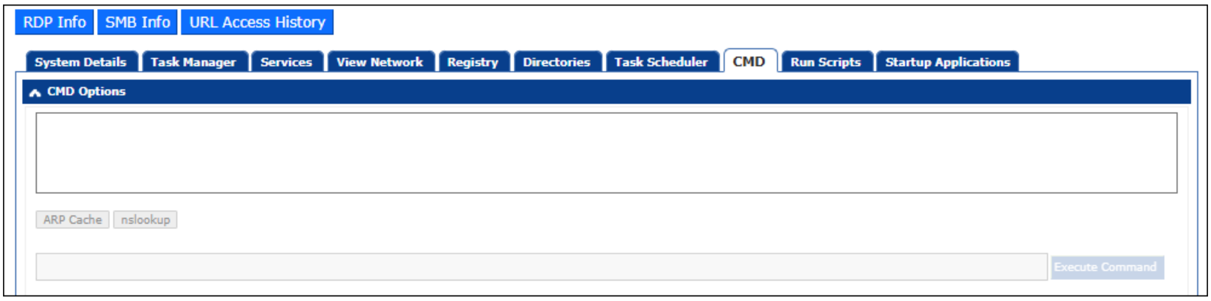
Click on **Task Scheduler Option,** to filter the settings as per your requirements.
The Task Scheduler Option field expands.



You can refresh the settings, run task, stop task, and delete task using provided buttons.

CMD

The CMD in the Remediation console enables administrators to execute a range of system commands on endpoints, helping to resolve issues, implement fixes, or carry out tasks. Clicking the **ARP cache** button allows you to view IP-to-MAC address mappings. Click on the **nslookup** button to resolve domain names to IP addresses.

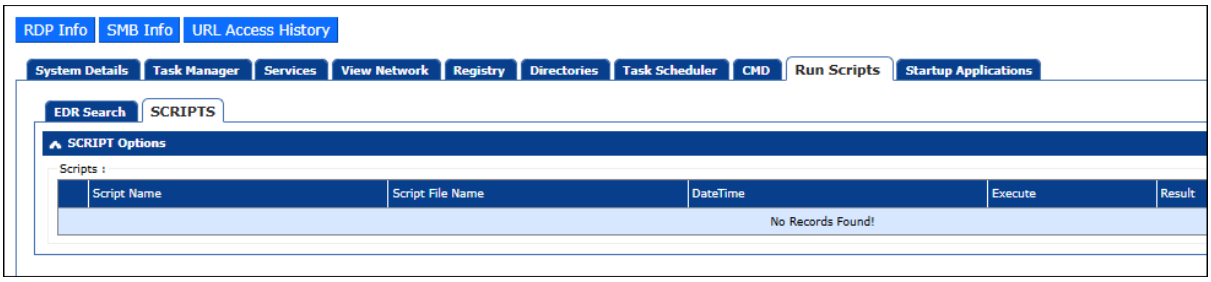


Run Scripts

The Run Scripts tab displays the execution of the files containing a sequence of commands. The EDR Search tab involves searching through data collected by an Endpoint Detection and Response system to identify threats or suspicious behaviour. Scripts are files containing instructions that automate tasks or add functionality to systems or applications.

SCRIPTS

The Scripts tab displays the Script Name, Script File Name, DateTime, Execute, and Result.

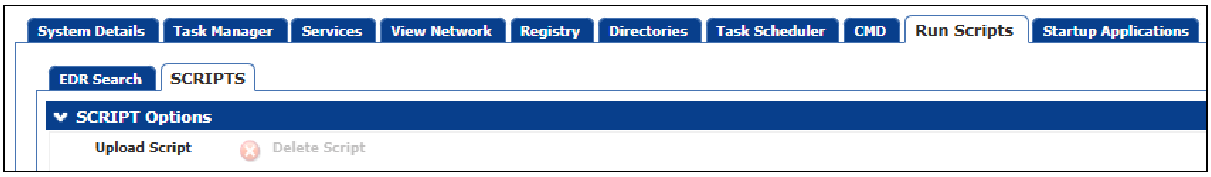


Scripts :

	Script Name	Script File Name	DateTime	Execute	Result
			No Records Found!		

SCRIPT Options

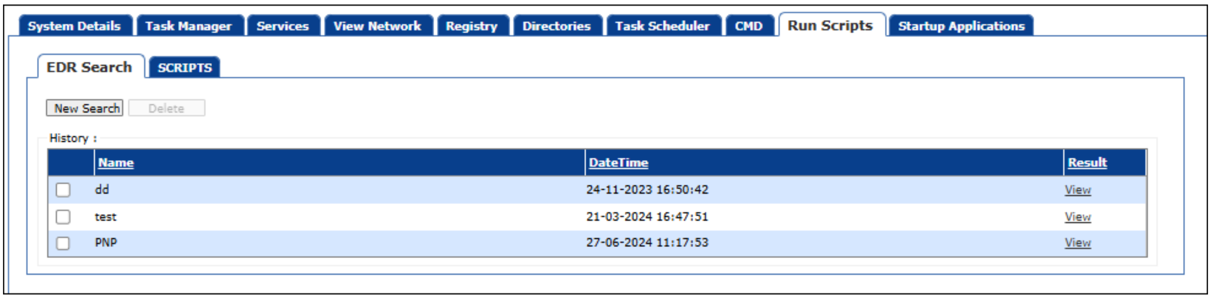
Click on **Scripts Option,** to filter the settings as per your requirements.
Script Option field expands.



- **Upload Script:** Click on this button to upload the script.
- **Delete Script:** Select a script and click on **Delete** button.

EDR Search

Click on **EDR Search** tab, to filter the settings as per your requirements.
The field expands.

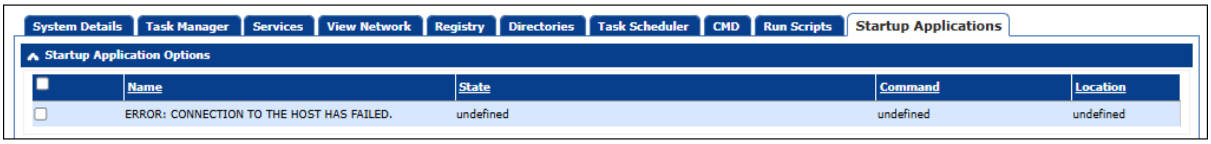


	Name	DateTime	Result
□	dd	24-11-2023 16:50:42	View
□	test	21-03-2024 16:47:51	View
□	PNP	27-06-2024 11:17:53	View

- **New Search:** Click on this button and enter new search.
- **Delete:** Select an option from the history and click on **delete**.

Startup Application

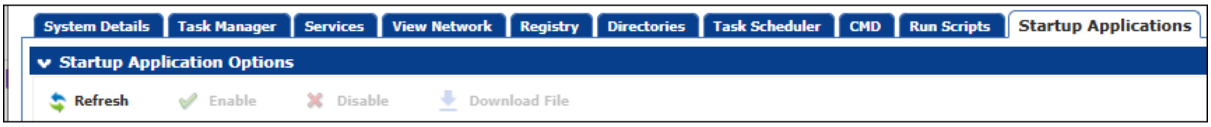
The startup application feature performs real-time scanning of the programs set to run at system startup. Administrators can view endpoint's details of Startup applications and the currently defined actions on those applications (enabled or disabled).



☐	Name	State	Command	Location
☐	ERROR: CONNECTION TO THE HOST HAS FAILED.	undefined	undefined	undefined

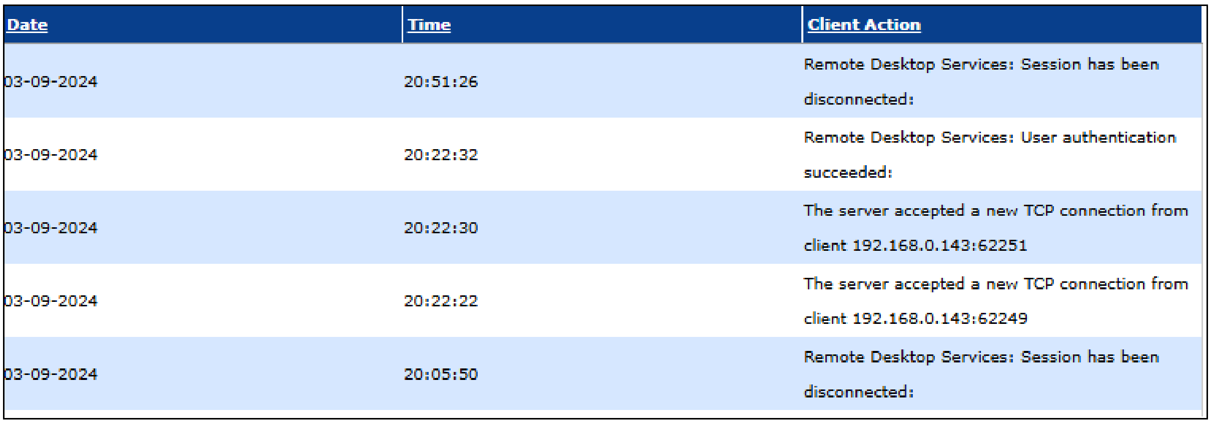
Startup Application Options

You can refresh the list, enable or disable the program, and download the file.



RDP Info

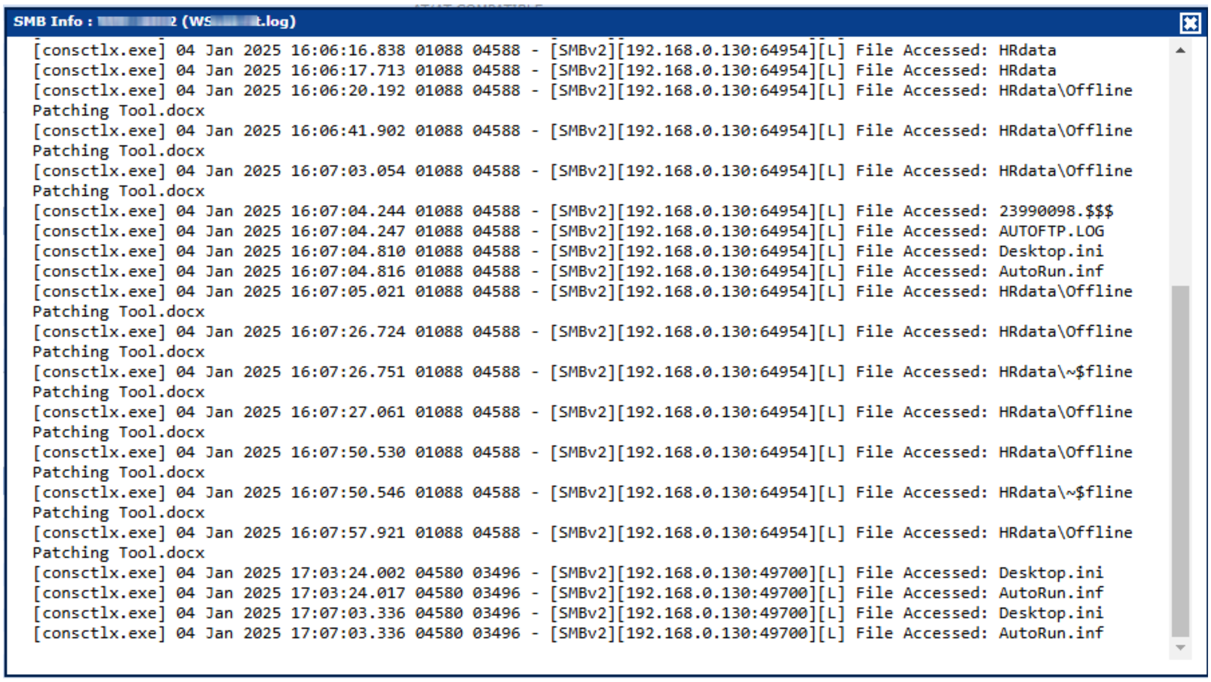
Remote Desktop Protocol (RDP) is a widely used protocol that enables users to connect to and control remote systems over a network. The RDP info tab allows the security team to view basic session details, including the date, time when the RDP sessions are connected and disconnected of an endpoint.



Date	Time	Client Action
03-09-2024	20:51:26	Remote Desktop Services: Session has been disconnected:
03-09-2024	20:22:32	Remote Desktop Services: User authentication succeeded:
03-09-2024	20:22:30	The server accepted a new TCP connection from client 192.168.0.143:62251
03-09-2024	20:22:22	The server accepted a new TCP connection from client 192.168.0.143:62249
03-09-2024	20:05:50	Remote Desktop Services: Session has been disconnected:

SMB Info

The eScan's SMB Info module allows the security team to view details about the applications that have been accessed, providing information on which specific application was used and when it was accessed, thus enabling better tracking and monitoring of application usage on a particular endpoint.

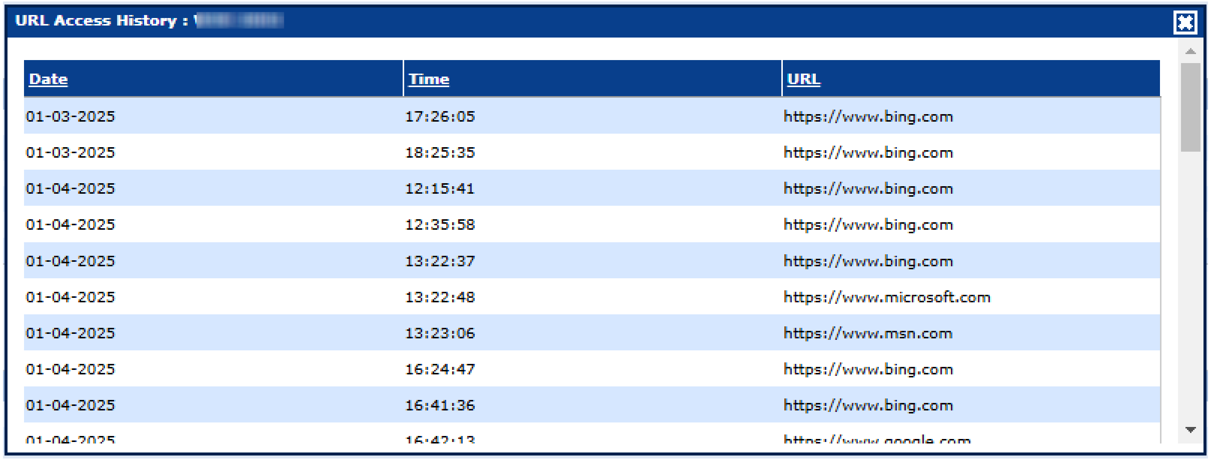


SMB Info : [redacted] (WS[redacted].log)

```
[consctlx.exe] 04 Jan 2025 16:06:16.838 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: HRdata
[consctlx.exe] 04 Jan 2025 16:06:17.713 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: HRdata
[consctlx.exe] 04 Jan 2025 16:06:20.192 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: HRdata\Offline
Patching Tool.docx
[consctlx.exe] 04 Jan 2025 16:06:41.902 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: HRdata\Offline
Patching Tool.docx
[consctlx.exe] 04 Jan 2025 16:07:03.054 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: HRdata\Offline
Patching Tool.docx
[consctlx.exe] 04 Jan 2025 16:07:04.244 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: 23990098.$$$
[consctlx.exe] 04 Jan 2025 16:07:04.247 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: AUTOFTP.LOG
[consctlx.exe] 04 Jan 2025 16:07:04.810 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: Desktop.ini
[consctlx.exe] 04 Jan 2025 16:07:04.816 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: AutoRun.inf
[consctlx.exe] 04 Jan 2025 16:07:05.021 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: HRdata\Offline
Patching Tool.docx
[consctlx.exe] 04 Jan 2025 16:07:26.724 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: HRdata\Offline
Patching Tool.docx
[consctlx.exe] 04 Jan 2025 16:07:26.751 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: HRdata\~$fline
Patching Tool.docx
[consctlx.exe] 04 Jan 2025 16:07:27.061 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: HRdata\Offline
Patching Tool.docx
[consctlx.exe] 04 Jan 2025 16:07:50.530 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: HRdata\Offline
Patching Tool.docx
[consctlx.exe] 04 Jan 2025 16:07:50.546 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: HRdata\~$fline
Patching Tool.docx
[consctlx.exe] 04 Jan 2025 16:07:57.921 01088 04588 - [SMBv2][192.168.0.130:64954][L] File Accessed: HRdata\Offline
Patching Tool.docx
[consctlx.exe] 04 Jan 2025 17:03:24.002 04580 03496 - [SMBv2][192.168.0.130:49700][L] File Accessed: Desktop.ini
[consctlx.exe] 04 Jan 2025 17:03:24.017 04580 03496 - [SMBv2][192.168.0.130:49700][L] File Accessed: AutoRun.inf
[consctlx.exe] 04 Jan 2025 17:07:03.336 04580 03496 - [SMBv2][192.168.0.130:49700][L] File Accessed: Desktop.ini
[consctlx.exe] 04 Jan 2025 17:07:03.336 04580 03496 - [SMBv2][192.168.0.130:49700][L] File Accessed: AutoRun.inf
```

URL Access History

URL Access History is the record of web addresses (URLs) that a user has accessed over a specific period of time. This sub module allows security team to view the details, such as date, time, and the URLs that were visited on a particular endpoint.



URL Access History : [redacted]

Date	Time	URL
01-03-2025	17:26:05	https://www.bing.com
01-03-2025	18:25:35	https://www.bing.com
01-04-2025	12:15:41	https://www.bing.com
01-04-2025	12:35:58	https://www.bing.com
01-04-2025	13:22:37	https://www.bing.com
01-04-2025	13:22:48	https://www.microsoft.com
01-04-2025	13:23:06	https://www.msn.com
01-04-2025	16:24:47	https://www.bing.com
01-04-2025	16:41:36	https://www.bing.com
01-04-2025	16:42:13	https://www.google.com

Unmanaged Computers

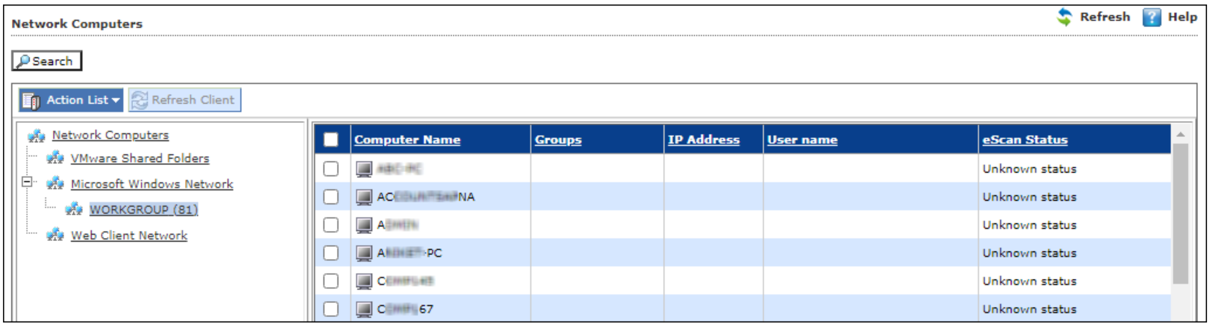
To install eScan Client, define policies and tasks on the basis of group, it is necessary to move computers to the created groups. You can move the computers from **Unmanaged Computers** to desired groups created in the **Managed Computers** using the following submodules:

- **Network Computers**
- **IP Range**
- **Active Directory**
- **New Computers Found**

Network Computers

This submodule displays a list of available networks. You can move the computers from the list of computers present in the Network Computers using the following steps:

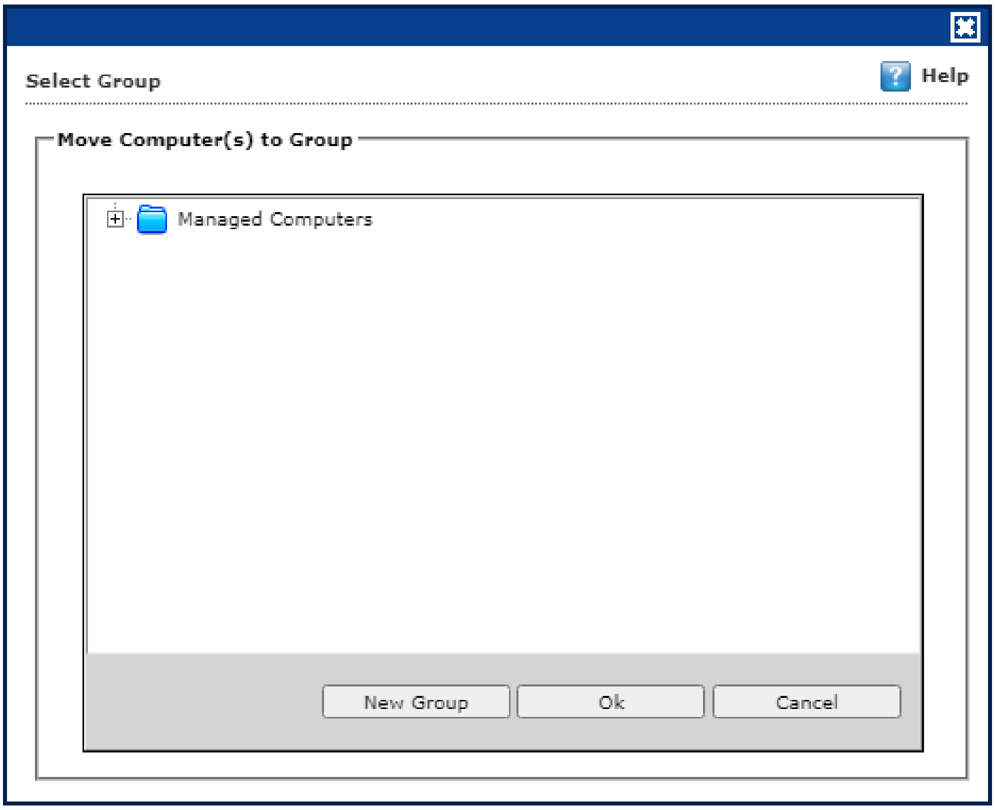
1. In the navigation panel, click **Unmanaged Computers** > **Network Computers**.
2. Click **Microsoft Windows Network**.
3. Select the workgroup from where you want to move computers to the group created in Managed Computers section. A list of computers appears.



□	Computer Name	Groups	IP Address	User name	eScan Status
□	[redacted]				Unknown status
□	AC[redacted]NA				Unknown status
□	A[redacted]				Unknown status
□	A[redacted]-PC				Unknown status
□	C[redacted]				Unknown status
□	C[redacted]67				Unknown status

4. Select the computer(s) you want to move to the desired groups.
5. Click **Action List** > **Move to Group**. Select Group window appears.

6. Click **Managed Computers** tree to view the groups.

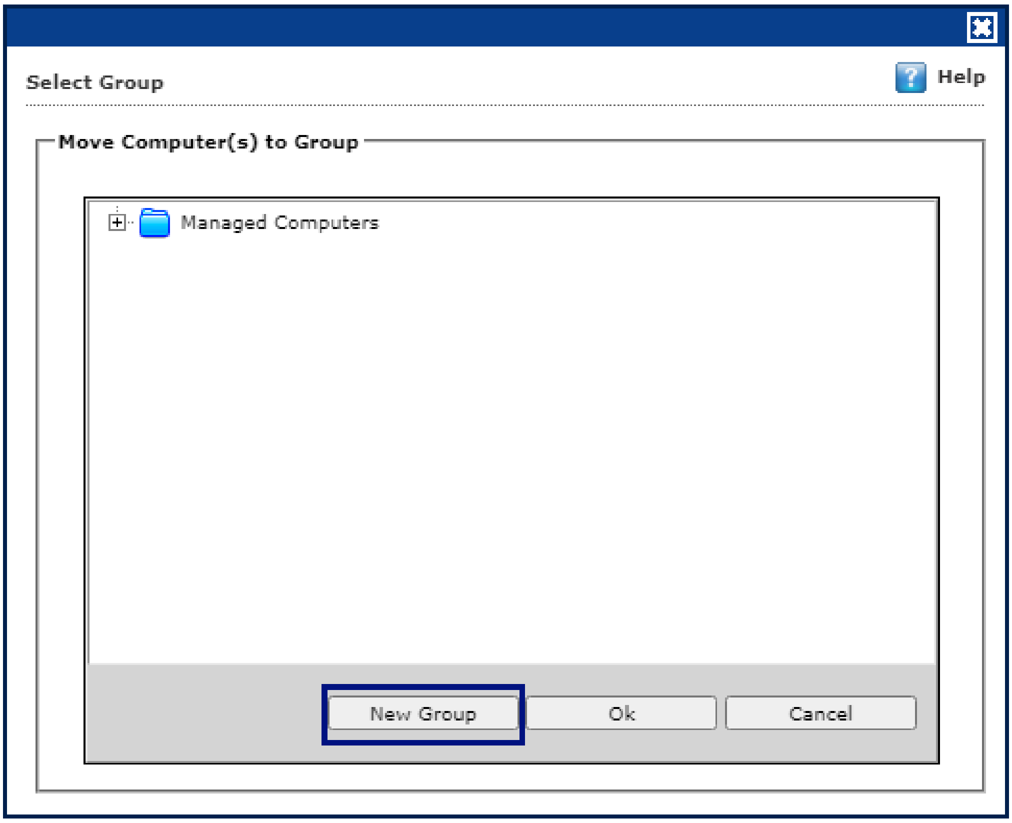


7. Select the group where you wish to move the selected computer(s) and click **OK**.
   The selected computer(s) will be moved to the group.

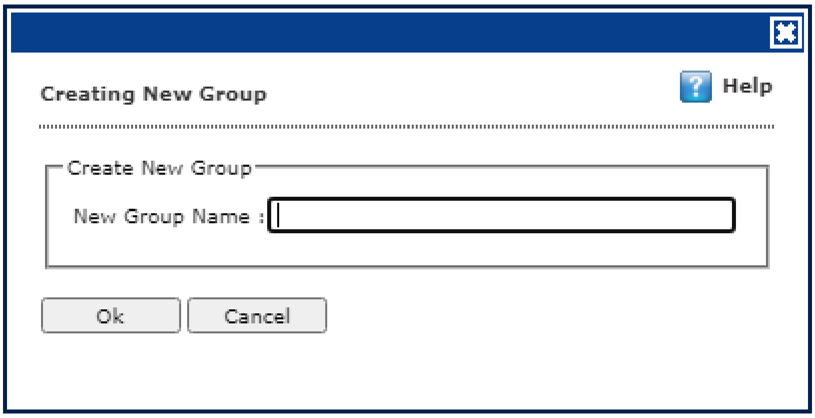
Creating a New Group from the Select Group window

To create a new group from the Select Group window, follow the steps given below:

1. In the Select Group window, click **Managed Computers** > **New Group**.



Creating New Group window appears.



2. Enter a name for the group.
3. Click **OK**. A new group will be created.

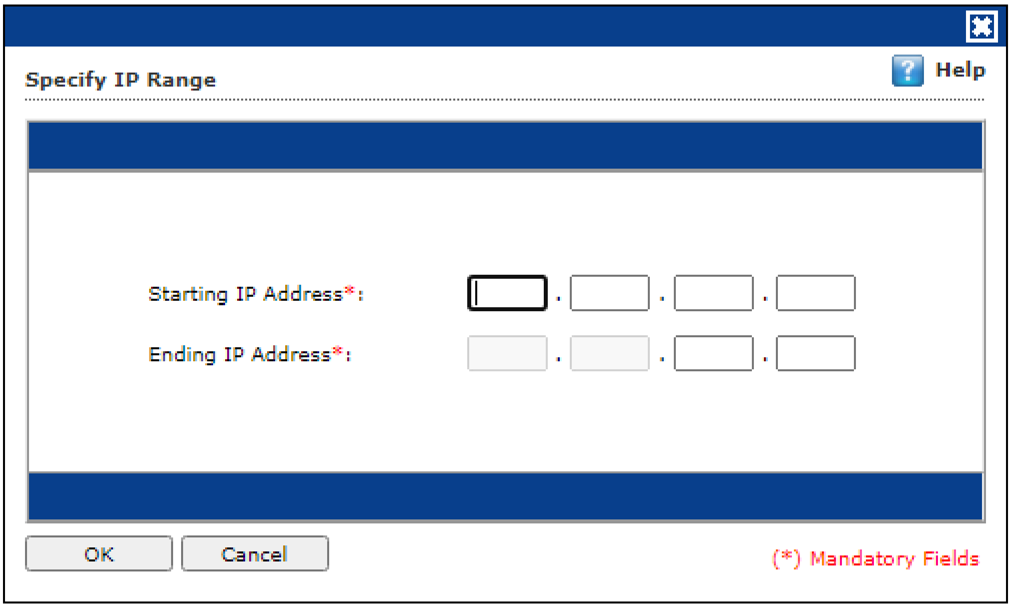
IP Range

The **IP Range** submodule lets you scan the desired IP address or range of IP address and add the required computers to any of the managed groups. It also lets you add, search and delete an IP range.

Adding New IP Range

To add an IP range, follow the steps given below:

1. In the IP range screen, click **New IP Range**.
   Specify IP Range window appears.



Specify IP Range

Starting IP Address*: ___ . ___ . ___ . ___

Ending IP Address*: ___ . ___ . ___ . ___

(*) Mandatory Fields

2. Enter the Starting and Ending IP address.
3. Click **OK**. The 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

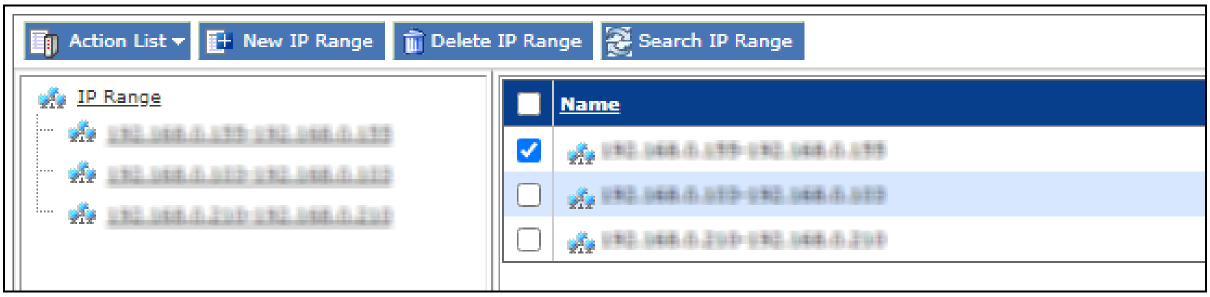
To move an entire IP range to a group, follow the steps given below:

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.

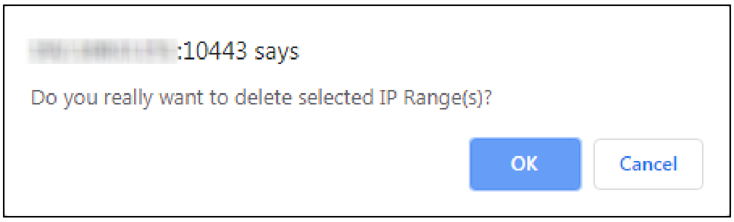
Deleting an IP Range

To delete an IP range, follow the steps given below:

1. Select an IP Range.
2. Click **Delete IP Range**.



A confirmation prompt appears.


[redacted]:10443 says

Do you really want to delete selected IP Range(s)?

3. Click **OK**. The IP range will be deleted.

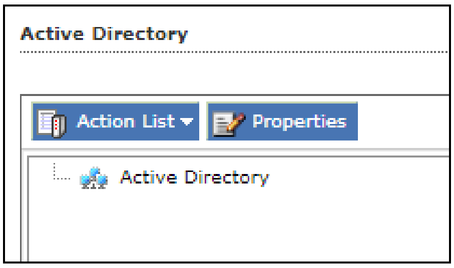
Active Directory

The Active Directory submodule lets you add computers from an Active Directory.

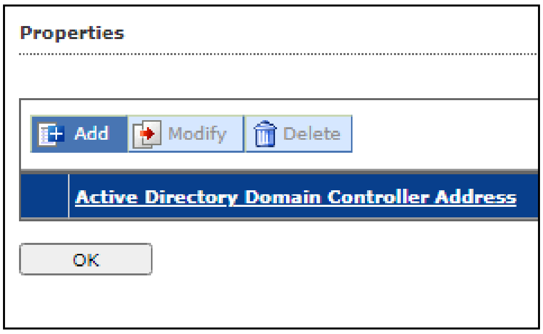
Adding an Active Directory

To add an Active Directory, follow the steps given below:

1. Click **Unmanaged Computers** > **Active Directory**.
2. Click **Properties**.

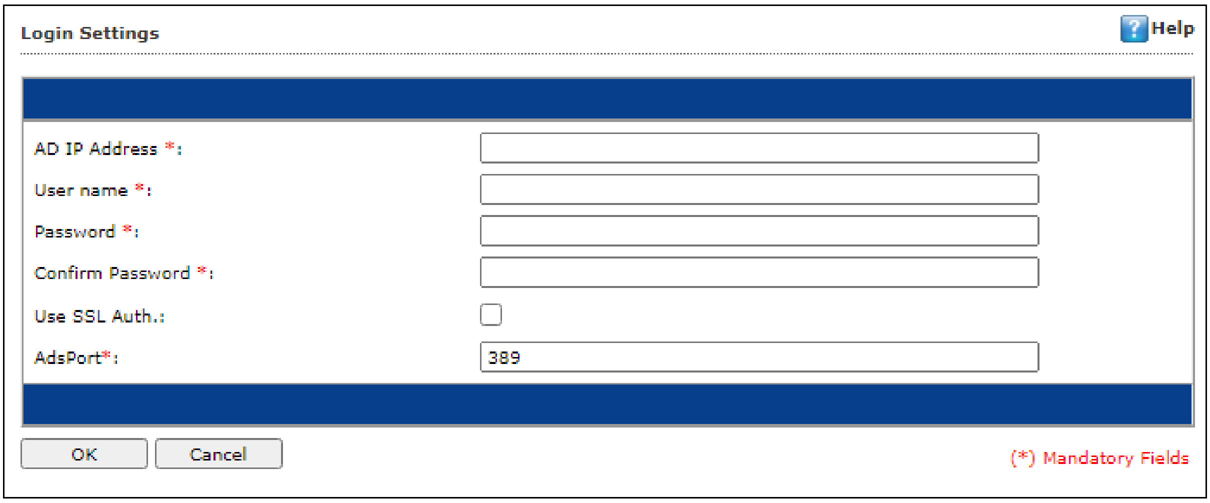


Properties window appears.


Properties

Active Directory Domain Controller Address

3. Click **Add**. Login Settings window appears.


Login Settings

AD IP Address *:

User name *:

Password *:

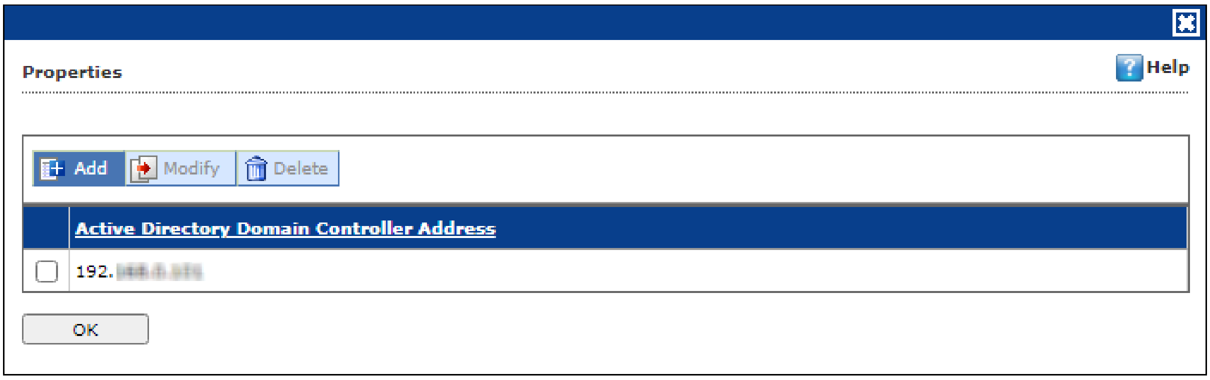
Confirm Password *:

Use SSL Auth.: □

AdsPort*: 389

(*) Mandatory Fields

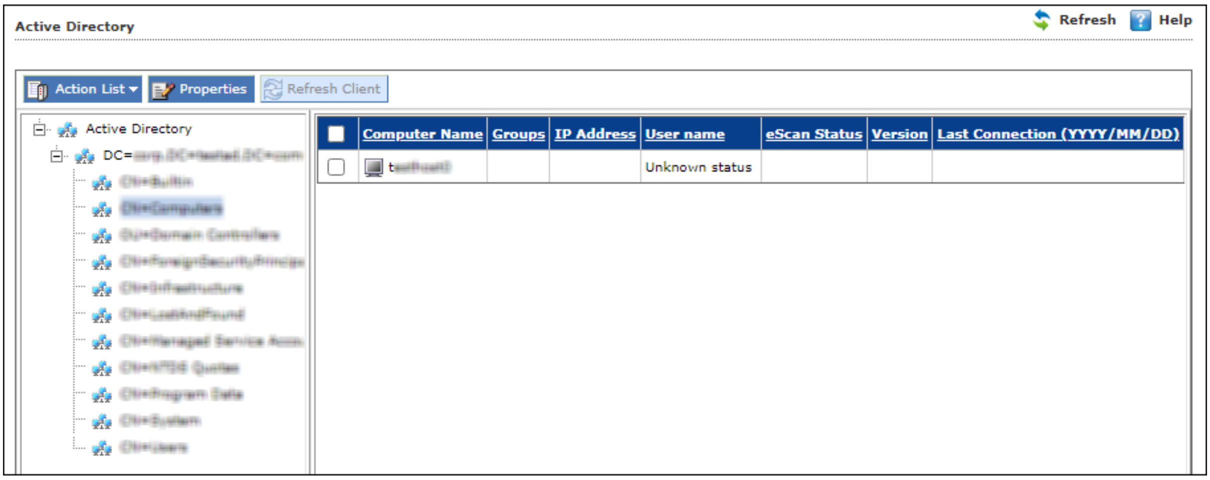
4. Fill in the required Login Credentials and click **OK**.
   The details including IP Addresses from active directory will be added instantly.


Properties

Active Directory Domain Controller Address

□ 192.[redacted]

5. Select the Active Directory and click **OK**. The selected Active Directory will be added to the Active directory tree.
6. To view the details, click the **Active Directory**.



Active Directory

[redacted]

☐	Computer Name	Groups	IP Address	User name	eScan Status	Version	Last Connection (YYYY/MM/DD)
☐	[redacted]			Unknown status			

Moving Computers from an Active Directory

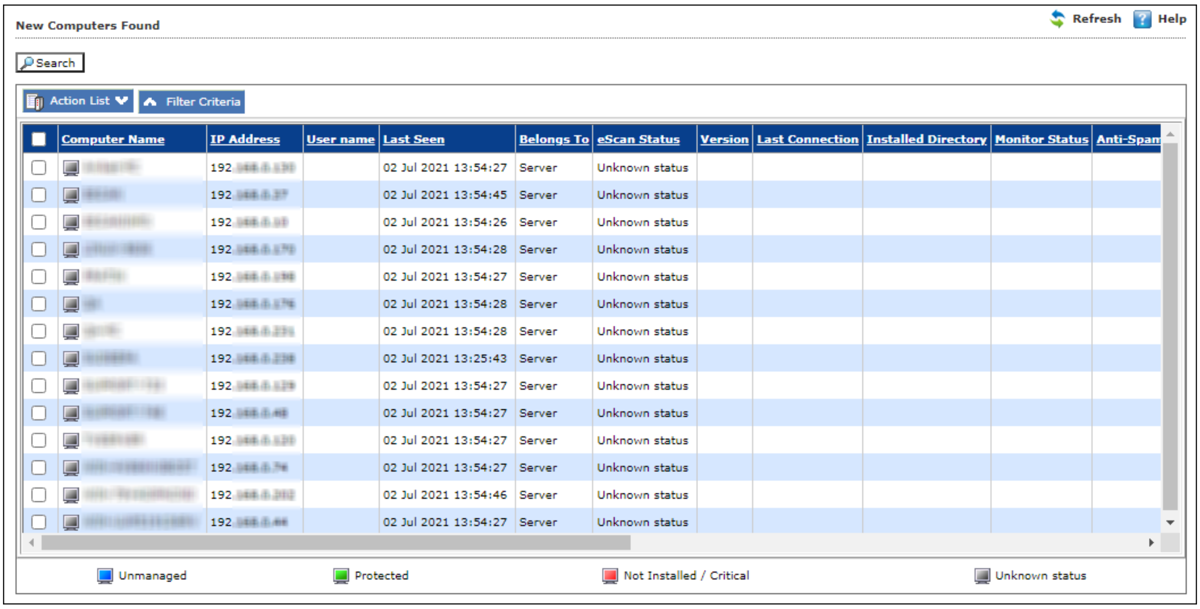
To move computers from an Active Directory, follow the steps given below:

1. Click an Active Directory.
2. Select the computers you want to move to other group.
3. Click **Action List** > **Move to Group**.
   Select Group window appears.
4. Select the Group and Click **OK**.

The selected computers will be moved to the selected group.

New Computers Found

The New Computers Found submodule displays list of all new computers connected to the network. With the Action List drop-down you can set Host Configuration, Move Computers to a Group, view Properties and Refresh Client. You can also export the New Computers List to .xls file format. After the computers are moved from Unmanaged Computers to groups under Managed Computers, you can assign tasks to them, Set host configuration, Manage Policies, Deploy/Upgrade Client or deploy a Hotfix on all or any of the Managed Computer individually or in group.



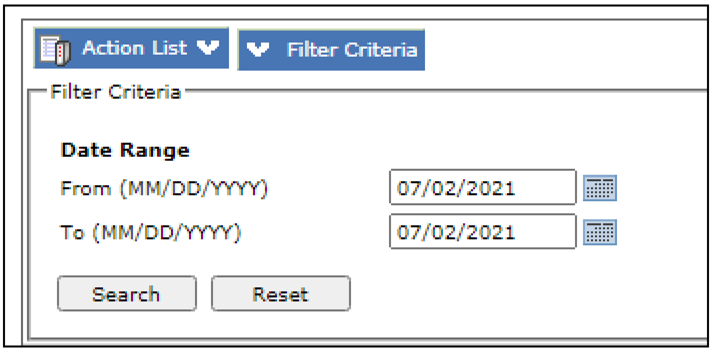
New Computers Found

☐	Computer Name	IP Address	User name	Last Seen	Belongs To	eScan Status	Version	Last Connection	Installed Directory	Monitor Status	Anti-Spam
☐	[redacted]	192.[redacted]		02 Jul 2021 13:54:27	Server	Unknown status					
☐	[redacted]	192.[redacted]		02 Jul 2021 13:54:45	Server	Unknown status					
☐	[redacted]	192.[redacted]		02 Jul 2021 13:54:26	Server	Unknown status					
☐	[redacted]	192.[redacted]		02 Jul 2021 13:54:28	Server	Unknown status					
☐	[redacted]	192.[redacted]		02 Jul 2021 13:54:27	Server	Unknown status					
☐	[redacted]	192.[redacted]		02 Jul 2021 13:54:28	Server	Unknown status					
☐	[redacted]	192.[redacted]		02 Jul 2021 13:54:28	Server	Unknown status					
☐	[redacted]	192.[redacted]		02 Jul 2021 13:25:43	Server	Unknown status					
☐	[redacted]	192.[redacted]		02 Jul 2021 13:54:27	Server	Unknown status					
☐	[redacted]	192.[redacted]		02 Jul 2021 13:54:27	Server	Unknown status					
☐	[redacted]	192.[redacted]		02 Jul 2021 13:54:27	Server	Unknown status					
☐	[redacted]	192.[redacted]		02 Jul 2021 13:54:27	Server	Unknown status					
☐	[redacted]	192.[redacted]		02 Jul 2021 13:54:46	Server	Unknown status					
☐	[redacted]	192.[redacted]		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.



Date Range

From (MM/DD/YYYY) 07/02/2021

To (MM/DD/YYYY) 07/02/2021

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.

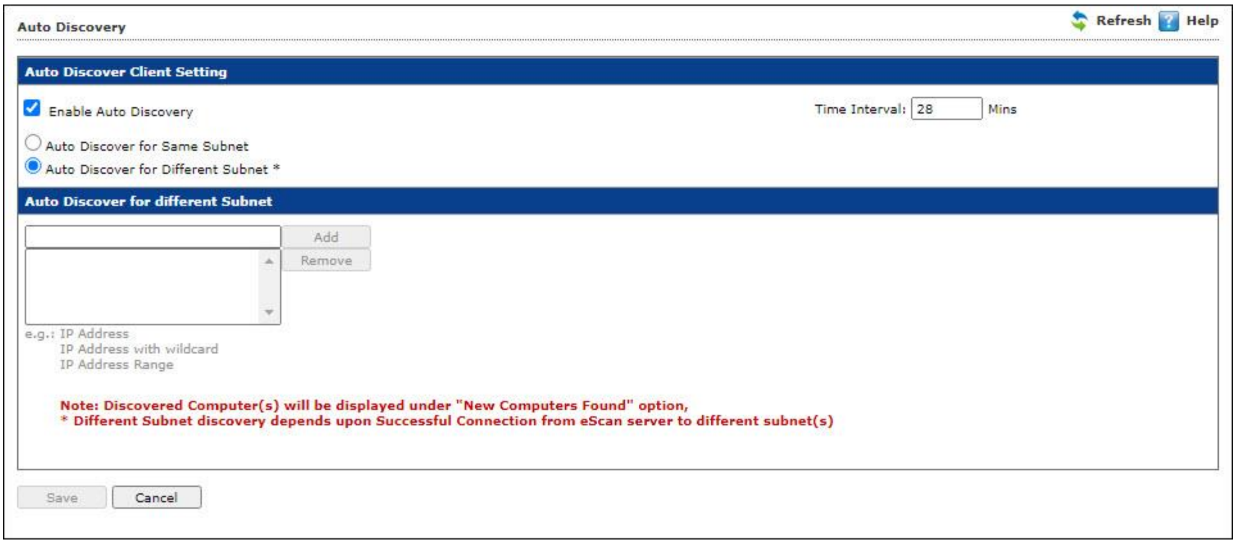
Action List

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.

Auto Discovery

The Auto Discovery allows you to keep automatically detecting the new computers connected to the network after a user-defined time interval.


Auto Discovery
Refresh
Help
Auto Discover Client Setting

☑ Enable Auto Discovery

Time Interval: 28 Mins

○ Auto Discover for Same Subnet
● Auto Discover for Different Subnet *

Auto Discover for different Subnet
Add
Remove

e.g.: IP Address
IP Address with wildcard
IP Address Range

Note: Discovered Computer(s) will be displayed under "New Computers Found" option,
* Different Subnet discovery depends upon Successful Connection from eScan server to different subnet(s)

Enable Auto Discovery

This option enables you to configure the settings involved in this submodule.

Auto Discover for Same Subnet

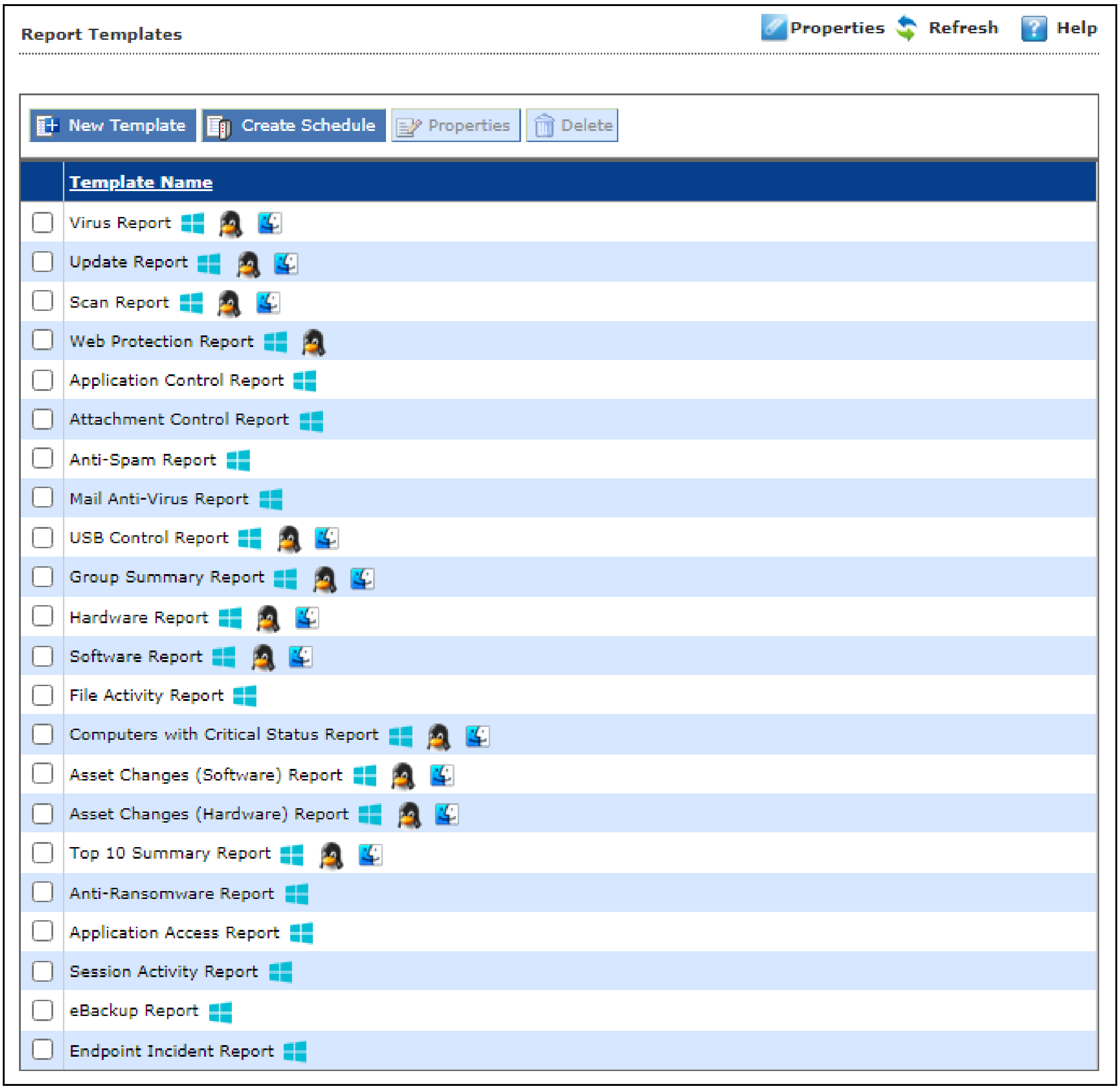
Using this option, you can allow eScan to automatically discover new computers connected to the same sub network.

Auto Discover for Different Subnet

Select this option to allow eScan to automatically discover new computers connected to the different sub network as per your requirement. To use this function, you need to add IP Address, IP Address with wildcard or IP range in the provided field.

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.

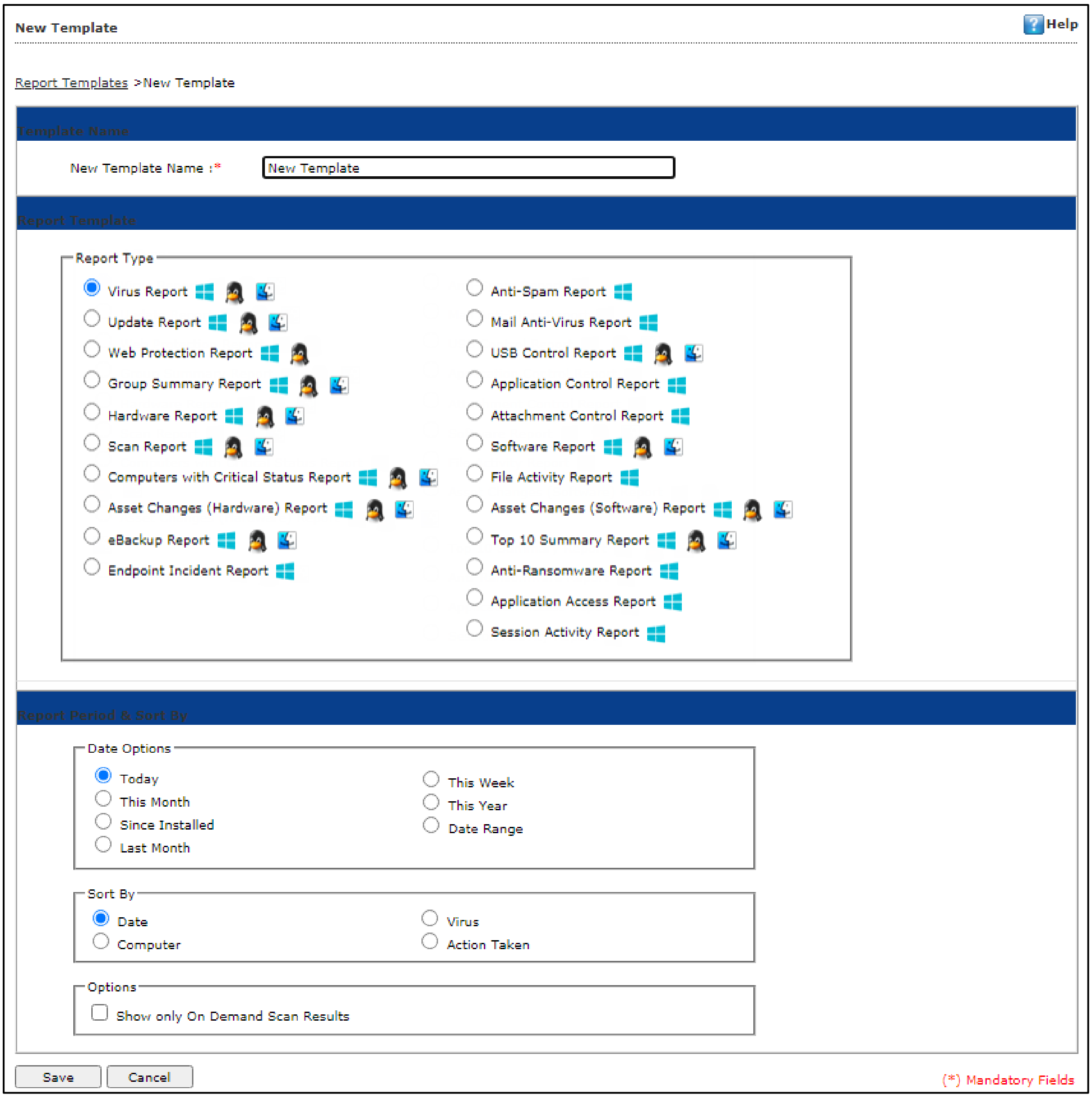


	Template Name
☐	Virus Report
☐	Update Report
☐	Scan Report
☐	Web Protection Report
☐	Application Control Report
☐	Attachment Control Report
☐	Anti-Spam Report
☐	Mail Anti-Virus Report
☐	USB Control Report
☐	Group Summary Report
☐	Hardware Report
☐	Software Report
☐	File Activity Report
☐	Computers with Critical Status Report
☐	Asset Changes (Software) Report
☐	Asset Changes (Hardware) Report
☐	Top 10 Summary Report
☐	Anti-Ransomware Report
☐	Application Access Report
☐	Session Activity Report
☐	eBackup Report
☐	Endpoint Incident Report

Creating a Report Template

To create a Report Template, follow the steps given below:

1. In the navigation panel, click **Report Templates**.
2. Click **New Template**.
   New Template screen appears.



New Template

Help

Report Templates >New Template

Template Name

New Template Name :* New Template

Report Template

Report Type

● Virus Report
○ Update Report
○ Web Protection Report
○ Group Summary Report
○ Hardware Report
○ Scan Report
○ Computers with Critical Status Report
○ Asset Changes (Hardware) Report
○ eBackup Report
○ Endpoint Incident Report
○ Anti-Spam Report
○ Mail Anti-Virus Report
○ USB Control Report
○ Application Control Report
○ Attachment Control Report
○ Software Report
○ File Activity Report
○ Asset Changes (Software) Report
○ Top 10 Summary Report
○ Anti-Ransomware Report
○ Application Access Report
○ Session Activity Report

Report Period & Sort By

Date Options

● Today
○ This Month
○ Since Installed
○ Last Month
○ This Week
○ This Year
○ Date Range

Sort By

● Date
○ Computer
○ Virus
○ Action Taken

Options

□ Show only On Demand Scan Results

Save Cancel

(*) Mandatory Fields

3. Enter a name for the template.
4. Select a report type.
   Depending upon the report type, the additional setting varies.
5. After making the necessary selections/filling data, click **Save**.
   The template will be created according to your preferences.

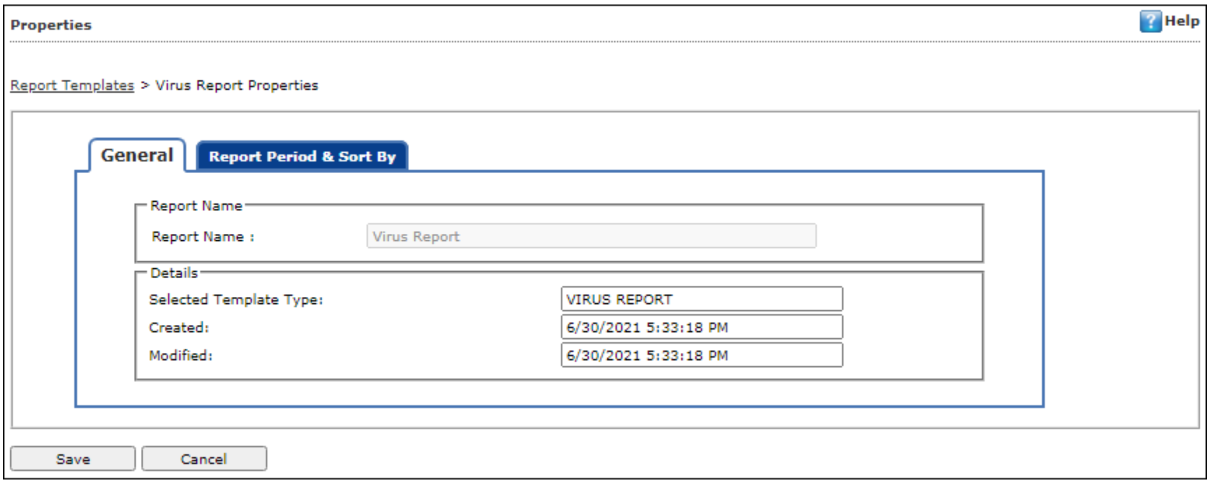
Creating Schedule for a Report Template

The Report Template module lets you create a new schedule for the report templates. To learn more, **click here**.

Viewing Properties of a Report Template

To view the properties of Report Template, follow the steps given below:

1. Select the Report Template whose properties you want to view.
2. Click **Properties**. Properties screen appears.



Report Name
Report Name : Virus Report

Details
Selected Template Type: VIRUS REPORT
Created: 6/30/2021 5:33:18 PM
Modified: 6/30/2021 5:33:18 PM

NOTE	Depending upon the Report Template enter, the Properties varies.

3. After making the necessary changes, click **Save**.
   The Report Template's properties will be updated.

Deleting a Report Template

To delete a Report Template, follow the steps given below:

1. Select the template you want to delete.
2. Click **Delete**.
   A confirmation prompt appears.
3. Click **OK**.
   The Report Template will be deleted.

NOTE	Default Report Templates cannot be deleted.

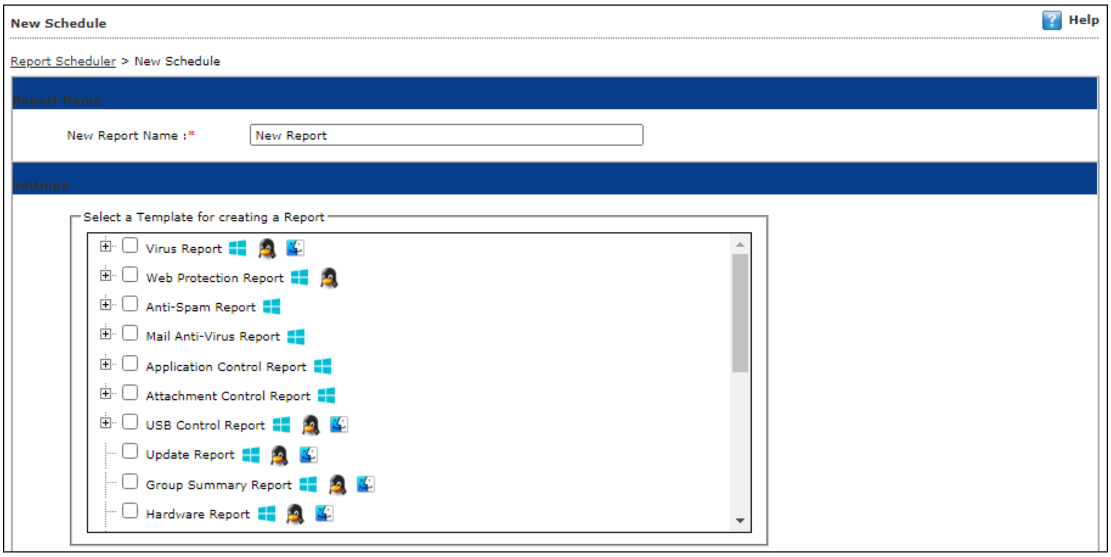
Report Scheduler

The Report Scheduler module lets you create schedule, update and run the task according to your preferences.

Creating a Schedule

To create a Schedule:

1. In the Report Scheduler screen, click **New Schedule**.
   New Schedule screen appears.



New Schedule | Help

Report Scheduler > New Schedule

Report Name

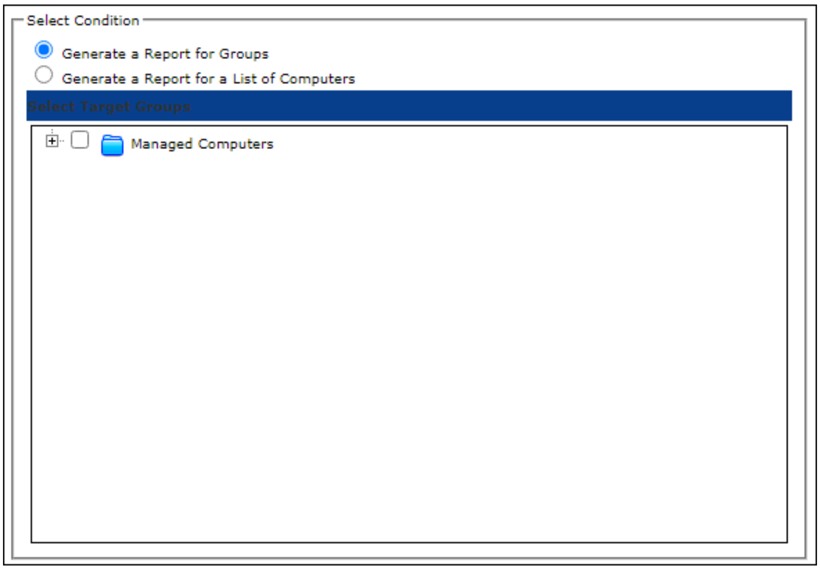
New Report Name :* New Report

Settings

Select a Template for creating a Report

- ☐ Virus Report
- ☐ Web Protection Report
- ☐ Anti-Spam Report
- ☐ Mail Anti-Virus Report
- ☐ Application Control Report
- ☐ Attachment Control Report
- ☐ USB Control Report
- ☐ Update Report
- ☐ Group Summary Report
- ☐ Hardware Report

2. Enter a name for the report.
3. In the Settings section, select preferred templates.
4. In the Select Condition section, select a condition for groups or specific computers.



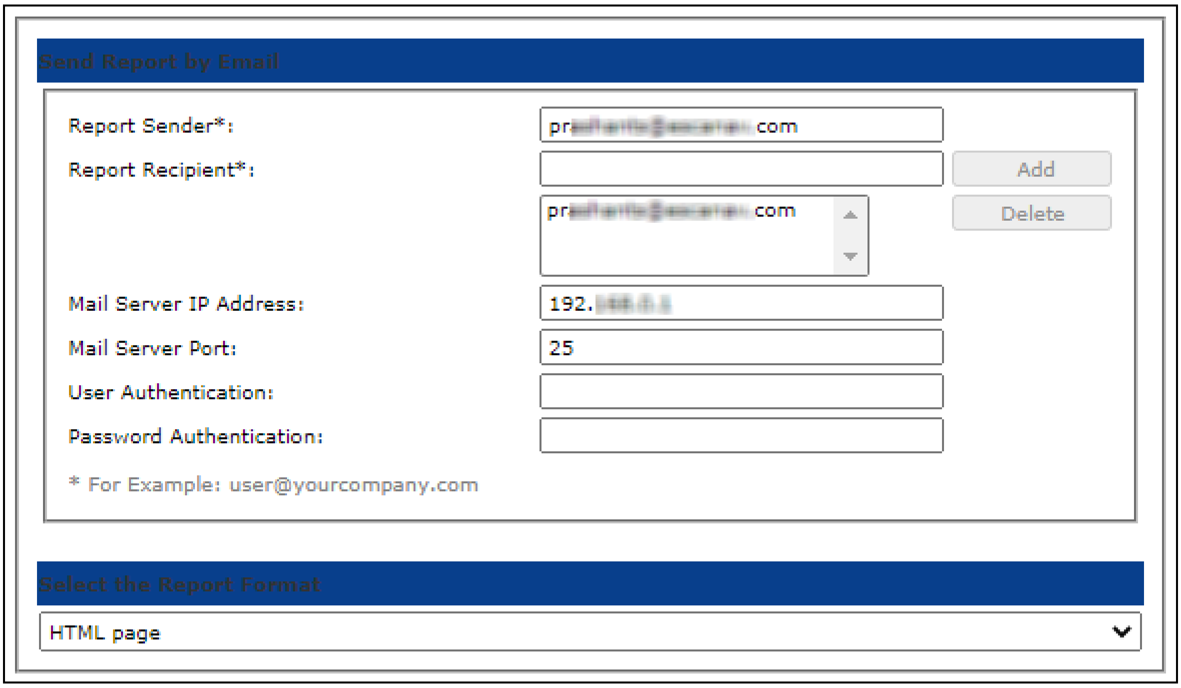
Select Condition

- ● Generate a Report for Groups
- ○ Generate a Report for a List of Computers

Select Target Groups

- ☐ Managed Computers

5. In the Send Report by email section, fill the required information to receive reports via email.



Send Report by Email

Report Sender*: pr[redacted] com

Report Recipient*:

pr[redacted] com

Mail Server IP Address: 192.[redacted]

Mail Server Port: 25

User Authentication:

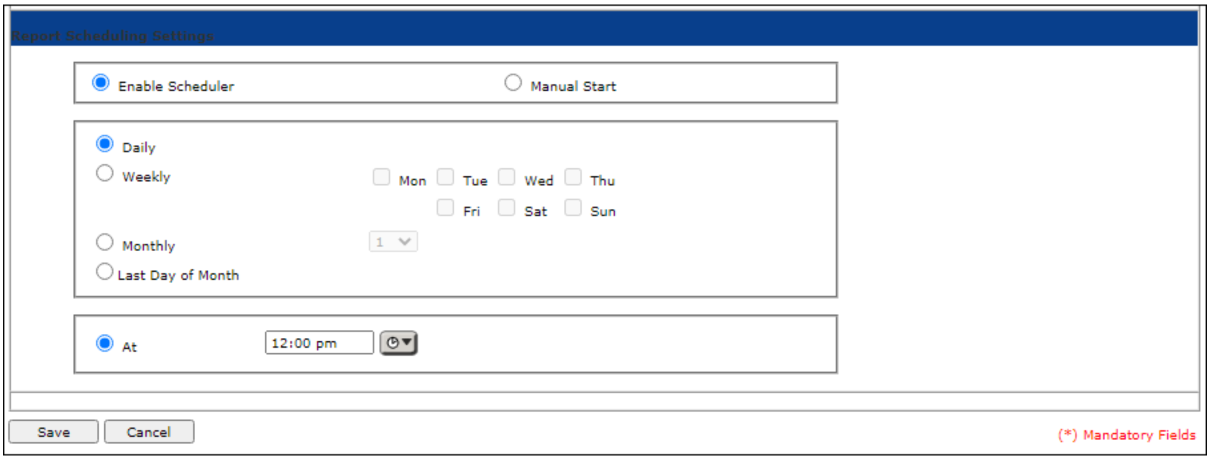
Password Authentication:

* For Example: user@yourcompany.com

Select the Report Format

HTML page

6. Select the preferred report format.
7. In Report Scheduling Settings section, make the necessary changes.



Report Scheduling Settings

● Enable Scheduler ○ Manual Start

● Daily

○ Weekly □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

○ Monthly 1

○ Last Day of Month

● At 12:00 pm

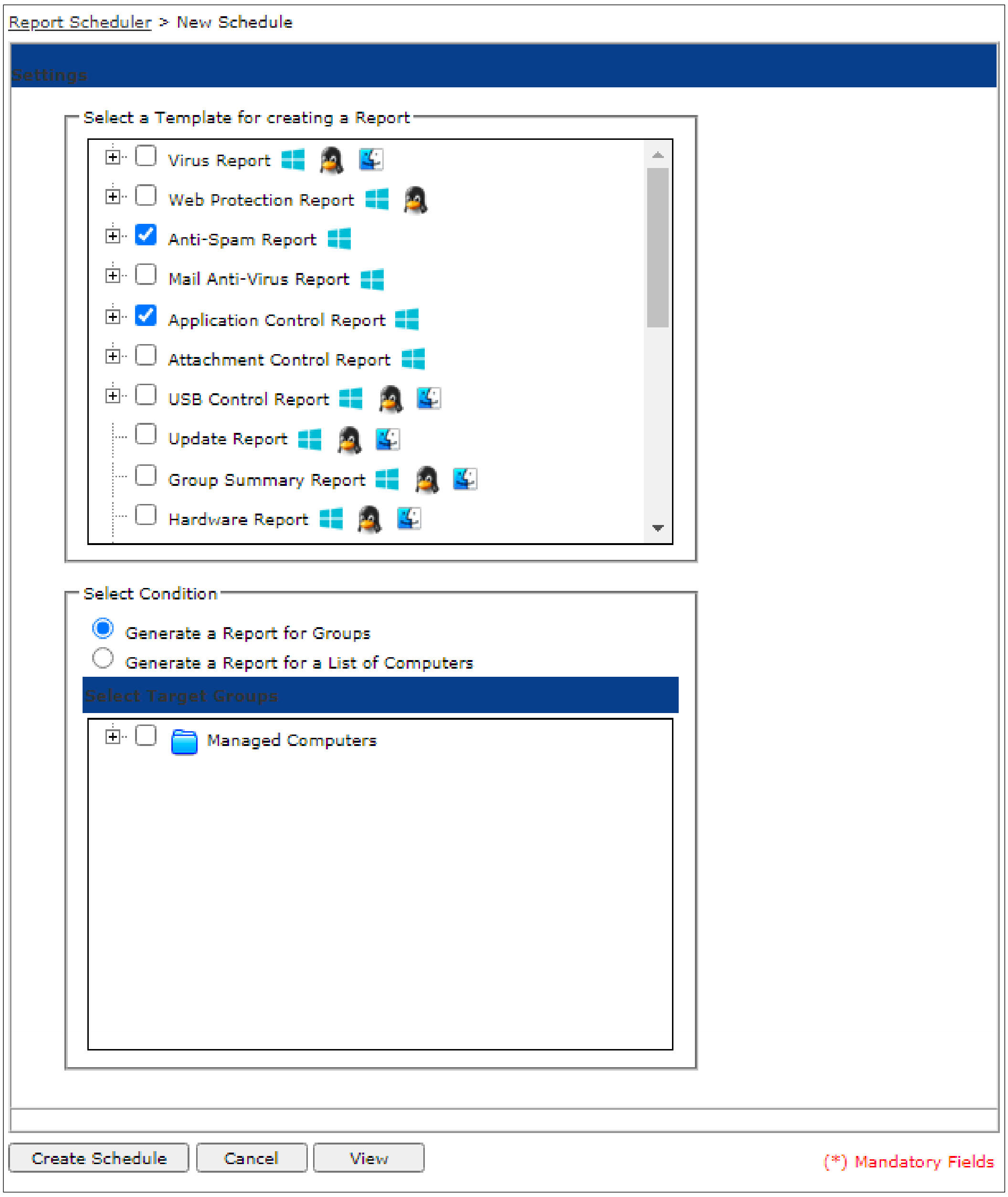
(*) Mandatory Fields

8. Click **Save**.
   New schedule will be created.

Viewing Reports on Demand

To view a report or a set of reports immediately:

1. Click **Report Scheduler** > **View & Create**.
   New Schedule screen appears.



Report Scheduler > New Schedule

Settings

Select a Template for creating a Report

- ☐ Virus Report
- ☐ Web Protection Report
- ☑ Anti-Spam Report
- ☐ Mail Anti-Virus Report
- ☑ Application Control Report
- ☐ Attachment Control Report
- ☐ USB Control Report
- ☐ Update Report
- ☐ Group Summary Report
- ☐ Hardware Report

Select Condition

● Generate a Report for Groups
○ Generate a Report for a List of Computers

Select Target Groups

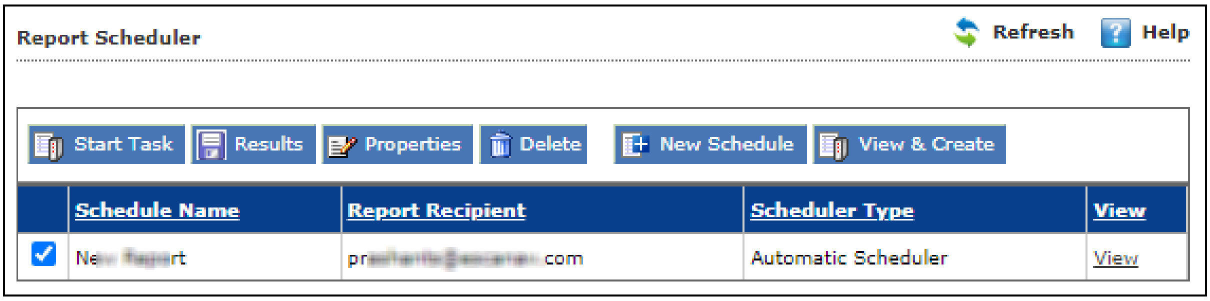
☐ Managed Computers

2. Select the **Template** options, the **Condition** and the **Target Groups**.
3. Click **View**.
4. A new window appears displaying the created report.

Clicking **Create Schedule** lets you create a new Schedule.

Managing Existing Schedules

The Report Scheduler module lets you manage the existing schedules.



Report Scheduler

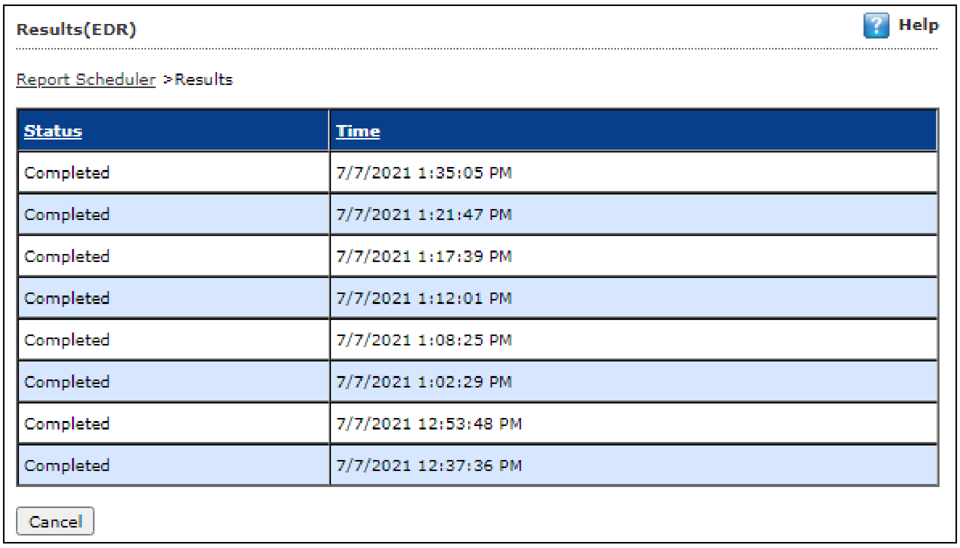
	Schedule Name	Report Recipient	Scheduler Type	View
☑	Ne[redacted]rt	pr[redacted]com	Automatic Scheduler	View

Generating Task Report of a Schedule

To generate a task report, select the preferred report schedule name and then click **Start Task**. A task window appears displaying the name of the report being generated.

Viewing Results of a Schedule

To see the results of a schedule and its time stamp, select the report schedule and then click **Results**. Results screen appears.



Results(EDR)

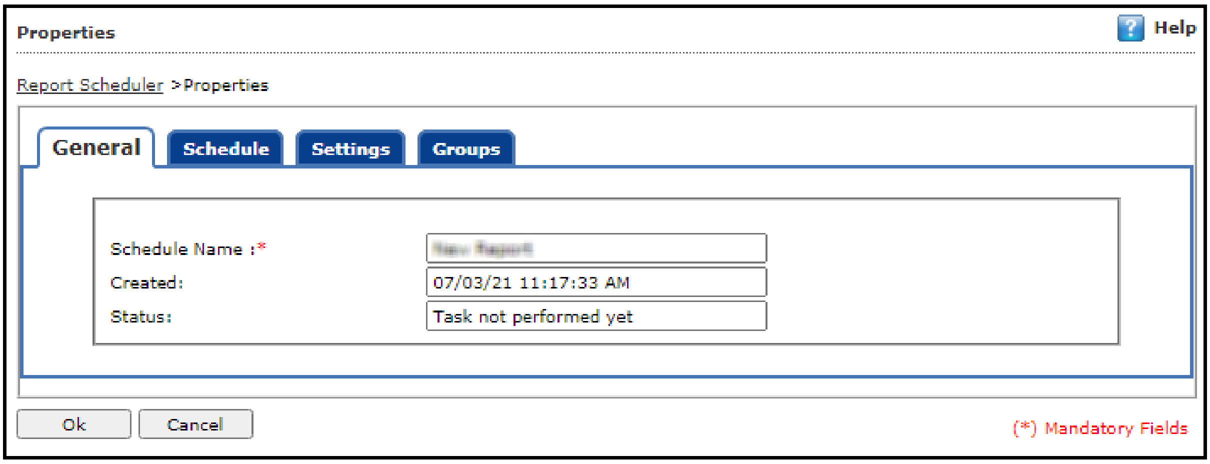
Report Scheduler >Results

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.



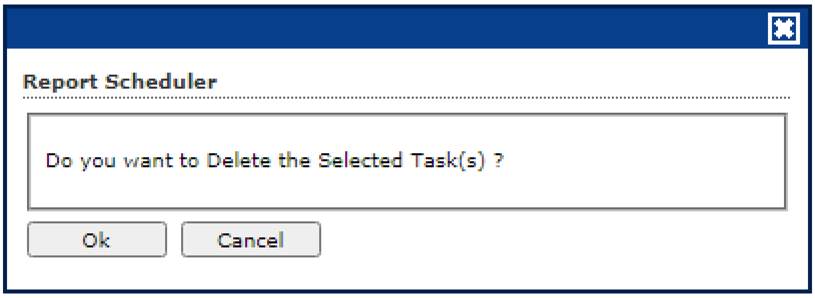
Schedule Name :* [redacted]
Created: 07/03/21 11:17:33 AM
Status: Task not performed yet

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.

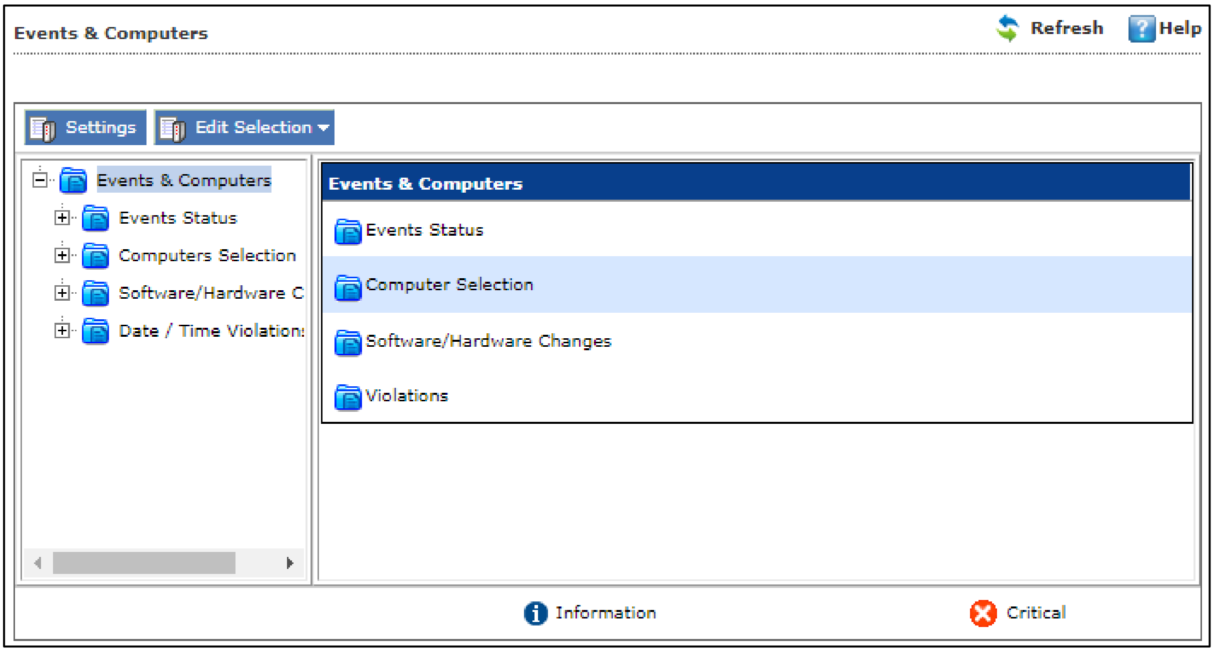


Do you want to Delete the Selected Task(s) ?

3. Click **OK**.
   The schedule will be deleted.

Events and Computers

eScan Management Console maintains the record of all the events sent by the client computer. Through the events & computers module, the administrator can monitor the Events and Computers; the module lets you sort the computer with specific properties.



Events Status

The Event Status subfolder is divided into following sections:

- **Recent**
- **Critical**
- **Information**

Recent

The Recent section displays both Information and Critical events.

Critical ☒

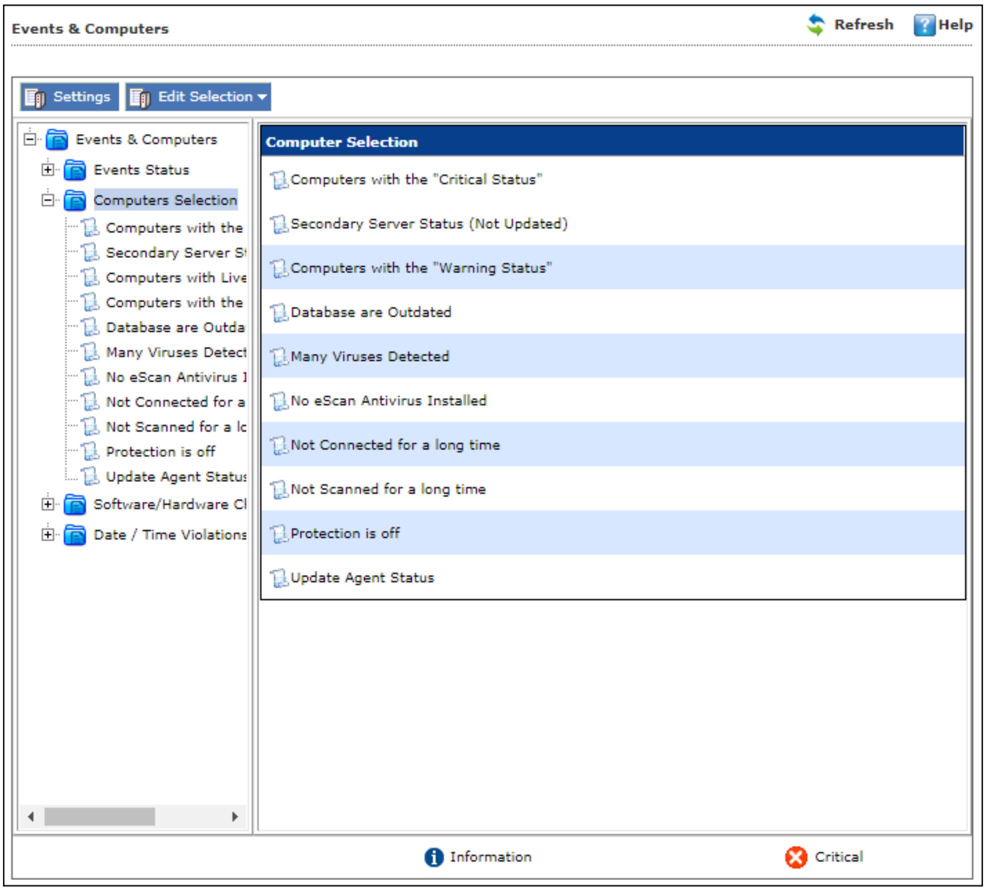
The Critical section displays Critical events and immediate attention.
For example, Virus detection, Monitor disabled.
The Critical events can be filtered on the basis of date range and the report can be exported in .xls or .html format.

Information ⓘ

The Information section displays basic information events.
For example, Virus database update, Status.

Computer Selection

The Computer Selection subfolder displays computers that fall under different categories. It lets you select the computer and take the preferred action. You can also set the criteria for each section and sort the computer accordingly.



Computer Selection

- Computers with the "Critical Status"
- Secondary Server Status (Not Updated)
- Computers with the "Warning Status"
- Database are Outdated
- Many Viruses Detected
- No eScan Antivirus Installed
- Not Connected for a long time
- Not Scanned for a long time
- Protection is off
- Update Agent Status

The Computer Selection subfolder consists following sections:

- **Computers with "Critical Status"**
- **Secondary Server Status (Not Updated)**
- **Computers with Live Status**
- **Computer with "Warning Status"**
- **Database is outdated**
- **Many Viruses Detected**
- **No eScan Installed**
- **Not connected for a long time**
- **Not scanned for a long time**
- **Protection is off**
- **Update Agent Status**

This section displays computers marked with Critical status.

Computers with critical status
This section displays computers marked with Critical status.

Secondary Server Status (Not Updated)

A secondary server receives downloads from the primary server and further distributes to the client computers. If the secondary server is not updated, it will be mentioned in the log.

Computers with Live status

This section displays whether the computers present in the network are online or offline.

To get the details of the specific computers' status, select **Computers with Live Status** option. This will display the computers with default online status along with other details such as IP Address, Group, Description, and more. To display all the endpoints in the network, you can use filter options that filters out based on **Status Type**.

After selecting the computer from the list, you can choose **System Action List** drop-down option from the top panel. This option allows you to perform specific set of actions on the selected endpoints.

NOTE	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.

Database is outdated

This section displays computers whose virus database is outdated.

Many Viruses Detected

This section displays the computers whose virus count has exceeded.

No eScan installed

This section displays computers on which eScan is not installed.

Not connected for a long time

This section displays the computers which didn’t connect to the eScan server for the set duration.

Not scanned for a long time
This section displays the computers which weren't scanned for the set duration.

Protection is off
This section displays the computers on which File Protection is disabled.

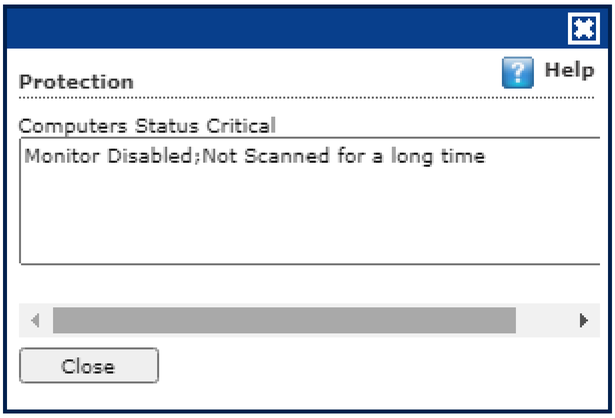
Update Agent Status
This section displays the status of computers assigned as Update Agent.

The additional settings vary depending upon the Computer Status.

Edit Selection

This drop-down menu allows to configure various option based on selected options. The following options are present in the menu:

- **Protection**: This option displays the protection status of the selected computer.

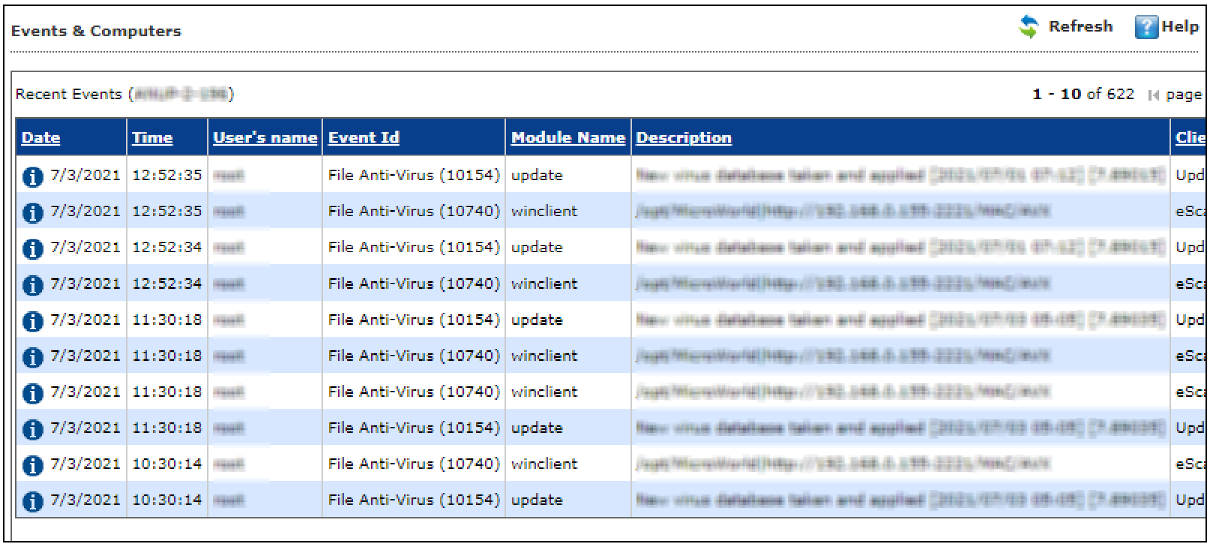


Protection

Computers Status Critical

Monitor Disabled;Not Scanned for a long time

- **Events**: This option displays the events that were performed in particular computer.



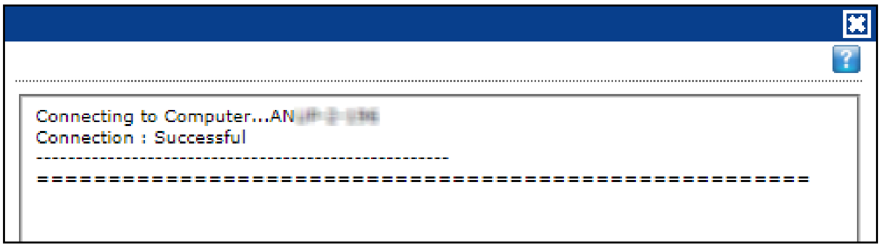
Events & Computers

Recent Events ([redacted])

1 - 10 of 622

Date	Time	User's name	Event Id	Module Name	Description	Clie
7/3/2021	12:52:35	[redacted]	File Anti-Virus (10154)	update	[redacted]	Upd
7/3/2021	12:52:35	[redacted]	File Anti-Virus (10740)	winclient	[redacted]	eSca
7/3/2021	12:52:34	[redacted]	File Anti-Virus (10154)	update	[redacted]	Upd
7/3/2021	12:52:34	[redacted]	File Anti-Virus (10740)	winclient	[redacted]	eSca
7/3/2021	11:30:18	[redacted]	File Anti-Virus (10154)	update	[redacted]	Upd
7/3/2021	11:30:18	[redacted]	File Anti-Virus (10740)	winclient	[redacted]	eSca
7/3/2021	11:30:18	[redacted]	File Anti-Virus (10740)	winclient	[redacted]	eSca
7/3/2021	11:30:18	[redacted]	File Anti-Virus (10154)	update	[redacted]	Upd
7/3/2021	10:30:14	[redacted]	File Anti-Virus (10740)	winclient	[redacted]	eSca
7/3/2021	10:30:14	[redacted]	File Anti-Virus (10154)	update	[redacted]	Upd

- **Deploy/Upgrade Client**: To learn about this option, click here.
- **Check Connection**: This option will verify if the client machine is online or offline.



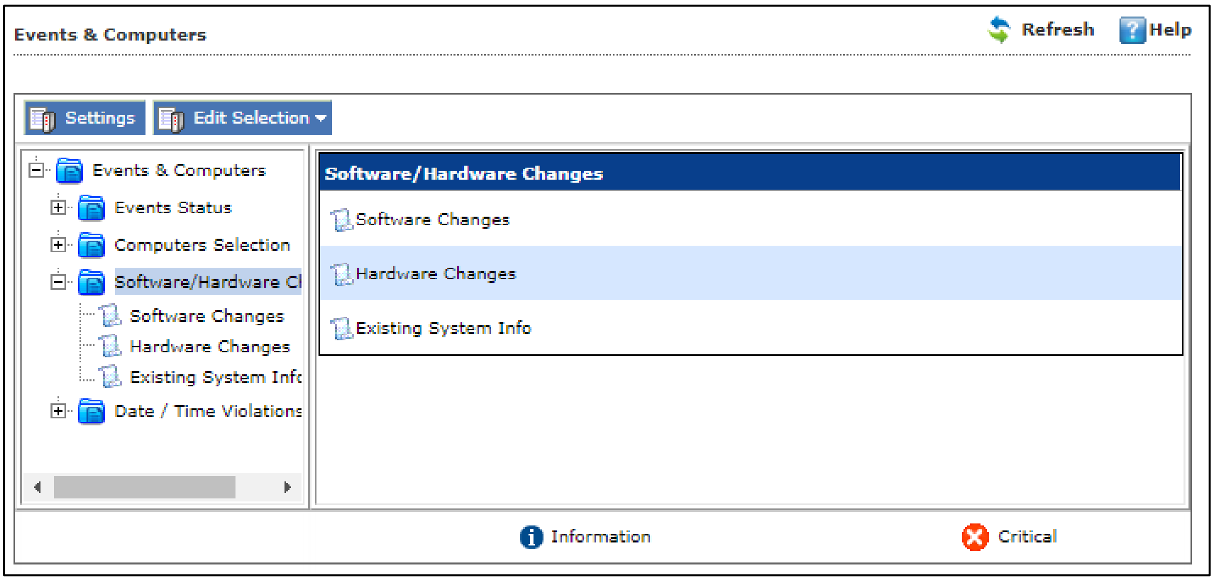
```
Connecting to Computer...AN[redacted]
Connection : Successful
------------------------------------------------------
==========================================================
```

- **Remove from Group**: To learn about this option, click here.
- **Connect to Client (RMM)**: To learn about this option, click here.
- **Force Download**: To learn about this option, click here.
- **On Demand Scanning**: To learn about this option, click here.
- **Send Message**: To learn about this option, click here.
- **Properties**: To learn about this option, click here.

Software/Hardware Changes

This subfolder displays all software/ hardware changes that occurred on computers. It consists following sections:

- **Software Changes**
- **Hardware Changes**
- **Existing System Info**



Software Changes

This section displays software changes i.e. installation, uninstallation or software upgrades.

Hardware Changes

This section displays hardware changes that occurred on computers. For example, IP address. Hard Disk, RAM etc.

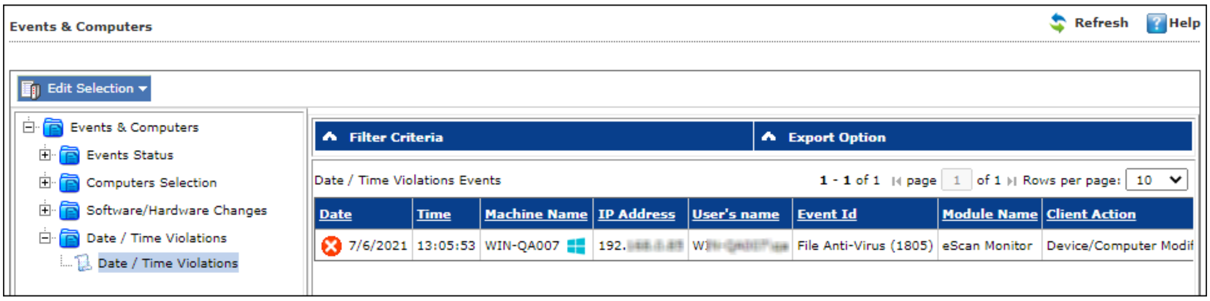
Existing System Info

This section displays a computer's existing hardware information.

Violations

Date/Time Violations

This subfolder consists Date/Time Violations that displays client computers whose users attempted to modify date and time.



Events & Computers

Date / Time Violations Events 1 - 1 of 1 page 1 of 1 Rows per page: 10

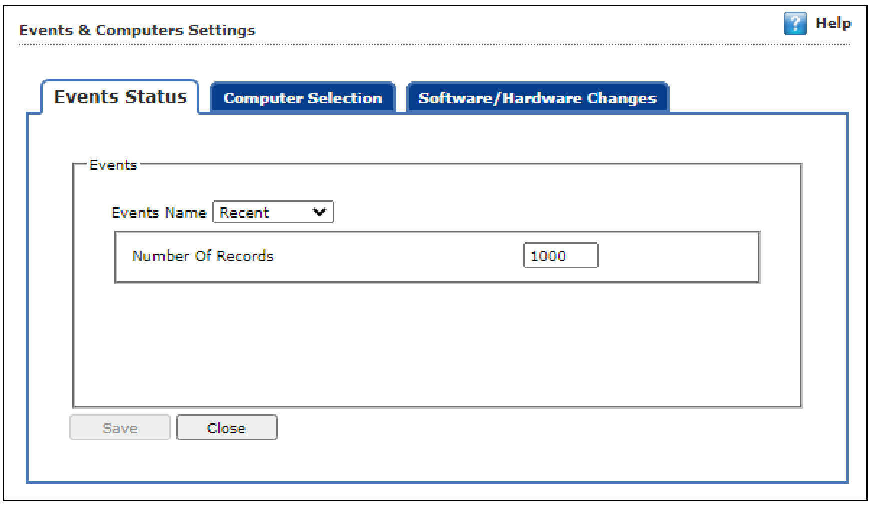
Date	Time	Machine Name	IP Address	User's name	Event Id	Module Name	Client Action
7/6/2021	13:05:53	WIN-QA007	192.[redacted]	W[redacted]	File Anti-Virus (1805)	eScan Monitor	Device/Computer Modif

Settings

You can define the Settings for Events, Computer Selection and Software/Hardware changes by clicking on the **Settings** option and defining the desired settings using the Tabs and options present on the Events and Computer settings window.

Event Status Setting

Basically, events are activities performed on client's computer.



Events & Computers Settings

Events Name: Recent

Number Of Records: 1000

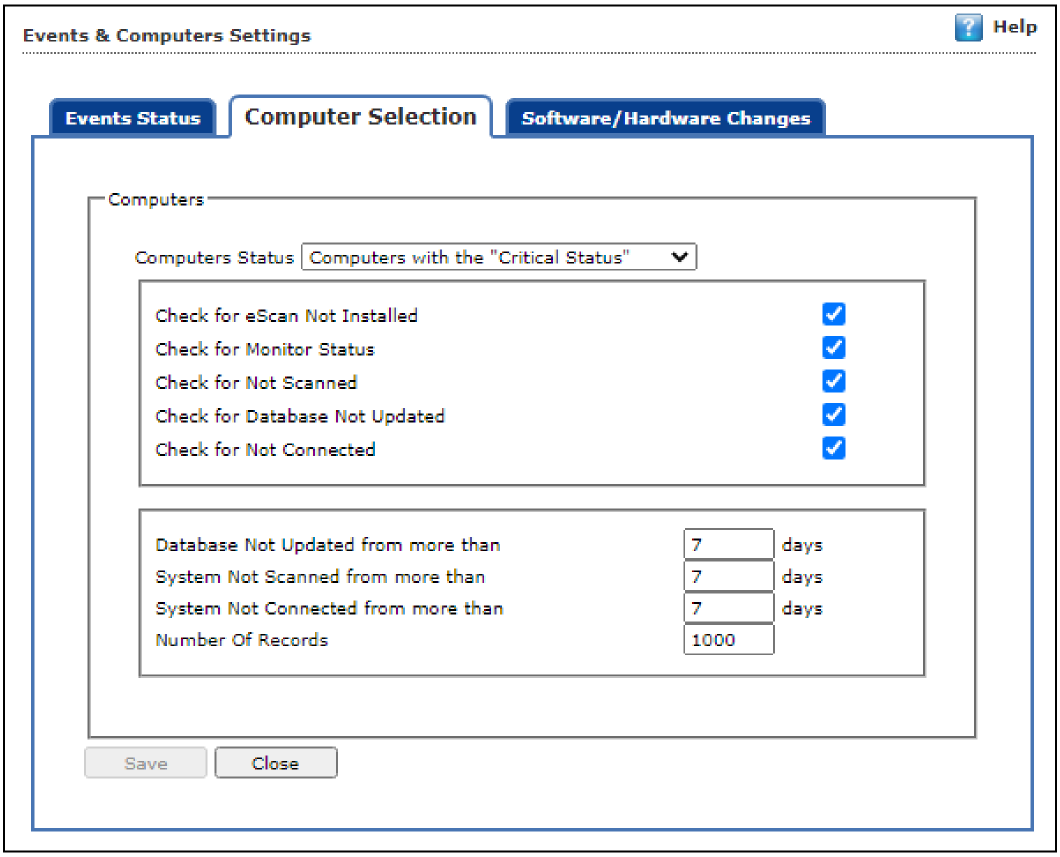
On the basis of severity, the events are categorized in to the following types:

- **Recent:** It displays both critical and information events that occurred recently on managed client computers.
- **Information:** It displays all informative types of events, such as virus database update, status, and so on.

Perform the following steps to define event status settings:

1. Select the appropriate **Events Name**.
2. Enter the number of events that you want to view in a list, in the **Number of Records** field.
3. Click **Save**. The settings get saved.

Computer Selection



Events & Computers Settings

Computers

Computers Status: Computers with the "Critical Status"

- Check for eScan Not Installed ☑
- Check for Monitor Status ☑
- Check for Not Scanned ☑
- Check for Database Not Updated ☑
- Check for Not Connected ☑

Database Not Updated from more than 7 days
System Not Scanned from more than 7 days
System Not Connected from more than 7 days
Number Of Records 1000

The **Computer Selection** lets you select and save the computer status settings. This module lets you perform the following activities:

Critical Status: It displays a list of computers that are critical in status as per the criteria's selected in computer settings. Specify the details in following fields:

- **Check for eScan Not Installed**: Select this checkbox to view the list of client systems under managed computers on which eScan has not been installed.
- **Check for Monitor Status**: Select this checkbox to view the client systems on which eScan monitor is not enabled.
- **Check for Not Scanned**: Select this checkbox to view the list of client systems which have not been scanned.
- **Check for Database Not Updated**: Select this checkbox to view the list of client systems on which database has not been updated.
- **Check for Not Connected**: Select this checkbox to view the list of eScan client systems that have not been communicated with eScan server.
- **Database Not Updated from more than**: Enter the number of days from when the database has not been updated.
- **System Not Scanned for more than**: Enter the number of days from when the system has not been scanned.
- **System Not Connected for more than**: Enter the number of days from when the client system has not been connected to eScan server.

- **Number Of Records**: Enter the number of client systems that you want to view in the list.

Secondary Server Status (Not Updated): It displays the list of systems on which the Secondary server status is not updated. Specify the following field details:

- **Number of records**: Enter the number of systems that you want to view in the list.

Live Status: It displays the list of systems on which the eScan protection is turned-on. Specify the following field details:

- **Number of records**: Enter the number of systems that you want to view in the list.

Warning Status: It displays the list of systems which are warning in status, as per the criteria's selected in computer settings. Specify the following field details:

- **Check for Not Scanned**: Select this checkbox to view the list of client systems which has not been scanned.
- **Check for Database Not Updated**: Select this checkbox to view the list of client systems on which database has not been updated.
- **Check for Not Connected**: Select this checkbox to view the list of eScan client systems that have not been communicated with eScan server.
- **Check for Protection off**: Select this checkbox to view the list of client systems on which protection for particular module is inactive.
- **Check for Many Viruses**: Select this checkbox to view the list of client systems on which maximum viruses are detected.
- **Database Not Updated from more than**: Enter the number of days from when the database has not been updated.
- **System Not Scanned for more than**: Enter the number of days from when the system has not been scanned.
- **System Not Connected for more than**: Enter the number of days from when the client system has not been connected to eScan server.
- **Number Of Virus**: Enter the number of viruses detected on client system.
- **Number Of Records**: Enter the number of client system that you want to view in the list.

Database are Outdated: It displays a list of systems on which virus database is outdated. Specify the following field details:

- **Database Not Updated from more than**: Enter the number of days from when the database has not been updated.
- **Number of Records**: Enter the number of client system that you want to view in the list.

Many viruses Detected: It displays a list of systems on which number of viruses exceed the specified count in computer settings. Specify the following field details:

- **Number of Virus**: Enter the number of viruses detected on client system.
- **Number of Records**: Enter the number of client systems that you want to view in the list.

No eScan Antivirus Installed: It displays the list of systems on which eScan has not been installed. Specify the following field detail:

- **Number of Records**: Enter the number of client system that you want to view in the list.

Not connected to the eScan server for a long time: It displays the list of systems which have not been connected to the server from a long time. Specify the following field detail:

- **Number of Records**: Enter the number of client system that you want to view in the list.

Not scanned for a long time: It displays the list of systems which have not been scanned from a long time, as specified in computer settings. Specify the following field details:

- **System Not Scanned for more than**: Enter the number of days from when the system has not been scanned.
- **Number of Records**: Enter the number of client system that you want to view in the list.

Protection is off: It displays the list of systems on which protection is inactive for any module, as per the protection criteria's selected in computer settings. It shows the status as "Disabled" in the list. Specify the following field details:

- **Check for Monitor Status**: Select this checkbox if you want to view the client systems on which eScan monitor is not enabled.
- **Check for Mail Anti-Phishing**: Select this checkbox if you want to view the list of client systems on which **Mail Anti-Phishing** protection is inactive.
- **Check for Mail Anti-Virus**: Select this checkbox if you want to view the list of client systems on which **Mail Anti-Virus** protection is inactive.
- **Check for Mail Anti-Spam**: Select this checkbox if you want to view the list of client systems on which **Mail Anti- Spam** protection is inactive.
- **Check for Endpoint Security**: Select this checkbox if you want to view the list of client systems on which **Endpoint Security** protection is inactive.
- **Check for Firewall**: Select this checkbox if you want to view the list of client systems on which **Firewall** protection is inactive.
- **Check for Proactive**: Select this checkbox if you want to view the list of client systems on which **Proactive** protection is inactive.
- **Check for Web Protection**: Select this checkbox if you want to view the list of client systems on which the **Web Protection** is inactive.
- **Number of Records**: Enter the number of client system that you want to view in the list.

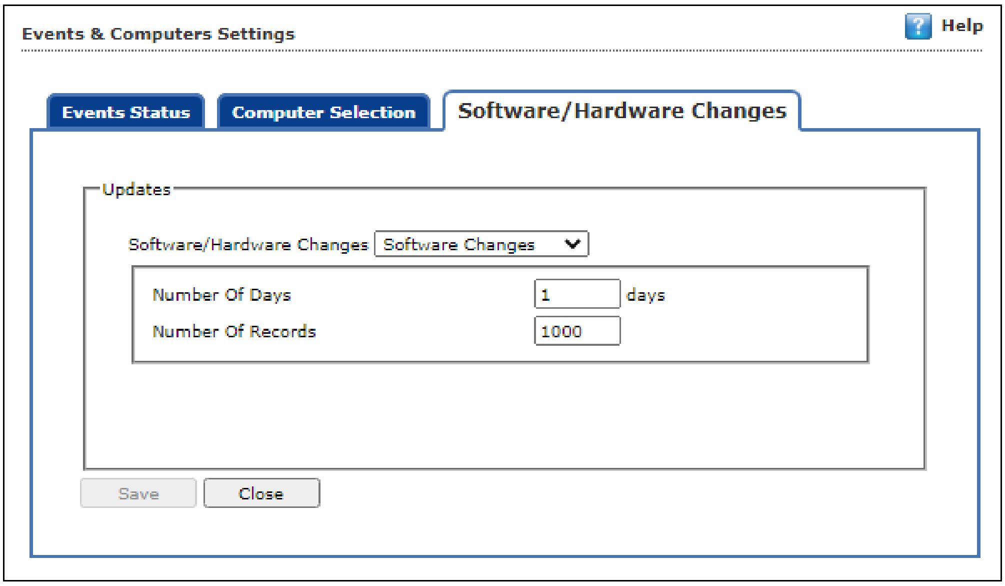
Steps to define computer settings

To save the computer settings, follow the steps given below:

1. Click **Computers Selection** tab.
2. Select a type of status for which you want to set criteria, from the **Computer status** drop-down.
3. Select the appropriate checkboxes, and then enter field details in the available fields. For more information, refer [Types and criteria of computer status] section.
4. Click **Save**. The settings will be saved.

Software/ Hardware Changes Setting

You can configure these settings to receive updates on any Software, Hardware, and existing system changes.



Events & Computers Settings

Software/Hardware Changes: Software Changes

Number Of Days: 1 days

Number Of Records: 1000

The **Software/ Hardware Changes** enable you to do the following activities:
Type of Software/Hardware Changes:

- **Software changes**
- **Hardware changes**
- **Existing system info**

To Change software/hardware settings, follow the steps given below:

1. Click the **Software/Hardware Changes** tab.
2. Specify the following field details:
   - **Software/Hardware Changes**: Click the drop-down and select the changes made.
   - **Number of Days**: Enter the number of days, to view changes made within the specified days.
   - **Number of Records**: Enter the number of client systems that you want to view in the list.
3. Click **Save**. The settings get saved.

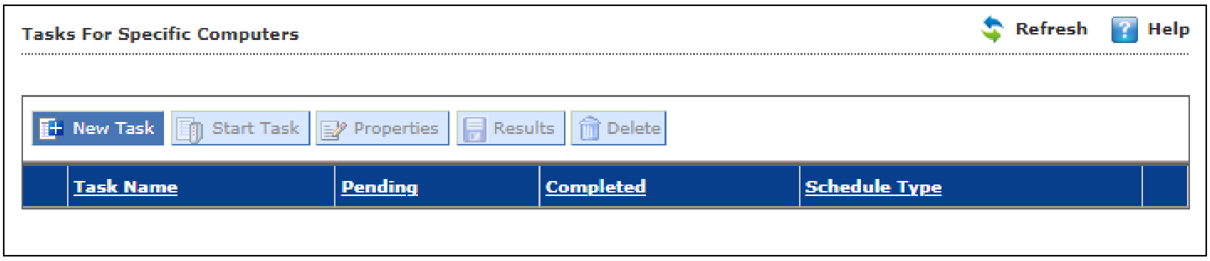
Performing an action for computer

To perform an action for a computer, follow the steps given below:

1. Select a computer.
2. Click **Edit Selection** drop-down. 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.



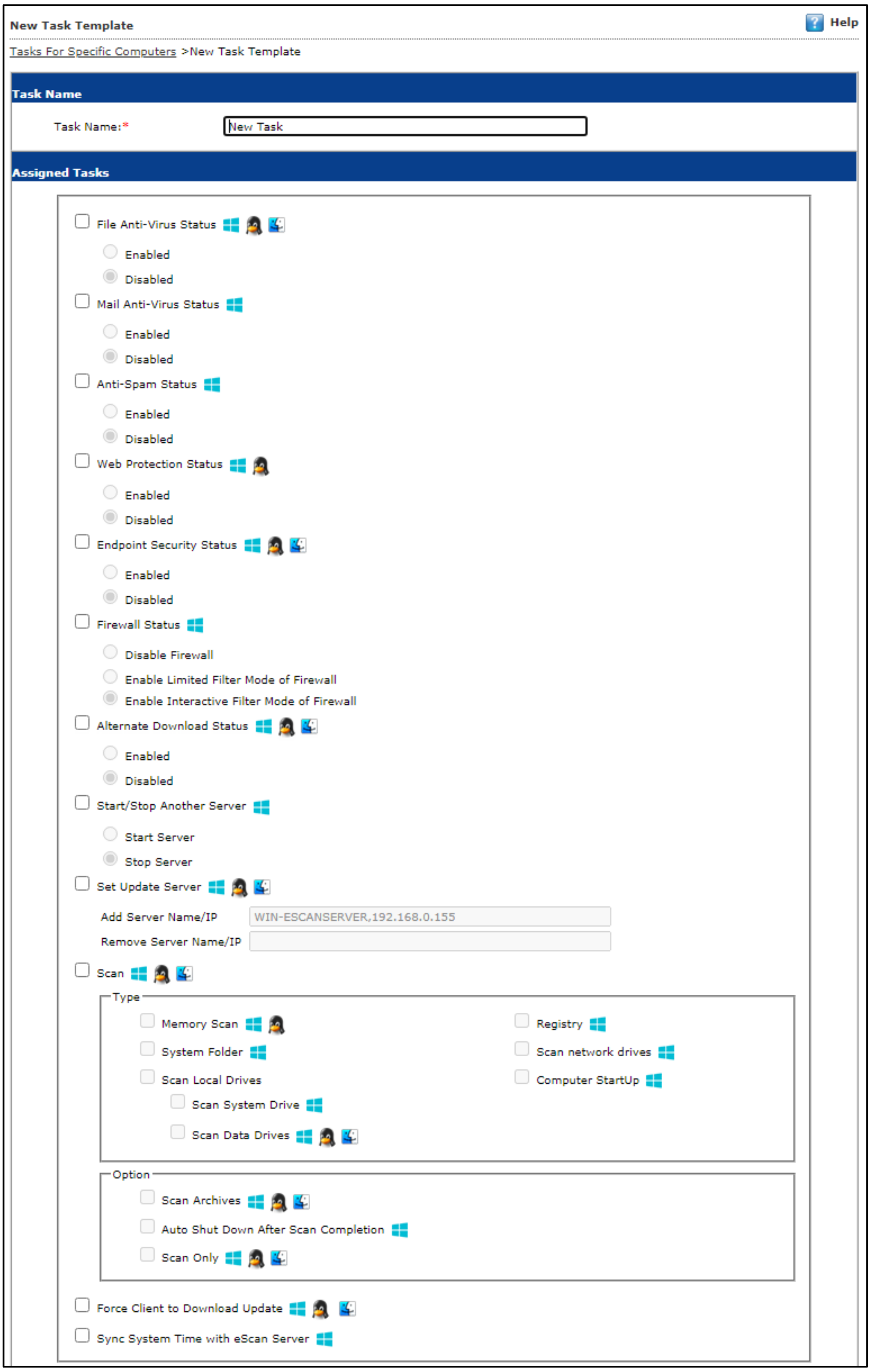
Task Name	Pending	Completed	Schedule Type

Creating a task for specific computers

To create a task for specific computer(s), follow the steps given below:

1. In the navigation panel, click **Tasks for Specific Computers**.
2. Click **New Task**.

New Task Template form appears.



New Task Template

Help

Tasks For Specific Computers >New Task Template

Task Name

Task Name:* New Task

Assigned Tasks

□ File Anti-Virus Status
- ○ Enabled
- ● Disabled

□ Mail Anti-Virus Status
- ○ Enabled
- ● Disabled

□ Anti-Spam Status
- ○ Enabled
- ● Disabled

□ Web Protection Status
- ○ Enabled
- ● Disabled

□ Endpoint Security Status
- ○ Enabled
- ● Disabled

□ Firewall Status
- ○ Disable Firewall
- ○ Enable Limited Filter Mode of Firewall
- ● Enable Interactive Filter Mode of Firewall

□ Alternate Download Status
- ○ Enabled
- ● Disabled

□ Start/Stop Another Server
- ○ Start Server
- ● Stop Server

□ Set Update Server
- Add Server Name/IP: WIN-ESCANSERVER,192.168.0.155
- Remove Server Name/IP:

□ Scan

Type
- □ Memory Scan
- □ System Folder
- □ Scan Local Drives
  - □ Scan System Drive
  - □ Scan Data Drives
- □ Registry
- □ Scan network drives
- □ Computer StartUp

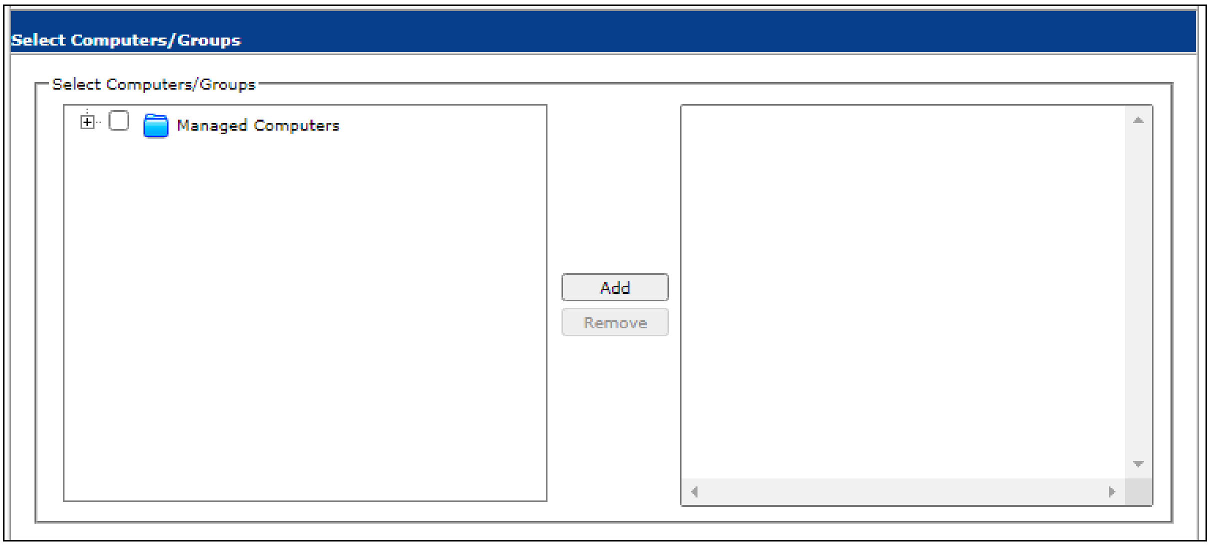
Option
- □ Scan Archives
- □ Auto Shut Down After Scan Completion
- □ Scan Only

□ Force Client to Download Update

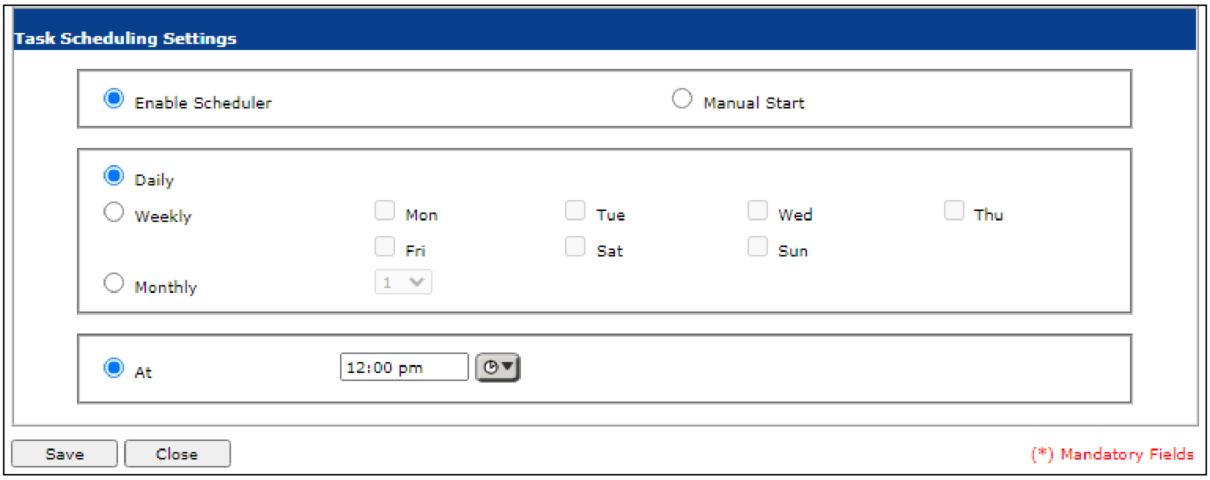
□ Sync System Time with eScan Server

3. Provide a name for the task.
4. In the **Assigned Tasks** section, select the modules and scanning types with its options to be run.

5. In the **Select Computers/Groups** section, select the computers/groups on which the tasks should be run and then click **Add**.



6. In the **Tasks Scheduling Settings** section, configure the schedule settings.



Task Scheduling Settings

● Enable Scheduler ○ Manual Start

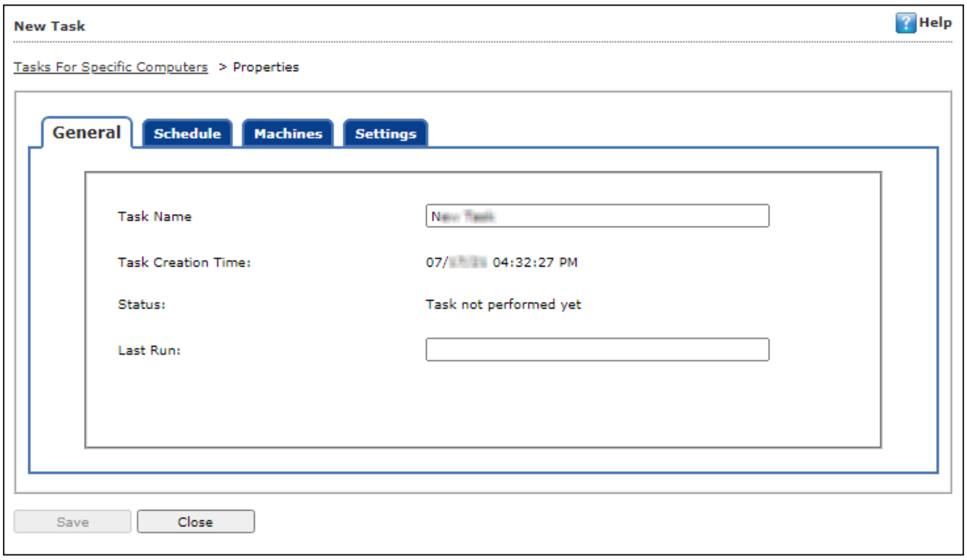
● Daily
○ Weekly □ Mon □ Tue □ Wed □ Thu
□ Fri □ Sat □ Sun
○ Monthly 1

● At 12:00 pm

7. Click **Save**. The task will be saved and run for specific computers as per the preferences.

Viewing Properties of a task

To view Properties of a task, select the task and click **Properties**.



New Task — Help

Tasks For Specific Computers > Properties

Task Name	[redacted]
Task Creation Time:	07/[redacted] 04:32:27 PM
Status:	Task not performed yet
Last Run:	

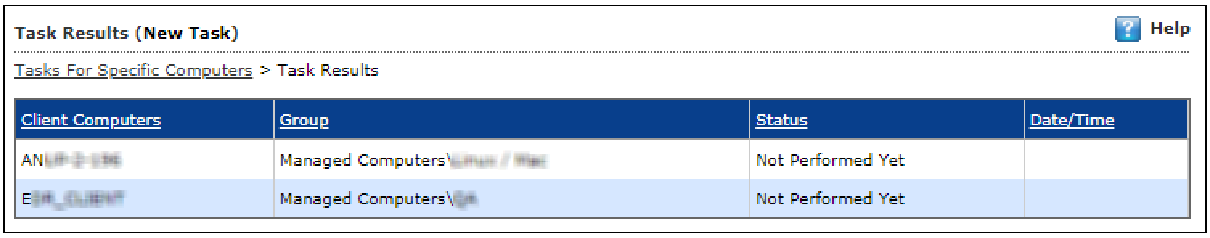
This section has following tabs to configure:

- **General**: This tab provides task name, details about the task creation, status, and last run.
- **Schedule**: This tab allows you to change the scheduler setting for particular task.
- **Machines**: This tab allows to add or remove the endpoints added to the particular task.
- **Settings**: This tab allows to modify or select the modules and scans to be run.

NOTE To run a scheduled task manually, select the task and then click **Start Task**.

Viewing Results of a task

To view Results of a task, select the task and click **Results**.



Task Results (New Task) — Help

Tasks For Specific Computers > Task Results

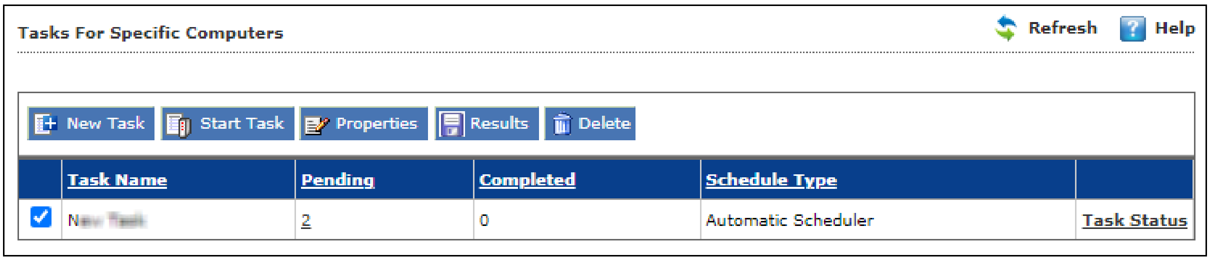
Client Computers	Group	Status	Date/Time
AN[redacted]	Managed Computers\[redacted]	Not Performed Yet	
E[redacted]	Managed Computers\[redacted]	Not Performed Yet	

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

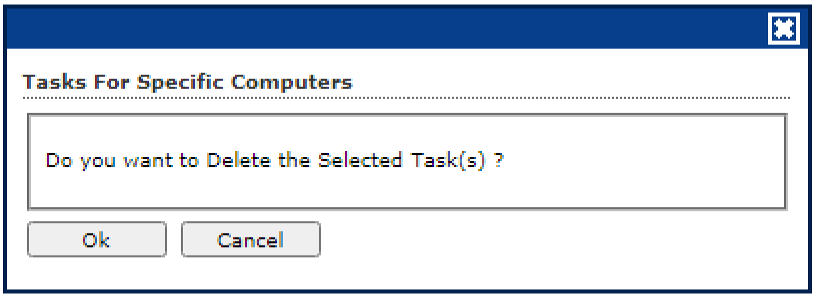
To delete a task, follow the steps given below:

1. In the Tasks for Specific Computers screen, select the task you want to delete.



	Task Name	Pending	Completed	Schedule Type	
☑	[redacted]	2	0	Automatic Scheduler	Task Status

2. Click **Delete**.
   A confirmation prompt appears.



Do you want to Delete the Selected Task(s) ?

3. Click **OK**. The task will be deleted.

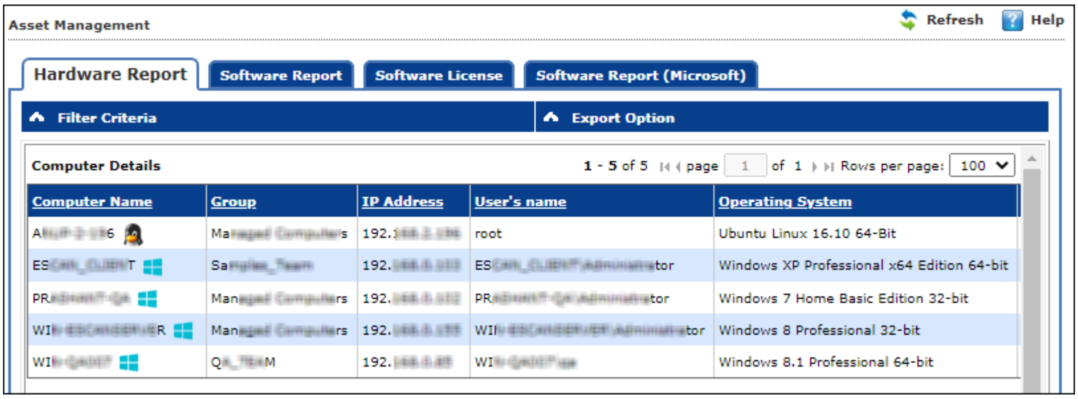
Asset Management

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.



Computer Details   1 - 5 of 5   page 1 of 1   Rows per page: 100

Computer Name	Group	IP Address	User's name	Operating System
A[redacted]6	Ma[redacted]s	192.[redacted]	root	Ubuntu Linux 16.10 64-Bit
ES[redacted]T	Sa[redacted]	192.[redacted]	ES[redacted]tor	Windows XP Professional x64 Edition 64-bit
PR[redacted]	Man[redacted]rs	192.[redacted]	PR[redacted]tor	Windows 7 Home Basic Edition 32-bit
WI[redacted]R	Man[redacted]rs	192.[redacted]	WI[redacted]tor	Windows 8 Professional 32-bit
WI[redacted]	Q[redacted]M	192.[redacted]	WI[redacted]	Windows 8.1 Professional 64-bit

The tab displays following details of managed computers:

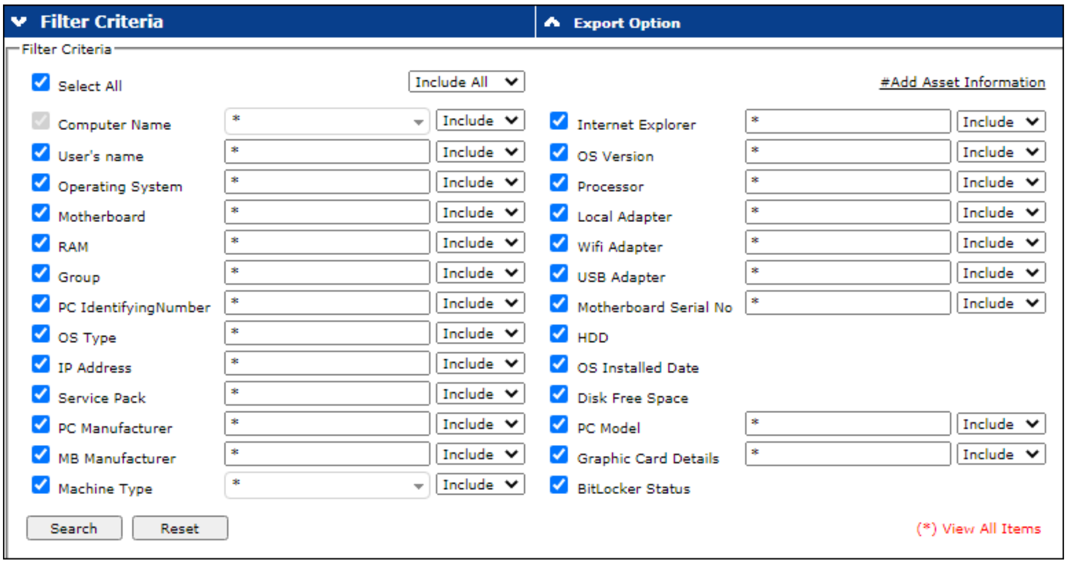
- Computer Name
- Group
- IP Address
- User name
- Operating System
- Service Pack
- OS Version
- OS Installed Date
- Internet Explorer
- Processor
- Motherboard
- RAM
- HDD
- Local MAC Adapter(s)
- Wi-Fi MAC [Adapter]
- USB MAC [Adapter]
- PC Identifying Number
- Motherboard Serial No
- Network Speed
- Disk Free Space
- PC Manufacturer

- PC Model
- MB Manufacturer
- Graphic Card Details
- Machine Type
- BitLocker Status
- Keyboard Vendor
- Software

To view the list of Software along with the version and installation dates, click **View** in Software column.

Filtering Hardware Report

To filter the Hardware Report as per your requirements, click **Filter Criteria** field.
Filter Criteria field expands.



Filter Criteria | Export Option

Filter Criteria

☑ Select All — Include All — #Add Asset Information

☑ Computer Name	*	Include	☑ Internet Explorer	*	Include
☑ User's name	*	Include	☑ OS Version	*	Include
☑ Operating System	*	Include	☑ Processor	*	Include
☑ Motherboard	*	Include	☑ Local Adapter	*	Include
☑ RAM	*	Include	☑ Wifi Adapter	*	Include
☑ Group	*	Include	☑ USB Adapter	*	Include
☑ PC IdentifyingNumber	*	Include	☑ Motherboard Serial No	*	Include
☑ OS Type	*	Include	☑ HDD		
☑ IP Address	*	Include	☑ OS Installed Date		
☑ Service Pack	*	Include	☑ Disk Free Space		
☑ PC Manufacturer	*	Include	☑ PC Model	*	Include
☑ MB Manufacturer	*	Include	☑ Graphic Card Details	*	Include
☑ Machine Type	*	Include	☑ BitLocker Status		

Search — Reset — (*) View All Items

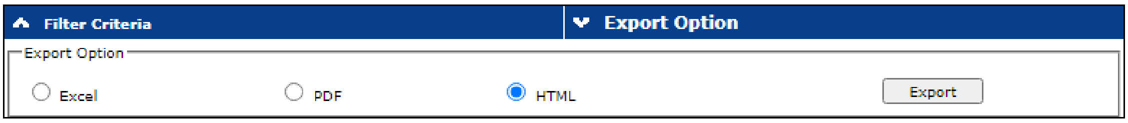
Select the parameters you want to be included in the filtered report.

Include/Exclude
Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After making the necessary selections, click **Search.**
The Hardware Report will be filtered according to your preferences.

Exporting Hardware Report

To export the Hardware Report, click **Export Option**. Export Option field expands.



Filter Criteria | Export Option

Export Option

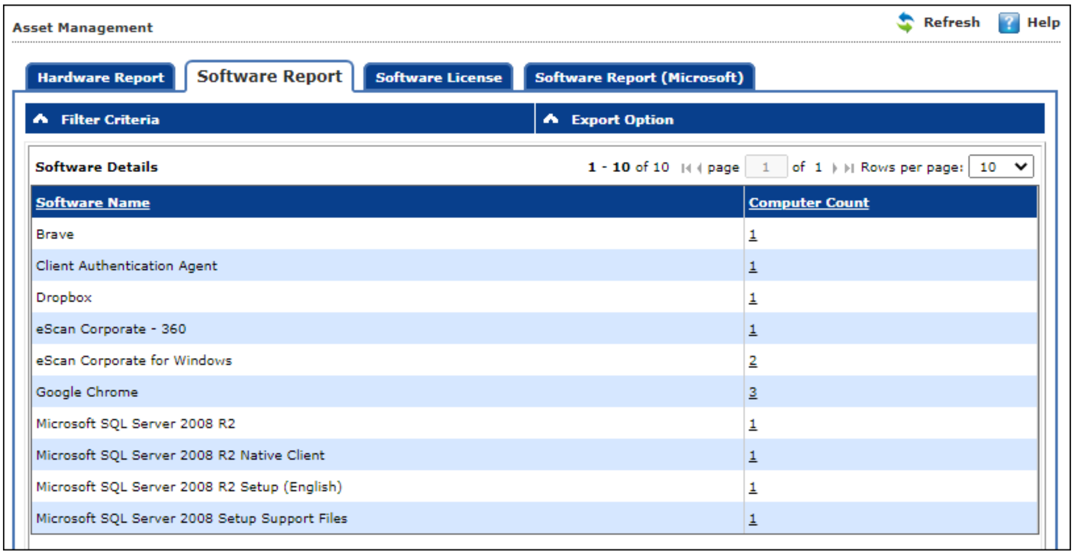
○ Excel ○ PDF ● HTML — Export

Select the preferred format and then click **Export**. A success message appears with the link to Open/Download the file.

Exported Successfully Click here to Open/Download

Software Report

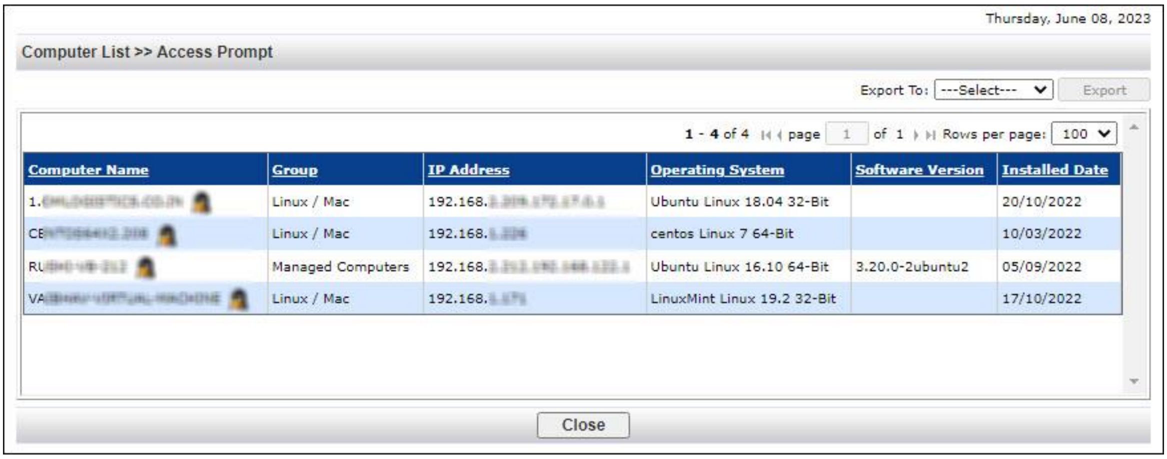
The Software Report tab displays list of Software along with the number of computers on which they are installed.



Software Details 1 - 10 of 10 page 1 of 1 Rows per page: 10

Software Name	Computer Count
Brave	1
Client Authentication Agent	1
Dropbox	1
eScan Corporate - 360	1
eScan Corporate for Windows	2
Google Chrome	3
Microsoft SQL Server 2008 R2	1
Microsoft SQL Server 2008 R2 Native Client	1
Microsoft SQL Server 2008 R2 Setup (English)	1
Microsoft SQL Server 2008 Setup Support Files	1

To view the computers on which the specific software is installed, click the numerical in Computer Count column.



Thursday, June 08, 2023

Computer List >> Access Prompt

1 - 4 of 4 page 1 of 1 Rows per page: 100

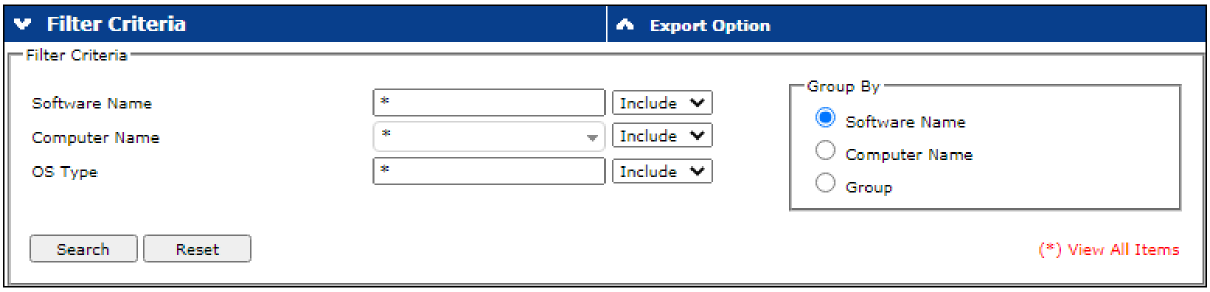
Computer Name	Group	IP Address	Operating System	Software Version	Installed Date
1.[redacted]	Linux / Mac	192.168.[redacted]	Ubuntu Linux 18.04 32-Bit		20/10/2022
CE[redacted]	Linux / Mac	192.168.[redacted]	centos Linux 7 64-Bit		10/03/2022
RU[redacted]	Managed Computers	192.168.[redacted]	Ubuntu Linux 16.10 64-Bit	3.20.0-2ubuntu2	05/09/2022
VA[redacted]	Linux / Mac	192.168.[redacted]	LinuxMint Linux 19.2 32-Bit		17/10/2022

Computer list window appears displaying following details:

- Computer Name
- Group
- IP Address
- Operating System
- Software Version
- Installed Date

Filtering Software Report

To filter Software Report, click **Filter Criteria** field.
Filter Criteria field expands.



Filter Criteria

Software Name	*	Include
Computer Name	*	Include
OS Type	*	Include

Group By
● Software Name
○ Computer Name
○ Group

The Software Report can be filtered on the basis of **Software Name** or **Computer Name**.

Software Name
Entering the Software name displays suggestions. Select the appropriate software.

Computer Name
Click the drop-down and select the preferred computer(s).

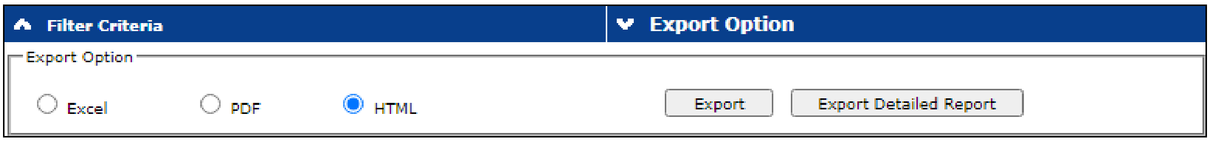
OS Type
Enter the OS type.

Group By
The results can be grouped by Software name, Computer name or Group.
If Group option is selected, the report can be filtered for a specific group.

After entering data in all fields, click **Search**.
The Software Report will be filtered according to your preferences.

Exporting Software Report

To export the Software Report, click **Export Option**.
Export Option field expands.

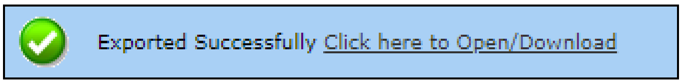


Filter Criteria | Export Option

Export Option

○ Excel ○ PDF ● HTML

Select the preferred option and then click **Export**.
OR
To export a detailed report, select the preferred option and then click **Export Detailed Report**.
A success message appears.

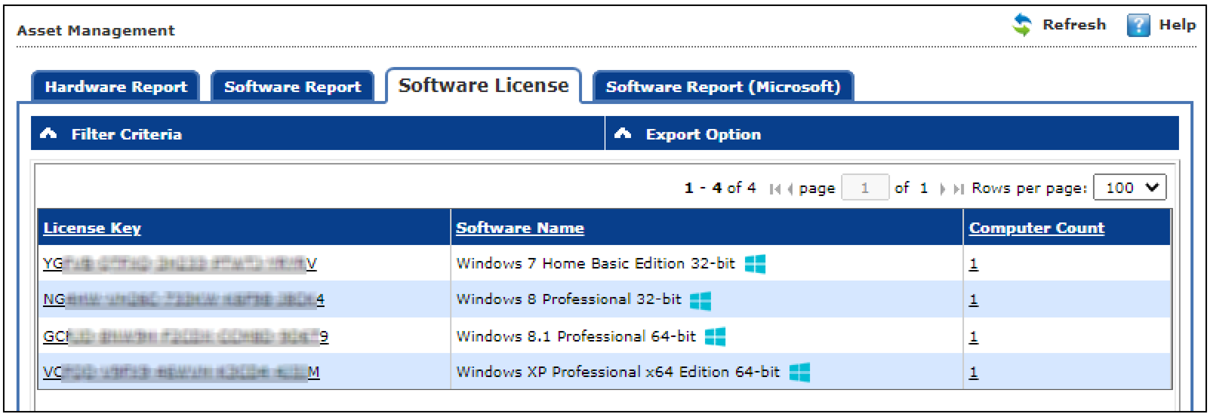


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Software License

The Software License tab displays list of Software Licenses of managed computers.



Asset Management

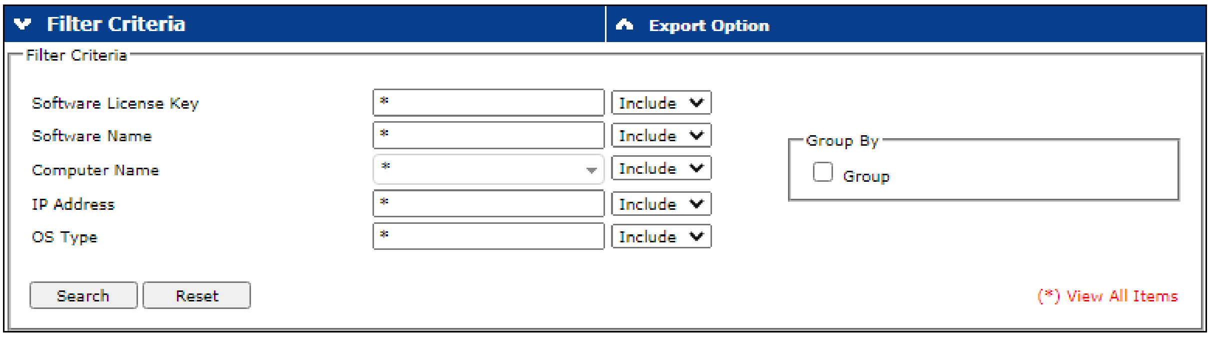
1 - 4 of 4 page 1 of 1 Rows per page: 100

License Key	Software Name	Computer Count
YG[redacted]V	Windows 7 Home Basic Edition 32-bit	1
NG[redacted]4	Windows 8 Professional 32-bit	1
GC[redacted]9	Windows 8.1 Professional 64-bit	1
VC[redacted]M	Windows XP Professional x64 Edition 64-bit	1

The log displays License Key, Software Name and Computer Count.
To see more details of the computer's license key installed, click the numerical value in License Key or Computer Count column.

Filtering Software License Report

To filter Software Report, click **Filter Criteria** field.
Filter Criteria field expands.



Filter Criteria | Export Option

Filter Criteria

Software License Key	*	Include
Software Name	*	Include
Computer Name	*	Include
IP Address	*	Include
OS Type	*	Include

Group By

□ Group

Software License Key

Entering the license key displays suggestions. Select the appropriate key.

Software Name

Entering the Software name displays suggestions. Select the appropriate software.

Computer Name

Click the drop-down and select the preferred computer(s).

IP Address

Entering the IP address displays suggestions. Select the appropriate IP address.

OS Type

Enter the OS type.

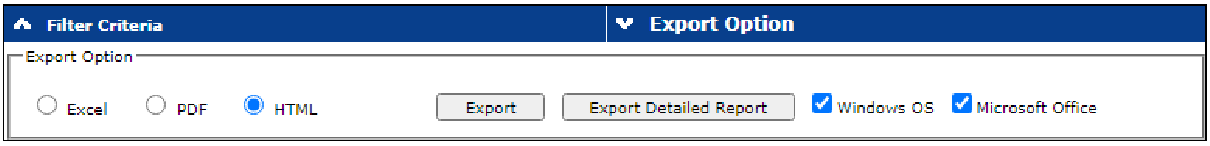
Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After entering data in all fields, click **Search**.
The Software License Report will be filtered according to your preferences.

Exporting Software License Report

To export the Software License Report, click **Export Option**.
Export Option field expands.



Filter Criteria | Export Option

Export Option

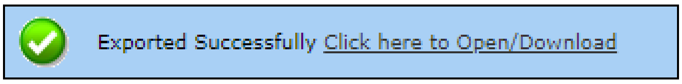
○ Excel ○ PDF ● HTML

Export | Export Detailed Report

☑ Windows OS ☑ Microsoft Office

Select whether you want report for Windows OS and Microsoft Office.

Select the preferred option and then click **Export**.
OR
To export a detailed report, select the preferred option and then click **Export Detailed Report**.
A success message appears.

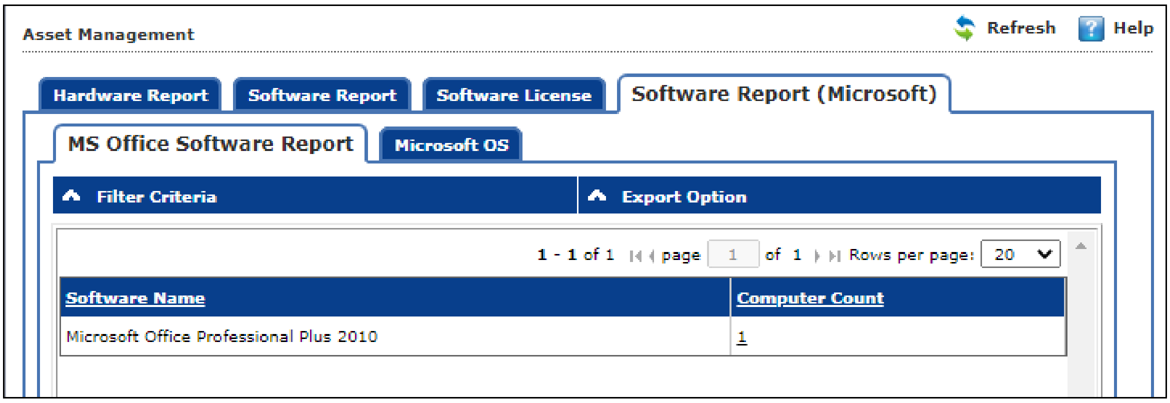


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Software Report (Microsoft)

The Software Report (Microsoft) displays details of the Microsoft Software installed on the computers.



1 - 1 of 1 page 1 of 1 Rows per page: 20

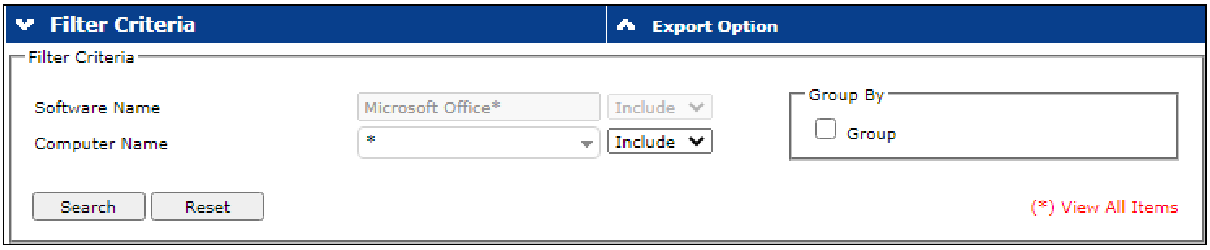
Software Name	Computer Count
Microsoft Office Professional Plus 2010	1

The tab consists following subtabs:
MS Office Software Report – It displays Microsoft software name and computer count.

Microsoft OS – It displays Operating System, Service Pack, OS version and computer count.

Filtering Software Report (Microsoft)

To filter Software Report (Microsoft), click **Filter Criteria** field.
Filter Criteria field expands.



Filter Criteria | Export Option

Filter Criteria

Software Name: Microsoft Office* — Include

Computer Name: * — Include

Group By: ☐ Group

Search | Reset

(*) View All Items

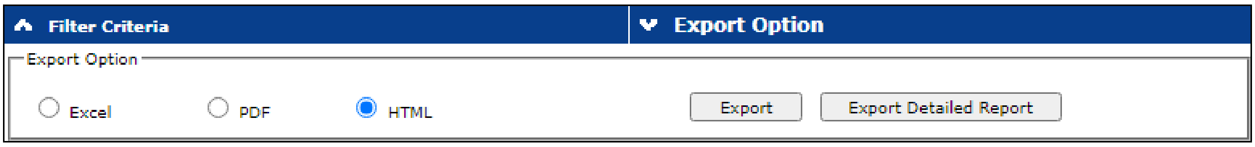
Computer Name
Click the drop-down and select the preferred computer(s).

Group By
If Group option is selected, the report can be filtered for a specific group.

After entering data in all fields, click **Search**.
The Software Report (Microsoft) will be filtered according to your preferences.

Exporting Software Report (Microsoft)

To export the Software Report (Microsoft), click **Export Option**.
Export Option field expands.



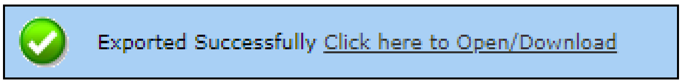
Filter Criteria | Export Option

Export Option

○ Excel ○ PDF ● HTML

Export | Export Detailed Report

Select the preferred option and then click **Export**.
OR
To export a detailed report, select the preferred option and then click **Export Detailed Report**.
A success message appears.

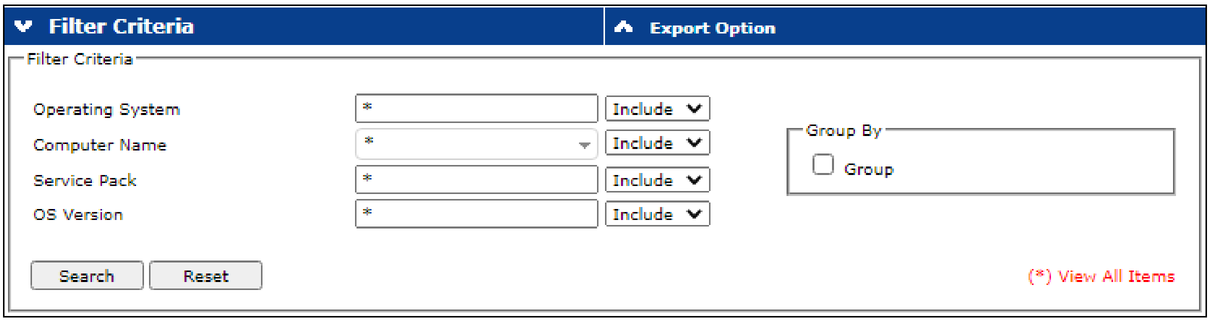


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Filtering Microsoft OS Report

To filter the Microsoft OS report, click **Filter Criteria** field.
Filter Criteria field expands.



Filter Criteria | Export Option

Filter Criteria

Operating System: * — Include

Computer Name: * — Include

Service Pack: * — Include

OS Version: * — Include

Group By: ☐ Group

Search | Reset

(*) View All Items

Operating System
Entering the operating system name displays list of suggestions. Select the appropriate OS.

Computer Name
Click the drop-down and select the preferred computer(s).

Service Pack
Entering the service pack name displays list of suggestions. Select the appropriate Service Pack.

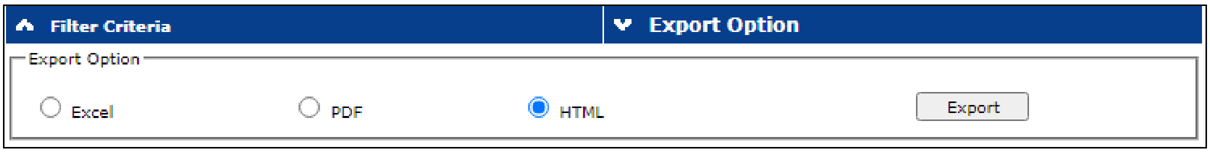
OS Version
Entering the OS version displays list of suggestions. Select the appropriate OS version.

Include/Exclude
Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

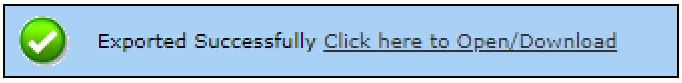
After filling all the fields, click **Search**.
The Microsoft OS report will be filtered according to your preferences.

Exporting Microsoft OS Report

To export the Microsoft OS Report, click **Export Option**.
Export Option field expands.



Select the preferred option and then click **Export**. A success message appears.


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Phishing Simulator

eScan's new functionality called Phishing Simulator enables organization's threat intelligence team to assess employees' understanding of email phishing threats widely used by attackers. In simple terms, phishing simulation is an internal activity where a mock phishing email is sent to employees to assess whether they click on embedded links or ignore the email. These phishing mails are created by mimicking the actual phishing emails. If the employees respond to the mail by clicking the email links, the action gets stored for further analysis of conducting phishing awareness program.

SMTP Server Configuration

Follow the steps given below to setup a mail server (this is only the initial requirement):

1. Open **Phishing Simulator** from navigation panel
   The Phishing Simulator's dashboard opens.
2. Click on **Settings** on top-right corner of the window
   The 'SMTP Configuration' prompt appears.
3. Enter the required details and click on **Save Configuration**.
   You can test this server configuration by using **Test Configuration** option.

Configuring Test Setup

Follow the steps given below to configure a Phishing email setup:

1. Click on **Setup Test Environment** from the dashboard.
2. Click on **Create New Test** to setup a dummy mail.
   The 'Create New Test' window appears.
3. Enter a test code in the provided field
4. In the **Organization Name** field, enter the organization's name on whose behalf you wish to send this simulated phishing email.
5. Using the **Country** drop-down, select your country where this test is being conducted
6. Select the company template from by whose name the email is to be sent using provided drop-down
7. In the **From Email id** field, enter the email address from which this email is to be sent
8. In the **Subject** field, enter the email subject to be displayed in the mail
9. Click on **Create Test** to save the test.
   The test is saved successfully.

Sending a Simulated Phishing Email

Follow the steps given below to send a simulated email to the users of the organization:

1. Go to **Setup Test Environment** from the dashboard
2. Find the test from which you want to use a mail template using available filters of 'Date' and 'Countries'
3. Click on the **Continue** button provided for the test
   The 'Email Sender' window appears.
4. Under 'Create Group' section, enter a group name and click on **Create** button
   The group has created.

5. The created group will be displayed in the **Select Group** drop-down.
6. Select the group from the drop-down list
7. Click on **Next**.
8. On the next page, enter target recipient name and the email address in the provided fields
9. Click on **Add Email** to add this user in recipient list
10. Alternatively, click on **Choose File** option under ‘Upload CSV’ section to upload the CSV file with recipient list
11. Select the checkboxes to choose target recipients from the list
12. Click on **Next**.
13. On the next page, reconfirm/edit the displayed information
14. Click on **Send Emails**.
    A confirmation prompt appears.
15. Click on **Send** to finally send the simulated phishing email.

Analyzing the Tests

This tab allows you to analyse the test results of all Phishing simulation tests. It shows the results summary in both graphical as well as tabular format.

The Click Analysis Pie chart shows the number of users fell victim to the mock phishing email by categorizing it under **Clicked** and **Not Clicked**.

The User Data table shows information of every user who responded or not responded to the mail. This information is displayed under username, email id, group, clicks, date, and status columns. You can filter the same using Filters button provided above the table.

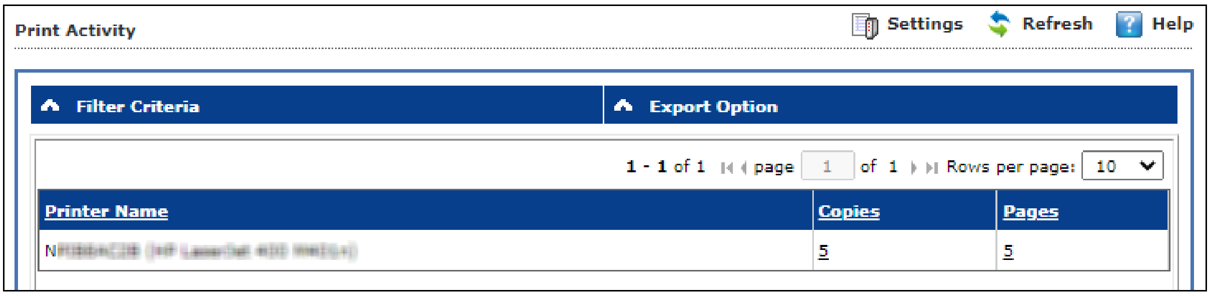
User Activity

The User Activity module lets you monitor Print, Session, and File activities occurring on the client computers. It also provides the reports of the running applications. It consists following submodules:

- **Print Activity**
- **Session Activity**
- **File Activity**
- **Application Access Report**

Print Activity

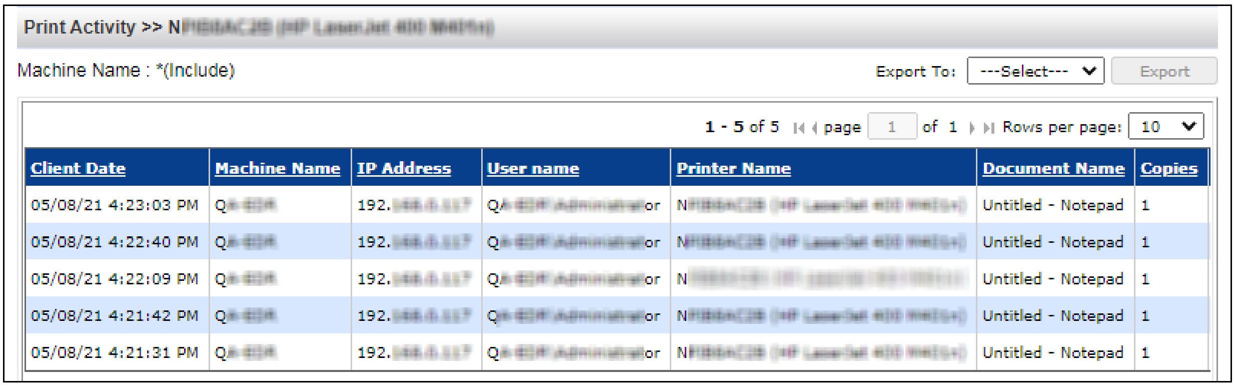
The Print Activity monitors and logs print commands sent by all computers. It also lets you filter the logs on the basis of Computer name, Printer, and Username. Furthermore, the module lets you export a detailed print activity report in XLS, PDF, and HTML formats. The log report generated consists of Print Date, Machine Name, IP Address, Username, Printer Name, Document Name along with number of Copies and Pages.



Printer Name	Copies	Pages
N[redacted]	5	5

Viewing Print Activity Log

To view the Print log of a Printer, click its numerical value under **Copies** or **Pages** column. Print Activity window appears displaying the details.


Print Activity >> N[redacted]
Export To: ---Select---
Export
1 - 5 of 5 page 1 of 1 Rows per page: 10

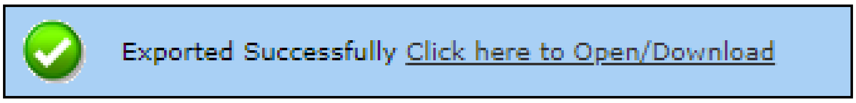
Machine Name : *(Include)

Client Date	Machine Name	IP Address	User name	Printer Name	Document Name	Copies
05/08/21 4:23:03 PM	Q[redacted]	192.[redacted]	Q[redacted]or	N[redacted]	Untitled - Notepad	1
05/08/21 4:22:40 PM	Q[redacted]	192.[redacted]	Q[redacted]or	N[redacted]	Untitled - Notepad	1
05/08/21 4:22:09 PM	Q[redacted]	192.[redacted]	Q[redacted]or	N[redacted]	Untitled - Notepad	1
05/08/21 4:21:42 PM	Q[redacted]	192.[redacted]	Q[redacted]or	N[redacted]	Untitled - Notepad	1
05/08/21 4:21:31 PM	Q[redacted]	192.[redacted]	Q[redacted]or	N[redacted]	Untitled - Notepad	1

Exporting Print Activity Log

To export this generated log:

1. Click the **Export to** drop-down.
2. Select a preferred format.
3. Click **Export**.
   A success message appears.

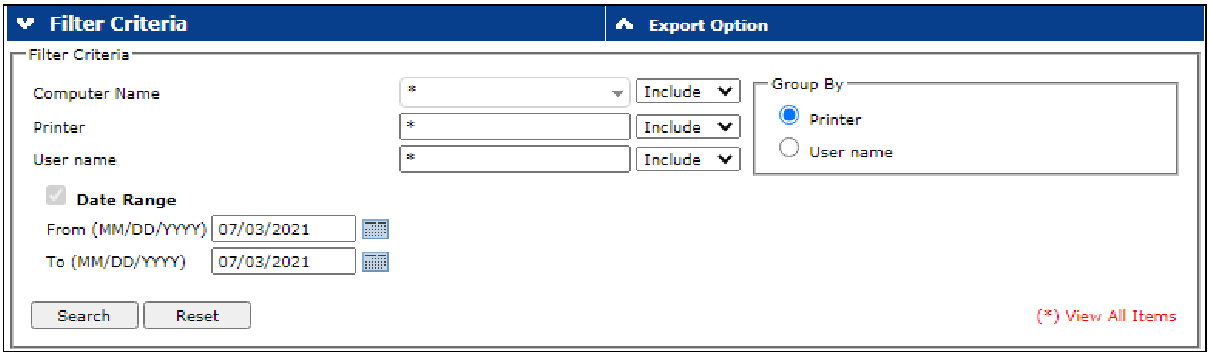


Exported Successfully Click here to Open/Download

4. Click the link to open/download the file.

Filtering Print Activity Log

To filter the print activity log, click **Filter Criteria**.
Filter criteria field expands.



Filter Criteria | Export Option

Filter Criteria

Computer Name	*	Include
Printer	*	Include
User name	*	Include

Group By
● Printer
○ User name

☑ Date Range
From (MM/DD/YYYY) 07/03/2021
To (MM/DD/YYYY) 07/03/2021

Computer Name
Click the drop-down and select the preferred computer.

Printer
Enter the printer's name.

User Name
Enter the User's name.

Include/Exclude
Selecting Include/Exclude for a Machine or Printer lets you include or exclude it from the log.

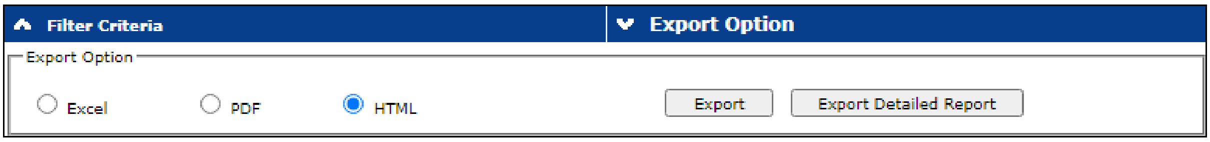
Date Range
To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the calendar icon and select **From** and **To** dates.

After filling all fields, click **Search**.
The Print activity log will be filtered and generated according to your preferences.

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.



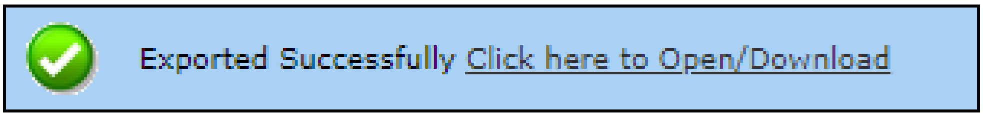
Filter Criteria | Export Option

Export Option

○ Excel ○ PDF ● HTML

Select the preferred option and then click **Export**.
OR
To export a detailed report, select the preferred option and then click **Export Detailed Report**.

A success message appears.



Exported Successfully Click here to Open/Download

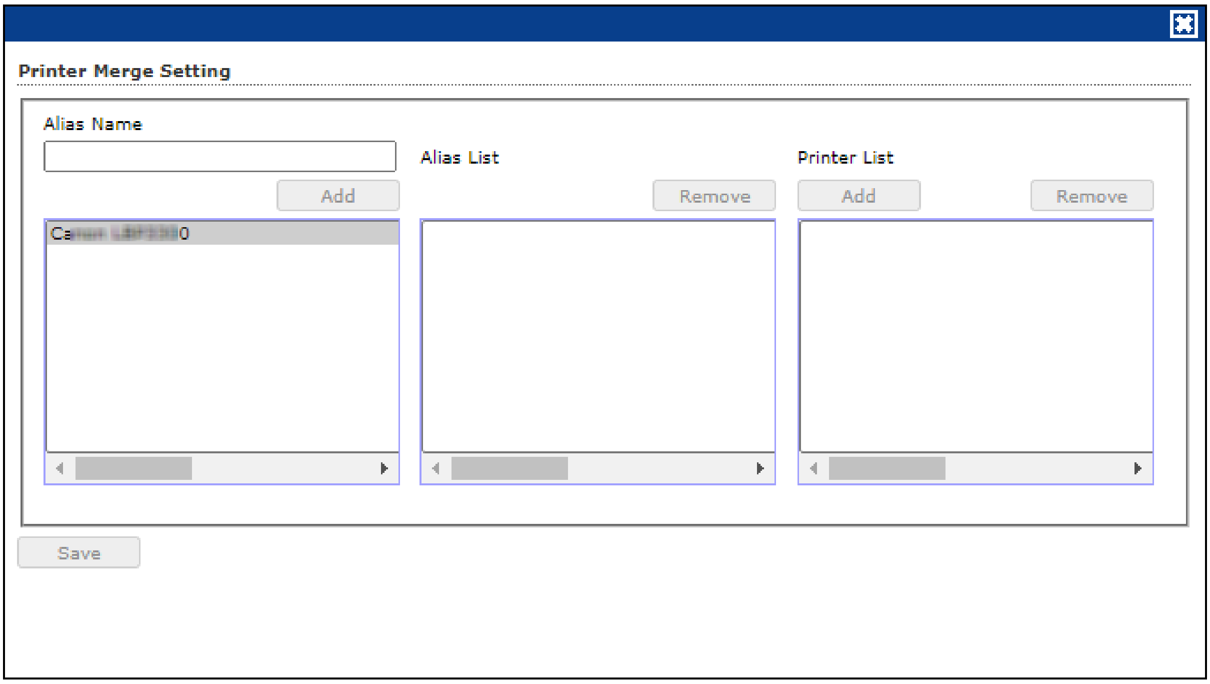
Click the link to open/download the file.

Print Activity Settings

Print Activity Settings lets you keep track of printers by adding them in a group and assigning it an alias name. The printers can be added or removed from this alias group.

To configure Print Activity Settings:

1. In the Print Activity screen, at the top right corner, click **Settings**.
   Printer Merge Setting window appears.



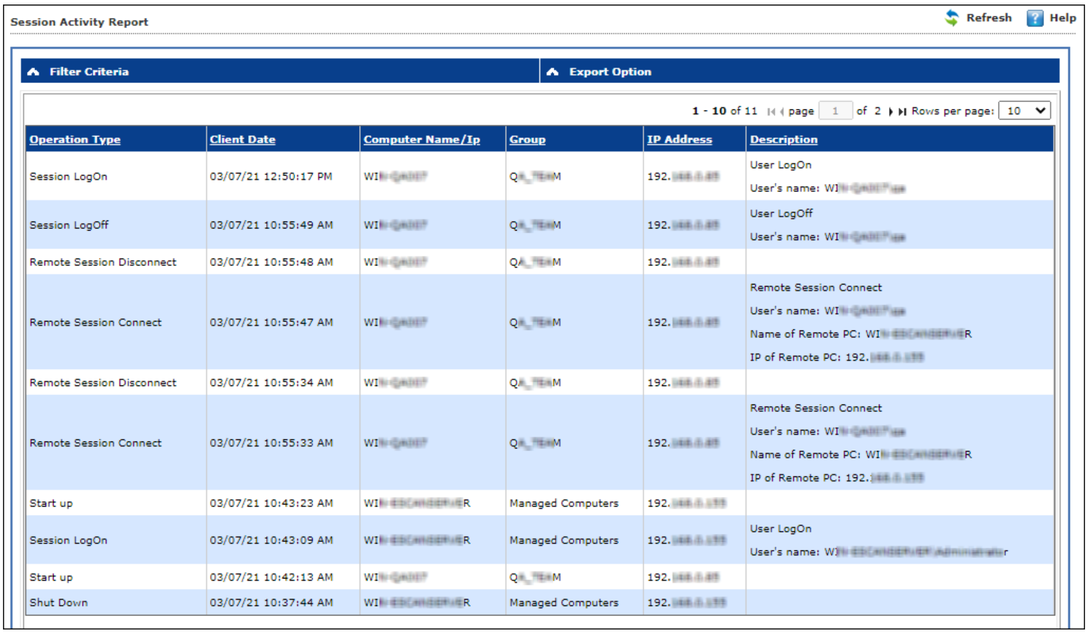
2. Enter name in Alias Name field.
3. Select printer(s) for the alias.
4. Click **Add**.
   The printer(s) will be added to the alias.
5. Click **Save**. The Print Activity Settings will be saved.

Session Activity Report

This submodule monitors and logs the session activity of the managed computers. It displays a report of the Operation type, Date, Computer name, Group, IP address and event description. With this report the administrator can trace the user Logon and Logoff activity along with remote sessions that took place on all managed computers.

Viewing Session Activity Log

In the navigation panel, click **User Activity** > **Session Activity Report**.
The log displays list of session activities and type of operation performed. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

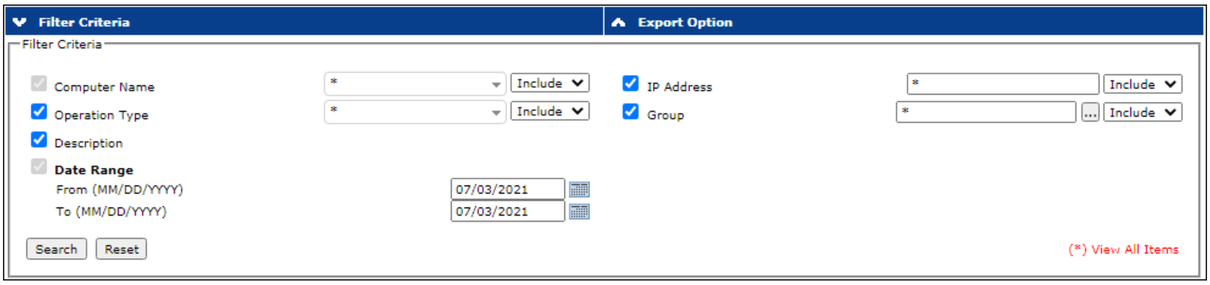


Session Activity Report

Operation Type	Client Date	Computer Name/Ip	Group	IP Address	Description
Session LogOn	03/07/21 12:50:17 PM	WI[redacted]	QA_[redacted]M	192.[redacted]	User LogOn User's name: WI[redacted]
Session LogOff	03/07/21 10:55:49 AM	WI[redacted]	QA_[redacted]M	192.[redacted]	User LogOff User's name: WI[redacted]
Remote Session Disconnect	03/07/21 10:55:48 AM	WI[redacted]	QA_[redacted]M	192.[redacted]	
Remote Session Connect	03/07/21 10:55:47 AM	WI[redacted]	QA_[redacted]M	192.[redacted]	Remote Session Connect User's name: WI[redacted] Name of Remote PC: WI[redacted]R IP of Remote PC: 192.[redacted]
Remote Session Disconnect	03/07/21 10:55:34 AM	WI[redacted]	QA_[redacted]M	192.[redacted]	
Remote Session Connect	03/07/21 10:55:33 AM	WI[redacted]	QA_[redacted]M	192.[redacted]	Remote Session Connect User's name: WI[redacted] Name of Remote PC: WI[redacted]R IP of Remote PC: 192.[redacted]
Start up	03/07/21 10:43:23 AM	WI[redacted]R	Managed Computers	192.[redacted]	
Session LogOn	03/07/21 10:43:09 AM	WI[redacted]R	Managed Computers	192.[redacted]	User LogOn User's name: WI[redacted]r
Start up	03/07/21 10:42:13 AM	WI[redacted]	QA_[redacted]M	192.[redacted]	
Shut Down	03/07/21 10:37:44 AM	WI[redacted]R	Managed Computers	192.[redacted]	

Filtering Session Activity Log

To filter session activities, click **Filter Criteria** field.
Filter Criteria field expands.



☑ Computer Name * Include
☑ Operation Type * Include
☑ Description
☑ Date Range
From (MM/DD/YYYY) 07/03/2021
To (MM/DD/YYYY) 07/03/2021
☑ IP Address * Include
☑ Group * ... Include

Filter Criteria lets you filter and generate the log according to your preferences. The checkbox selected will be added as a column in the report.

Computer Name

Click the drop-down and select the preferred computers.

Operation Type
Click the drop-down and select the preferred activities.

Include/Exclude
Selecting Include/Exclude for a parameter lets you include or exclude it from the log.

IP Address
Enter the IP address in this field.

Group

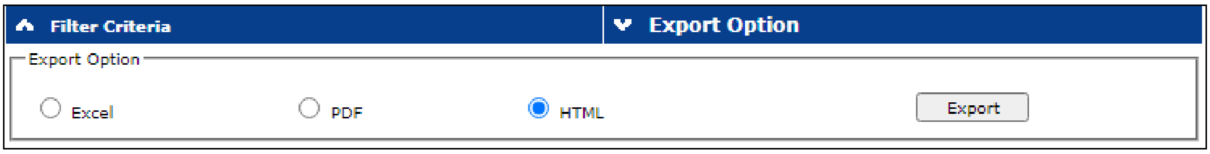
Enter the group's name or click ... and select a group.

Date Range
To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the calendar icon and select **From** and **To** dates.

After filling all fields, click **Search**.

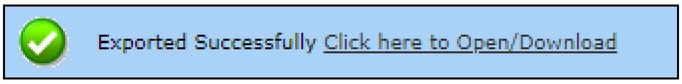
Exporting Session Activity Report

To export the generated log, click **Export Option**.
Export Option field expands.



○ Excel ○ PDF ● HTML

Select the preferred option and then click **Export**.
A success message appears.


Exported Successfully Click here to Open/Download

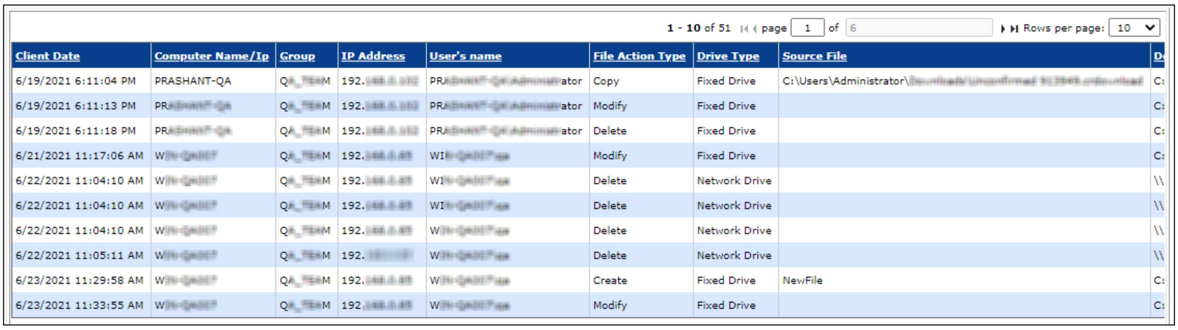
Click the link to open/download the file.

File Activity Report

The File Activity module displays a report of the files created, copied, modified, and deleted on managed computers. Additionally in case of a misuse of any official files can be tracked down to the user through the details captured in the report. Select and filter the report based on any of the details captured.

Viewing File Activity Log

In the navigation panel, click **User Activity** > **File Activity Report**.
The log displays list of files and the type of operation performed on them. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

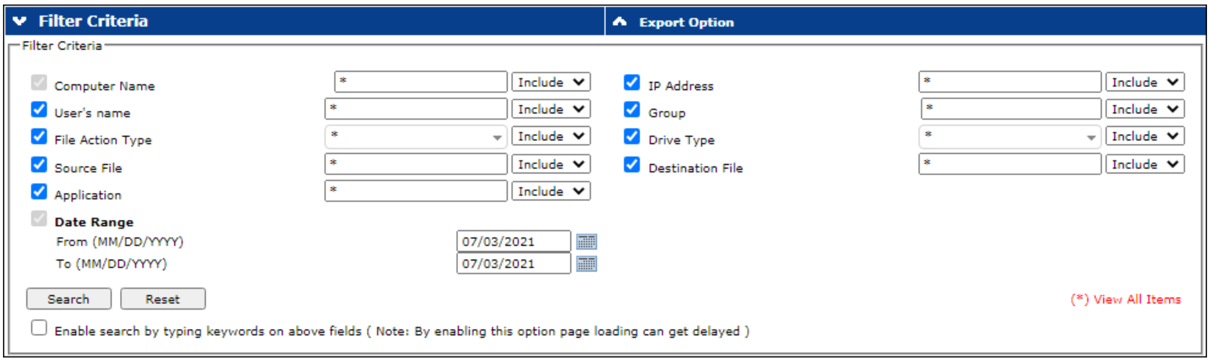


1 - 10 of 51 page 1 of 6 Rows per page: 10

Client Date	Computer Name/Ip	Group	IP Address	User's name	File Action Type	Drive Type	Source File	D
6/19/2021 6:11:04 PM	PRASHANT-QA	QA[redacted]M	192.[redacted]	PR[redacted]ator	Copy	Fixed Drive	C:\Users\Administrator\[redacted]	C:
6/19/2021 6:11:13 PM	PR[redacted]	QA_[redacted]M	192.[redacted]	PR[redacted]ator	Modify	Fixed Drive		C:
6/19/2021 6:11:18 PM	PR[redacted]	QA_[redacted]M	192.[redacted]	PR[redacted]ator	Delete	Fixed Drive		C:
6/21/2021 11:17:06 AM	W[redacted]	QA_[redacted]M	192.[redacted]	WI[redacted]	Modify	Fixed Drive		C:
6/22/2021 11:04:10 AM	W[redacted]	QA_[redacted]M	192.[redacted]	WI[redacted]	Delete	Network Drive		\\
6/22/2021 11:04:10 AM	W[redacted]	QA_[redacted]M	192.[redacted]	WI[redacted]	Delete	Network Drive		\\
6/22/2021 11:04:10 AM	W[redacted]	QA_[redacted]M	192.[redacted]	W[redacted]	Delete	Network Drive		\\
6/22/2021 11:05:11 AM	W[redacted]	QA_[redacted]M	192.[redacted]	W[redacted]	Delete	Network Drive		\\
6/23/2021 11:29:58 AM	W[redacted]	QA_[redacted]M	192.[redacted]	W[redacted]	Create	Fixed Drive	NewFile	C:
6/23/2021 11:33:55 AM	W[redacted]	QA_[redacted]M	192.[redacted]	W[redacted]	Modify	Fixed Drive		C:

Filtering File Activity Log

To filter file activities, click **Filter Criteria** field. Filter Criteria field expands.



Filter Criteria | Export Option

Filter Criteria

☑ Computer Name	*	Include	☑ IP Address	*	Include
☑ User's name	*	Include	☑ Group	*	Include
☑ File Action Type	*	Include	☑ Drive Type	*	Include
☑ Source File	*	Include	☑ Destination File	*	Include
☑ Application	*	Include			

☑ **Date Range**

From (MM/DD/YYYY) 07/03/2021

To (MM/DD/YYYY) 07/03/2021

Search Reset (*) View All Items

☐ Enable search by typing keywords on above fields (Note: By enabling this option page loading can get delayed)

Filter Criteria lets you filter and generate the log according to your preferences. The checkbox selected will be added as a column in the report.

Computer Name

Click the drop-down and select the preferred computers.

Username

Enter the username of the computer.

File Action type

Click the drop-down and select a preferred file action.

Source File

Enter the source file's name.

Application

Enter an application's name.

Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the log.

IP Address

Enter an IP address.

Group

Enter the group's name or click ... and select a group.

Drive Type

Click the drop-down and select the drive type.

Destination File
Enter the file path.

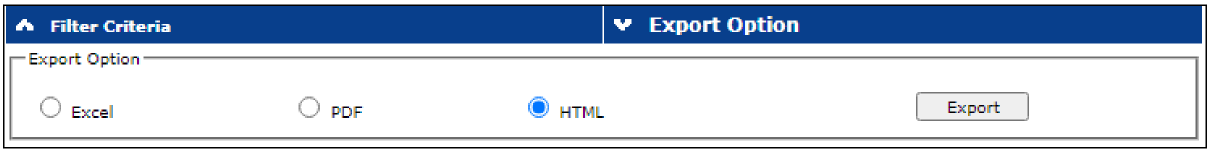
Date Range
To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the calendar icon and select **From** and **To** dates.

Enable search by typing keywords on above fields
Select this checkbox to filter the report as per keyword for particular field.

After filling all fields, click **Search**.
The Activity Log will be displayed.

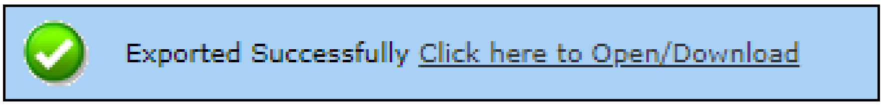
Exporting File activity Report

To export the generated report, click **Export Option**.
Export Option field expands.



Export Option
○ Excel ○ PDF ● HTML

Select the preferred option and then click **Export**.
A success message appears.



Exported Successfully Click here to Open/Download

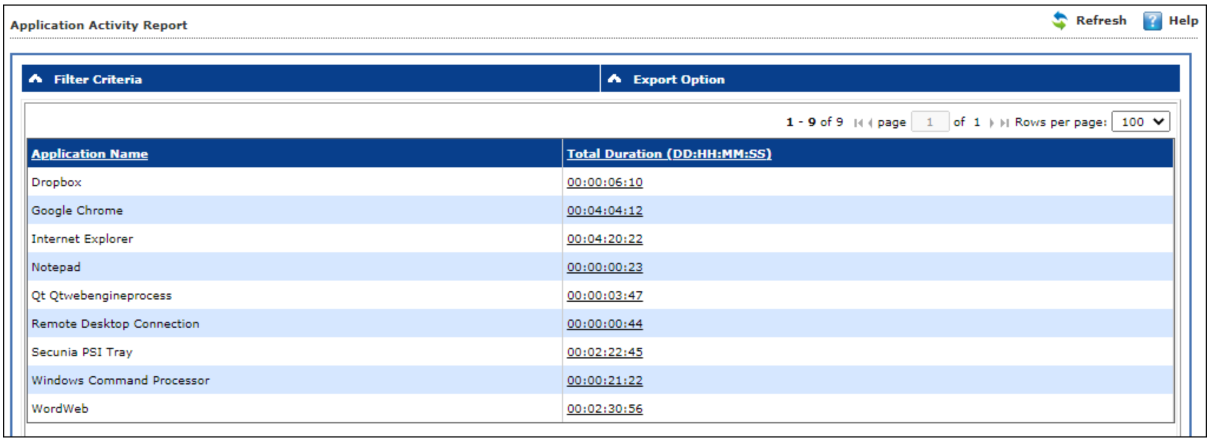
Click the link to open/download the file.

Application Access Report

The Application Access Report module gives the detailed view of all the applications accessed by the computers in the Managed Computers.

Viewing Application Access Report

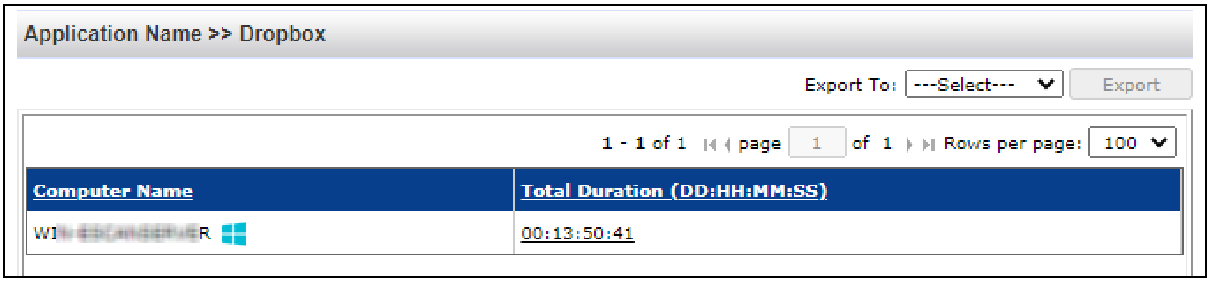
In the navigation panel, click **User Activity** > **Application Access Report**.
The log displays list of files and the type of operation performed on them. Options for Filtering or Exporting the log in desired formats are also present on the same interface.



Application Activity Report

Application Name	Total Duration (DD:HH:MM:SS)
Dropbox	00:00:06:10
Google Chrome	00:04:04:12
Internet Explorer	00:04:20:22
Notepad	00:00:00:23
Qt Qtwebengineprocess	00:00:03:47
Remote Desktop Connection	00:00:00:44
Secunia PSI Tray	00:02:22:45
Windows Command Processor	00:00:21:22
WordWeb	00:02:30:56

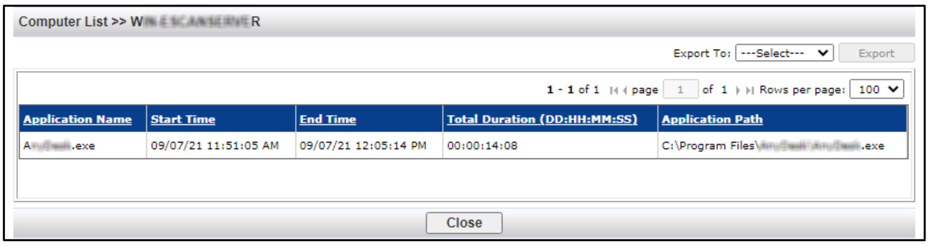
By clicking on the duration present under **Total Duration (DD:HH:MM:SS)** column, you will get the details of the computer name accessed the app and duration.



Application Name >> Dropbox

Computer Name	Total Duration (DD:HH:MM:SS)
WI[redacted]R	00:13:50:41

Again, if you click on the duration, you will get detailed view of the app accessed by the computer along with the date, time, and application path.



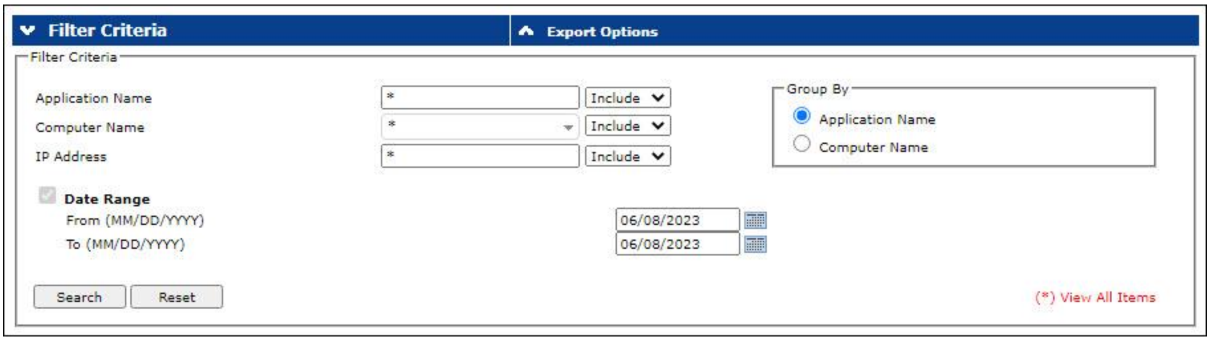
Computer List >> W[redacted]R

Application Name	Start Time	End Time	Total Duration (DD:HH:MM:SS)	Application Path
A[redacted].exe	09/07/21 11:51:05 AM	09/07/21 12:05:14 PM	00:00:14:08	C:\Program Files\[redacted].exe

You can export this report in PDF, CSV, and HTML format.

Filtering Application Access Report

To filter file activities, click **Filter Criteria** field. Filter Criteria field expands.



Application Name: * Include
Computer Name: * Include
IP Address: * Include

Group By
● Application Name
○ Computer Name

☑ Date Range
From (MM/DD/YYYY) 06/08/2023
To (MM/DD/YYYY) 06/08/2023

Filter Criteria lets you filter and generate the log according to your preferences. The checkbox selected will be added as a column in the report.

Application Name
Entering the Application name displays suggestions. Select the appropriate application.

Computer Name
Click the drop-down and select the preferred computer(s).

IP Address
Click the drop-down and select the preferred IP Address.

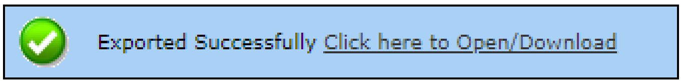
Group By
The results can be grouped by Application name or Computer name.

Date Range
To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the calendar icon and select **From** and **To** dates.

After entering data in all fields, click **Search**. The Application Access Report will be filtered according to your preferences.

Exporting Application Access Report

To export the generated report, click **Export Option**. Export Option field expands.
Select the preferred option and then click **Export**.
A success message appears.

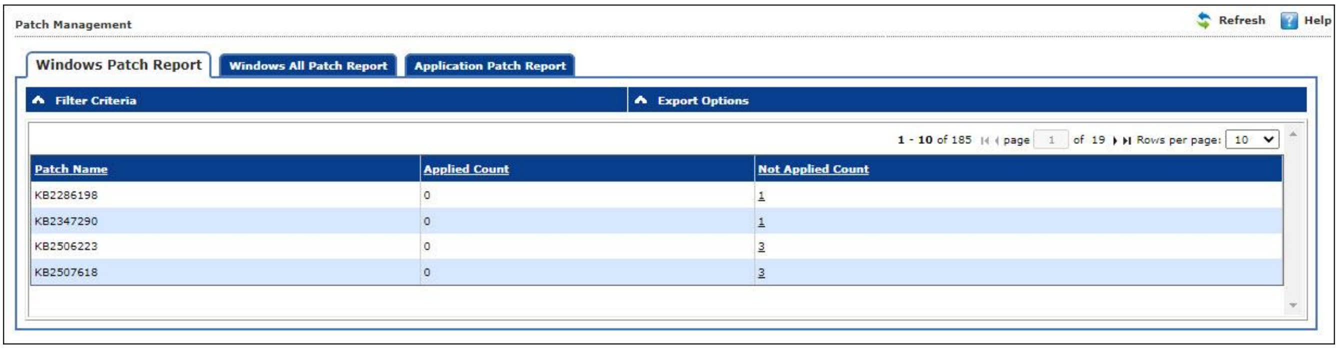


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Patch Report

The Patch Report module displays the number of windows security patches, Microsoft patches, and other third party application patches installed and not installed on the managed computers. This will help an administrator to identify the number of vulnerable systems in the network and to install the critical patches quickly.

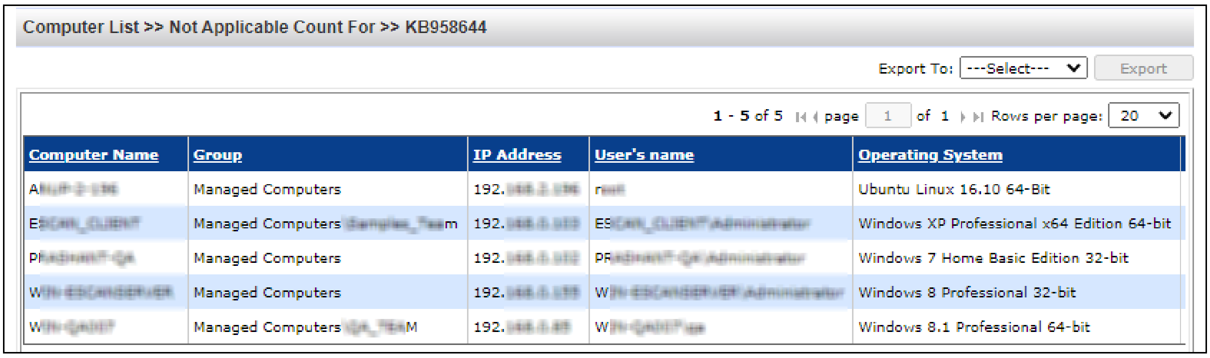


1 - 10 of 185 page 1 of 19 Rows per page: 10

Patch Name	Applied Count	Not Applied Count
KB2286198	0	1
KB2347290	0	1
KB2506223	0	3
KB2507618	0	3

Windows Patch Report

The Windows Patch Report tab displays the Patch Name, Applied Count, and Not Applied Count. Clicking the numerical displays the patch name, details about the computer, the group it belongs to, IP address and User's name.


Computer List >> Not Applicable Count For >> KB958644

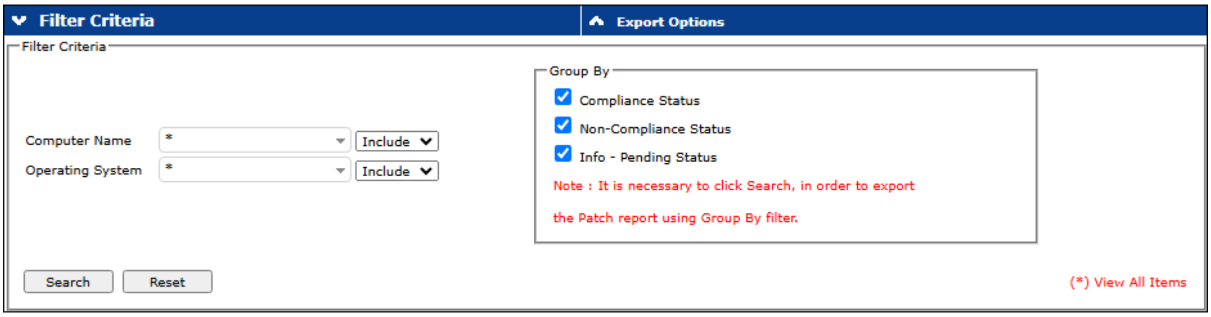
Export To: ---Select--- Export

1 - 5 of 5 page 1 of 1 Rows per page: 20

Computer Name	Group	IP Address	User's name	Operating System
A[redacted]	Managed Computers	192.[redacted]	r[redacted]	Ubuntu Linux 16.10 64-Bit
E[redacted]	Managed Computers[redacted]m	192.[redacted]	ES[redacted]	Windows XP Professional x64 Edition 64-bit
P[redacted]	Managed Computers	192.[redacted]	PR[redacted]	Windows 7 Home Basic Edition 32-bit
W[redacted]	Managed Computers	192.[redacted]	W[redacted]	Windows 8 Professional 32-bit
W[redacted]	Managed Computers[redacted]M	192.[redacted]	W[redacted]	Windows 8.1 Professional 64-bit

Filtering Patch Report

To filter the Patch Report as per your requirements, click **Filter Criteria** field.
Filter Criteria field expands.



Computer Name: * Include

Operating System: * Include

Group By

☑ Compliance Status

☑ Non-Compliance Status

☑ Info - Pending Status

Note : It is necessary to click Search, in order to export the Patch report using Group By filter.

(*) View All Items

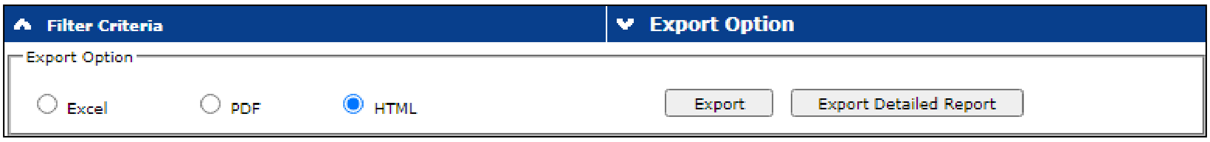
Enter the Patch Name and Computer Name to be included in the filtered report.

Include/Exclude
Selecting Include/Exclude allows you to include or exclude the parameter from the report.

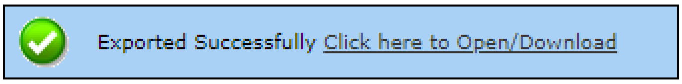
After making the necessary selections, click **Search.**
The Patch Report will be filtered and displayed as per ‘Group By’ selection.

Exporting Patch Report

To export the Patch Report, click **Export Option**. Export Option field expands.



Select the preferred option and then click **Export**.
OR
To export a detailed report, select the preferred option and then click **Export Detailed Report**.
A success message appears.



Exported Successfully Click here to Open/Download

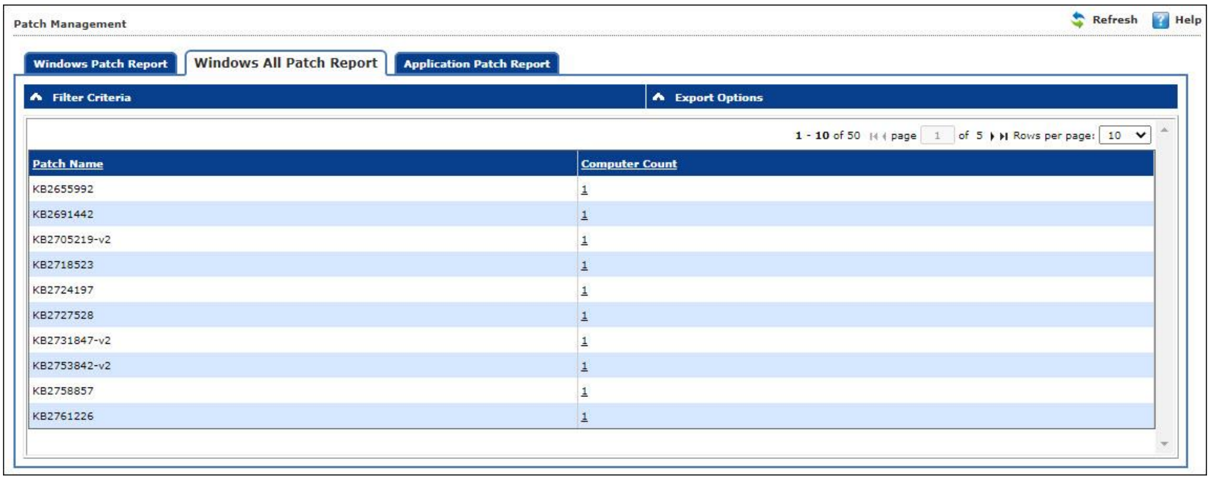
Click the link to open/download the file.

Other than security patch – for all patch Microsoft patch based on events
File AV > **Advanced Setting**

Windows All Patch Report

The Windows All Patch Report tab displays all Microsoft patches based on following specific events:

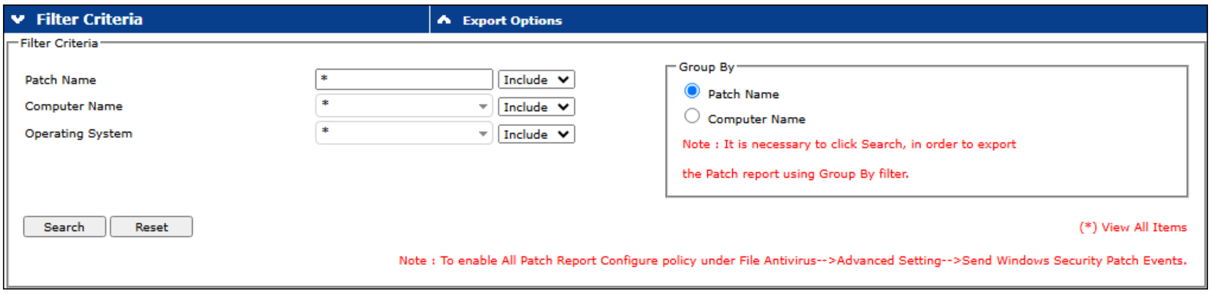
- **1-KB patches**
- **2-Security Update**
- **4-Hotfix**
- **8-Update**
- **16-Service Pack**
- **31-All**



Patch Name	Computer Count
KB2655992	1
KB2691442	1
KB2705219-v2	1
KB2718523	1
KB2724197	1
KB2727528	1
KB2731847-v2	1
KB2753842-v2	1
KB2758857	1
KB2761226	1

Filtering All Patch Report

To filter the All Patch Report as per your requirements, click **Filter Criteria** field.
Filter Criteria field expands.



Filter Criteria | Export Options

Filter Criteria

Patch Name	*	Include
Computer Name	*	Include
Operating System	*	Include

Group By
● Patch Name
○ Computer Name
Note : It is necessary to click Search, in order to export the Patch report using Group By filter.

Search | Reset

(*) View All Items

Note : To enable All Patch Report Configure policy under File Antivirus-->Advanced Setting-->Send Windows Security Patch Events.

Enter the **Patch Name** and **Computer Name** to be included in the filtered report.

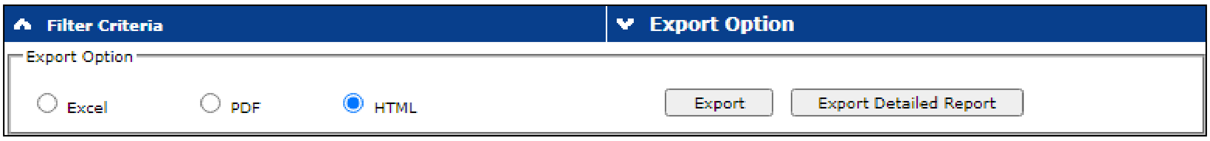
NOTE	To enable All Patch Report Configure policy by going to **File Antivirus--> Advanced Setting-->Send Windows Security Patch Events**.

Include/Exclude
Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After making the necessary selections, click **Search.**
The Patch Report will be filtered according to your preferences.

Exporting All Patch Report

To export the All Patch Report, click **Export Option**. Export Option field expands.



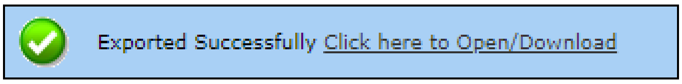
Filter Criteria | Export Option

Export Option

○ Excel ○ PDF ● HTML

Export | Export Detailed Report

Select the preferred option and then click **Export**.
OR
To export a detailed report, select the preferred option and then click **Export Detailed Report**.
A success message appears.

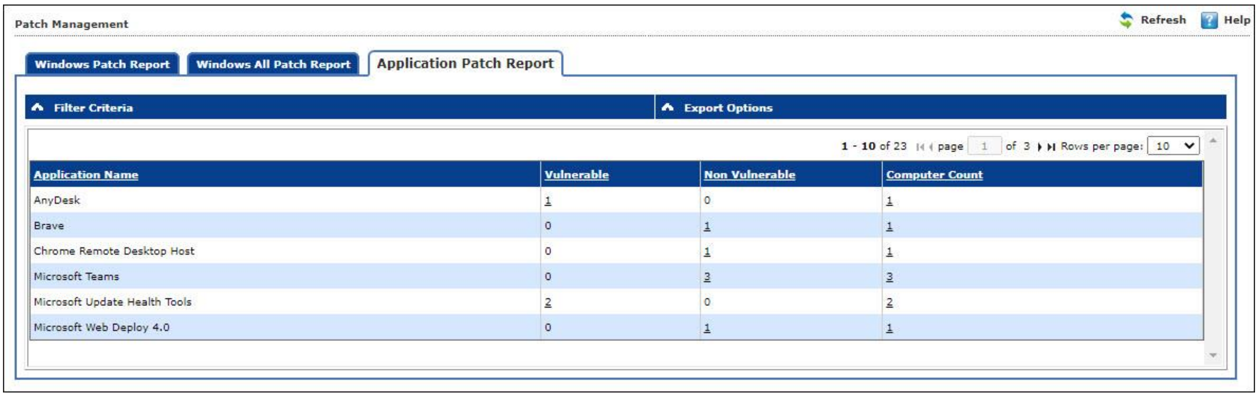


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Application Patch Report

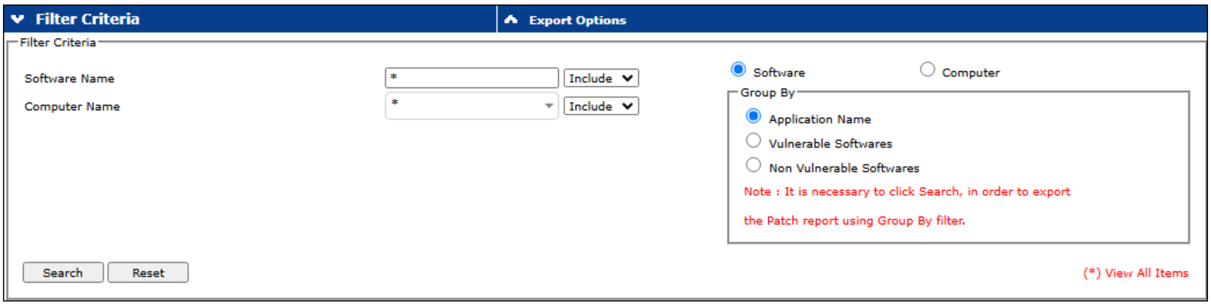
The Application Patch Report tab displays the Application name, Vulnerable applications count, Non-vulnerable applications count, and Computer count. Clicking the numerical displays the application name, details about the computer, the group it belongs to, IP address and User's name, etc.



Application Name	Vulnerable	Non Vulnerable	Computer Count
AnyDesk	1	0	1
Brave	0	1	1
Chrome Remote Desktop Host	0	1	1
Microsoft Teams	0	3	3
Microsoft Update Health Tools	2	0	2
Microsoft Web Deploy 4.0	0	1	1

Filtering Application Patch Report

To filter the Application Patch Report as per your requirements, click **Filter Criteria** field. Filter Criteria field expands with both Windows and Linux OS data.



Software Name: * Include
Computer Name: * Include

● Software ○ Computer

Group By
● Application Name
○ Vulnerable Softwares
○ Non Vulnerable Softwares

Note : It is necessary to click Search, in order to export the Patch report using Group By filter.

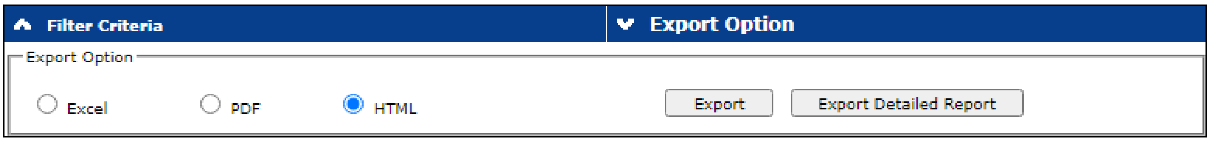
Enter the Software Name and Computer Name to be included in the filtered report.

Include/Exclude
Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After making the necessary selections, click **Search.**
The Application Patch Report will be filtered and displayed as per 'Group By' selection.

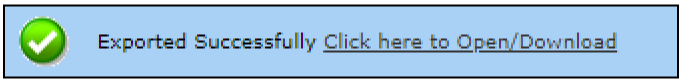
Exporting Application Patch Report

To export the Application Patch Report, click **Export Option**. Export Option field expands.



○ Excel ○ PDF ● HTML

Select the preferred option and then click **Export**.
OR
To export a detailed report, select the preferred option and then click **Export Detailed Report**.
A success message appears.



Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Notifications

This module lets you configure notifications for different actions/incidents that occur on the server. The Notifications module consists following submodules:

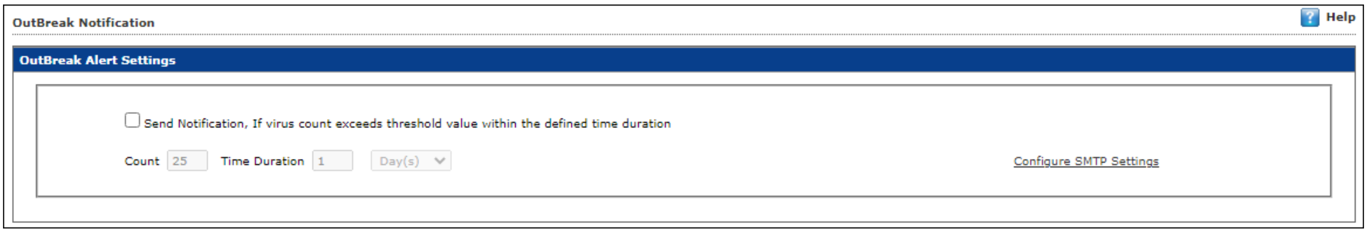
- **Outbreak Alert**
- **Event Alert**
- **Unlicensed Move Alert**
- **New Computer Alert**
- **Configure SIEM**
- **Scan Alert Notification**
- **SMTP Settings**

Outbreak Alert

If the virus count exceeds the limits set by you, an outbreak email notification will be sent to the recipient.

To set an outbreak alert, follow the steps given below:

1. In the navigation panel, click **Notifications** > **Outbreak Alert**.
   Outbreak Notification window appears.



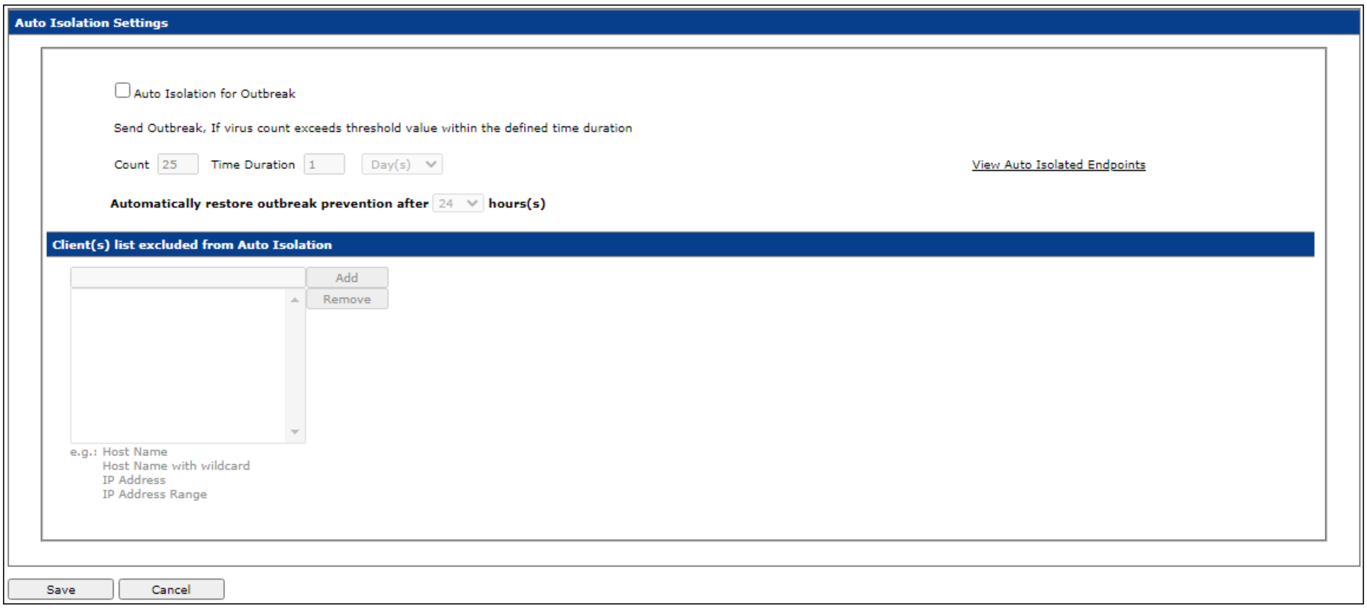
OutBreak Notification

OutBreak Alert Settings

□ Send Notification, If virus count exceeds threshold value within the defined time duration

Count 25 Time Duration 1 Day(s)

2. Select the checkbox **Send notification**.
3. Enter the preferred values in Count and Time Limit field.



Auto Isolation Settings

□ Auto Isolation for Outbreak

Send Outbreak, If virus count exceeds threshold value within the defined time duration

Count 25 Time Duration 1 Day(s)

Automatically restore outbreak prevention after 24 hours(s)

Client(s) list excluded from Auto Isolation

e.g.: Host Name
Host Name with wildcard
IP Address
IP Address Range

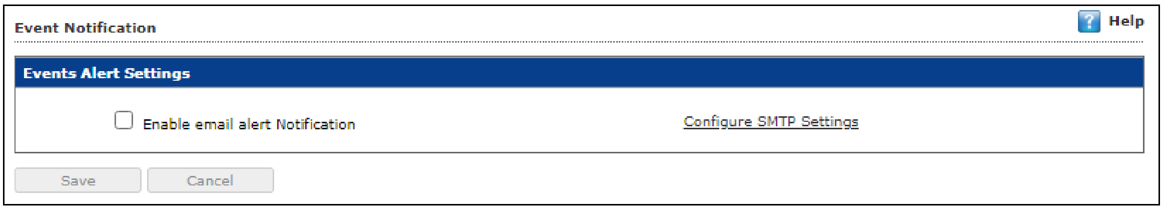
4. In **Auto Isolation Settings** section, select checkbox **Auto Isolation for Outbreak**.

5. Enter the preferred values in Count and Time Limit field.
6. Select the value in **Automatically restore outbreak prevention after hours(s)** field.
7. You can also add/remove clients list to exclude it from auto isolation in the below table. To do the same, refer the following:
    - Enter the host name, IP Address, or IP address range and click **Add**.
    - To delete a particular client, select the client and click **Remove**.
8. After configuring accordingly, click **Save.** Outbreak Alert Settings will be saved.

NOTE	In order to receive notification emails, it is necessary to configure SMTP settings. Learn more about SMTP Settings by clicking **here**. To view the Auto-Isolated Endpoints, click **View Auto Isolated Endpoints** hyperlink in the window. The list of auto-isolated endpoints will be displayed.

Event Alert

This submodule lets you enable email notifications about any event that occurs on the client computers connected to the server.



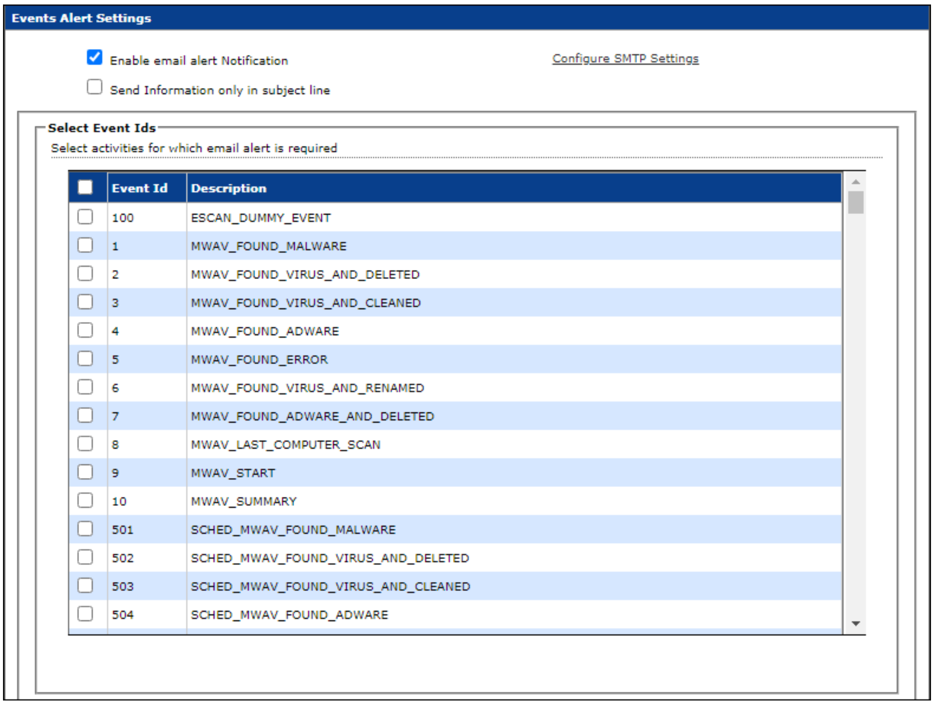
Event Notification

Events Alert Settings

☐ Enable email alert Notification

To enable the event alert:

1. In the navigation panel, click **Notifications** > **Event Alert**.
2. Select the checkbox Enable email alert Notification.
3. Select the events from the list for which you prefer an alert.



Events Alert Settings

☑ Enable email alert Notification Configure SMTP Settings

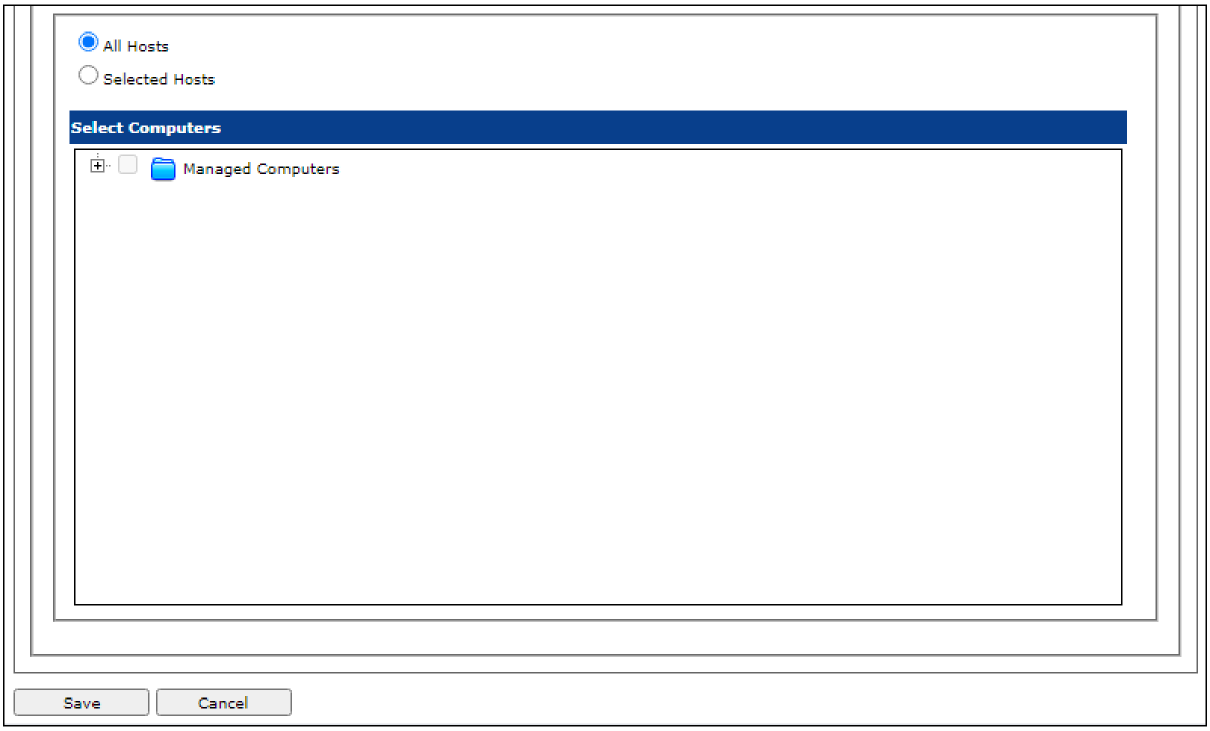
□ Send Information only in subject line

Select Event Ids

Select activities for which email alert is required

□	Event Id	Description
□	100	ESCAN_DUMMY_EVENT
□	1	MWAV_FOUND_MALWARE
□	2	MWAV_FOUND_VIRUS_AND_DELETED
□	3	MWAV_FOUND_VIRUS_AND_CLEANED
□	4	MWAV_FOUND_ADWARE
□	5	MWAV_FOUND_ERROR
□	6	MWAV_FOUND_VIRUS_AND_RENAMED
□	7	MWAV_FOUND_ADWARE_AND_DELETED
□	8	MWAV_LAST_COMPUTER_SCAN
□	9	MWAV_START
□	10	MWAV_SUMMARY
□	501	SCHED_MWAV_FOUND_MALWARE
□	502	SCHED_MWAV_FOUND_VIRUS_AND_DELETED
□	503	SCHED_MWAV_FOUND_VIRUS_AND_CLEANED
□	504	SCHED_MWAV_FOUND_ADWARE

4. Select the required hosts or group.



● All Hosts

○ Selected Hosts

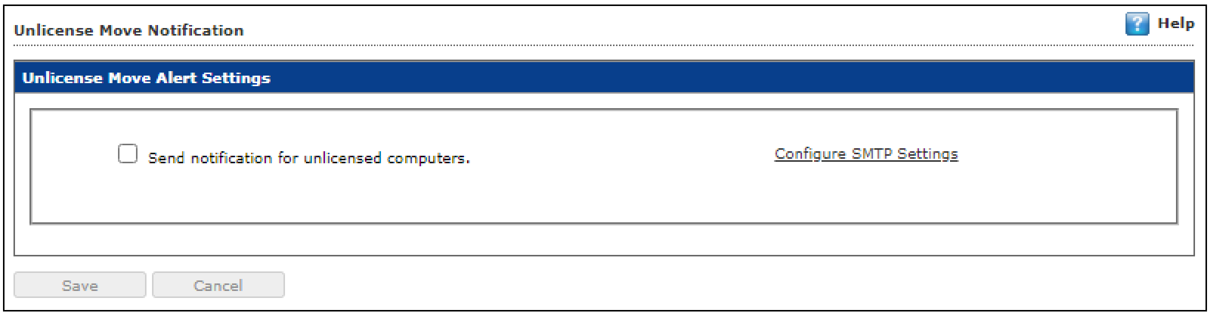
Select Computers

⊞ □ Managed Computers

5. Click **Save.**
   The Event Alert Settings will be saved.

Unlicensed Move Alert

This sub module lets you enable notification alert when a computer automatically moves to Unlicensed Computers category based on the setting done (under events and computers) for the computer which is not connected to the server for a long time.



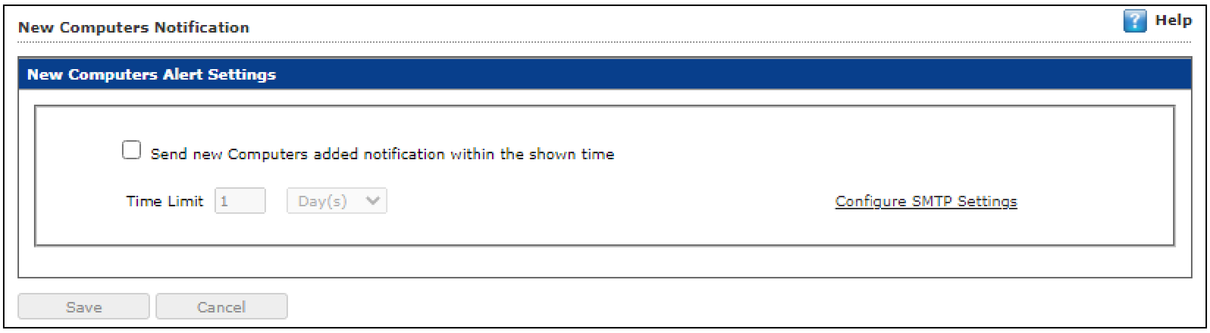
□ Send notification for unlicensed computers.

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 submodule lets eScan send you a notification alert when a new computer is connected to the server within the IP range mentioned under the Managed Computers.



□ Send new Computers added notification within the shown time

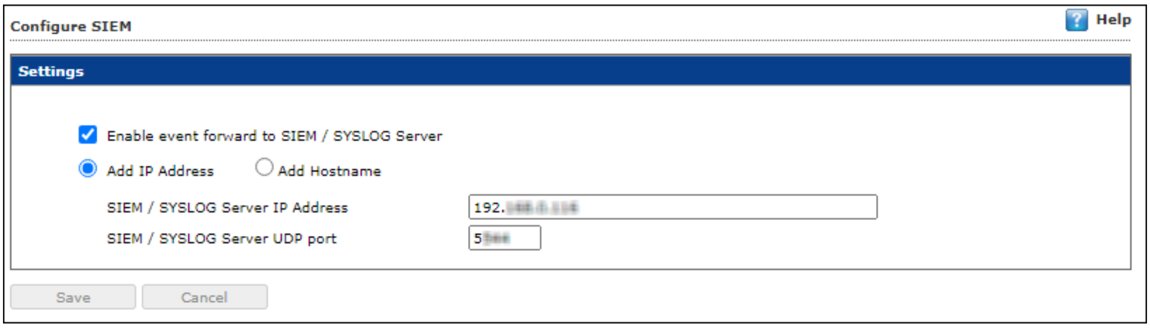
Time Limit 1 Day(s)

To enable the new computer alert, follow the steps given below:

1. In the navigation panel, click **Notifications > New Computer Alert**.
2. Select the checkbox **Send new Computers added notification within the shown time**.
3. Enter the preferred values in Time limit field.
4. Click **Save**.
   The New Computer Alert Settings will be saved.

Configure SIEM

SIEM technology provides real-time management of security events generated for hardware changes and applications installed/uninstalled/upgraded where eScan is installed. eScan is equipped with variety of features that facilitate real-time monitoring, correlating captured events, notifications and console views and provides long-term storage, analysis and reporting of data.



Configure SIEM

Settings

☑ Enable event forward to SIEM / SYSLOG Server

● Add IP Address ○ Add Hostname

SIEM / SYSLOG Server IP Address: 192.[redacted]

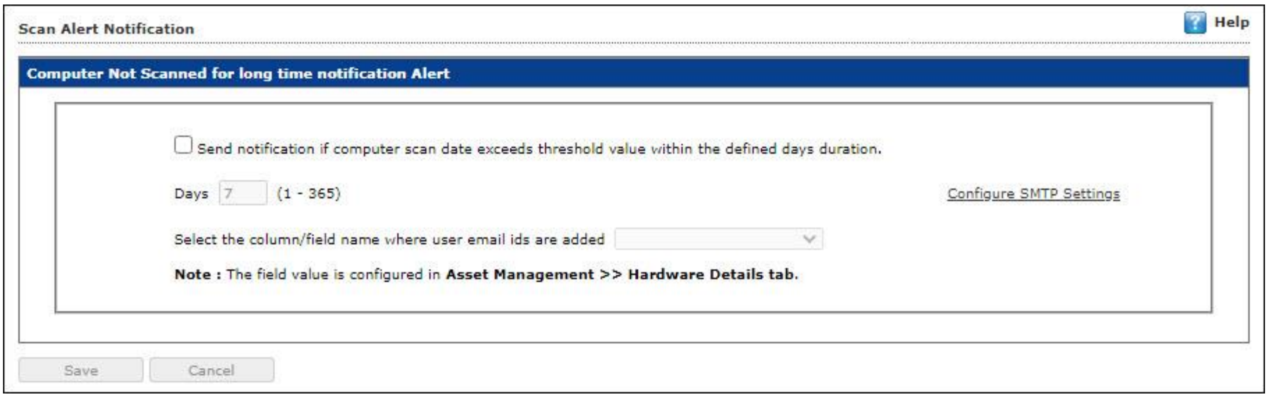
SIEM / SYSLOG Server UDP port: 5[redacted]

To configure SIEM, follow the steps given below:

1. In the navigation panel, click **Notification** > **Configure SIEM**.
2. Select the **Enable event forward to SIEM/SYSLOG Server** checkbox.
3. After selecting the checkbox, it will enable the rest of the options that can be configured. You can enter the details of the SIEM/SYSLOG Server.
4. Click **Save**.
   The SIEM settings will be saved.

Scan Alert Notification

This submodule allows you to send an alert notification to the user-defined email ID if the computer is not scanned for the defined period of time. You can define the threshold period between 1-365 days.



Scan Alert Notification

Computer Not Scanned for long time notification Alert

□ Send notification if computer scan date exceeds threshold value within the defined days duration.

Days 7 (1 - 365)

Select the column/field name where user email ids are added

Note : The field value is configured in **Asset Management >> Hardware Details tab.**

To configure this setting, follow the steps given below:

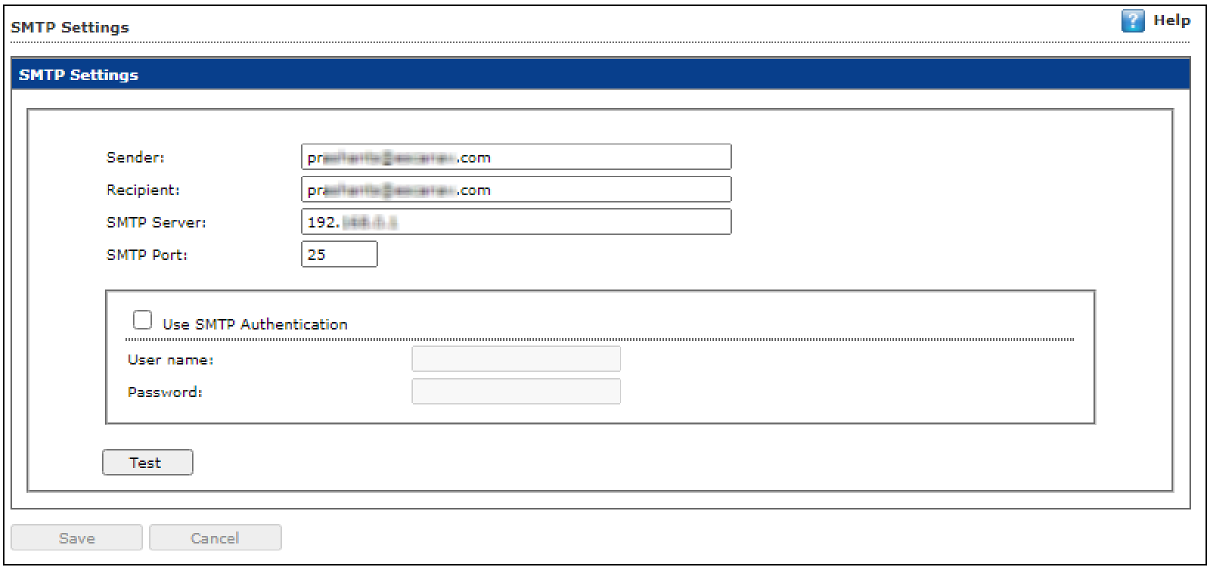
1. Select the checkbox **Send notification if computer scan date exceeds threshold value within the defined days duration**.
2. Enter the value (days) to define the threshold period in provided field.
3. Select field from the added user email IDs using provided drop-down.
4. Click on **Configure SMTP Settings** to configure SMTP parameters for alert notifications to

be sent.

5. After configuring SMTP settings, click on **Save**.
   The Scan Alert Notification settings have been set.

SMTP Settings

This submodule lets you configure the SMTP settings for all the email notifications.



SMTP Settings

Help

SMTP Settings

Sender: pr[redacted].com

Recipient: pr[redacted].com

SMTP Server: 192.[redacted]

SMTP Port: 25

□ Use SMTP Authentication

User name:

Password:

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

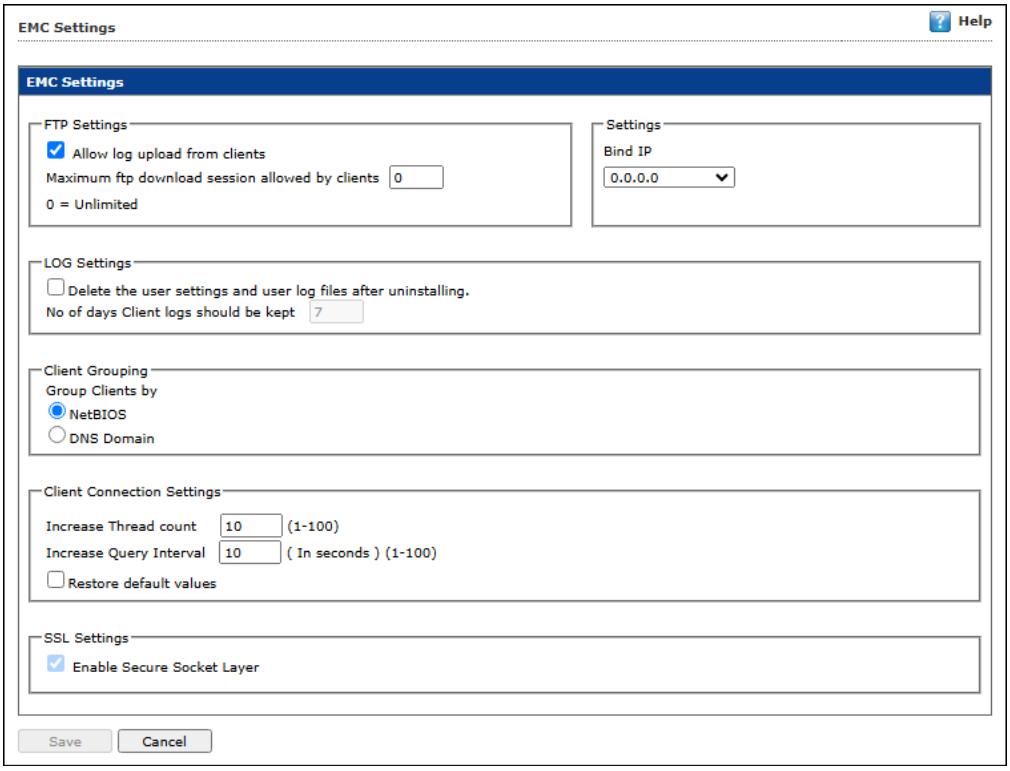
The Settings module lets you to configure general settings using following submodules:

- **EMC Settings**: This submodule lets you define settings for FTP sessions, Log Settings, Client Grouping and Client connection settings.
- **Web Console Settings**: This submodule lets you define settings for web console timeout, Dashboard Settings, Login Page settings, SQL Server Connection settings, SQL Database compression settings.
- **Update Settings**: This submodule lets you define settings for General Configuration, Update Notifications, and Scheduling.
- **Auto-Grouping**: This submodule lets you define settings for Grouping of computers after installation of eScan client is carried out.
- **Two-Factor Authentication**: This submodule lets you to add extra layer of protection to your endpoints.
- **Roaming Client**: This submodule allows the remote client to download all the updates via Cloud while Server uploads all the required client updates to Cloud.

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.



EMC Settings

EMC Settings

FTP Settings

☑ Allow log upload from clients

Maximum ftp download session allowed by clients: 0

0 = Unlimited

Settings

Bind IP: 0.0.0.0

LOG Settings

□ Delete the user settings and user log files after uninstalling.

No of days Client logs should be kept: 7

Client Grouping

Group Clients by

● NetBIOS

○ DNS Domain

Client Connection Settings

Increase Thread count: 10 (1-100)

Increase Query Interval: 10 (In seconds) (1-100)

□ Restore default values

SSL Settings

☑ Enable Secure Socket Layer

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 the 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.

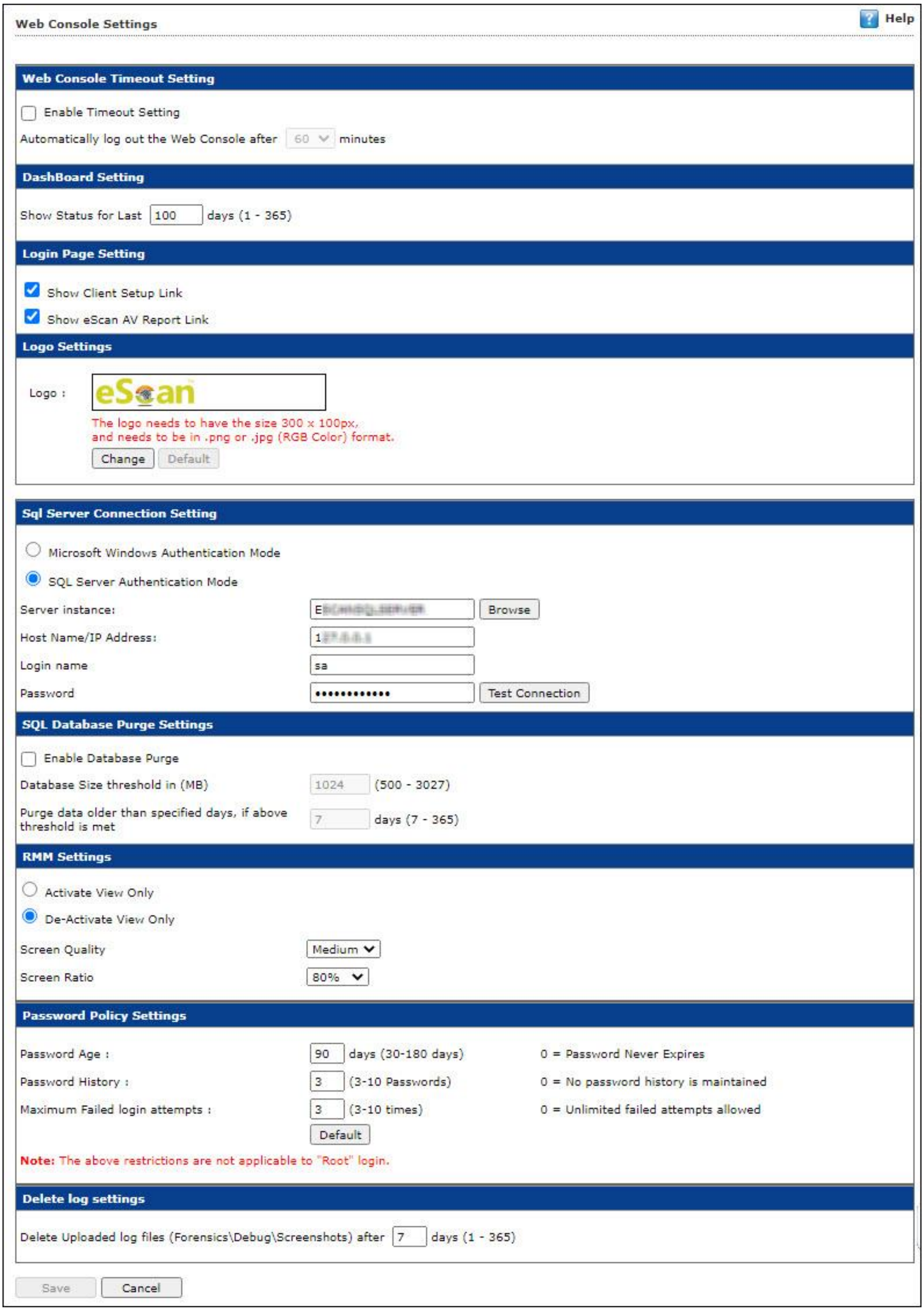
Client Connection Settings
This setting lets you modify **Thread Count** and **Query Interval** (In Seconds). To reset the values, select **Restore default values** checkbox.

After performing the necessary changes, click **Save**. The EMC Settings will be updated.

SSL Settings
This option enables Secure Sockets Layer (SSL) for the web console.

Web Console Settings

Web Console Settings submodule lets you configure web console Timeout, Dashboard, Login Page, SQL Server Connection, SQL Database compression, Password Policy Settings, and Delete Log Settings.



Web Console Timeout Setting

□ Enable Timeout Setting

Automatically log out the Web Console after 60 minutes

DashBoard Setting

Show Status for Last 100 days (1 - 365)

Login Page Setting

☑ Show Client Setup Link

☑ Show eScan AV Report 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

Server instance:	E[redacted]
Host Name/IP Address:	1[redacted]
Login name	sa
Password	•••••••••••••

SQL Database Purge Settings

□ Enable Database Purge

Database Size threshold in (MB)	1024	(500 - 3027)
Purge data older than specified days, if above threshold is met	7	days (7 - 365)

RMM Settings

○ Activate View Only

● De-Activate View Only

Screen Quality	Medium
Screen Ratio	80%

Password Policy Settings

Password Age :	90	days (30-180 days)	0 = Password Never Expires
Password History :	3	(3-10 Passwords)	0 = No password history is maintained
Maximum Failed login attempts :	3	(3-10 times)	0 = Unlimited failed attempts allowed

Note: The above restrictions are not applicable to "Root" login.

Delete log settings

Delete Uploaded log files (Forensics\Debug\Screenshots) after 7 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, Agent setup and AV Report. 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 between Microsoft Windows Authentication Mode to SQL Server Authentication Mode. Select the **SQL Server Authentication Mode** and define **Server instance** and **Host Name** along with the credentials for connecting to the database.

Server Instance

It displays the current server instance in use. To select another server instance, click **Browse**. Select an instance from the list and click **OK**.

Hostname/IP Address

It displays the Hostname or IP Address of the server instance computer.

Enter the credentials in **Username** and **Password** fields.
To check whether correct credentials are entered, click **Test Connection**.

SQL Database Purge Settings

This setting lets you define the maximum SQL database size in MB and purge data older than the specified days. To enable SQL Database Purge Settings, select **Enable Database Purge** checkbox.
Enter the preferred value in **Database Size threshold in (MB)** field.
Enter the preferred number of days in **Purge data older than specified days, if above threshold** is met field.

RMM Settings

This setting lets you configure default RMM setting for connecting to client via RMM service:

Activate View Only

By default, after taking a remote connection, you can only view the endpoint screen and are unable to perform any activity.

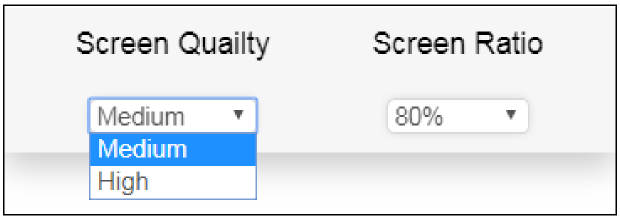
De-Activate View Only

To perform activity on an endpoint after taking remote connection, click **De-Activate View Only**.

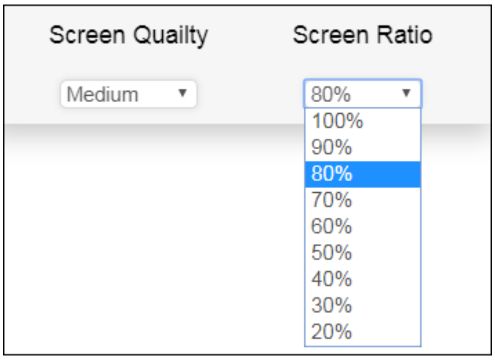
Screen Quality Settings

This option lets you configure the screen as per your requirements. It consists following suboptions:

- **Screen Quality** can be set to **Medium** or **High**.



- **Screen Ratio** can be set to anywhere from **20%** to **100%**.



NOTE	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.

NOTE	This setting will not be applicable for the root login

After making necessary changes, click **Save.** The web console Settings will be updated.

Delete log settings

This option allows you to delete the uploaded log files on eScan server after user-defined time interval. You can set the time interval between 1-365 days. The default time is 7 days.

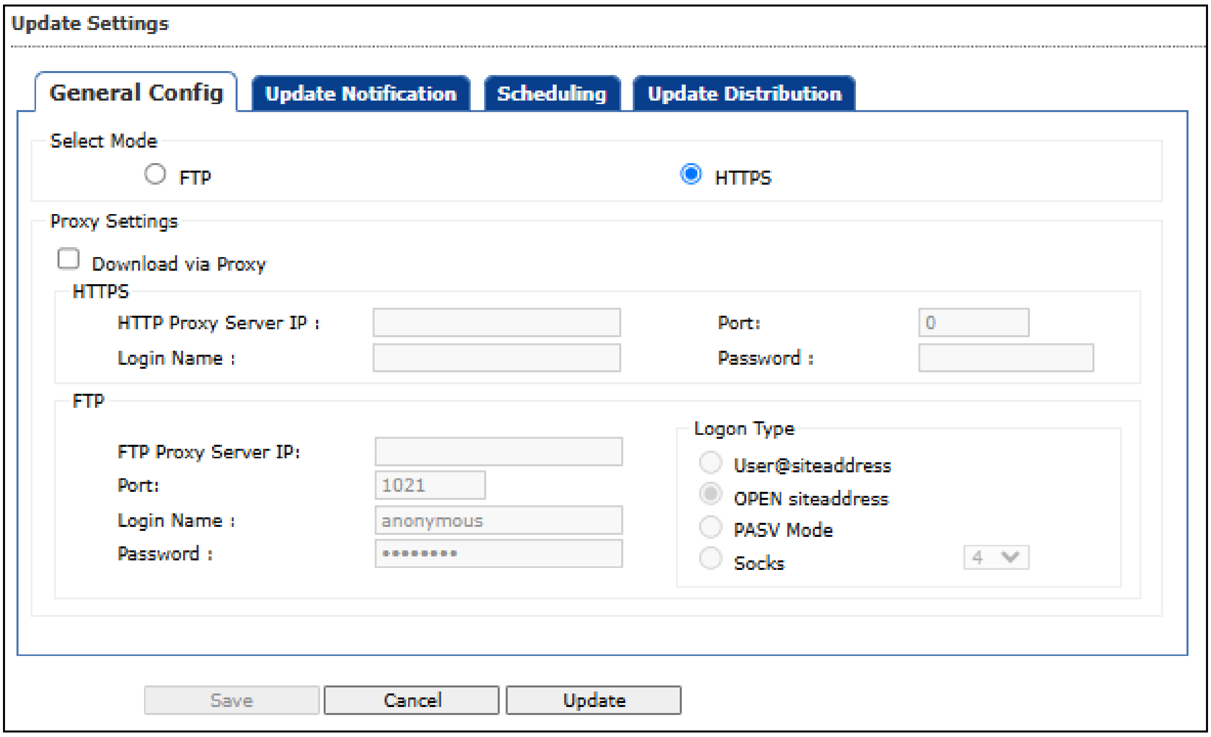
Update Settings

The Update Settings submodule keeps your virus definitions up-to-date and protects your computer from emerging species of viruses and other malicious programs. This submodule lets you configure update settings, update notifications and schedule updates according to your need.

You can configure eScan to download updates automatically either from eScan update servers or from the local network by using FTP or HTTP. You can configure following settings:

General Config

This tab allows you to configure update settings. The settings let you select the mode of update and configure proxy settings.



Update Settings

Select Mode

○ FTP ● HTTPS

Proxy Settings

□ Download via Proxy

HTTPS

HTTP Proxy Server IP :
Port: 0
Login Name :
Password :

FTP

FTP Proxy Server IP:
Port: 1021
Login Name : anonymous
Password : ********

Logon Type
○ User@siteaddress
● OPEN siteaddress
○ PASV Mode
○ Socks 4

Select Mode
Select the mode for downloading updates. Following options are available:

- FTP
- HTTPS

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.

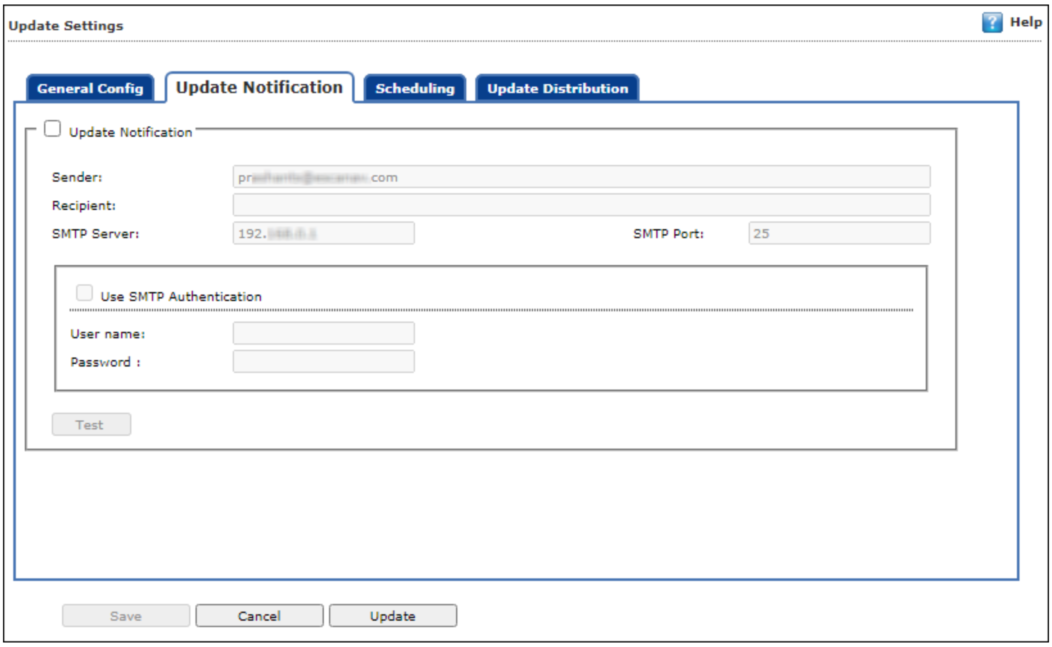
If you are using HTTP proxy servers, enter the HTTP proxy server IP address, port number and HTTP proxy server's authentication credentials.

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 Type.

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 Settings

General Config | Update Notification | Scheduling | Update Distribution

□ Update Notification

Sender: pr[redacted].com

Recipient:

SMTP Server: 192.[redacted]

SMTP Port: 25

□ Use SMTP Authentication

User name:

Password :

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.

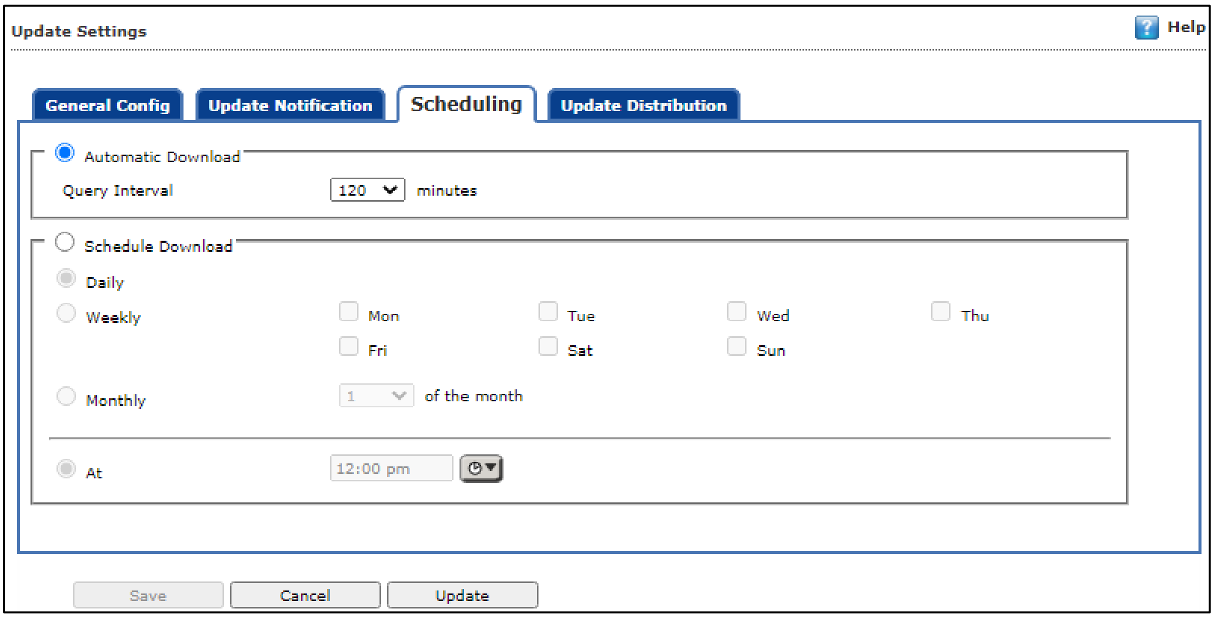
SMTP Server and Port
Enter the SMTP server's IP address and Port number in the respective fields.

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.



Update Settings Help

● Automatic Download

Query Interval 120 minutes

○ Schedule Download

○ Daily

○ Weekly □ Mon □ Tue □ Wed □ Thu

□ Fri □ Sat □ Sun

○ Monthly 1 of the month

○ At 12:00 pm

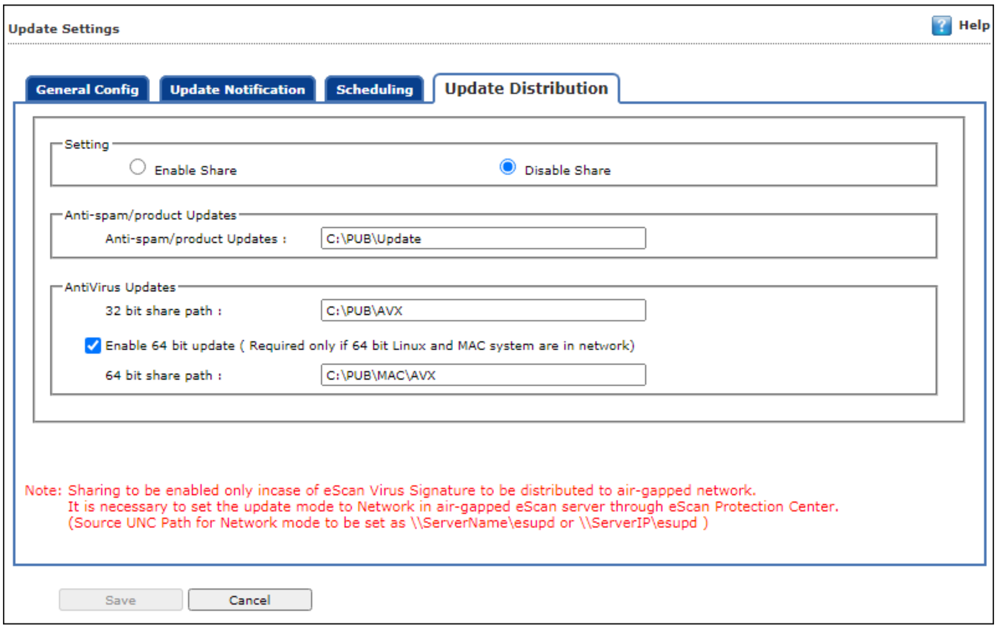
Automatic Download
The eScan Scheduler sends a query to the update server at set intervals and downloads the latest updates if available. To set an interval, click the **Query Interval** drop-down and select a preferred duration.

Schedule Download
The eScan Scheduler lets you set a schedule the download for daily, weekly, or monthly basis at a specified time. The scheduled query will be sent to the update server as per your preferences.

After filling the necessary data, click **Save** > **Update**. The Scheduling tab will be saved and updated.

Update Distribution

The Update Distribution tab allows the admin to enable and disable the sharing of eScan Virus signature to be distributed to air-gapped/isolated network.



Update Settings Help

Setting

○ Enable Share ● Disable Share

Anti-spam/product Updates

Anti-spam/product Updates : C:\PUB\Update

AntiVirus Updates

32 bit share path : C:\PUB\AVX

☑ Enable 64 bit update (Required only if 64 bit Linux and MAC system are in network)

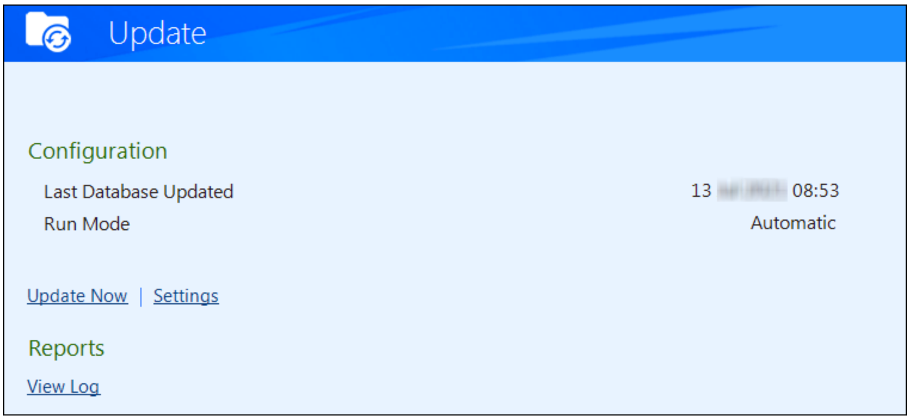
64 bit share path : C:\PUB\MAC\AVX

Note: Sharing to be enabled only incase of eScan Virus Signature to be distributed to air-gapped network.
It is necessary to set the update mode to Network in air-gapped eScan server through eScan Protection Center.
(Source UNC Path for Network mode to be set as \\ServerName\esupd or \\ServerIP\esupd)

Select **Enable Share** in **Setting** section, this will allow the distribution of eScan Virus Signatures to the isolated/air-gapped network. After enabling this, it is mandatory to set the update mode to the network in network that is isolated/air-gapped through eScan Protection Center.

To update it, follow the below steps:

1. Open the eScan Protection Center in air-gapped network; click **Update** option present in the Quick Link section.



Update

Configuration

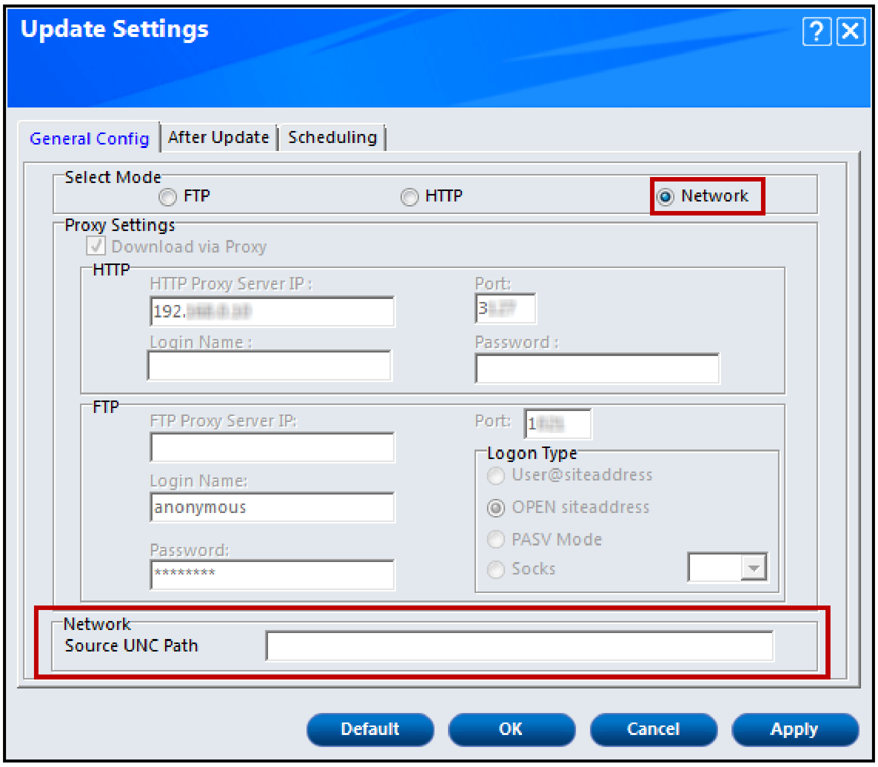
Last Database Updated	13 [redacted] 08:53
Run Mode	Automatic

Update Now | Settings

Reports

View Log

2. Click **Settings**. Update Settings window appears.



Update Settings

General Config | After Update | Scheduling

Select Mode: ○ FTP ○ HTTP ● Network

Proxy Settings
☑ Download via Proxy

HTTP
HTTP Proxy Server IP : 192.[redacted]
Port: 3[redacted]
Login Name :
Password :

FTP
FTP Proxy Server IP:
Port: 1[redacted]
Login Name: anonymous
Password: ********
Logon Type: ○ User@siteaddress ● OPEN siteaddress ○ PASV Mode ○ Socks

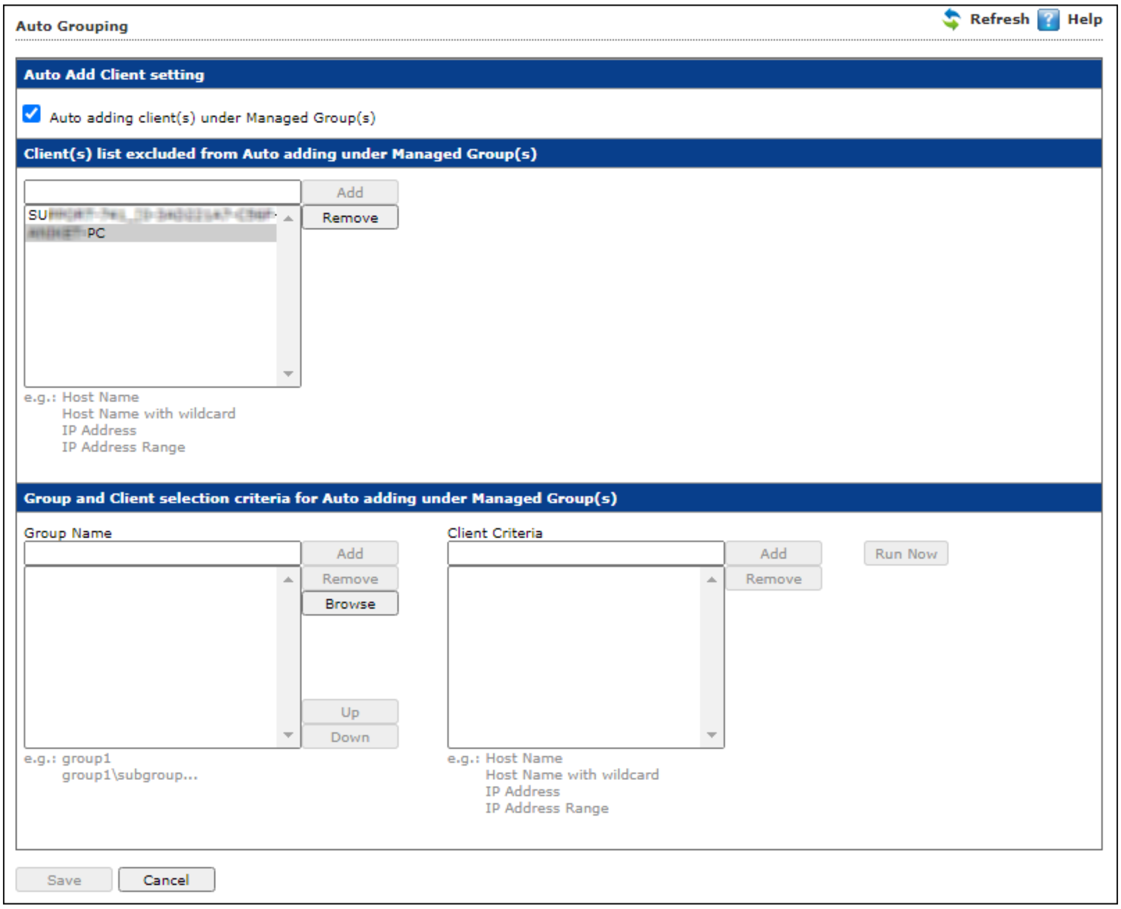
Network
Source UNC Path

3. Select **Network** option and set the **Source UNC Path** as **\\ServerName\esupd** or **\\ServerIP\esupd**.
   E.g.: \\192.0.2.0\esupd
   After setting UNC path for the air-gapped network, the update will be available automatically to the Isolated/Air-gapped network.

Auto-Grouping

The Auto grouping submodule consists following subsections:

- **Auto Add Client setting**
- **Client(s) list excluded from Auto adding under Managed Group(s)**
- **Group and Client selection criteria for Auto adding under Managed Group(s)**



Auto Grouping

Auto Add Client setting

☑ Auto adding client(s) under Managed Group(s)

Client(s) list excluded from Auto adding under Managed Group(s)

SU[redacted]
[redacted]PC

e.g.: Host Name
Host Name with wildcard
IP Address
IP Address Range

Group and Client selection criteria for Auto adding under Managed Group(s)

Group Name

e.g.: group1
group1\subgroup...

Client Criteria

e.g.: Host Name
Host Name with wildcard
IP Address
IP Address Range

Auto Add Client setting

Selecting the checkbox **Auto adding client(s) under Managed Group(s)** enables automatic adding computers under Managed group(s) after manual installation of eScan client.

Client(s) list excluded from Auto adding under Managed Group(s)

Adding a client in this list ensures that it does not auto add itself again after you remove it from the Managed computer(s).

Group and Client selection criteria for Auto adding under Managed Group(s)

This section lets you define/create groups with client criteria for auto adding under managed group(s). You can add a list of clients under a particular group name here and then add it under the exclusion list if required.

Excluding clients from auto adding under Managed Group(s)

To exclude clients from auto adding under managed group(s), follow the steps given below:

1. Enter either the host name, host name with wildcard, IP address or IP address range.
2. Click **Add**. The computer will be displayed in the list below.

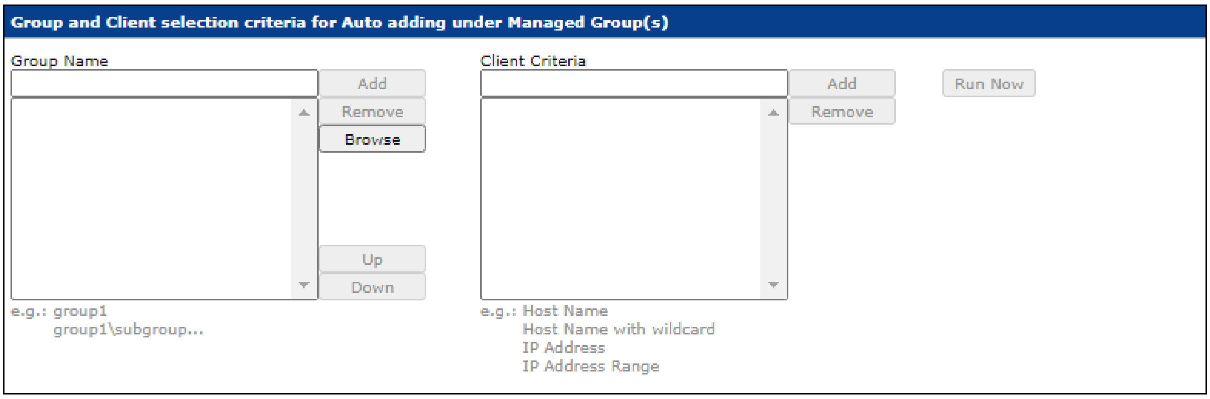
Removing clients from the excluded list

1. Select the computer you want to remove.
2. Click **Remove**. The computer will be removed from the list.

Group and Client selection criteria for Auto adding under Managed Group(s)
This feature can be used to automate the process of adding computers/clients under a particular group. This process is manually done under unmanaged computers.

Defining a group and client selection criteria for auto adding under managed computer(s)

To define group and client selection criteria for auto adding under managed groups(s), follow the steps given below:



1. Under the Group Name, enter the group's name and click **Add.**
   OR
   Click **Browse** and select the group from the existing list.

NOTE	To change the order of the group in the list, click **Up** or **Down**.

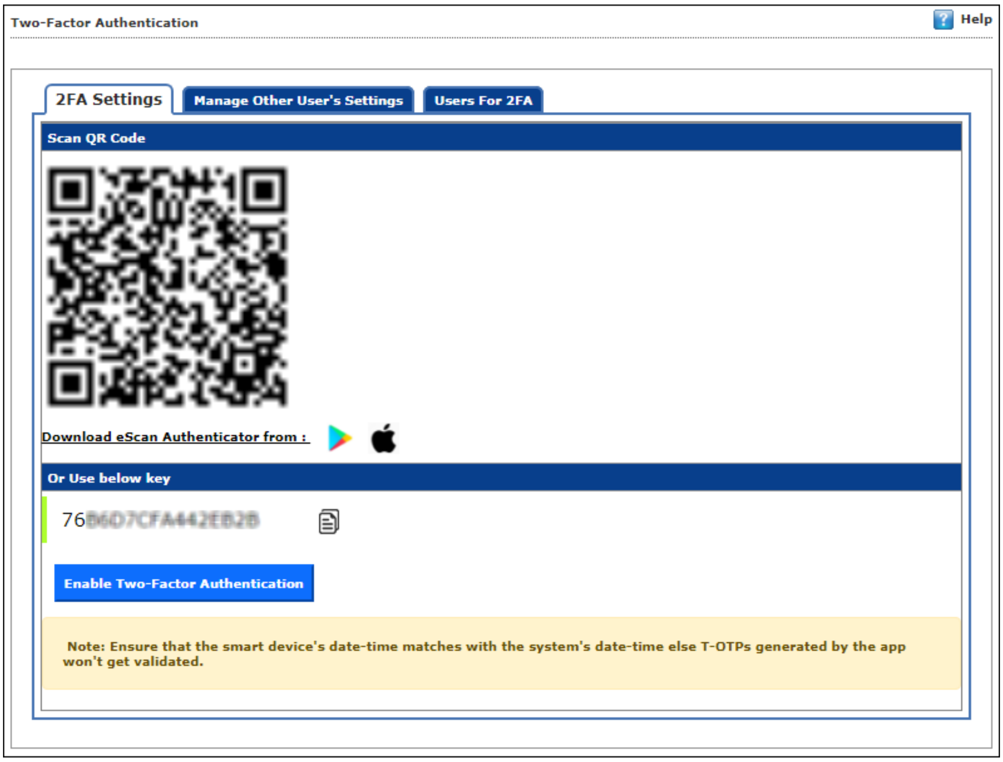
2. Select the group for which you want to define the criteria.
3. Under the Client Criteria, enter either Hostname, Hostname with wildcard, IP address or IP address range and click **Add.** The clients displayed in the list will be added under the selected group.
4. Click **Save**. The client will be saved under that group.
5. To apply the settings for the newly added client, click **Run Now**.

Two-Factor Authentication (2FA)*

The system login password is Single-Factor Authentication which is considered less secured and it may put your organization's data at high risk of compromise. The Two-Factor Authentication, also more commonly known as 2FA, adds an extra layer of protection to your eScan web console login.

The 2FA feature mandates you to enter a Time-based One-Time Password (TOTP) after entering eScan credentials. So, even if somebody knows your eScan credentials, the 2FA feature secures data against unauthorized logins. Only administrator can enable/disable the 2FA feature. It can also be enabled for added users.

To use 2FA login feature, you need to install the Authenticator app for Android devices from Play Store or for iOS devices from App Store on your smart device. The Authenticator app needs camera access for scanning a QR code. If a COD or BYOD policy restricts you from using device's camera in your organization, enter the Account Key in the Authenticator app.


Two-Factor Authentication
Help
2FA Settings
Manage Other User's Settings
Users For 2FA
Scan QR Code
Download eScan Authenticator from :
Or Use below key
Enable Two-Factor Authentication

76[redacted]

Note: Ensure that the smart device's date-time matches with the system's date-time else T-OTPs generated by the app won't get validated.

NOTE	Ensure that the smart device's date and time matches with the system's date and time or else TOTPs generated by app won't get validated.

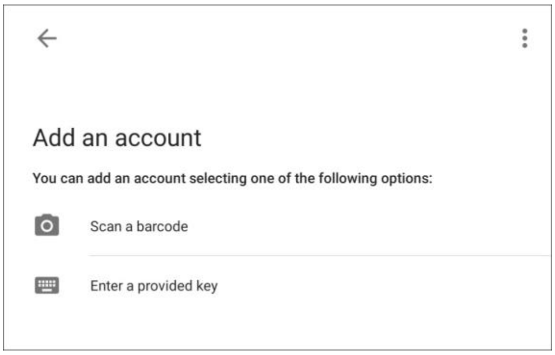
IMPORTANT	We recommend that you save/store the **Account Key** in offline storage or a paperback copy, in case you lose the account access.

Enabling 2FA login

To enable 2FA login:

1. Go to **Settings** > **Two-Factor Authentication**.

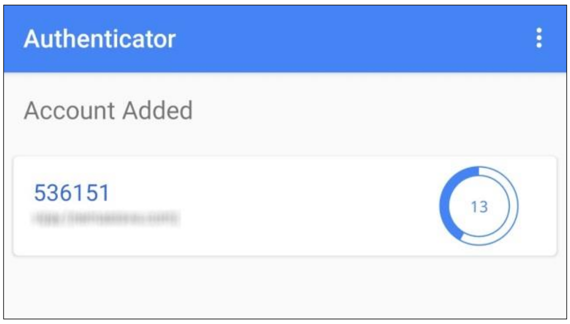
2. Open the Authenticator app.
   After basic configuration following screen appears on smart device.



Add an account

You can add an account selecting one of the following options:

3. Select a preferred option. If you tapped **Scan a barcode**, scan the onscreen QR code via your smart device. If you tapped **Enter a provided key**, enter the Account Key and then tap **ADD**. After scanning the Account QR code or entering Account Key, the eScan server account gets added to the Authenticator app. The app then starts displaying a Time-based One-Time Password (TOTP) that is valid for 30 seconds.

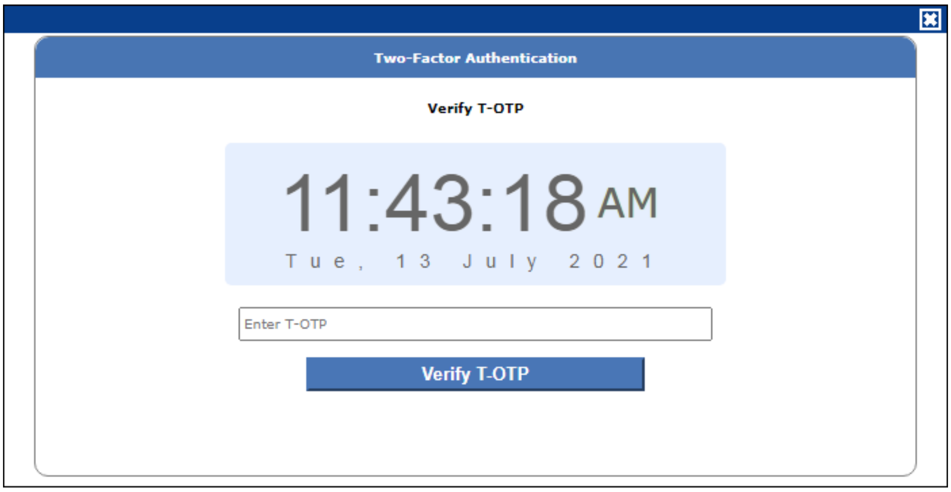


Authenticator

Account Added

536151

4. Click **Enable Two-Factor Authentication**.
   Verify T-OTP window appears.



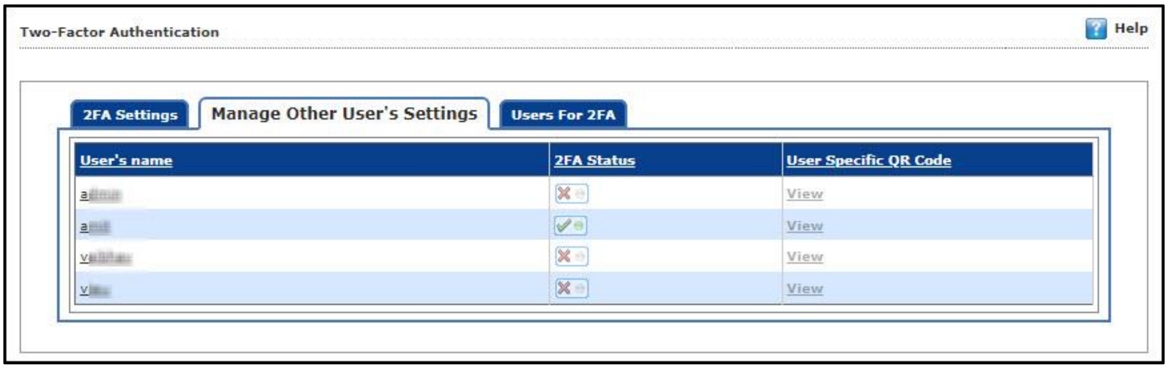
Two-Factor Authentication

Verify T-OTP

11:43:18 AM
Tue, 13 July 2021

5. Enter the TOTP displayed on smart device and then click **Verify TOTP**.
   The 2FA login feature gets enabled.

6. To apply the login feature for specific users, click **Manage Other User Settings** tab. The tab displays list of added users and whether 2FA status is enabled or disabled as shown below.
   ✗ - 2FA Disabled
   ✓ - 2FA Enabled



Two-Factor Authentication

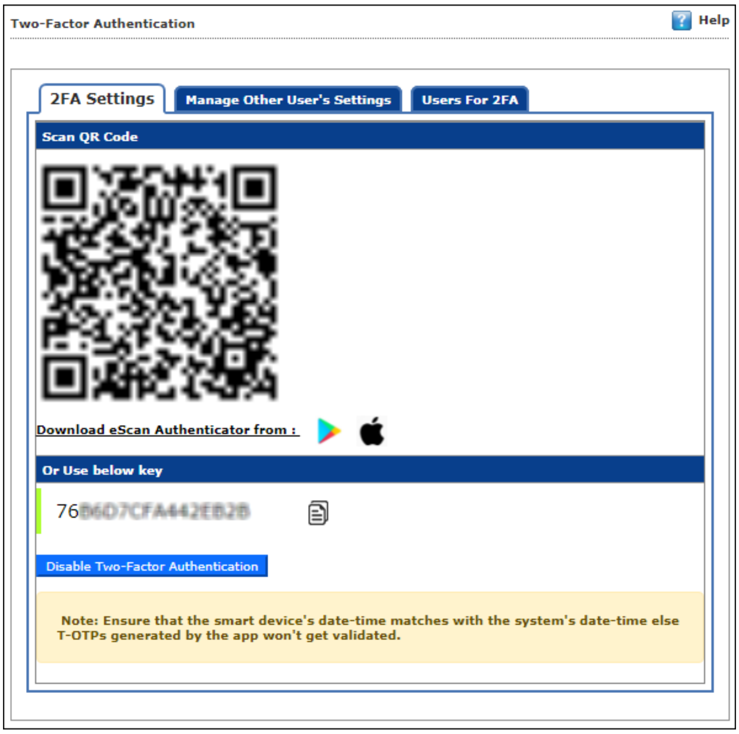
User's name	2FA Status	User Specific QR Code
a[redacted]	✗	View
a[redacted]	✓	View
v[redacted]	✗	View
v[redacted]	✗	View

7. To enable 2FA login for an added user, click the button to check icon.
   The 2FA login for added users gets enabled. After enabling the 2FA login for users, whenever they log in to eScan web console Verify TOTP window appears.
8. To view the QR Code of specific user, click **View** option in the User Specified QR Code column.

Disabling 2FA login

To disable 2FA login:

1. Go to **Settings** > **Two Factor Authentication**.
2. Click **Disable Two-Factor Authentication**.



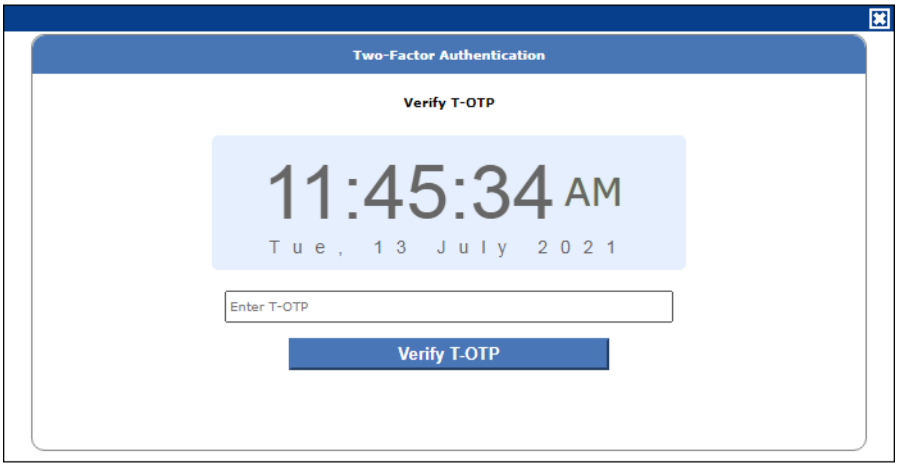
Two-Factor Authentication
Help
2FA Settings
Manage Other User's Settings
Users For 2FA
Scan QR Code
Download eScan Authenticator from :
Or Use below key

76[redacted]

Disable Two-Factor Authentication

Note: Ensure that the smart device's date-time matches with the system's date-time else T-OTPs generated by the app won't get validated.

Verify T-OTP window appears.



Two-Factor Authentication

Verify T-OTP

11:45:34 AM
Tue, 13 July 2021

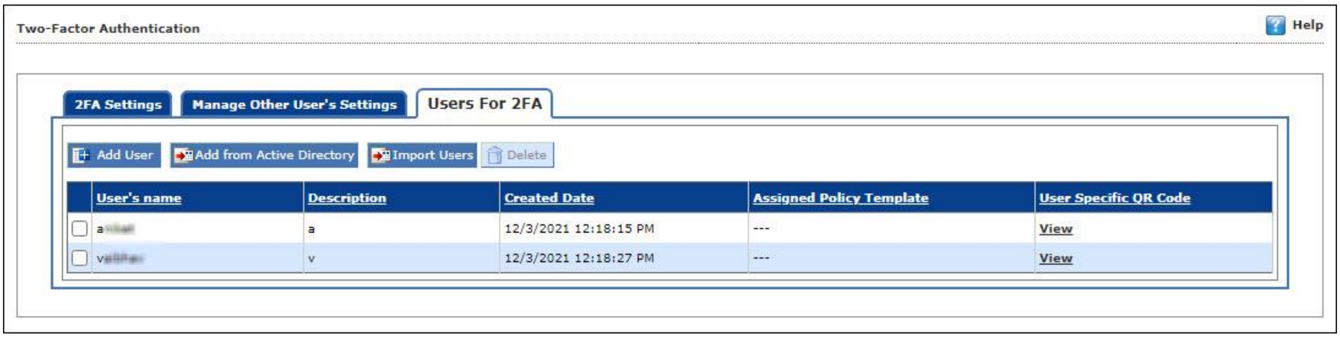
Enter T-OTP

3. Enter the T-OTP and then click **Verify T-OTP**.
   The 2FA feature gets disabled.

NOTE	After disabling the 2FA feature and enabling it again, the 2FA login status will be reinstated for added users.

Users For 2FA

This tab helps to add the users and apply 2FA to the endpoints via policy template. The users can be added directly or from Active Directory.



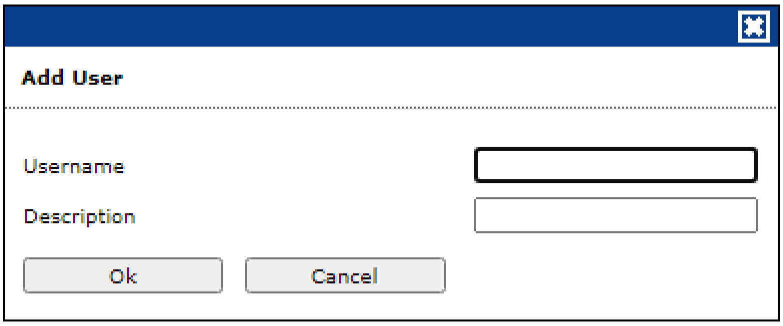
Two-Factor Authentication

	User's name	Description	Created Date	Assigned Policy Template	User Specific QR Code
□	a[redacted]	a	12/3/2021 12:18:15 PM	---	View
□	v[redacted]	v	12/3/2021 12:18:27 PM	---	View

Method 1: Adding user

To add users for the same, follow the below steps:

1. Go to **Settings** > **Two-Factor Authentication** > **Users For 2FA**.
2. Click **Add User**.
   Add User window appears.

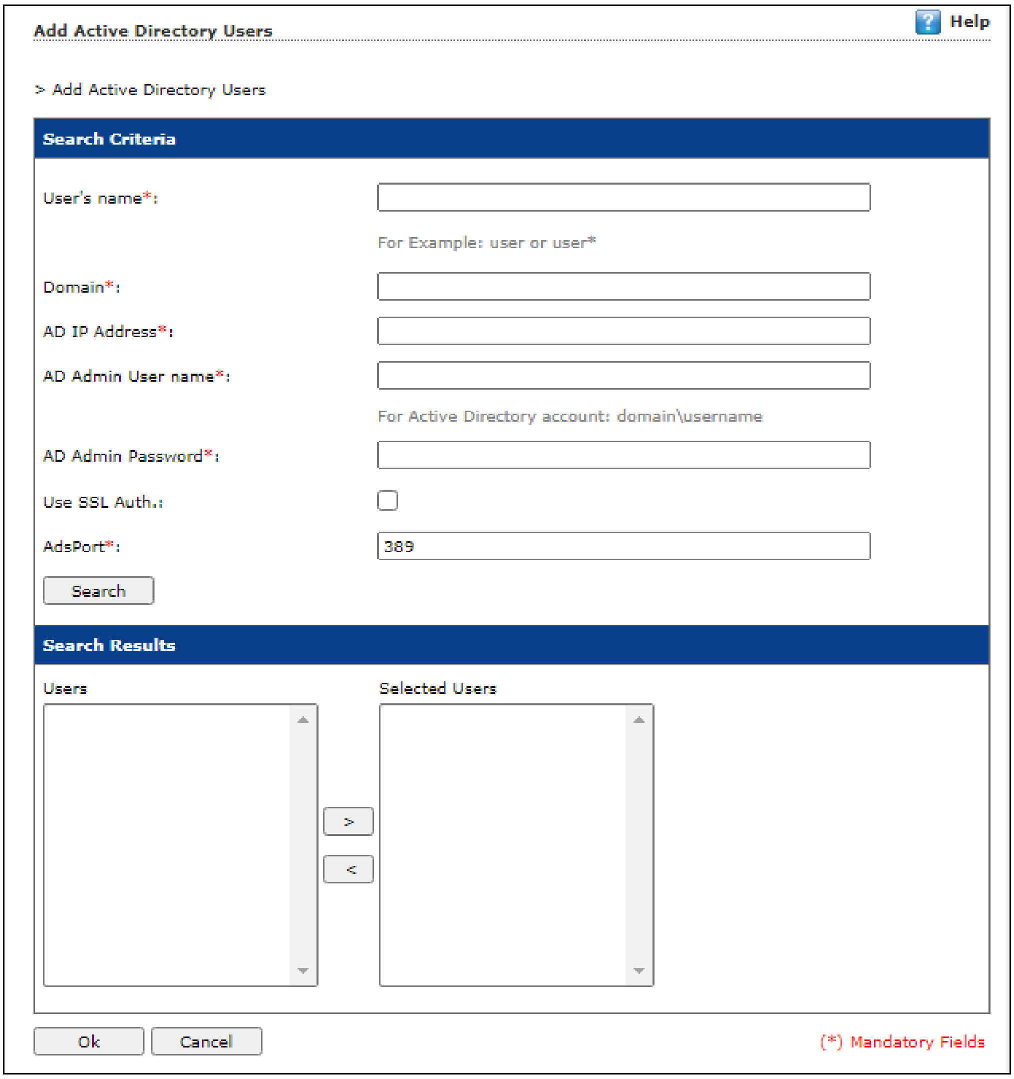


3. Enter the **Username** and **Description**.
4. Click **OK**.

Method 2: 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.



3. Enter the required information.
4. Click **Ok**.
   The Active Directory Users will be added.

Method 3: Importing Users

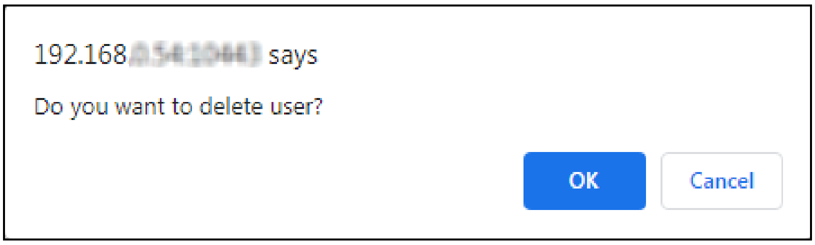
To import the users, follow the below steps:

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.



192.168[redacted] says

Do you want to delete user?

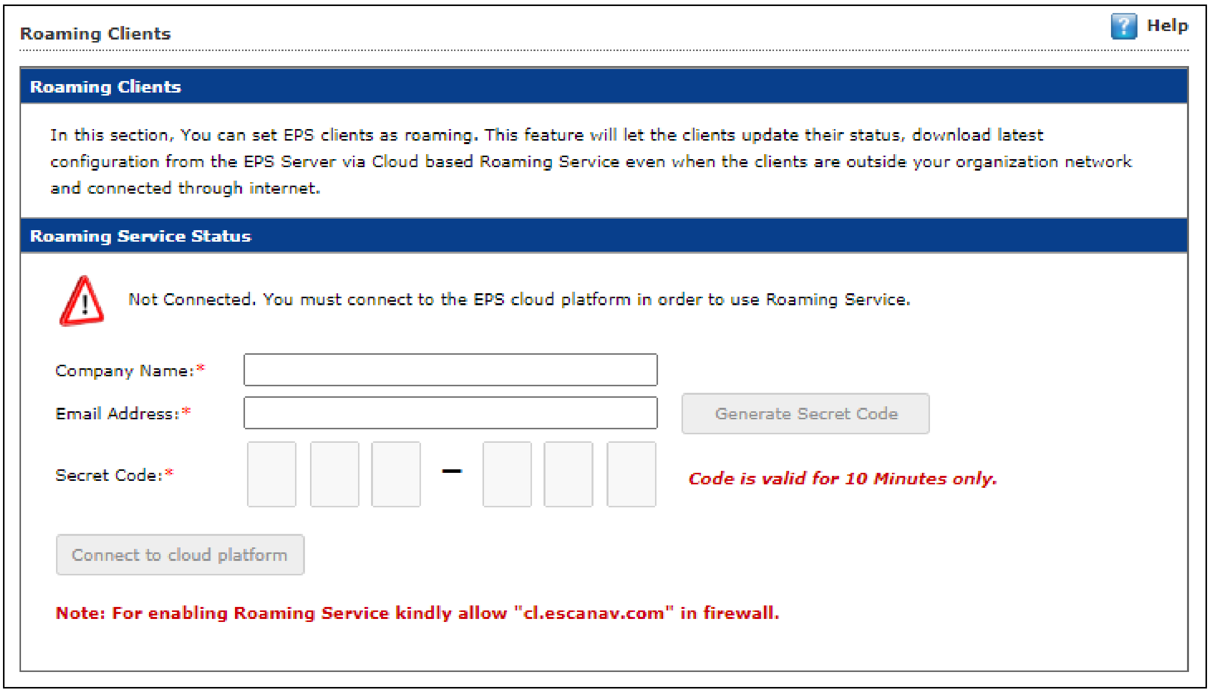
3. Click **OK**.
   The user will be deleted.

Roaming Clients

Roaming Clients submodule provides protection for the remote endpoints when not connected to the organization’s network, adding another layer of security. According to the needs of the business, admins might want to continue the protection of roaming clients on the organization network. Using this feature admin can provide protection via cloud for such clients connected to both organization’s network and the internet.

This feature is quite helpful for the remote clients. Apart from this, it does not require any additional machine set up other than the (on-premise) EPS Server in the network. All the communication is handled by the EPS Server via Cloud to the client with stable internet connection.

Here, the remote clients will update their status and download the latest configuration from the EPS Server via Cloud.



Roaming Clients

Roaming Clients

In this section, You can set EPS clients as roaming. This feature will let the clients update their status, download latest configuration from the EPS Server via Cloud based Roaming Service even when the clients are outside your organization network and connected through internet.

Roaming Service Status

Not Connected. You must connect to the EPS cloud platform in order to use Roaming Service.

Company Name:*

Email Address:*

Secret Code:*

Code is valid for 10 Minutes only.

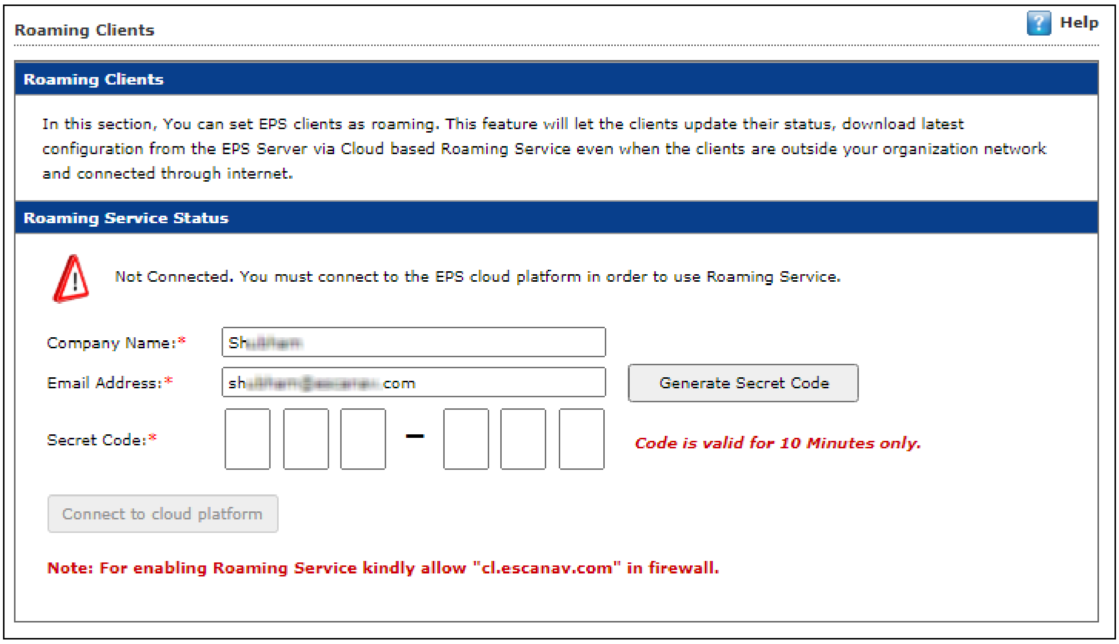
Note: For enabling Roaming Service kindly allow "cl.escanav.com" in firewall.

This service allows admin to apply policies to the client from EPS Server. All events from the clients such as Application Control Scan, Vulnerability Scan, Virus Scan, etc. are collected and managed on EPS server via Cloud Platform.

Adding Roaming Client

To add roaming client, it is mandatory to connect to the Cloud Platform. Follow the below steps, to do the same:

1. Go to **Settings** > **Roaming Clients**.
2. Enter the company name and email address.
3. Click **Generate Secret Code**.



Roaming Clients

Roaming Clients

In this section, You can set EPS clients as roaming. This feature will let the clients update their status, download latest configuration from the EPS Server via Cloud based Roaming Service even when the clients are outside your organization network and connected through internet.

Roaming Service Status

Not Connected. You must connect to the EPS cloud platform in order to use Roaming Service.

Company Name:* Sh[redacted]

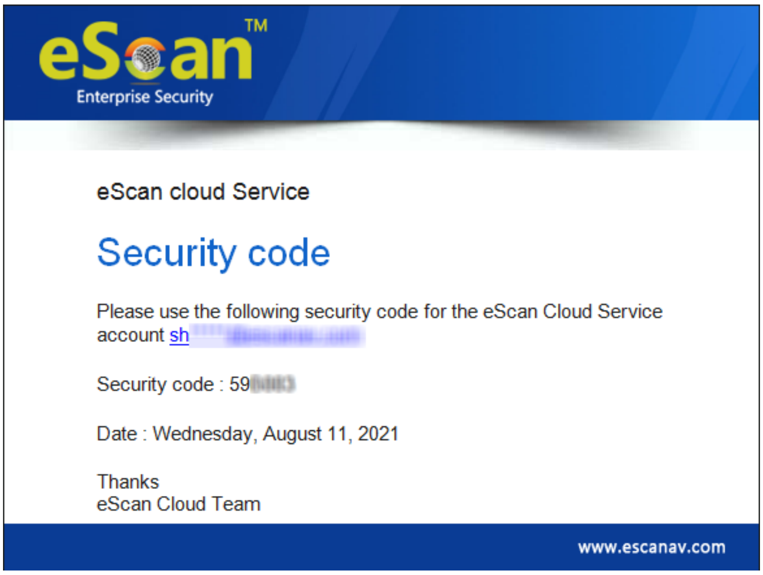
Email Address:* sh[redacted] com

Secret Code:*

Code is valid for 10 Minutes only.

Note: For enabling Roaming Service kindly allow "cl.escanav.com" in firewall.

A secret security code will be generated and sent to given email address.



eScan cloud Service

Security code

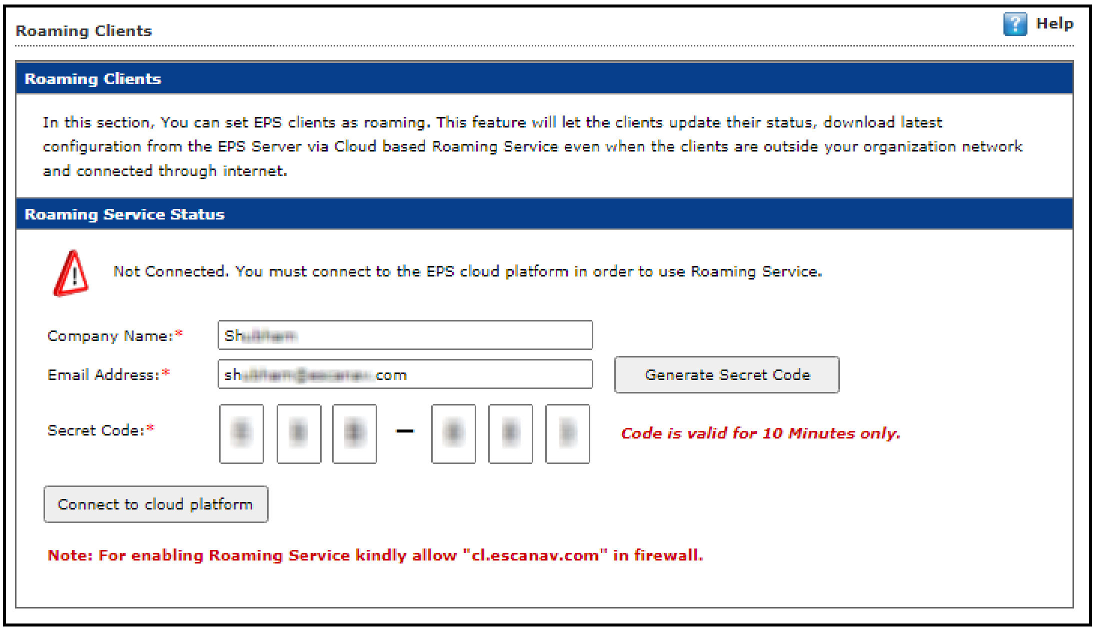
Please use the following security code for the eScan Cloud Service account sh[redacted]

Security code : 59[redacted]

Date : Wednesday, August 11, 2021

Thanks
eScan Cloud Team

4. Enter the secret code received via email, click **Connect to cloud platform**.



Roaming Clients

In this section, You can set EPS clients as roaming. This feature will let the clients update their status, download latest configuration from the EPS Server via Cloud based Roaming Service even when the clients are outside your organization network and connected through internet.

Roaming Service Status

Not Connected. You must connect to the EPS cloud platform in order to use Roaming Service.

Company Name:* Sh[redacted]

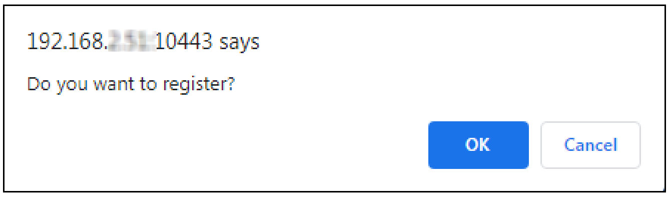
Email Address:* sh[redacted].com

Secret Code:* [redacted] [redacted] [redacted] – [redacted] [redacted] [redacted]

Code is valid for 10 Minutes only.

Note: For enabling Roaming Service kindly allow "cl.escanav.com" in firewall.

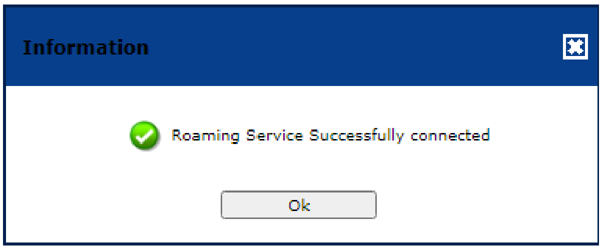
5. A confirmation window appears. Click **OK**, this will authenticate and allows to connect to Cloud Platform.



192.168.[redacted]10443 says

Do you want to register?

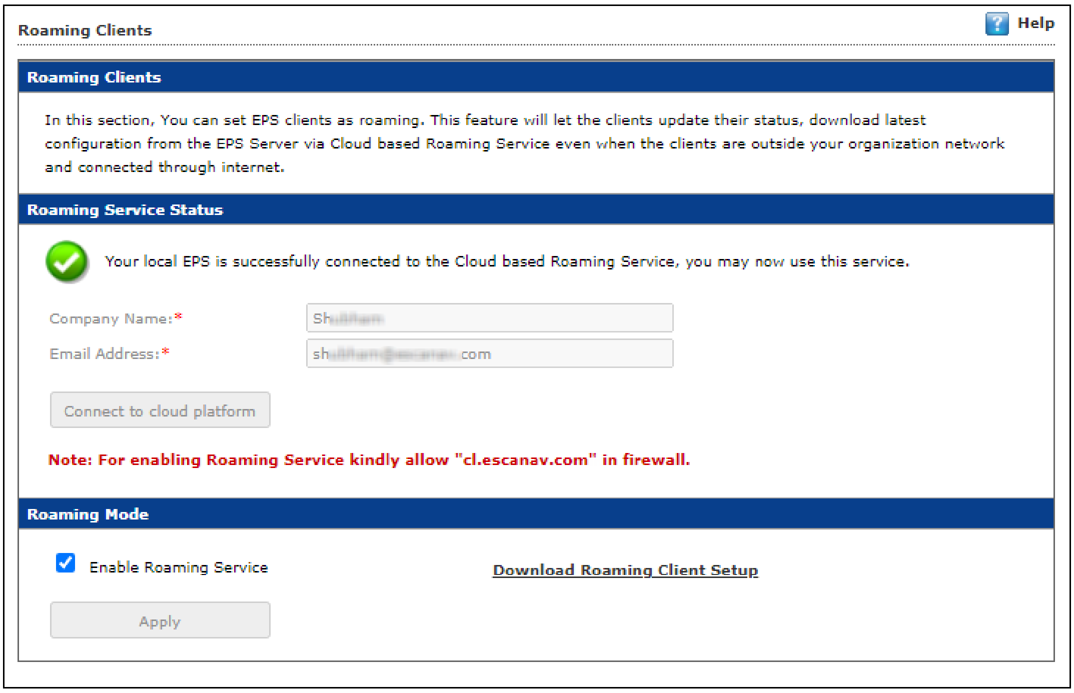
An information window appears.



Information

Roaming Service Successfully connected

6. After connecting to the cloud platform successfully, you can manually enable and disable the roaming service.



Roaming Clients

Roaming Clients

In this section, You can set EPS clients as roaming. This feature will let the clients update their status, download latest configuration from the EPS Server via Cloud based Roaming Service even when the clients are outside your organization network and connected through internet.

Roaming Service Status

Your local EPS is successfully connected to the Cloud based Roaming Service, you may now use this service.

Company Name:* Sh[illegible]

Email Address:* sh[illegible].com

Note: For enabling Roaming Service kindly allow "cl.escanav.com" in firewall.

Roaming Mode

☑ Enable Roaming Service

7. Click **Download Roaming Client Setup** to download the setup file. Install the set up file in the client system to make it as roaming client and it should be connected to the internet.

NOTE	eScan Server should be able to communicate to eScan Cloud Server. To allow communication, make sure the cloud console URL and port is allowed under Gateway Security device. **Port**: 2221 The client system should be connected to the internet.

Installing Roaming Clients

To install Roaming Clients setup, follow the below steps:

1. Go to **Settings** > **Roaming Clients** > **Download Roaming Client Setup**.
2. Transfer the file to the client system.
3. Double-click and install the setup file.
   It will connect to eScan Cloud Server and automatically gets added and managed by eScan EPS Server.

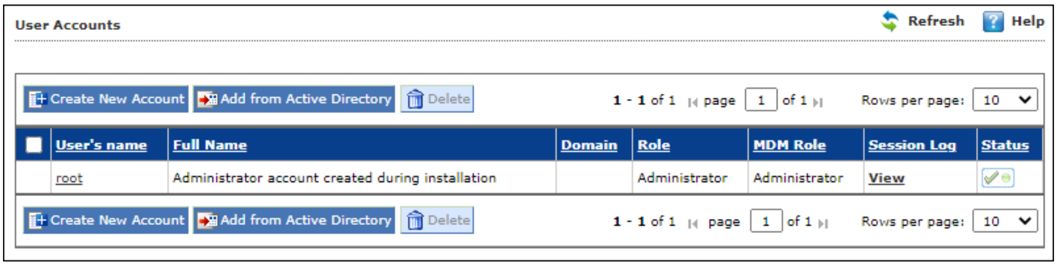
Administration

The Administration module lets you create User Accounts and allocate them Admin rights for using eScan Management Console. In a large organization, installing eScan client on all computers may consume lot of time and efforts. With this option, you can allocate rights to the other employees and allow them to install eScan Client, implement Policies and Tasks.
The Administration module consists following submodules:

- **User Accounts**
- **User Roles**
- **Export & Import**
- **Customize Setup**
- **Audit Trail**

User Accounts

For a large organization, installing eScan Client and monitoring activities may become a difficult task. With User Accounts submodule, you can create new user accounts and assign Administrator role to added users and reduce the workload. This submodule displays a list of users and their details like Domain, Role, Session Log and Status.



1 - 1 of 1 page 1 of 1 Rows per page: 10

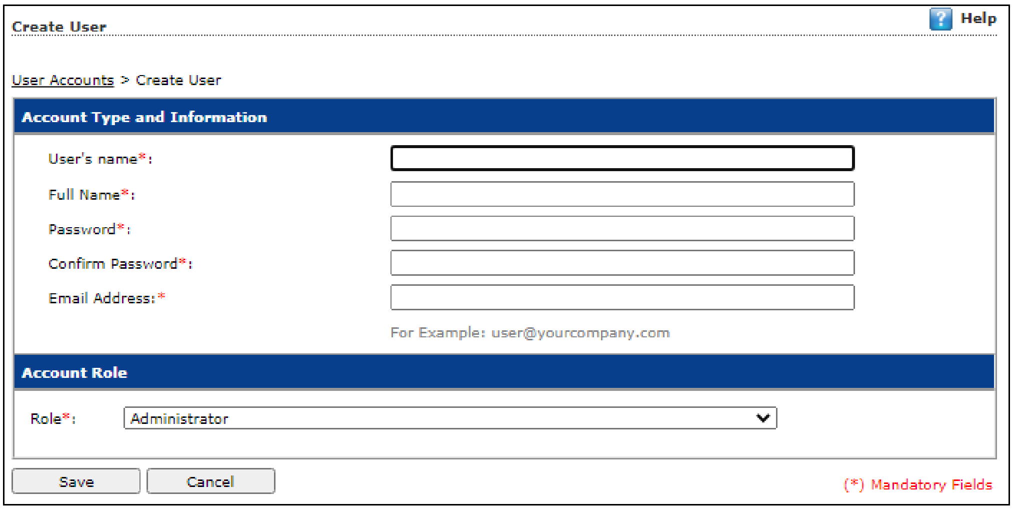
□	User's name	Full Name	Domain	Role	MDM Role	Session Log	Status
	root	Administrator account created during installation		Administrator	Administrator	View	✓

1 - 1 of 1 page 1 of 1 Rows per page: 10

Create New Account

To create a User Account:

1. In the User Accounts screen, click **Create New Account**.
   Create User window appears.



Account Type and Information

User's name*:
Full Name*:
Password*:
Confirm Password*:
Email Address:*
For Example: user@yourcompany.com

Account Role

Role*: Administrator

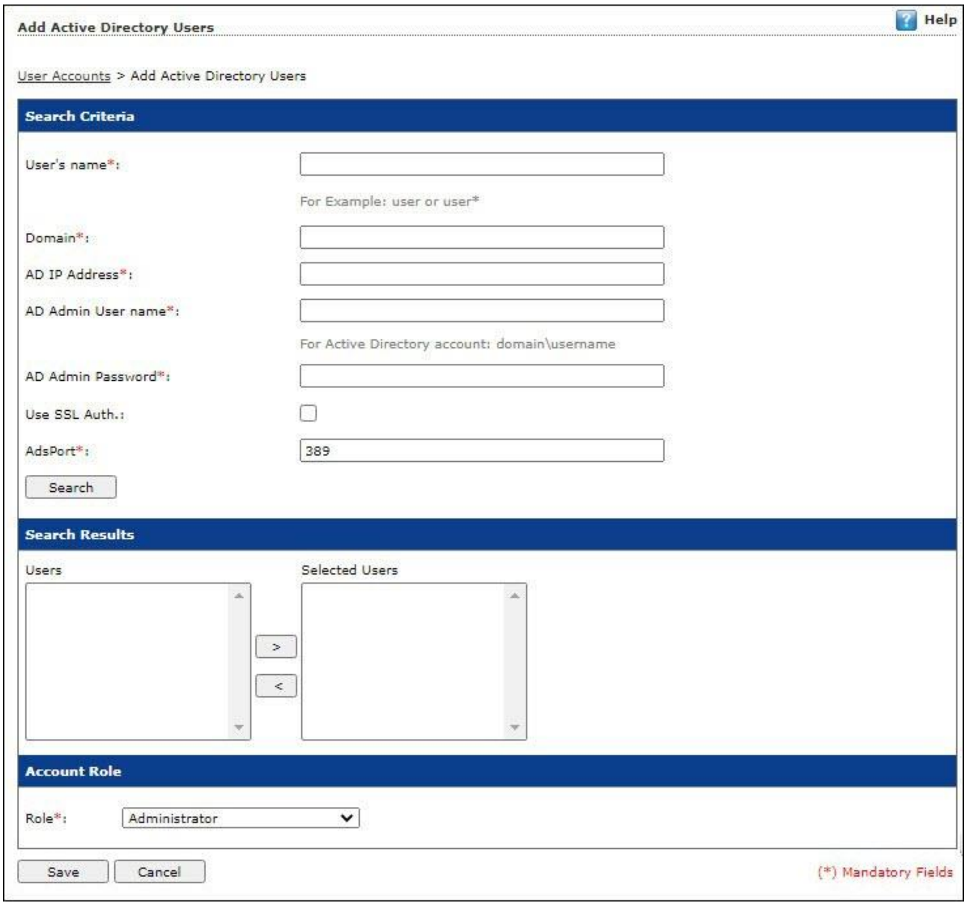
(*) Mandatory Fields

2. After filling all the details, click **Save**.
   The user will be added to the User Accounts list.

Adding Users from Active Directory

To add users from the Active Directory (AD), follow the steps below:

1. In the User Accounts screen, click **Add from Active Directory**.
   Add Active Directory Users window appears.



Add Active Directory Users

User Accounts > 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*: 389

Search Results

Users

Selected Users

Account Role

Role*: Administrator

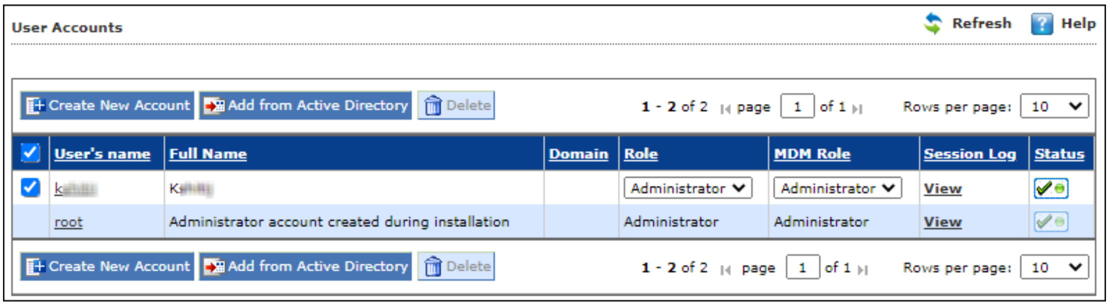
(*) Mandatory Fields

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. Select appropriate user role and MDM role using provided drop-downs in Account Role section.
7. Click **Save**.
   The user will be added to the User Accounts list.

Delete a User Account

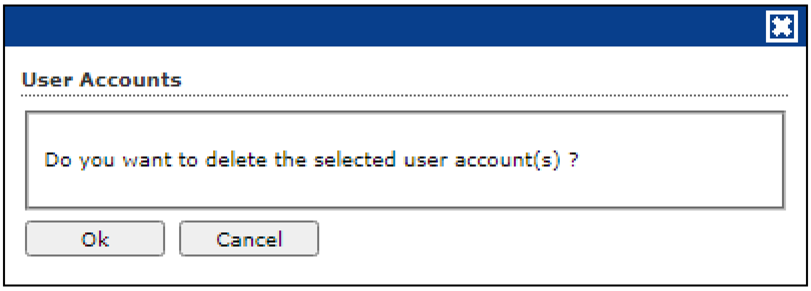
To delete a user account:

1. In the User Accounts screen, select the user you want to delete.



☑	User's name	Full Name	Domain	Role	MDM Role	Session Log	Status
☑	[redacted]	[redacted]		Administrator	Administrator	View	✓
	root	Administrator account created during installation		Administrator	Administrator	View	✓

2. Click **Delete**.
   A confirmation prompt appears.

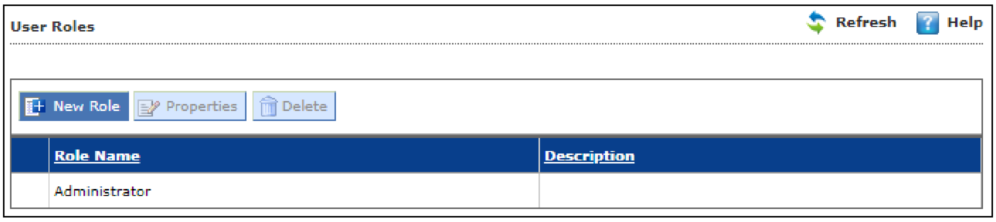


Do you want to delete the selected user account(s) ?

3. Click **OK**.
   The User Account will be deleted.

User Roles

The User Roles submodule lets you create a role and assign it to the **User Accounts** with variable permissions and rights as defined in the role being assigned to them. It can be an Administrator role with set of permissions and rights, Group Admin Role or a Read only Role.



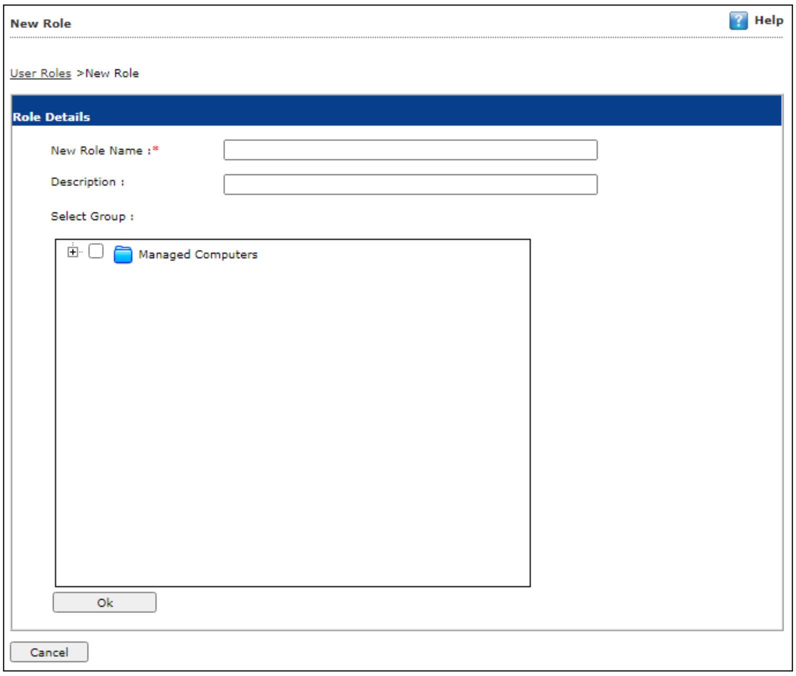
Role Name	Description
Administrator	

You can re-define the Properties of the created role for configuring access to various section of eScan Management Console and the networked Computers. It also lets you delete any existing role after the task is completed by them. It allows the administrator to give permission to sub administrators to access defined modules of eScan and perform installation/uninstallation of eScan Client on network computers or define Policies and tasks for the computers allocated to them.

New Role

To add a user role:

1. In the User Roles screen, click **New Role**.
   New Role form appears.



New Role

Help

User Roles >New Role

Role Details

New Role Name :*

Description :

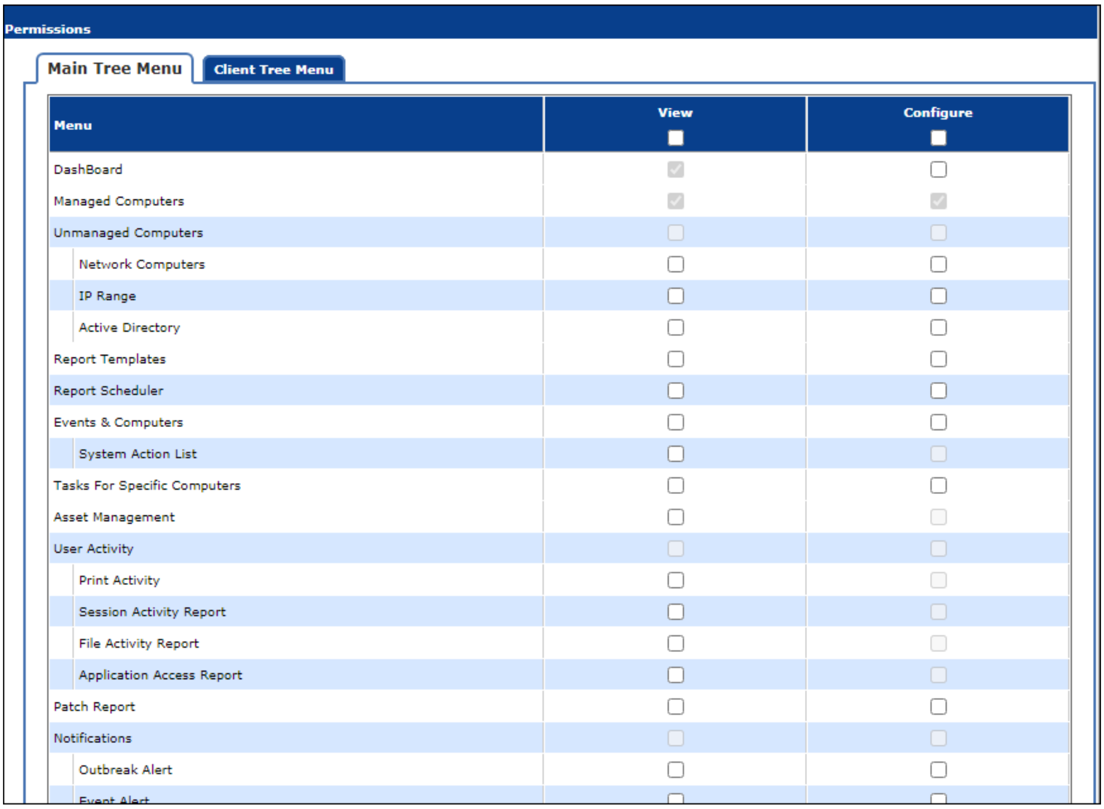
Select Group :

⊞ □ Managed Computers

Ok

Cancel

2. Enter name and description for the role.
3. Click **Managed Computers** and select the specific group to assign the role.
   The added role will be able to manage and monitor only the selected group's activities.
4. Click **OK.**
   Permissions section appears displaying Main Tree Menu and Client Tree Menu tabs. The Main Tree Menu consists of Navigation Panel Access permissions while the Client Tree Menu consists the permissions for selected group(s) that the user is allowed to take further.



Permissions

Main Tree Menu | Client Tree Menu

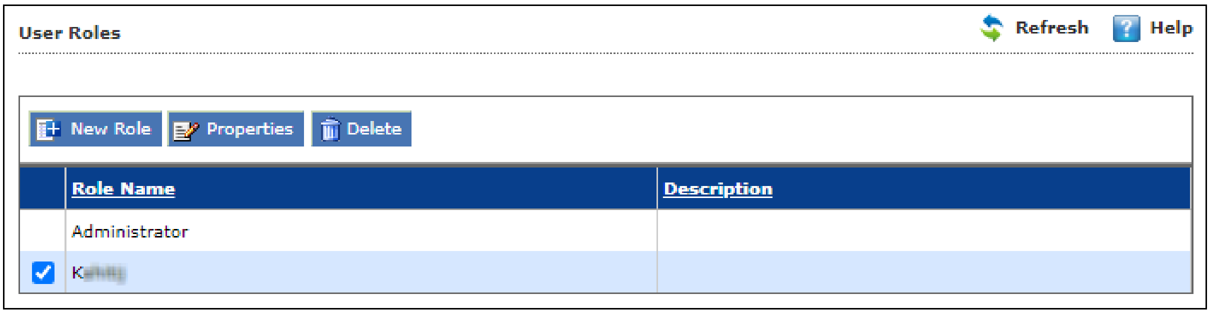
Menu	View □	Configure □
DashBoard	☑	□
Managed Computers	☑	☑
Unmanaged Computers	□	□
Network Computers	□	□
IP Range	□	□
Active Directory	□	□
Report Templates	□	□
Report Scheduler	□	□
Events & Computers	□	□
System Action List	□	□
Tasks For Specific Computers	□	□
Asset Management	□	□
User Activity	□	□
Print Activity	□	□
Session Activity Report	□	□
File Activity Report	□	□
Application Access Report	□	□
Patch Report	□	□
Notifications	□	□
Outbreak Alert	□	□
Event Alert	□	□

5. Select the checkboxes that will allow the role to view/configure the module.
6. After selecting the necessary checkboxes, click **Save**.
   The role will be added to the User Roles list.

View Role Properties

To view the properties of a role:

1. In the User Roles screen, select a role.
2. This enables **Properties** and **Delete** buttons.



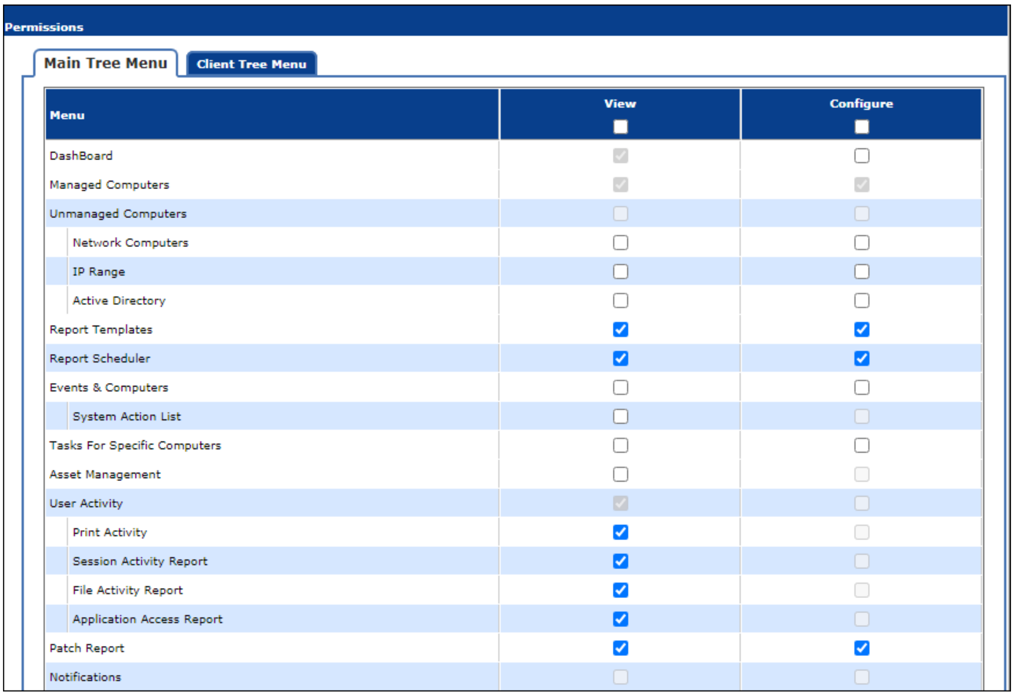
User Roles

Refresh   Help

New Role   Properties   Delete

	Role Name	Description
□	Administrator	
☑	K[redacted]	

3. Click **Properties**.
   Properties screen appears. It lets you modify role description, permissions for accessing and configuring modules and assign the role to other groups by clicking **Select Group Tree**.



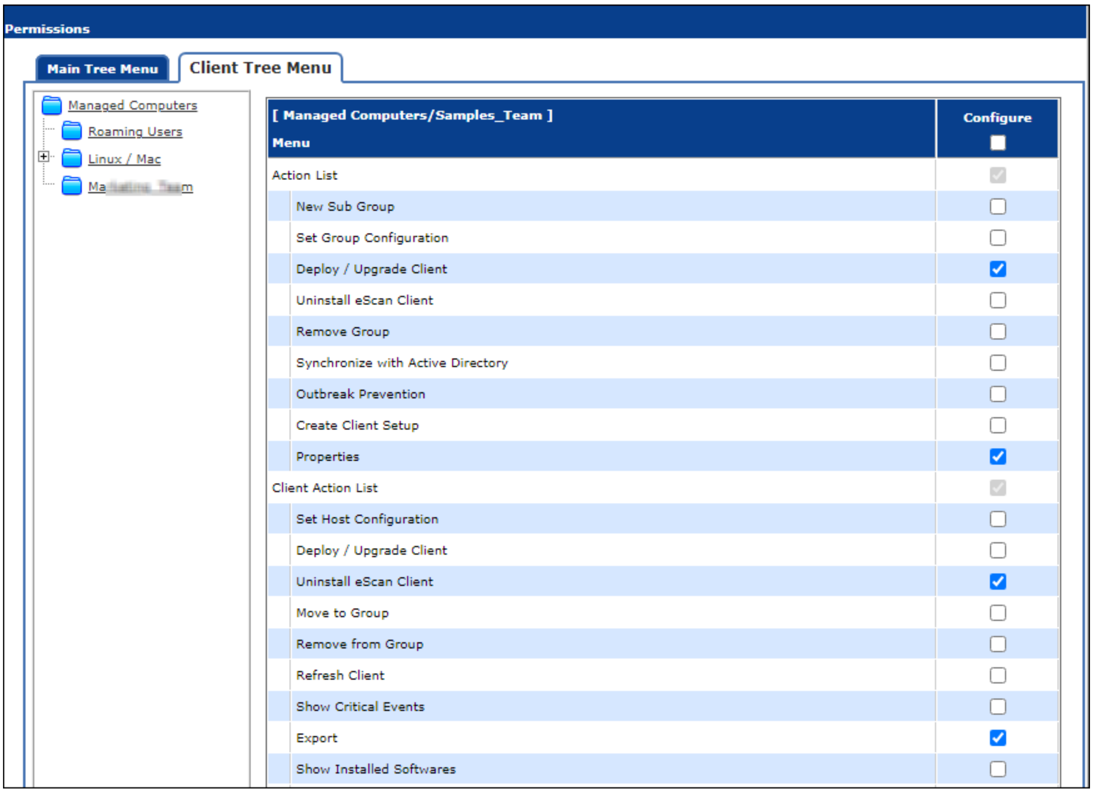
Permissions

Main Tree Menu   Client Tree Menu

Menu	View □	Configure □
DashBoard	☑	□
Managed Computers	☑	☑
Unmanaged Computers	□	□
Network Computers	□	□
IP Range	□	□
Active Directory	□	□
Report Templates	☑	☑
Report Scheduler	☑	☑
Events & Computers	□	□
System Action List	□	□
Tasks For Specific Computers	□	□
Asset Management	□	□
User Activity	☑	□
Print Activity	☑	□
Session Activity Report	☑	□
File Activity Report	☑	□
Application Access Report	☑	□
Patch Report	☑	☑
Notifications	□	□

4. To modify client configuration permissions, click **Client Tree Menu**.
   Client Tree Menu

Define the Actions that the created role can configure for the allocated group. The menu has Action List, Client Action List, Select Policy Template, Policy Criteria, and Group Tasks.



Permissions

Main Tree Menu | Client Tree Menu

- Managed Computers
  - Roaming Users
  - Linux / Mac
  - Ma[redacted]

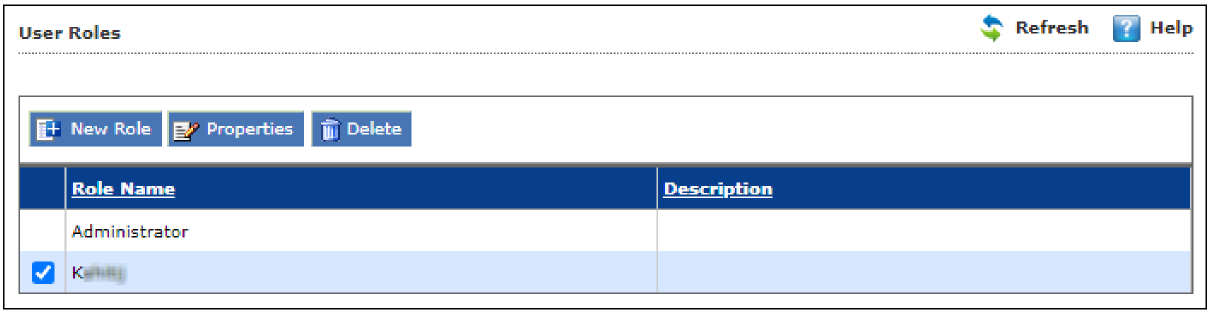
[Managed Computers/Samples_Team] Menu	Configure □
Action List	☑
New Sub Group	□
Set Group Configuration	□
Deploy / Upgrade Client	☑
Uninstall eScan Client	□
Remove Group	□
Synchronize with Active Directory	□
Outbreak Prevention	□
Create Client Setup	□
Properties	☑
Client Action List	☑
Set Host Configuration	□
Deploy / Upgrade Client	□
Uninstall eScan Client	☑
Move to Group	□
Remove from Group	□
Refresh Client	□
Show Critical Events	□
Export	☑
Show Installed Softwares	□

5. To let the role configure these actions, under the Configure column select the checkboxes of corresponding actions.
6. Click **Save**.
   The Role Properties will be updated accordingly.

Delete a User Role

To delete a user role:

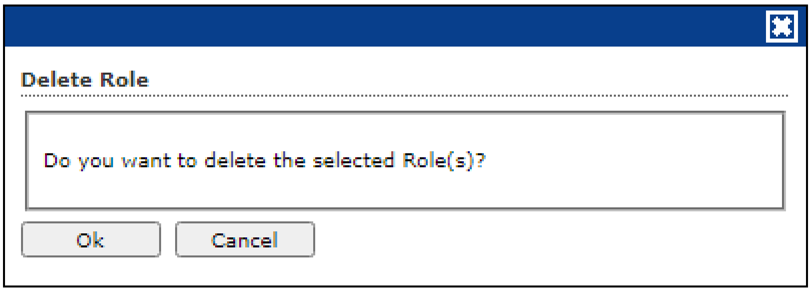
1. In the User Roles screen, select the user role you want to delete**.**



User Roles

	Role Name	Description
	Administrator	
☑	K[redacted]	

2. Click **Delete**.
   A delete confirmation prompt appears.



Delete Role

Do you want to delete the selected Role(s)?

3. Click **OK**.
   The User Role will be deleted.

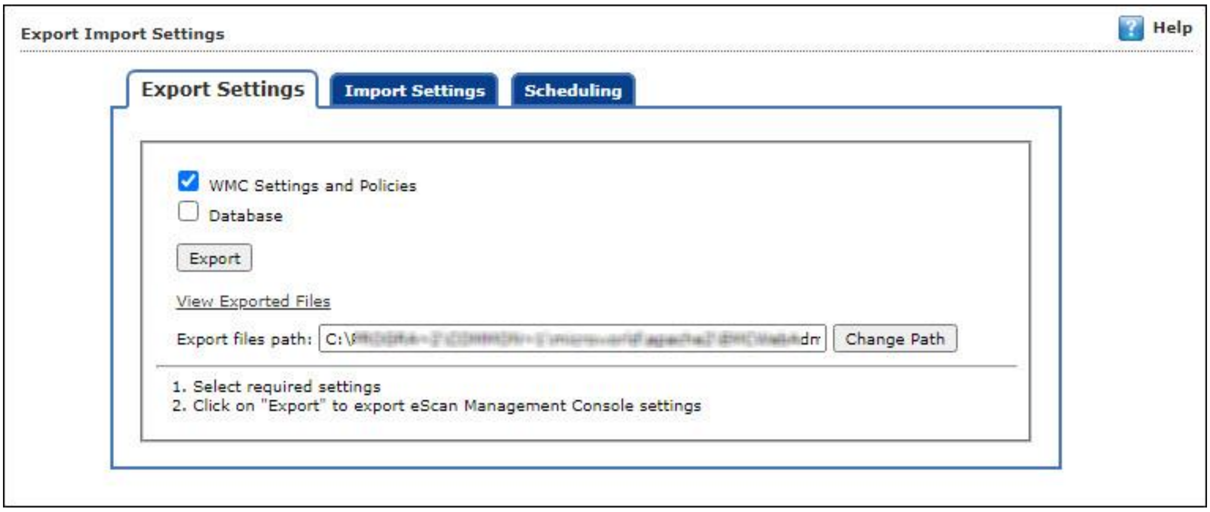
Export & Import

The Export & Import submodule lets you to take a backup of your eScan server settings, in case you want to replace the existing eScan server. You can export the Settings, Policies and the Database from existing server to a local drive and import it to the new server.

Export Settings

This tab lets you export the eScan Server Settings, Policies, and Database. To export the eScan Server settings, follow the steps given below:

1. In the Export Import Settings screen, click **Export Settings** tab.



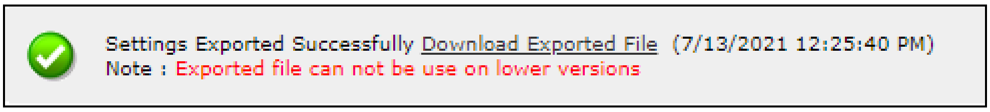
Export Import Settings

☑ WMC Settings and Policies
☐ Database

Export files path: C:\[redacted]

1. Select required settings
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**. In the Add Folder window, enter the file path and click **Add**.
3. Click **Export**.
   The backup file will be exported to the destination path. A success message appears at the top displaying date, time, and a download link for the exported file.

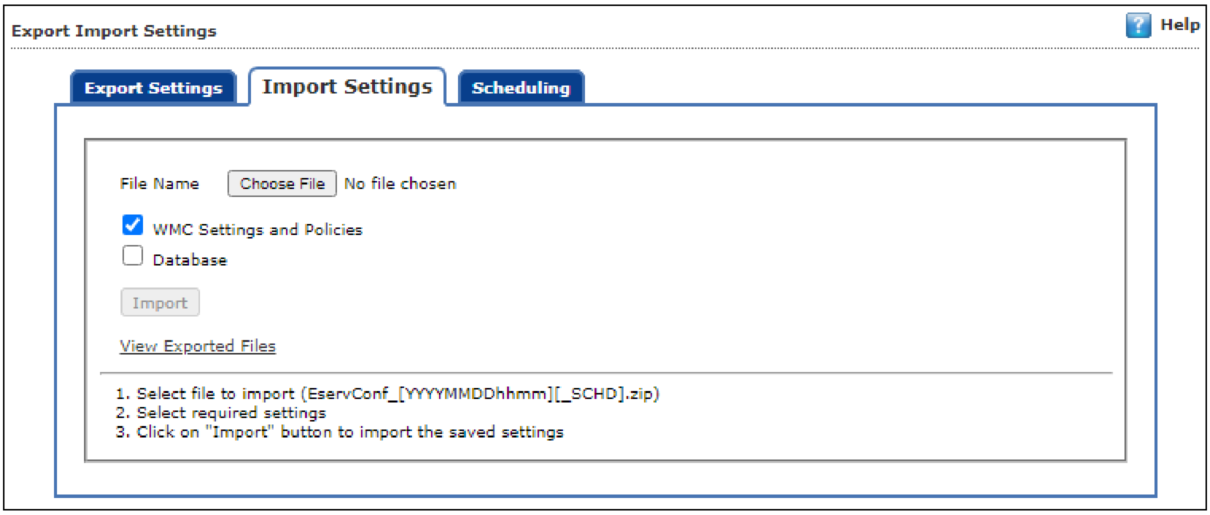


Settings Exported Successfully Download Exported File (7/13/2021 12:25:40 PM)
Note : Exported file can not be use on lower versions

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.



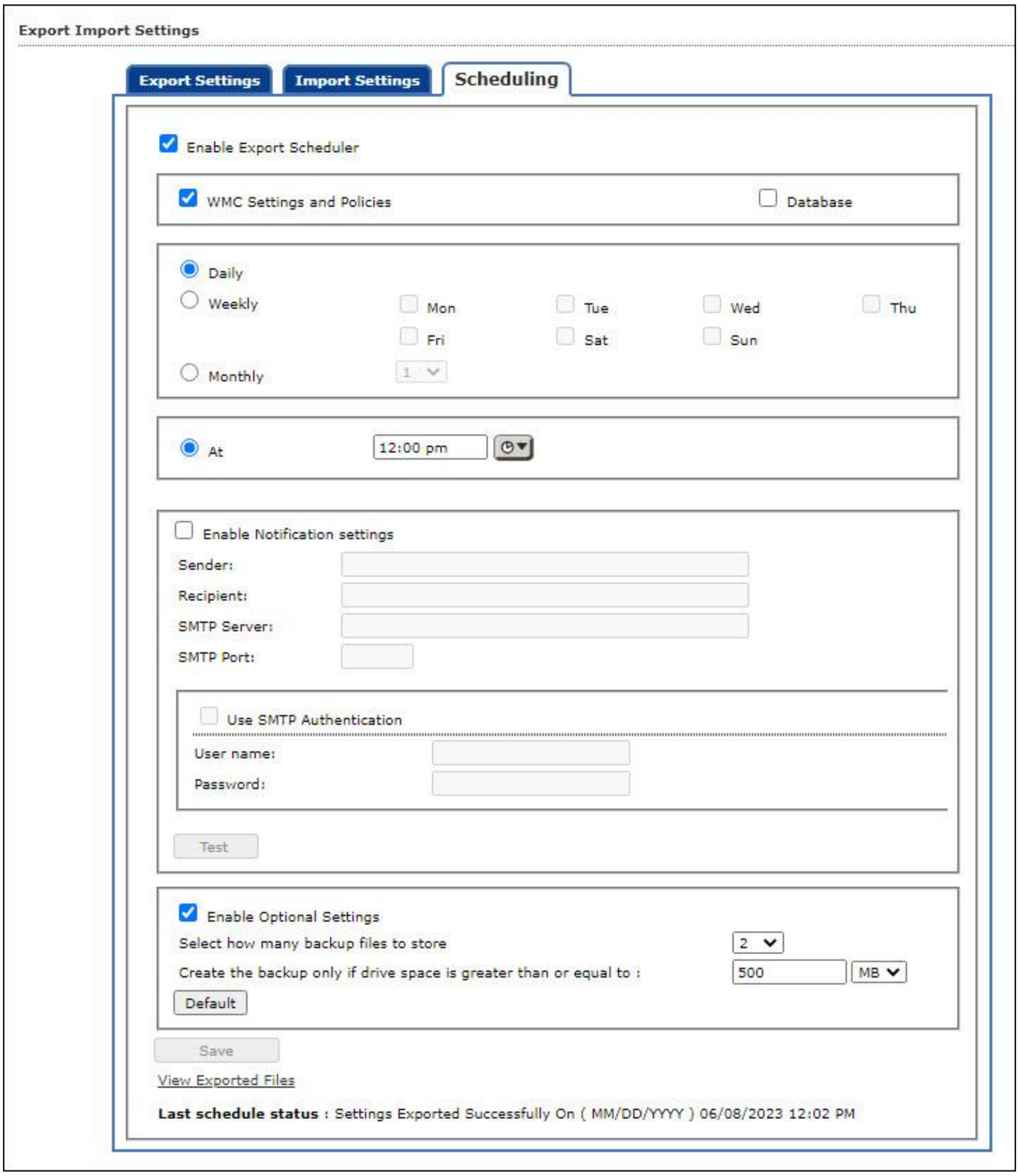
1. Select file to import (EservConf_[YYYYMMDDhhmm][_SCHD].zip)
2. Select required settings
3. Click on "Import" button to import the saved settings

2. Click **Choose File**.
3. To import **WMC Settings and Policies** and **Database**, select both the checkboxes.
4. Click **Import**.
   The backup file will be imported. A success message is displayed after complete import.

NOTE	- After successfully taking a backup, eScan asks you to restart the server. - The Import Settings tab lets you import only Settings and Policies or Database.

Scheduling

This tab lets you schedule auto-backing up of Settings, Policies, and Database.



Export Import Settings

☑ Enable Export Scheduler

☑ WMC Settings and Policies ☐ Database

● Daily
○ Weekly ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun
○ Monthly 1

● At 12:00 pm

☐ Enable Notification settings

Sender:
Recipient:
SMTP Server:
SMTP Port:

☐ Use SMTP Authentication

User name:
Password:

☑ Enable Optional Settings

Select how many backup files to store: 2

Create the backup only if drive space is greater than or equal to : 500 MB

Last schedule status : Settings Exported Successfully On (MM/DD/YYYY) 06/08/2023 12:02 PM

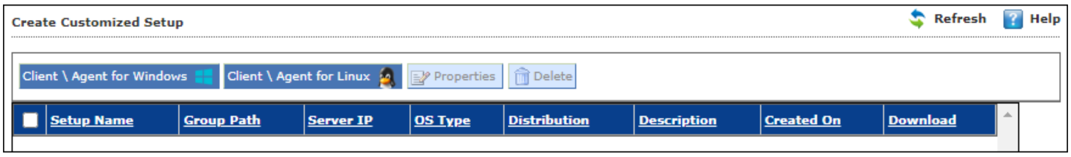
To create a Schedule for export, follow the steps given below:

1. Select **Enable Export Scheduler** checkbox.
2. Select the checkboxes whether to back up both Settings and Policies and Database.
3. Schedule the backup for a **Daily**, **Weekly** (Select a day) or **Monthly** (Select a date) basis.
4. For the **At** field, click the drop-down and select a time for backing up data.
   If you want to receive email notifications about the procedure, select Enable Notifications Settings checkbox and fill in the necessary details. If the SMTP server requires authentication, select the Use SMTP Authentication checkbox and enter the credentials. To check if the SMTP settings are correct, click **Test**. A test email will be sent to recipient email ID.
   To configure additional settings for backup file, select the Enable Optional Settings, and make the necessary changes. To restore the changes made, click **Default**.

5. After performing all the necessary steps, click **Save**.
   The export schedule will be saved.

Customize Setup

This submodule lets you create a customized setup for a Client or an Agent with fewer modules and deploy it to various locations. This can be very useful, if there are locations to which a server is unable to push the setup or locations that are unable to connect to the server directly. The custom setup can be downloaded as a file and sent to different locations.

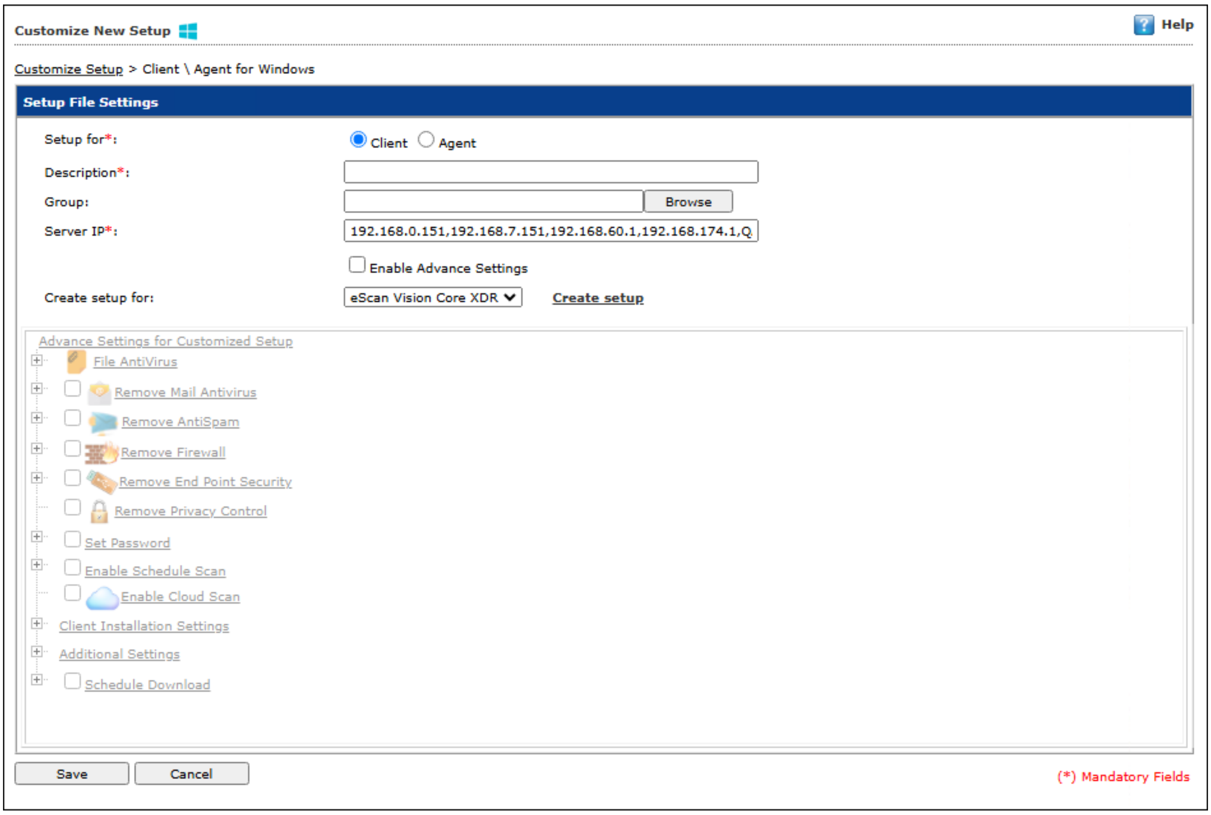


☐	Setup Name	Group Path	Server IP	OS Type	Distribution	Description	Created On	Download

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.



Setup for*: ● Client ○ Agent

Description*:

Group:

Server IP*: 192.168.0.151,192.168.7.151,192.168.60.1,192.168.174.1,Q

☐ Enable Advance Settings

Create setup for: eScan Vision Core XDR

Advance Settings for Customized Setup
- File AntiVirus
- ☐ Remove Mail Antivirus
- ☐ Remove AntiSpam
- ☐ Remove Firewall
- ☐ Remove End Point Security
- ☐ Remove Privacy Control
- ☐ Set Password
- ☐ Enable Schedule Scan
- ☐ Enable Cloud Scan
- Client Installation Settings
- Additional Settings
- ☐ Schedule Download

(*) Mandatory Fields

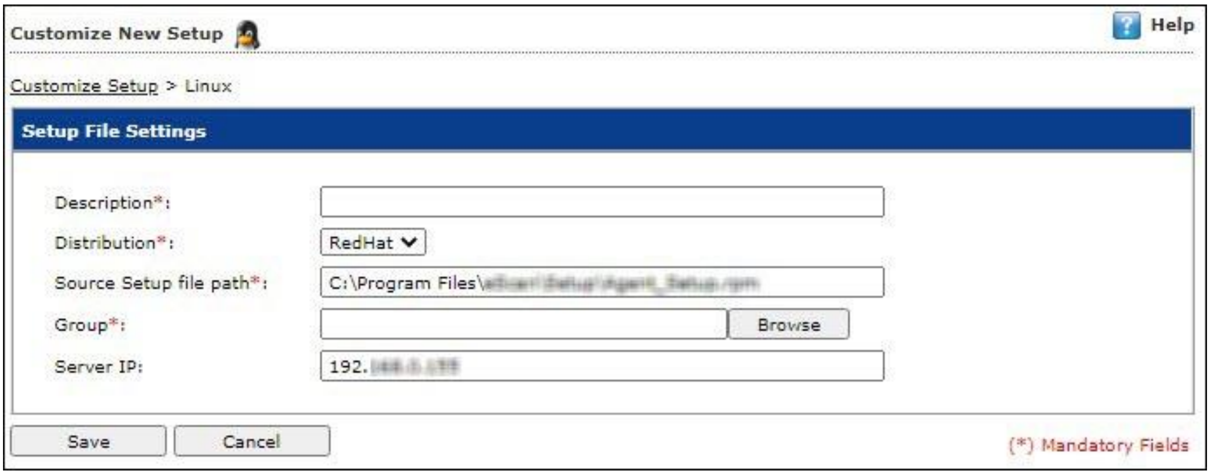
2. Select whether the setup file is being created for **Client** or **Agent**.
3. Enter description for the setup file.
4. Click **Browse** and select a group for which this setup is being created.
5. Enter eScan Server IP address.

6. If you want to provide advanced settings with the setup, select the **Enable Advance Settings** checkbox. Doing so enables the bottom field.
7. Select the product from provided drop-down list for which this setup is being created. Or else, click on Create setup to setting up new setup or selecting from existing setups.
8. Select the settings' checkboxes you want to provide.
9. Click **Save**.
   The customized setup for Windows will be created.

Creating a customized setup for Linux

To create a customized setup for Linux, follow the steps given below:

1. In Create Customized Setup screen, click **Client\Agent for Linux**.
   Customize New Setup screen appears.



Customize New Setup

Customize Setup > Linux

Setup File Settings

Description*:

Distribution*: RedHat

Source Setup file path*: C:\Program Files\[redacted]

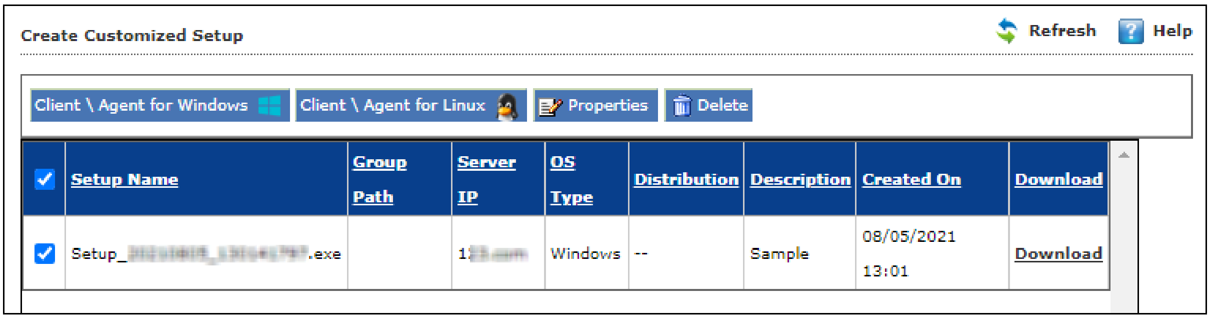
Group*:

Server IP: 192.[redacted]

2. Enter a description for the setup.
3. Click on the Distribution drop-down to select whether the setup is to be created for Red Hat or Debian.
4. Source Setup file path field displays the setup file's location. If you want to change path, enter the new path in this field.
5. Click **Browse** and select a group for which this setup is being created.
6. Enter eScan Server IP address.
7. Click **Save**.
   The customized setup for Linux will be created.

Editing Setup Properties (only Windows)

The properties can be edited for only customized Windows setup. To edit the customized Windows setup's properties, follow the steps given below:



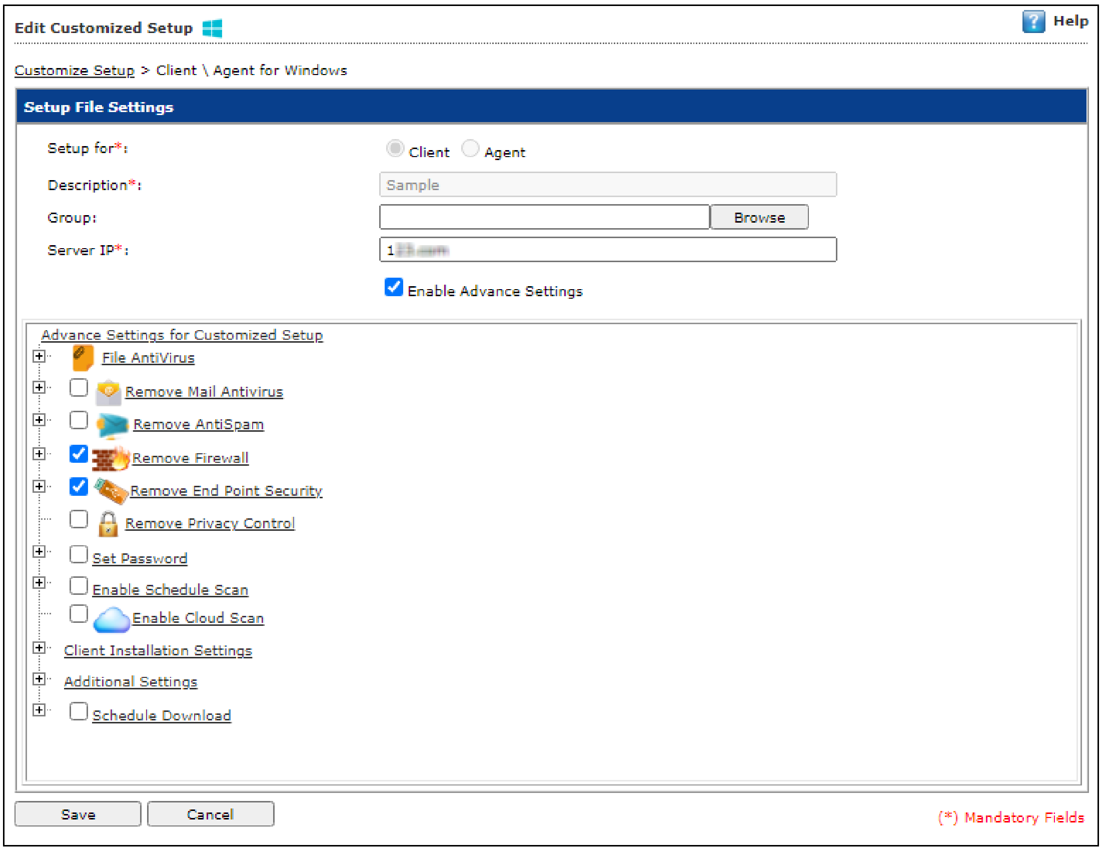
Create Customized Setup

Refresh | Help

Client \ Agent for Windows | Client \ Agent for Linux | Properties | Delete

☑	Setup Name	Group Path	Server IP	OS Type	Distribution	Description	Created On	Download
☑	Setup_[redacted].exe		1[redacted]	Windows	--	Sample	08/05/2021 13:01	Download

1. In the Create Customized Setup screen, select the Windows setup you want to edit.
2. Click **Properties**.
   Edit Customized Setup screen appears.



Edit Customized Setup

Help

Customize Setup > Client \ Agent for Windows

Setup File Settings

Setup for*: ● Client ○ Agent

Description*: Sample

Group: [ ] Browse

Server IP*: 1[redacted]

☑ Enable Advance Settings

Advance Settings for Customized Setup

- File AntiVirus
- □ Remove Mail Antivirus
- □ Remove AntiSpam
- ☑ Remove Firewall
- ☑ Remove End Point Security
- □ Remove Privacy Control
- □ Set Password
- □ Enable Schedule Scan
- □ Enable Cloud Scan
- Client Installation Settings
- Additional Settings
- □ Schedule Download

Save | Cancel

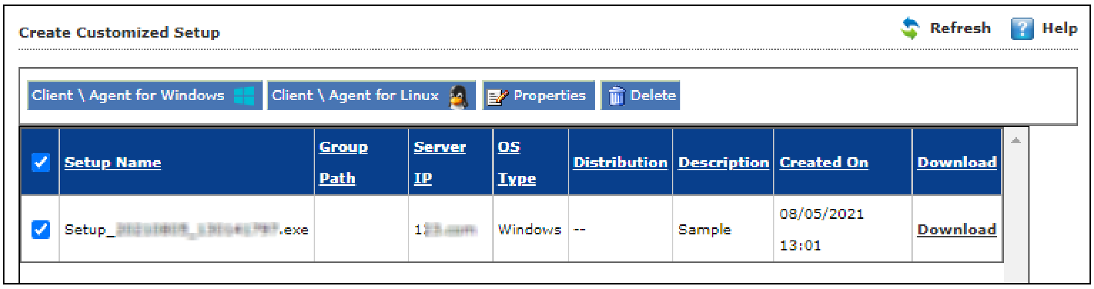
(*) Mandatory Fields

3. Make the necessary changes and then click **Save**. The setup will be updated.

Deleting a Setup

To delete a setup, follow the steps given below:

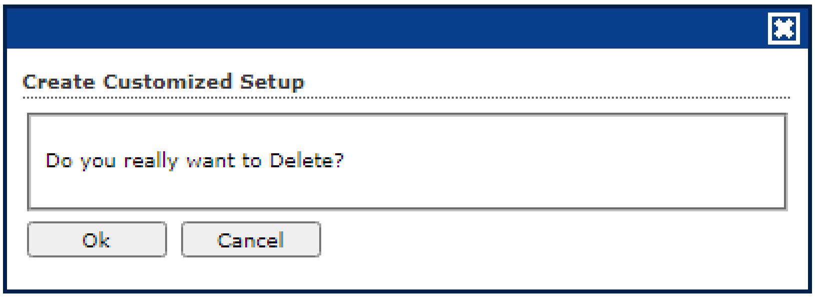
1. In the Create Customized Setup screen, select the setup you want to delete.



Create Customized Setup

☑	Setup Name	Group Path	Server IP	OS Type	Distribution	Description	Created On	Download
☑	Setup_[redacted].exe		1[redacted]	Windows	--	Sample	08/05/2021 13:01	Download

2. Click **Delete**.
   A confirmation window appears.



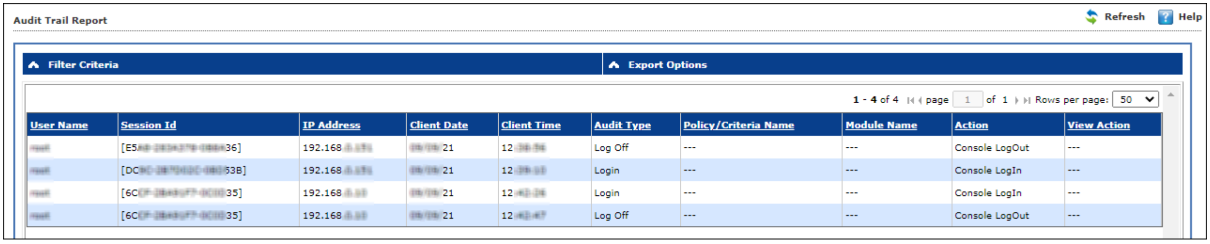
Create Customized Setup

Do you really want to Delete?

3. Click **Ok**.
   The setup will be deleted.

Audit Trail

The Audit Trail submodule lets you record the security relevant data, operation, event, Action, policy updates. Audit logs are used to track the date, time and activity of each user, including the policy/criteria that have been changed. A record of the changes that have been made to a database. You can get audit trail of user activity across all these systems.



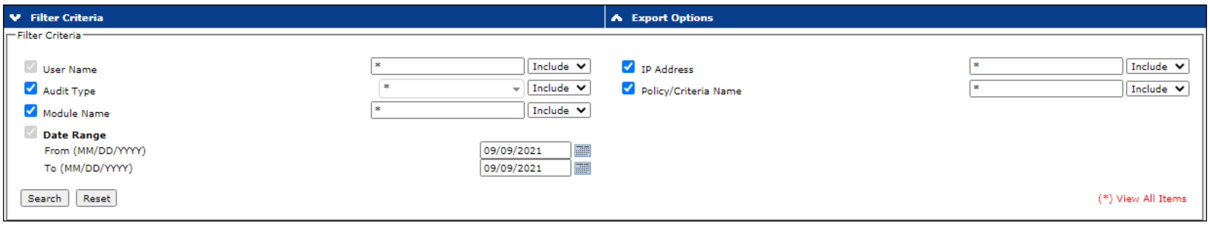
Audit Trail Report

1 - 4 of 4 page 1 of 1 Rows per page: 50

User Name	Session Id	IP Address	Client Date	Client Time	Audit Type	Policy/Criteria Name	Module Name	Action	View Action
[redacted]	[E5[redacted]36]	192.168[redacted]	[redacted]21	12[redacted]	Log Off	---	---	Console LogOut	---
[redacted]	[DC[redacted]53B]	192.168[redacted]	[redacted]21	12[redacted]	Login	---	---	Console LogIn	---
[redacted]	[6C[redacted]35]	192.168[redacted]	[redacted]21	12[redacted]	Login	---	---	Console LogIn	---
[redacted]	[6C[redacted]35]	192.168[redacted]	[redacted]21	12[redacted]	Log Off	---	---	Console LogOut	---

Filter all Audit Trail report

To filter the Audit Trail Report as per your requirements, click **Filter Criteria** drop-down.
Filter Criteria field expands.



Filter Criteria

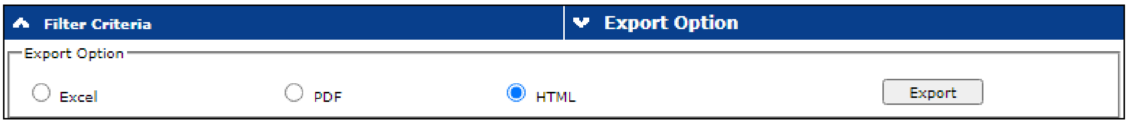
☑ User Name	*	Include	☑ IP Address	*	Include
☑ Audit Type	*	Include	☑ Policy/Criteria Name	*	Include
☑ Module Name	*	Include			
☑ Date Range					
From (MM/DD/YYYY)	09/09/2021				
To (MM/DD/YYYY)	09/09/2021				

(*) View All Items

Select the parameters you want to be included in the filtered report.

Include/Exclude
Selecting Include/Exclude for a parameter lets you include or exclude it from the report.
After making the necessary selections, click **Search.**
The Hardware Report will be filtered according to your preferences.

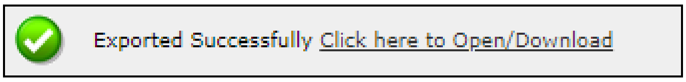
Exporting Hardware Report
To export the Hardware Report, click **Export Option**. Export Option field expands.



Export Option

○ Excel ○ PDF ● HTML

Select the preferred option and then click **Export**. A success message appears.

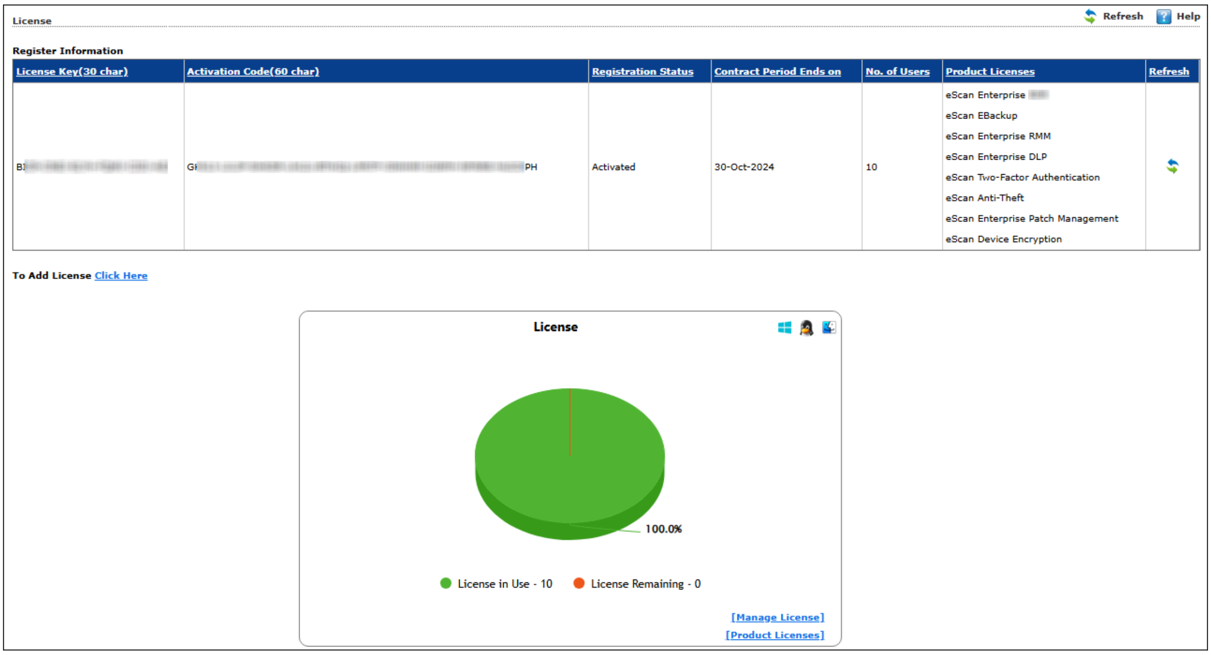


✓ Exported Successfully Click here to Open/Download

Click the link to open/download the file.

License

The License module lets you manage user licenses. You can add, activate, and view the total number of licenses available for deployment, previously deployed licenses and remaining licenses with their corresponding values. The module also lets you move the licensed computers to non-licensed computers and vice versa. Here you can also view the number of Add-On licenses along with the names.



License Refresh Help

Register Information

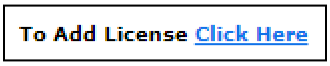
License Key(30 char)	Activation Code(60 char)	Registration Status	Contract Period Ends on	No. of Users	Product Licenses	Refresh
BI[redacted]	GI[redacted]PH	Activated	30-Oct-2024	10	eScan Enterprise [redacted] eScan EBackup eScan Enterprise RMM eScan Enterprise DLP eScan Two-Factor Authentication eScan Anti-Theft eScan Enterprise Patch Management eScan Device Encryption	

To Add License Click Here

Adding and Activating a License

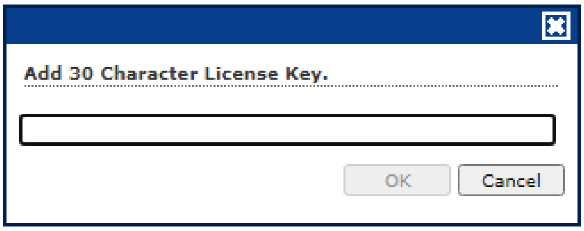
To add and activate a license:

1. In the License screen, click the **Click Here** link.



To Add License Click Here

Add License Key dialog box appears.



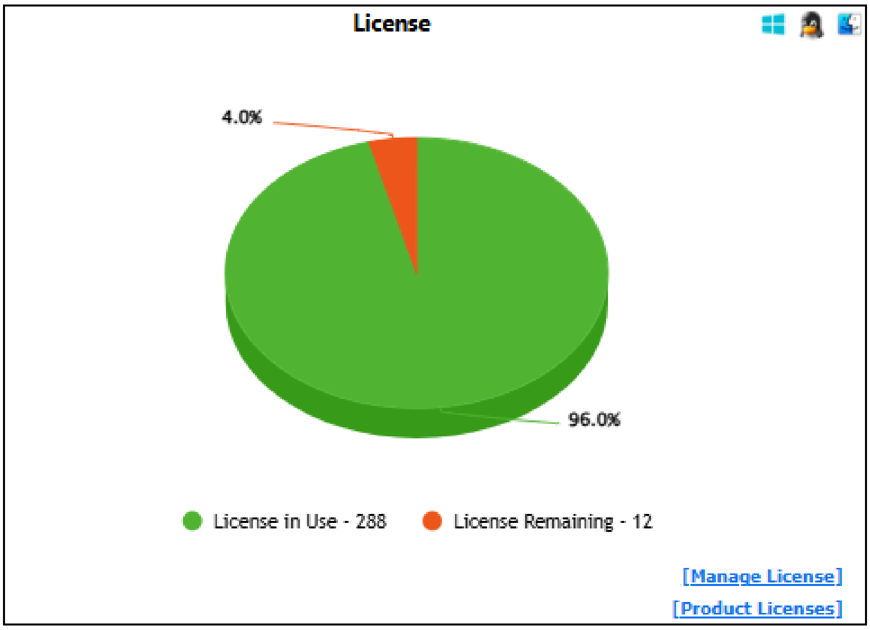
Add 30 Character License Key.

2. Enter the license key and then click **OK**.
   The license key will be added and displayed in the **Register Information** table.

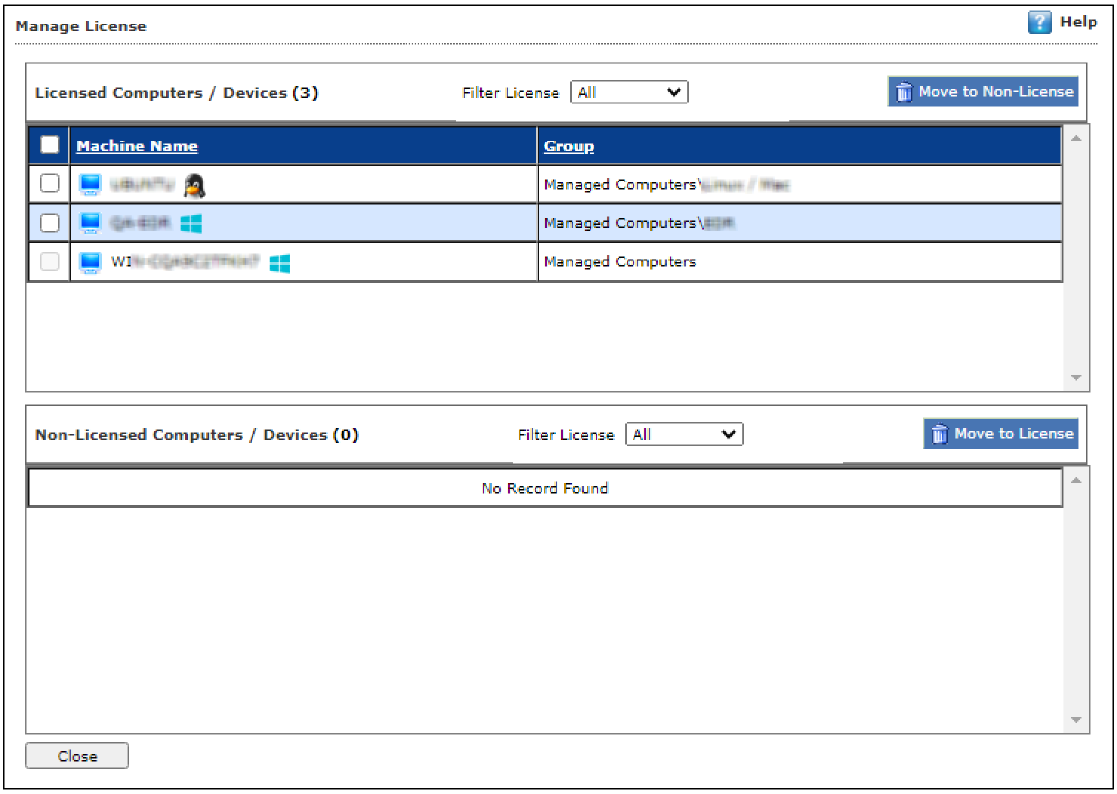
Moving Licensed Computers to Non-Licensed Computers

To move licensed computers to non-licensed computers:

1. In the License statistics box, click **Manage License**.



Manage License window appears.



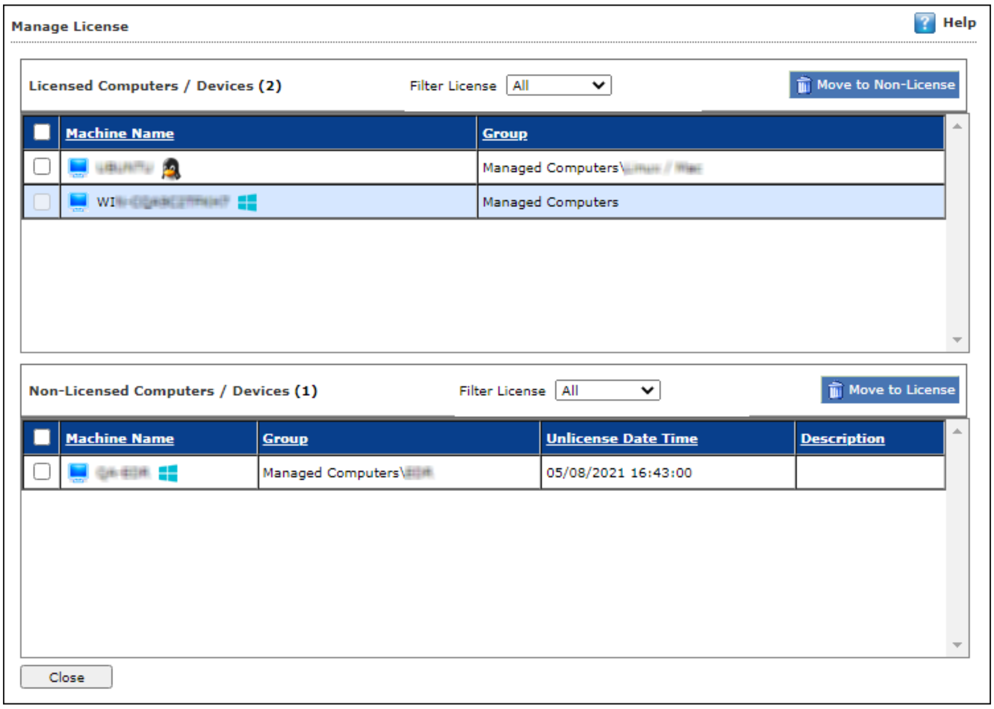
Licensed Computers / Devices (3) Filter License: All

□	Machine Name	Group
□	[redacted]	Managed Computers\[redacted]
□	[redacted]	Managed Computers\[redacted]
□	WI[redacted]	Managed Computers

Non-Licensed Computers / Devices (0) Filter License: All

No Record Found

2. Under the Licensed Computers section, select the computer(s) that you want to move to Non-Licensed Computers section.
3. Click **Move to Non-License**.
4. The selected computer(s) will be moved to Non-Licensed Computers section.



Manage License

Help

Licensed Computers / Devices (2)

Filter License All

Move to Non-License

☐	Machine Name	Group
☐	[redacted]	Managed Computers\[redacted]
☐	WI[redacted]	Managed Computers

Non-Licensed Computers / Devices (1)

Filter License All

Move to License

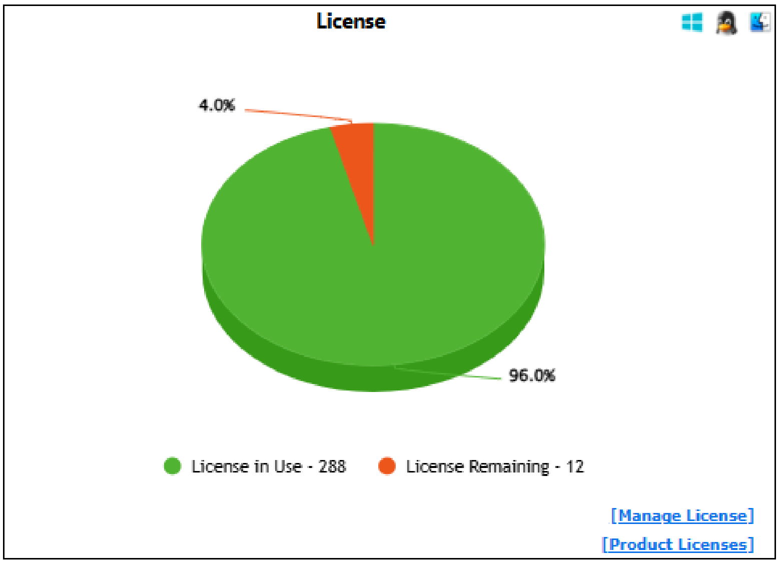
☐	Machine Name	Group	Unlicense Date Time	Description
☐	[redacted]	Managed Computers\[redacted]	05/08/2021 16:43:00	

Close

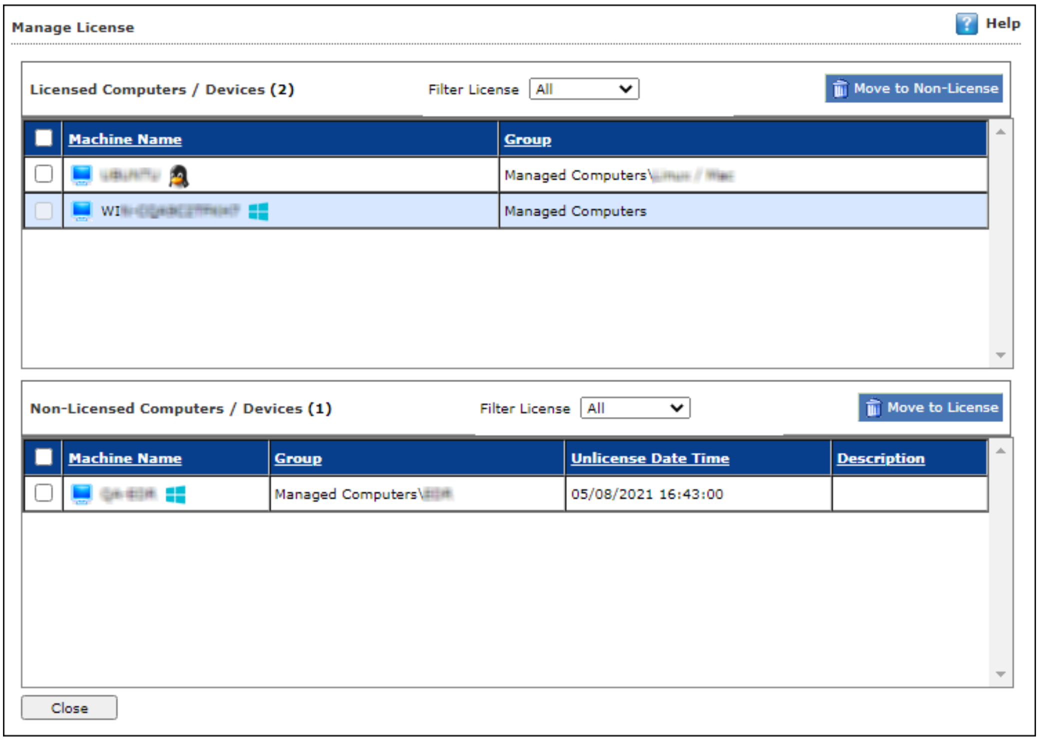
Moving Non-Licensed Computers to Licensed Computers

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 Move to Non-License

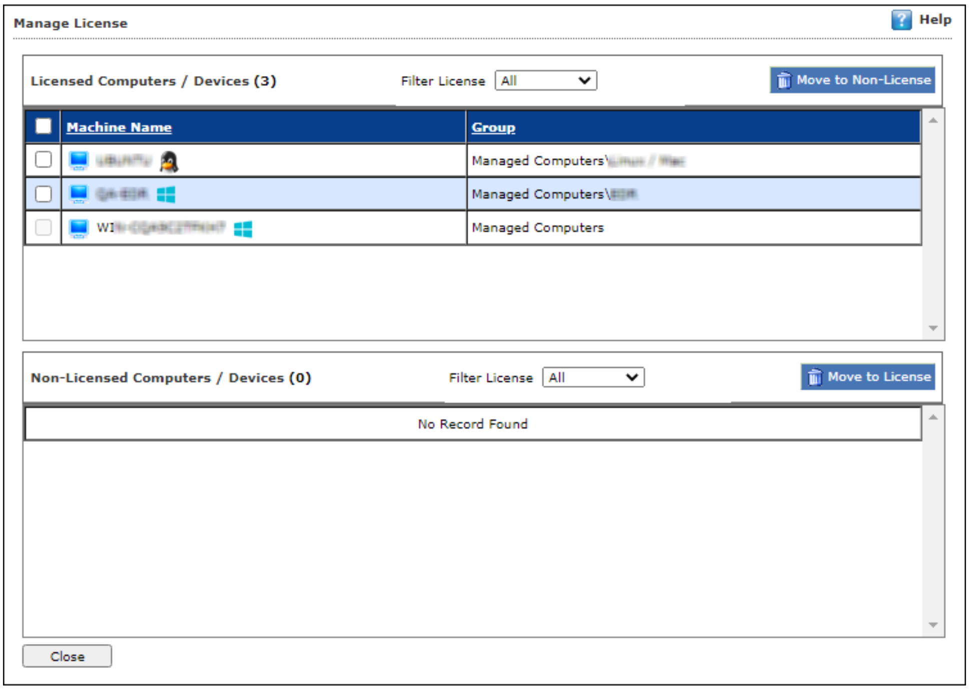
□	Machine Name	Group
□	[redacted]	Managed Computers\[redacted]
□	WI[redacted]	Managed Computers

Non-Licensed Computers / Devices (1) Filter License All Move to License

□	Machine Name	Group	Unlicense Date Time	Description
□	[redacted]	Managed Computers\[redacted]	05/08/2021 16:43:00	

Close

2. Under the Non-Licensed Computers section, select the computer(s) that you want to move to Licensed Computers section.
3. Click **Move to License**.
4. The selected computer(s) will be moved to Licensed Computers section.



Manage License

Help

Licensed Computers / Devices (3) Filter License All Move to Non-License

□	Machine Name	Group
□	[redacted]	Managed Computers\[redacted]
□	[redacted]	Managed Computers\[redacted]
□	WI[redacted]	Managed Computers

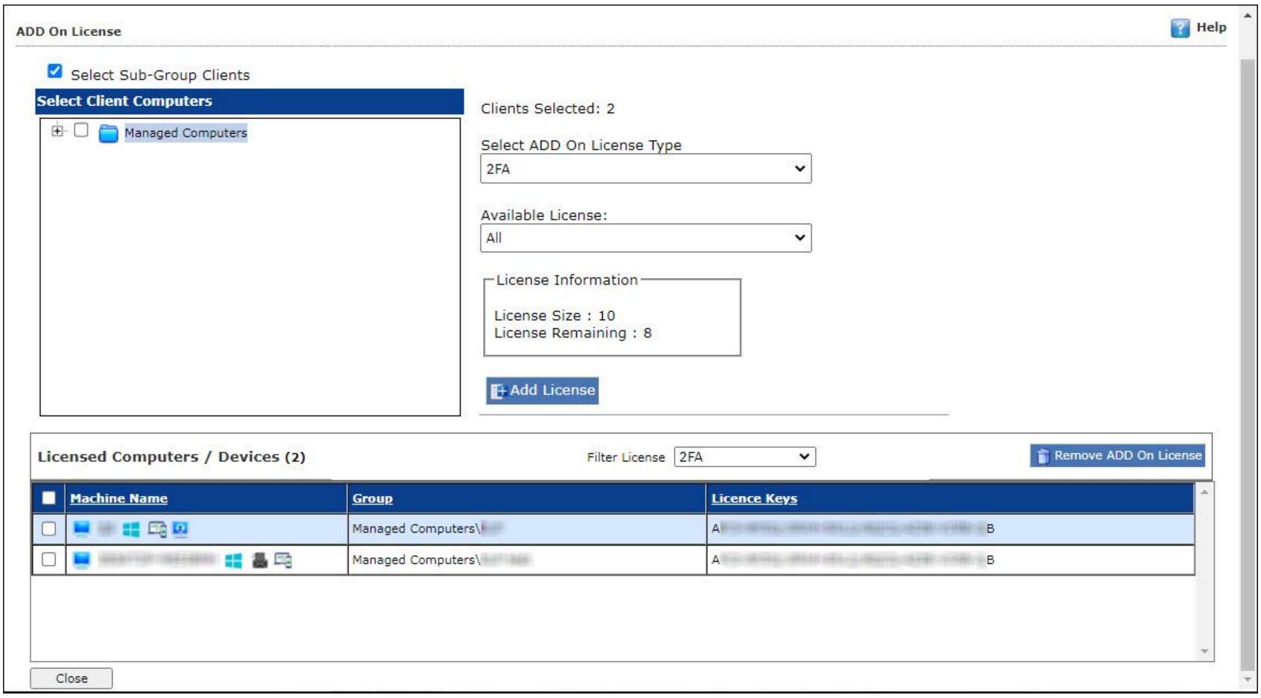
Non-Licensed Computers / Devices (0) Filter License All Move to License

No Record Found

Close

Managing Add-On Licenses

You can manage multiple Add-On licenses deployed for networked computers using the ADD On License option from the License dashboard. This option allows you to Add or Delete particular Add-On license to/from specific computer or the group. It also shows basic license information like license size and remaining number of license for selected license type.



☑ Select Sub-Group Clients

⊞ □ Managed Computers

Clients Selected: 2

Select ADD On License Type: 2FA

Available License: All

License Information

License Size : 10
License Remaining : 8

Licensed Computers / Devices (2)

Filter License: 2FA

□	Machine Name	Group	Licence Keys
□	[redacted]	Managed Computers\[redacted]	A[redacted]B
□	[redacted]	Managed Computers\[redacted]	A[redacted]B

Adding an Add-On license

In order to add a license to the computer or the group, follow the steps given below:

1. In the License tab, click on **ADD On License** option.
   The **ADD On License** window opens.
2. Select the computer/group on which the license is to be added.
3. Select the License type from the provided drop-down list.
4. Select available license from the provided drop-down list.
5. Click on **Add License** button.
   The license is now added to the selected computer/group.

Removing Add-On license

In order to remove a license from the computer(s), follow the steps given below:

1. Select the computer from the Licensed Computers/Devices list.
   You can use the Filter License drop-down to filter the list.
2. Click on **Remove ADD On License** button.
   The license is now removed from the selected computer(s).

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**