eScan™

Enterprise Security

eScan Elite for Business

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/10.08.2021/22.x
Current Software Version:	22.0.0000.xxxx
Technical Support:	**support@escanav.com**
Sales:	**sales@escanav.com**
Forums:	**http://forums.escanav.com**
eScan Wiki:	**https://wiki.escanav.com/wiki/index.php/**
Live Chat:	**http://www.escanav.com/english/livechat.asp**
Printed by:	MicroWorld Software Services Private Limited
Date:	August, 2021

Content

Introduction 9
Pre-requisites for eScan Elite for Business 9
System Requirements 10
Installing eScan Elite for Business 11
- Installation 11
- Components of eScan Server 20
- Web Console Login 21
- Setup Links 23
- eScan AV Report 24
  - Filtering AV Report 25
- Main Interface 26
- Setup Wizard 27
- Navigation Panel 33

Dashboard 36
- Deployment Status 36
  - eScan Status 37
  - License 37
  - eScan Version 37
- Protection Status 39
  - Update Status 39
  - Scan Status 40
  - File Anti-Virus 41
  - Proactive 41
  - Mail Anti-Virus 42
  - Anti-Spam 42
  - Web Anti-Phishing 43
  - Mail Anti–Phishing 43
  - Web Protection 44
  - Firewall 44
  - Endpoint Security 45
  - Privacy 46
  - Anti – Ransomware 46
- Protection Statistics 47
  - File Anti-Virus 48
  - Mail Anti-Virus 50
  - Anti-Spam 50
  - Web Protection 51
  - Endpoint Security-USB 51
  - Endpoint Security-Application 52
- Summary Top 10 53
- Asset Changes 54
- Live Status 55
- Configure the Dashboard Display 56

Managed Computers 57
Search 58
Update Agent 59
Adding an Update Agent 59
Configuring UA Settings 61
Delete an Update Agent 61
Action List 63
Creating a Group 63
Removing a Group 64
Set Group Configuration 64
Managing Installations 65
Deploy/Upgrade Client 67
Manual installation of eScan Client on network computer(s) 69
Installing eScan Client Using Agent 69
Installing other Software (Third Party Software) 70
Uninstall eScan Client (Windows) 71
Synchronize with Active Directory 73
Outbreak Prevention 74
Create Client Setup 77
Properties of a group 78
Group Tasks 79
Creating a Group Task 79
Managing a Group Task 81
Assigning a Policy to the group 83
Client Action List 85
Set Host Configuration 86
Deploy/Upgrade Client 86
Uninstall eScan Client 87
Move to Group 88
Remove from Group 88
Refresh Client 88
Connect to Client (RMM) 89
Manage Add-On License 89
Assign Policy Template 90
Show Critical Events 90
Export 90
Show Installed Softwares 91
Force Download 92
Forensic-Port/Communication 93
On Demand Scanning 93
Send Message 94
Outbreak Prevention 95
Delete All Quarantine Files 95
Create OTP 95
Pause Protection 97
Resume Protection 98

Properties of Selected Computer 98
Anti-Theft 100
Anti-Theft Options 100
Disable Anti-Theft 103
Refresh Client 103
Understanding the eScan Client Protection Status 104
Select Columns 105
Policy Template 106
Managing Policies 106
Creating Policy Template for a group/specific computer 107
Configuring eScan Policies for Windows Computers 109
Assigning Policy Template to a group 181
Assigning Policy Template to Computer(s) 183
Copy a Policy Template 184
Exporting a Policy Template report 184
Parent Policy 185
Policy Criteria Templates 187
Adding a Policy Criteria Template (AND condition) 187
Adding a Policy Criteria Template (OR condition) 193
Viewing Properties of a Policy Criteria template 199
Deleting a Policy Criteria template 199
Unmanaged Computers 202
Network Computers 202
Creating a New Group from the Select Group window 203
IP Range 205
Adding New IP Range 205
Moving an IP Range to a Group 205
Deleting an IP Range 206
Active Directory 207
Adding an Active Directory 207
Moving Computers from an Active Directory 208
New Computers Found 209
Filter Criteria 209
Action List 209
Report Templates 211
Creating a Report Template 212
Creating Schedule for a Report Template 213
Viewing Properties of a Report Template 213
Deleting a Report Template 213
Report Scheduler 214
Creating a Schedule 214
Viewing Reports on Demand 216
Managing Existing Schedules 217
Generating Task Report of a Schedule 217
Viewing Results of a Schedule 217
Viewing Properties of a Schedule 218

Deleting a Schedule 218
Events and Computers 219
Events Status 219
Computer Selection 220
Edit Selection 222
Software/Hardware Changes 223
Violations 224
Settings 224
Event Status Setting 224
Computer Selection 225
Software/ Hardware Changes Setting 227
Performing an action for computer 228
Tasks for Specific Computers 229
Creating a task for specific computers 229
Viewing Properties of a task 232
Viewing Results of a task 232
Deleting a task for specific computers 232
Asset Management 234
Hardware Report 234
Filtering Hardware Report 235
Exporting Hardware Report 235
Software Report 236
Filtering Software Report 236
Exporting Software Report 237
Software License 238
Filtering Software License Report 238
Exporting Software License Report 239
Software Report (Microsoft) 240
Filtering Software Report (Microsoft) 240
Exporting Software Report (Microsoft) 240
Filtering Microsoft OS Report 241
Exporting Microsoft OS Report 242
User Activity 243
Print Activity 243
Viewing Print Activity Log 243
Exporting Print Activity Log 243
Filtering Print Activity Log 244
Exporting Print Activity Report 244
Print Activity Settings 245
Session Activity Report 246
Viewing Session Activity Log 246
Filtering Session Activity Log 246
Exporting Session Activity Report 247
File Activity Report 248
Viewing File Activity Log 248
Filtering File Activity Log 248

Exporting File activity Report.......249
Application Access Report.......250
Viewing Application Access Report.......250
Filtering Application Access Report.......251
Exporting Application Access Report.......251
Patch Report.......252
Patch Report.......252
Filtering Patch Report.......252
Exporting Windows Patch Report.......253
All Patch Report.......254
Filtering All Patch Report.......254
Exporting All Patch Report.......254
Notifications.......256
Outbreak Alert.......256
Event Alert.......258
Unlicensed Move Alert.......260
New Computer Alert.......261
Configure SIEM.......262
SMTP Settings.......263
Settings.......264
EMC Settings.......265
Web Console Settings.......267
Update Settings.......270
General Config.......270
Update Notification.......271
Scheduling.......272
Update Distribution.......273
Auto-Grouping.......275
Excluding clients from auto adding under Managed Group(s).......276
Removing clients from the excluded list.......276
Defining a group and client selection criteria for auto adding under managed computer(s).......276
Two-Factor Authentication (2FA).......278
Enabling 2FA login.......279
Disabling 2FA login.......280
Users For 2FA.......281
Administration.......283
User Accounts.......283
Create New Account.......283
Delete a User Account.......284
User Roles.......285
New Role.......285
View Role Properties.......286
Delete a User Role.......288
Export & Import.......289
Export Settings.......289
Import Settings.......290

- Scheduling ... 291
- Customize Setup ... 293
  - Creating a customized setup for Windows ... 293
  - Editing Setup Properties ... 294
  - Deleting a Setup ... 295
- Audit Trail ... 296
  - Filter all Audit Trail report ... 296
  - Exporting Audit Trail ... 296

License ... 297
- Adding and Activating a License ... 297
- Moving Licensed Computers to Non-Licensed Computers ... 298
- Moving Non-Licensed Computers to Licensed Computers ... 300

Getting Started ... 302

Graphical User Interface (GUI) ... 302
- Data Encryption ... 303
  - How to Create a Vault? ... 303
- Two-Factor Authentication ... 310
  - Enabling 2FA login ... 310
  - Disabling 2FA login ... 314
- Identity protection ... 315
  - Configuration ... 316
- Quick Access Links ... 318
  - Rescue Mode ... 318
  - eScan Remote Support ... 319
  - Password ... 320
  - License Information ... 321
  - Tools ... 323
  - Reports ... 333

Contact Us ... 335
- Forums ... 335
- Chat Support ... 335
- Email Support ... 335

Introduction

eScan Elite for Business protects the business network from different types of cyber security threats such as malware, ransomware, adware, bots, and more, using layered approach. With unique combination of basic and modern techniques, eScan blocks broad range of attacks. It offers various advance features like web filtering, signature-based malware detection, application control, and behavior analysis. It includes innovative techniques like malware detection, exploit prevention, heuristic scan, and many more. Packed with the sophisticated threat-detection and machine-learning virus protection that won't affect the system.

eScan offers advanced defence capabilities against malwares that includes script, macro and polymorphic viruses, Trojans, Internet worms, malicious Java applets, and ActiveX codes. It provides smart parental controls to keep the kids safe online by limiting the time and content filtering wherever they go. Along with all these, eScan Elite for Business equipped with a rescue disk, vulnerability scan, and several other tools designed to clean and optimize the PC.

Pre-requisites for eScan Elite for Business

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

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

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

System Requirements

Windows Server and Endpoints:

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

Hardware 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

eScan Management Console can be accessed by using following browsers:

- Internet Explorer 11 and above
- Firefox latest version
- Google Chrome latest version

Installing eScan Elite for Business

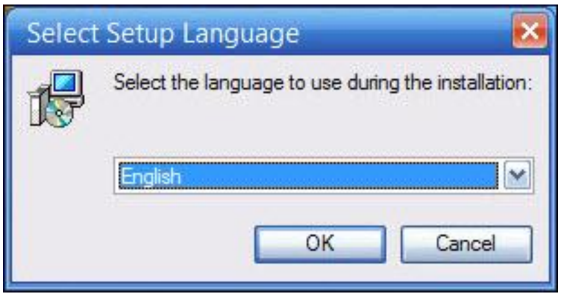
- **Installing eScan Elite for Business from CD/DVD**
  Installing eScan Elite for Business from the CD/DVD is very simple, insert the CD/DVD in the ROM and wait few seconds for the Autorun to run the installation wizard. In case the installation wizard does not run automatically, locate and double-click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

- **Downloading and installing eScan Elite for Business from internet**
  To download the setup file click here. To install eScan Server from the downloaded file, double click on **WMCTOTxxxx.exe** file and follow the instructions on screen to complete the installation process.

Installation

To install the eScan Elite for Business, follow the steps given below:

1. The installation wizard displays following window:



Select Setup Language

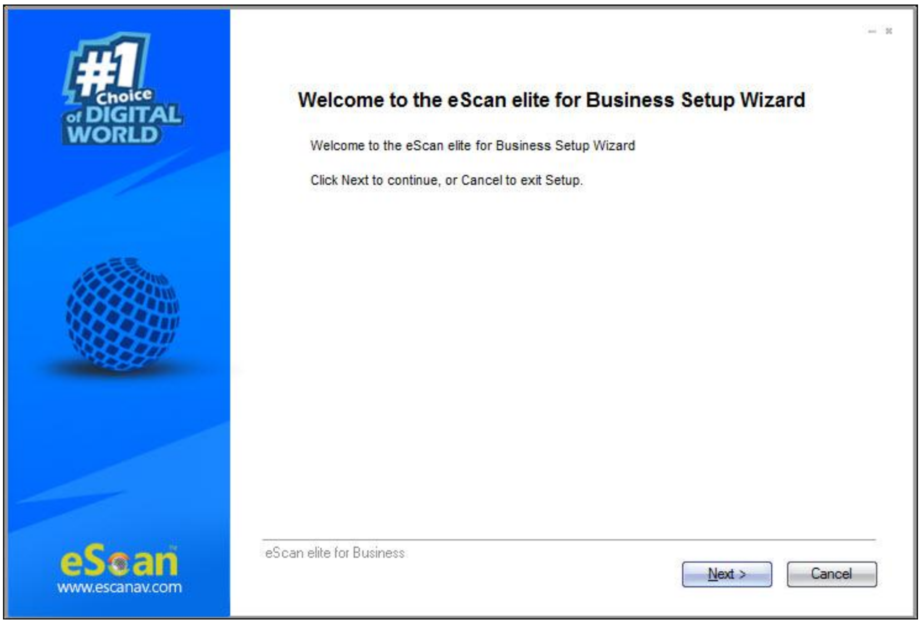
Select the language to use during the installation:

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.

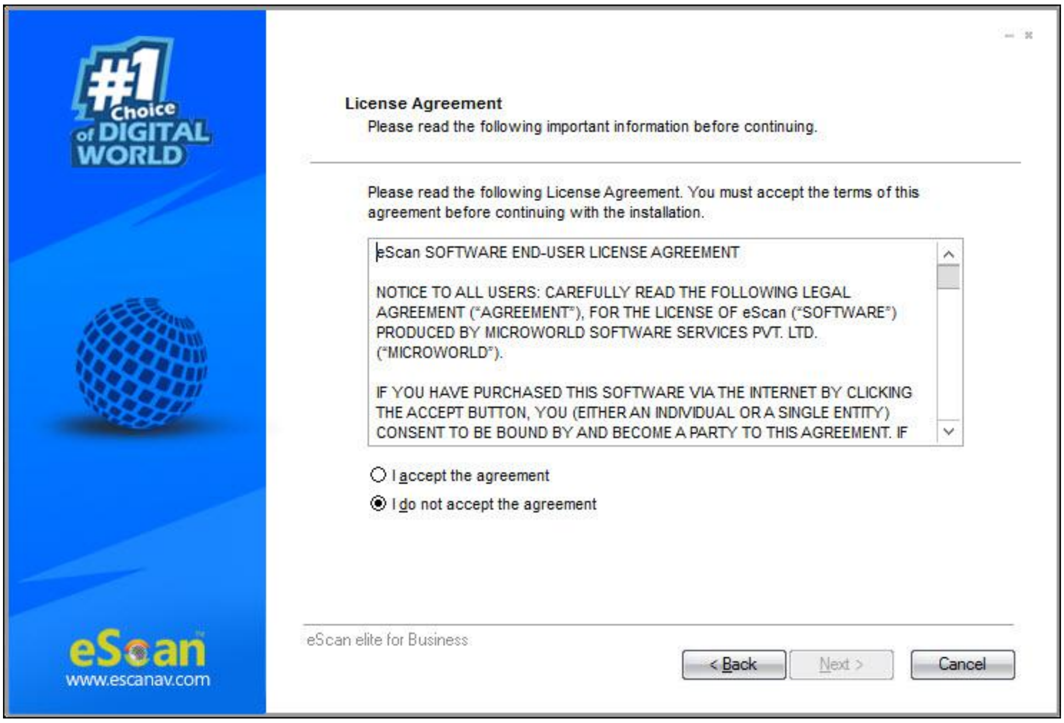


Welcome to the eScan elite for Business Setup Wizard

Welcome to the eScan elite for Business Setup Wizard

Click Next to continue, or Cancel to exit Setup.

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.

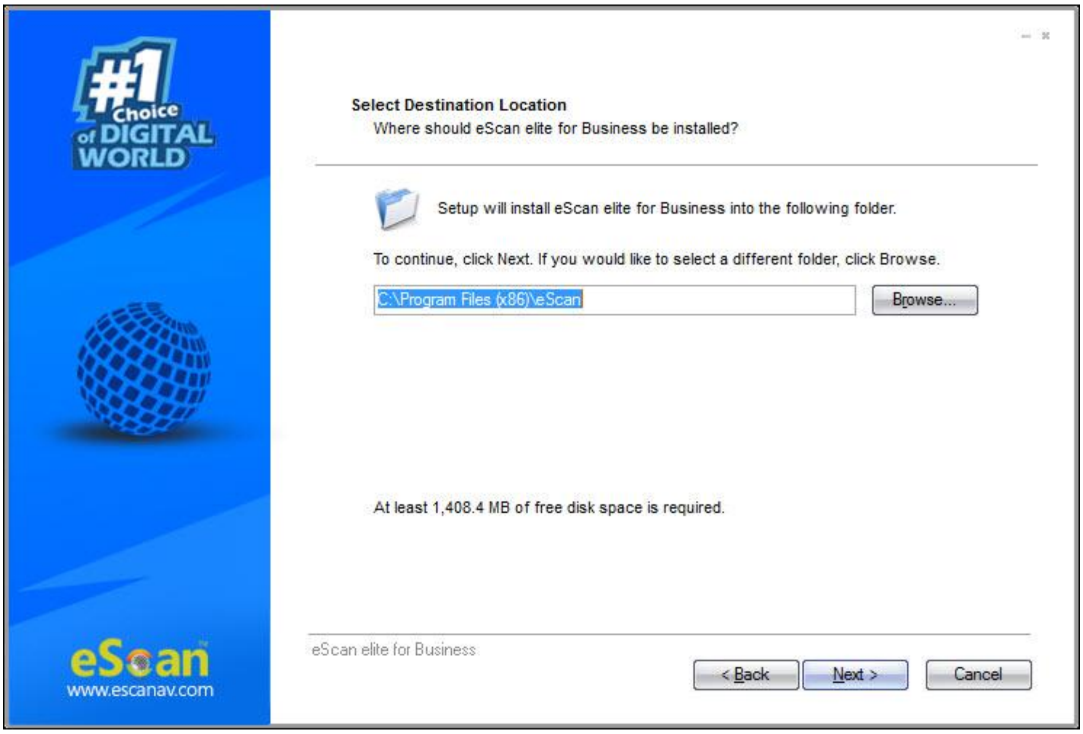
eScan SOFTWARE END-USER LICENSE AGREEMENT

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 elite for Business be installed?

Setup will install eScan elite for Business into the following folder.

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

C:\Program Files (x86)\eScan

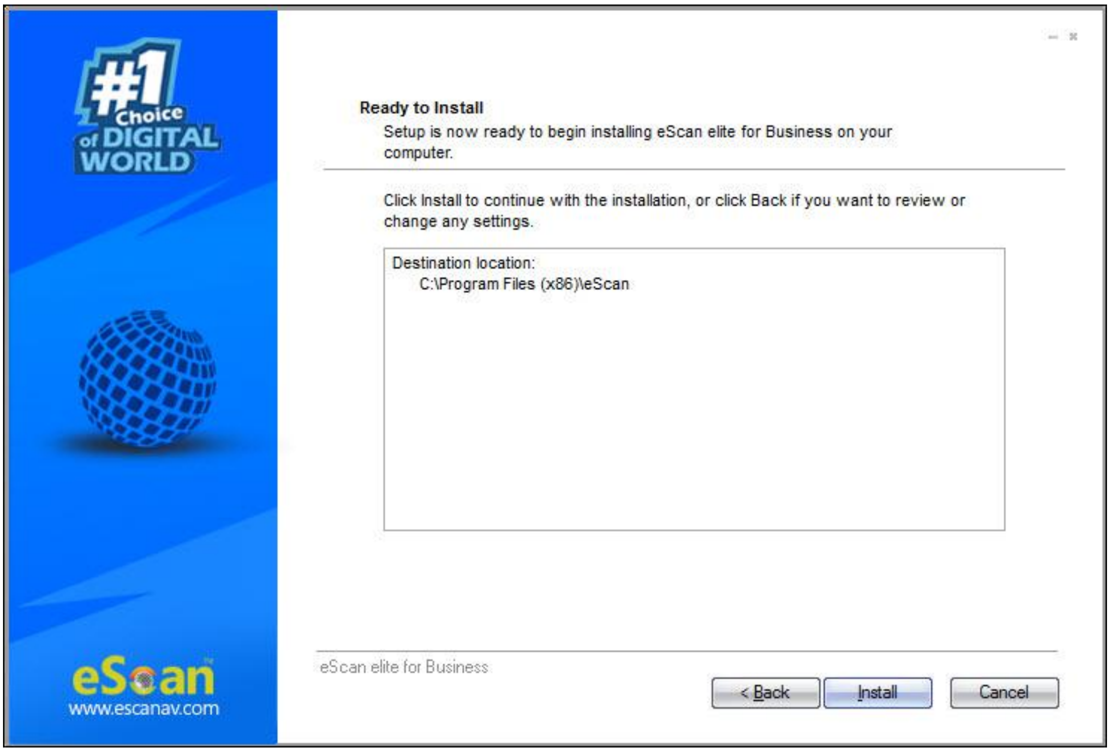
At least 1,408.4 MB of free disk space is required.

eScan elite for Business

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**

The Ready to Install screen appears displaying destination location.



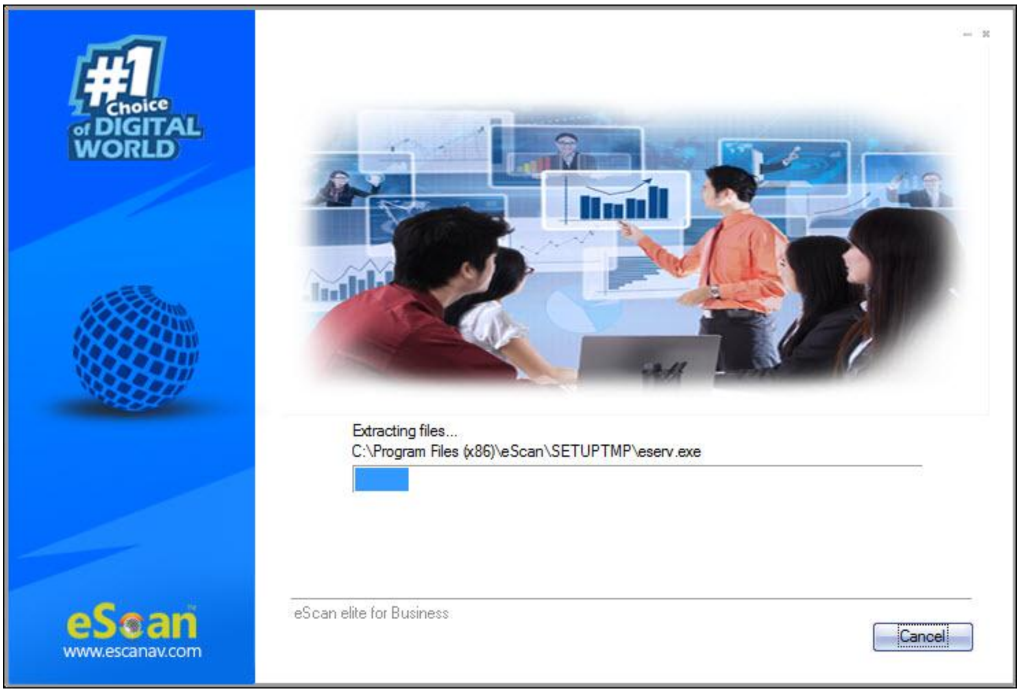
Ready to Install

Setup is now ready to begin installing eScan elite for Business on your computer.

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

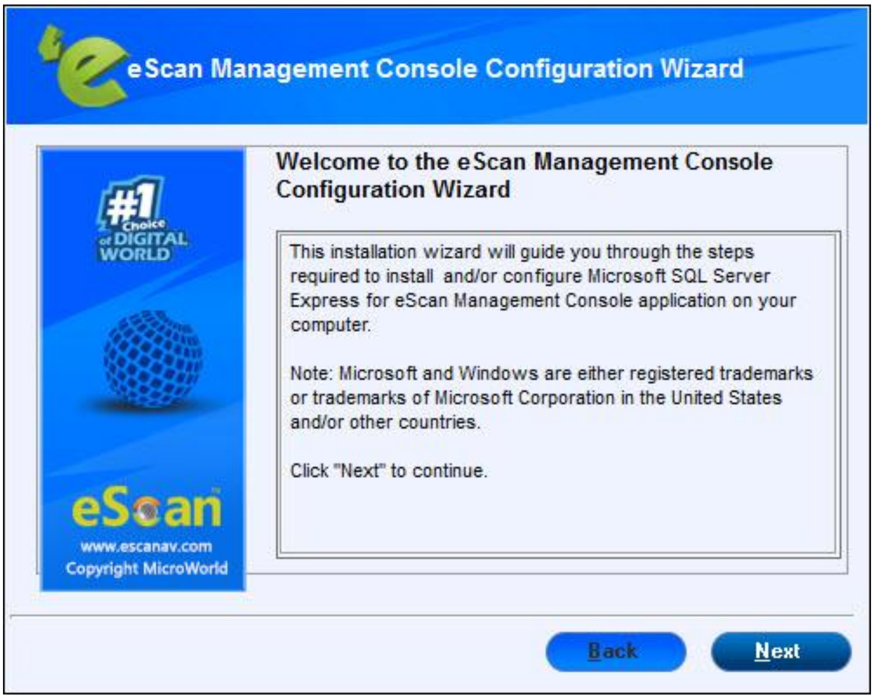
Destination location:
C:\Program Files (x86)\eScan

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



Extracting files...
C:\Program Files (x86)\eScan\SETUPTMP\eserv.exe

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

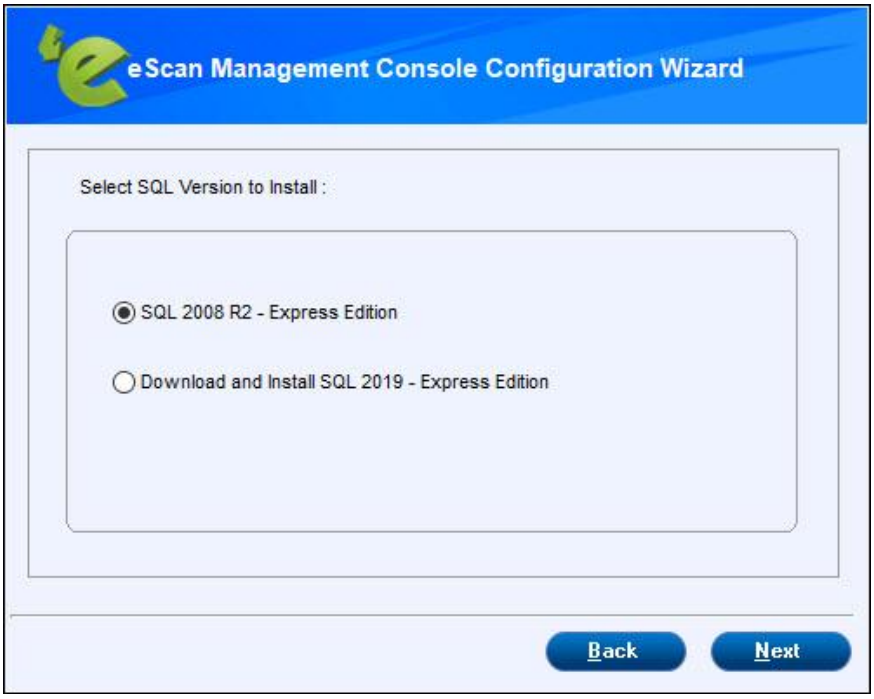
This installation wizard will guide you through the steps required to install and/or configure Microsoft SQL Server Express for eScan Management Console application on your computer.

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.



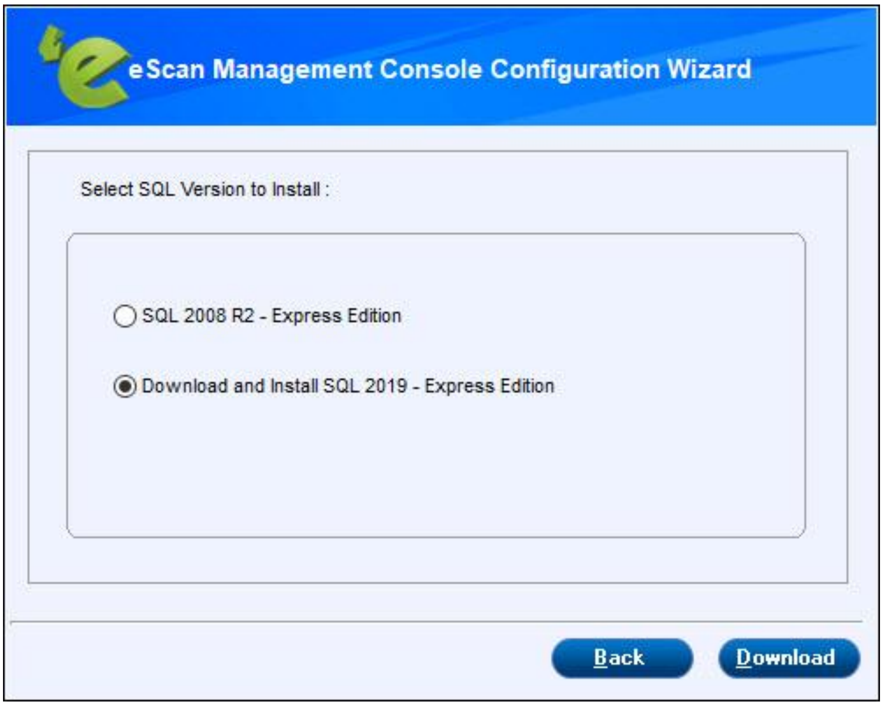
eScan Management Console Configuration Wizard

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**.

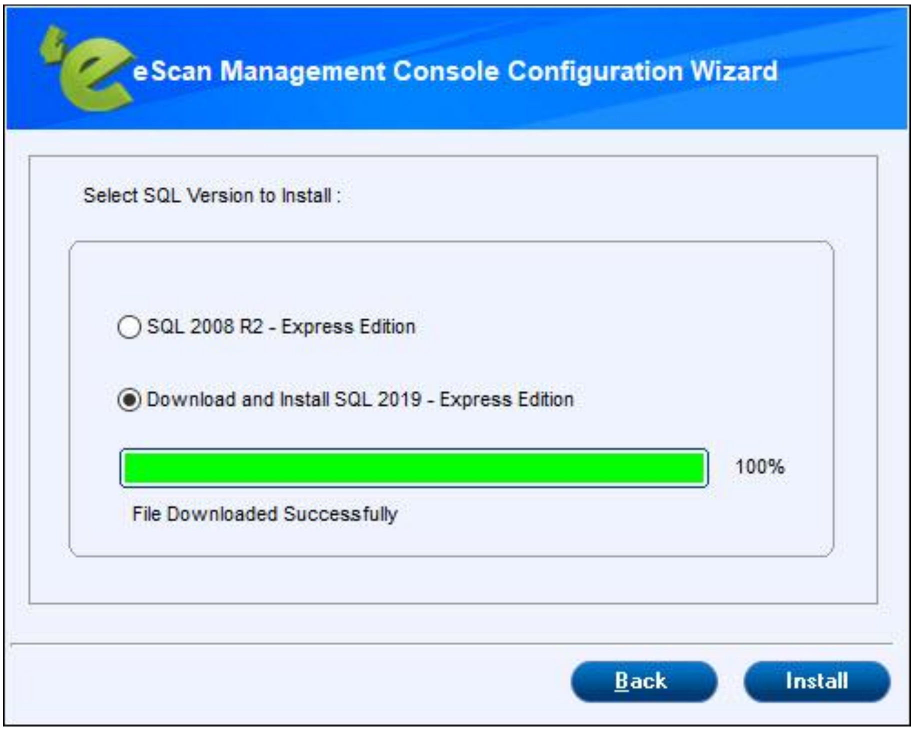


Select SQL Version to Install :

○ SQL 2008 R2 - Express Edition

● Download and Install SQL 2019 - Express Edition

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



Select SQL Version to Install :

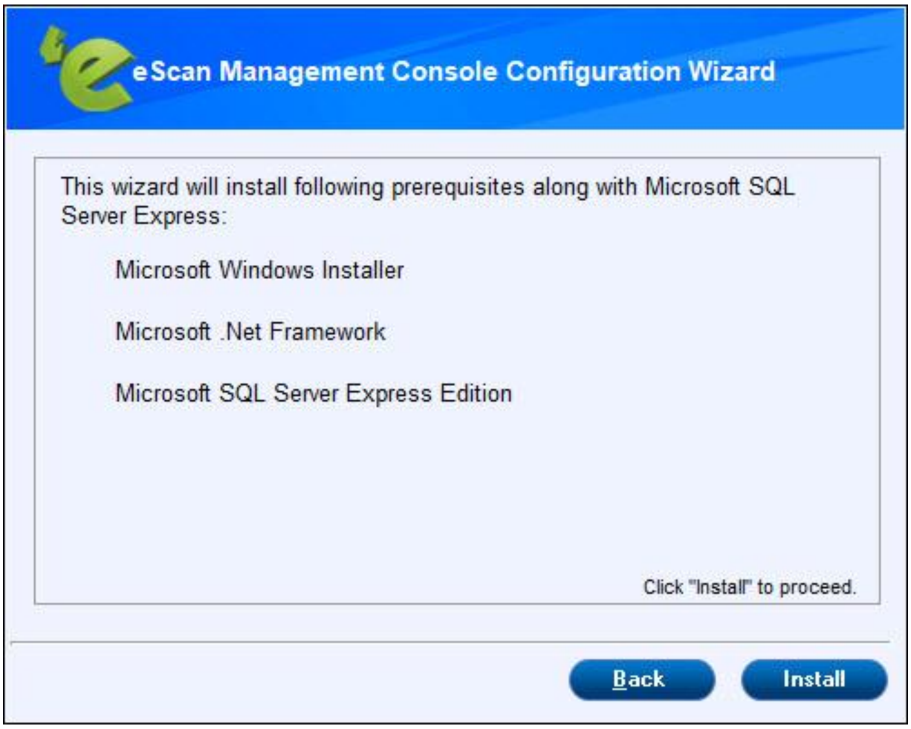
○ SQL 2008 R2 - Express Edition

● 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:

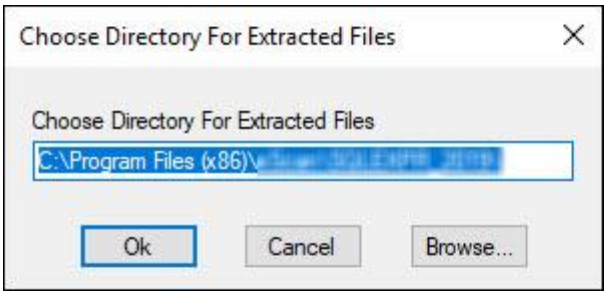
Microsoft Windows Installer

Microsoft .Net Framework

Microsoft SQL Server Express Edition

Click "Install" to proceed.

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



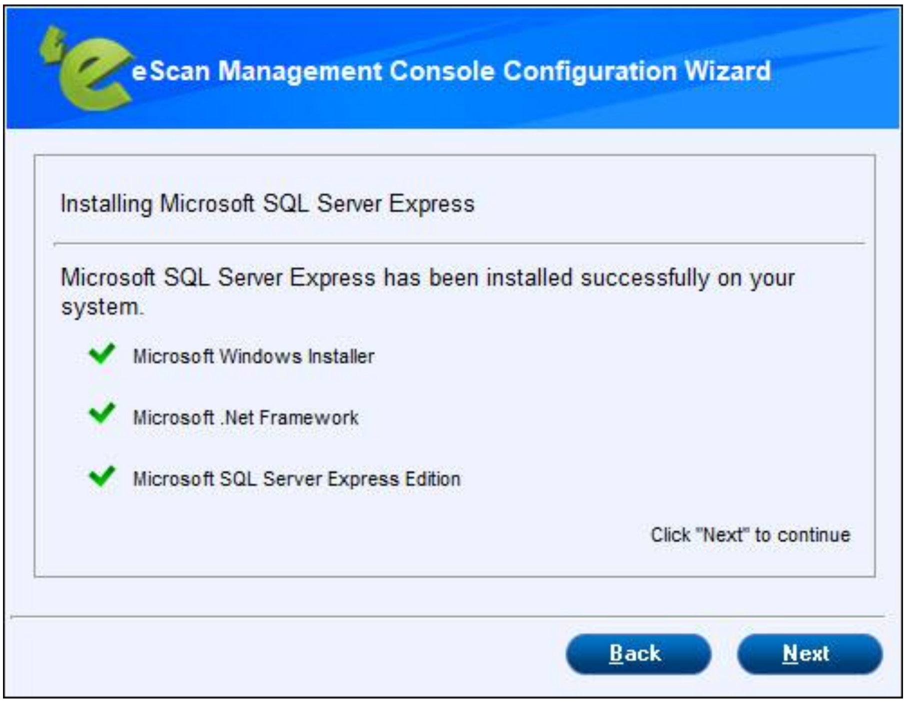
Choose Directory For Extracted Files

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**



eScan Management Console Configuration Wizard

Installing Microsoft SQL Server Express

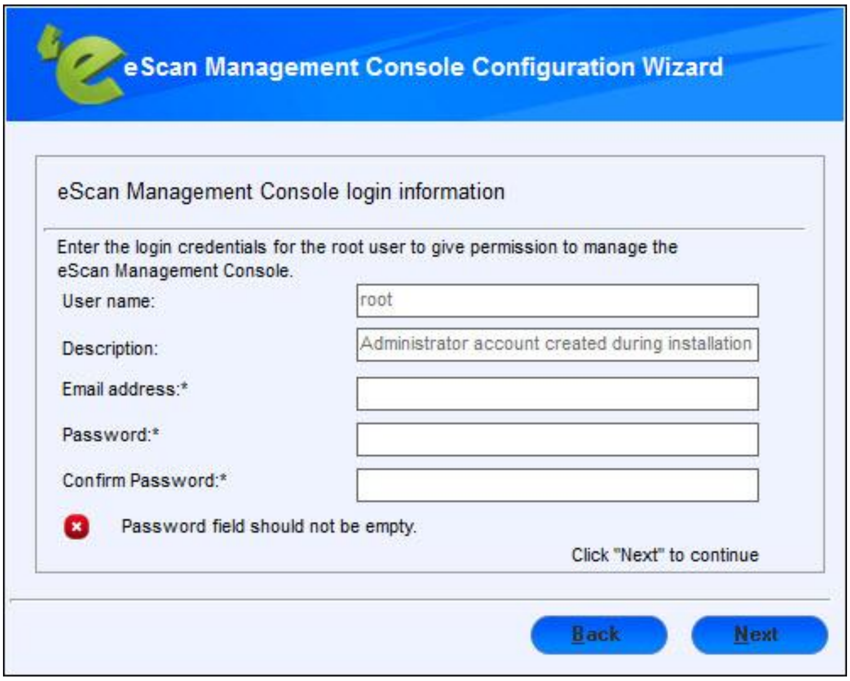
Microsoft SQL Server Express has been installed successfully on your system.

- ✓ 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 Configuration Wizard

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:*

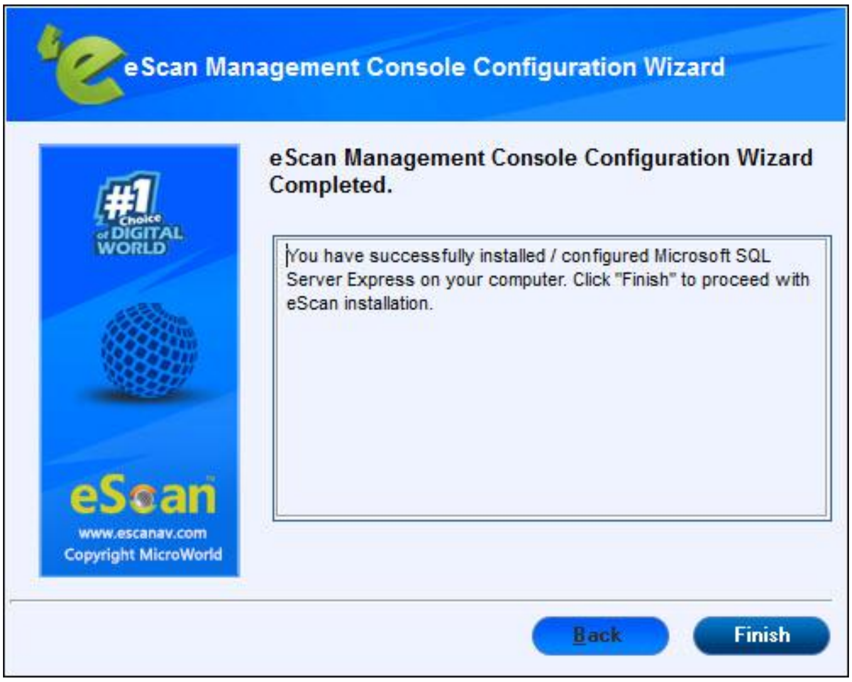
Password:*

Confirm Password:*

Password field should not be empty.

Click "Next" to continue

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

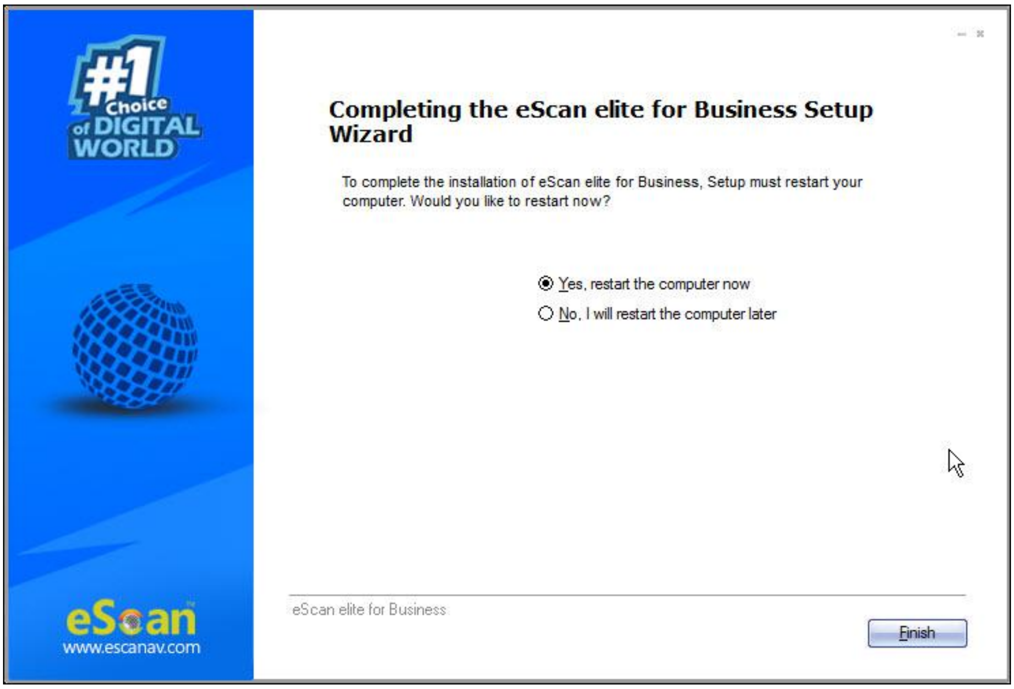


eScan Management Console Configuration Wizard Completed.

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.

    The wizard displays below window:



Completing the eScan elite for Business Setup Wizard

To complete the installation of eScan elite for Business, Setup must restart your computer. Would you like to restart now?

● Yes, restart the computer now

○ No, I will restart the computer later

16. Click **Finish** to restart the PC for completing the installation process.

    After the computer restarts, launch the eScan Elite for Business and enter the license key for activation.

NOTE	To run eScan services fully it is recommended that you restart the PC.

Components of eScan Server

The eScan Server is comprised of following components:

- **eScan Server**
  This is the core component that lets you manage, deploy and configure eScan client on computers. It stores the configuration information and log files about the computers connected across the network. Being the core component, it communicates with the following components.

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

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

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

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

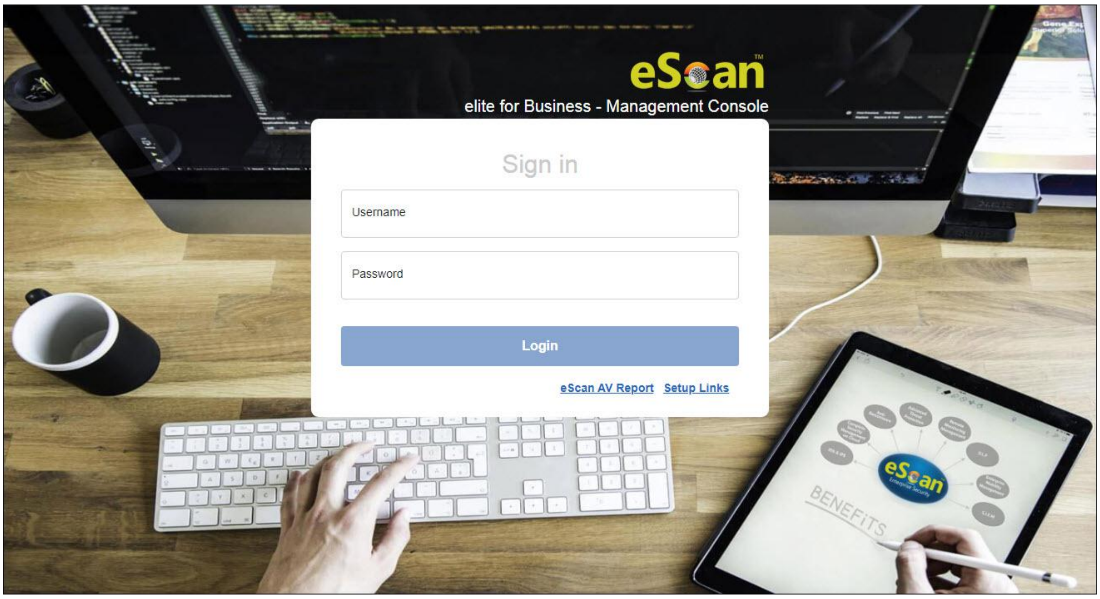
NOTE	For Windows 11 / 10 / 8 / 8.1 / 2008 / 2012 / 2016 / 2019 operating systems, the SQL 2008 Express edition will be installed. For Windows 7 and below, SQL 2005 Express edition will be installed. Uninstallation of eScan server won't remove SQL and APACHE from the endpoint. The user will have to uninstall these components manually.

Web Console Login

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

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

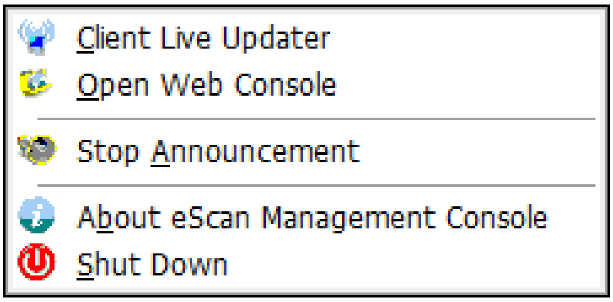
1. Launch a web browser.
2. Enter the following URL: **<IP address of the eScan Server installed system>:10443**
   Web console login page appears.



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

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

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

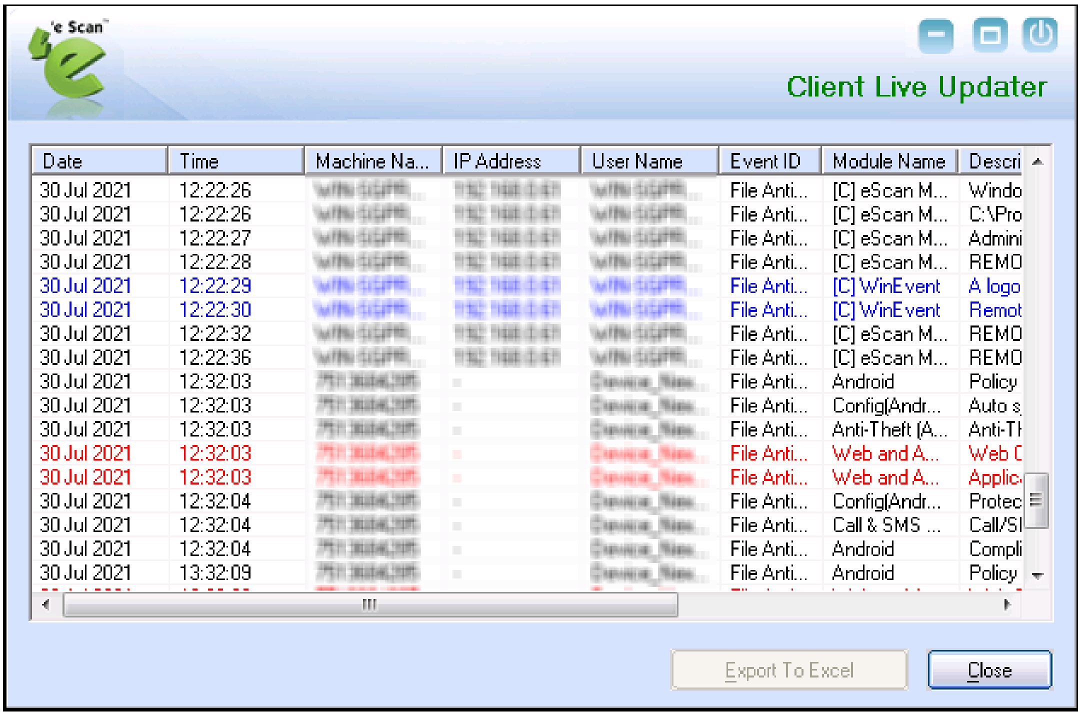


2. Click **Open Web Console**.
   Default browser launches and displays web console login page.

Rests of the options are explained below:

Client Live Updater

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



Date	Time	Machine Na...	IP Address	User Name	Event ID	Module Name	Descri
30 Jul 2021	12:22:26	[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.

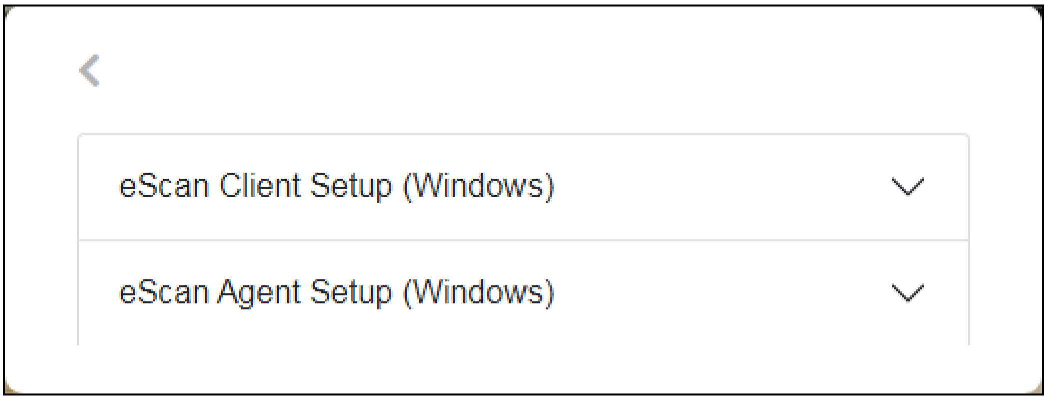
Shut Down

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.

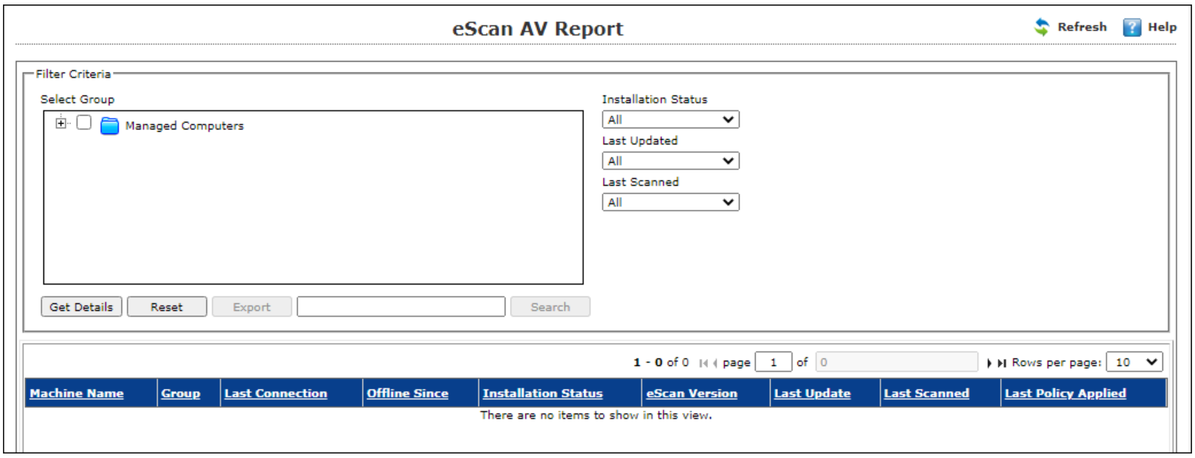


- **eScan Client Setup (Windows)**
  This link can be shared via email to the computer users where remote installation is impossible. By clicking this link users can download the eScan Client Setup and install it manually on their computers. Users can also directly access the eScan Management console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

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

eScan AV Report

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



eScan AV Report

Filter Criteria

Select Group

□ Managed Computers

Installation Status: All

Last Updated: All

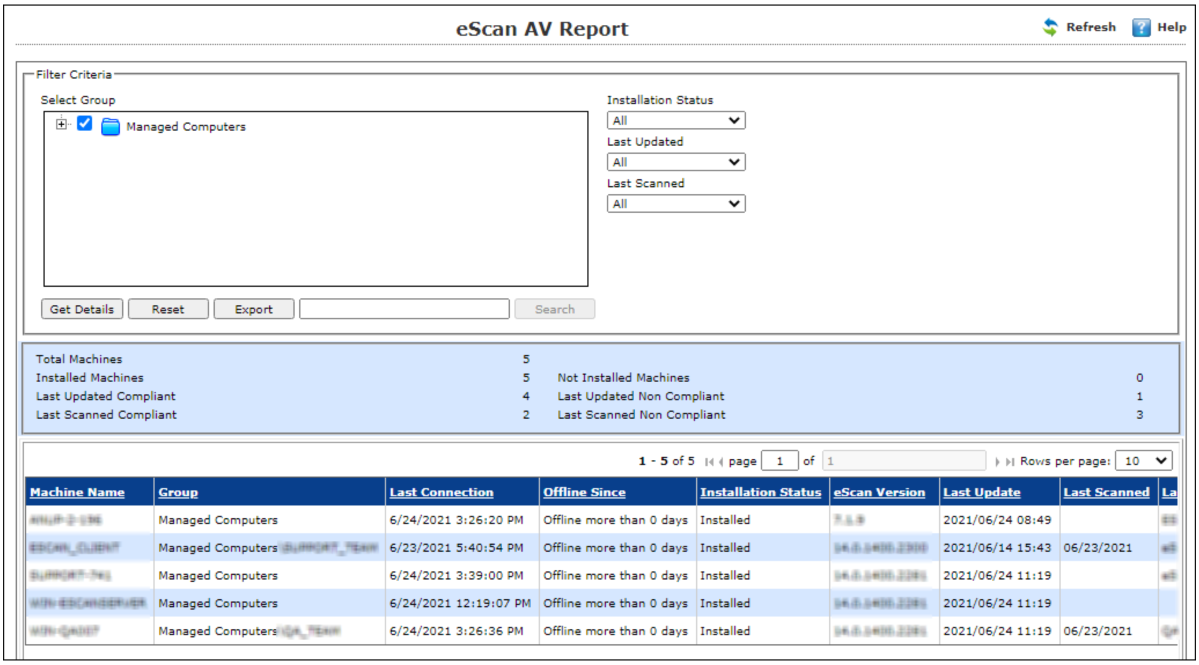
Last Scanned: All

1 - 0 of 0 page 1 of 0 Rows per page: 10

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.

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



eScan AV Report

Filter Criteria

Select Group

☑ Managed Computers

Installation Status: All

Last Updated: All

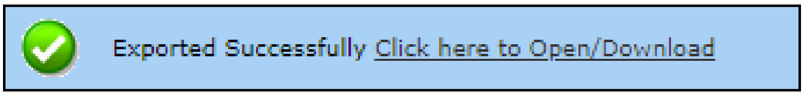
Last Scanned: All

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]

2. 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

Filtering AV Report

To filter AV report as per requirement,

Installation Status
It shows the report of eScan product installed on the client computer.

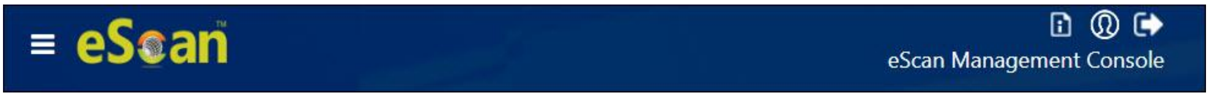
Last Update
It shows number of client computer have updated the eScan software.

Last Scanned
It display the list of computer have scanned.

The **Search** feature lets you find any computer added in Managed Computers.
Click **Reset**, to clear all search fields.

Main Interface

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



The links in the top right corner are explained below:

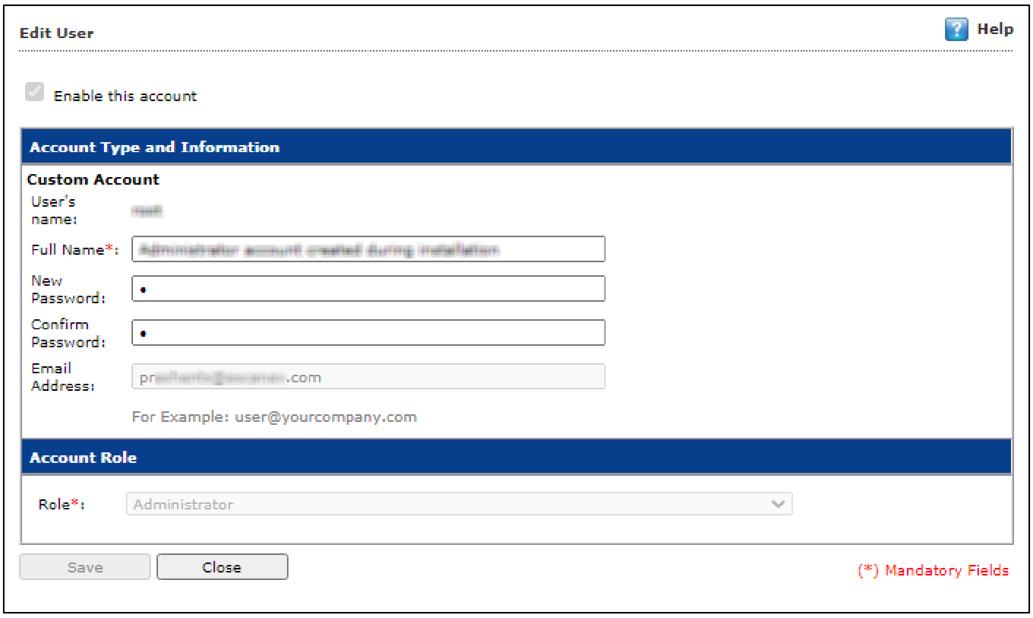
About eScan

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

Username

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

Note	It is not allowed to configure your email address.



Edit User

Help

☑ Enable this account

Account Type and Information

Custom Account

User's name: [redacted]

Full Name*: [redacted]

New Password: •

Confirm Password: •

Email Address: pr[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.

Refresh

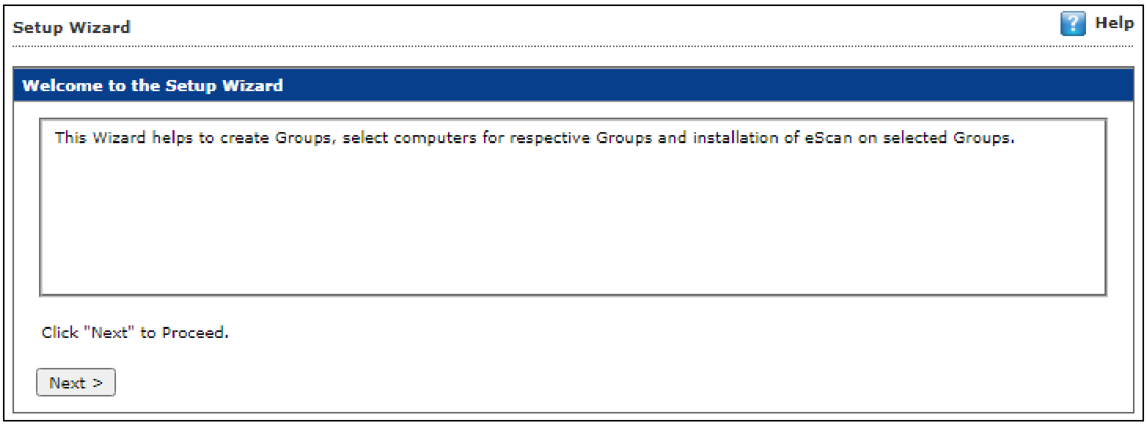
Clicking **Refresh** let you refresh the eScan Management Console.

Help

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

Setup Wizard

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



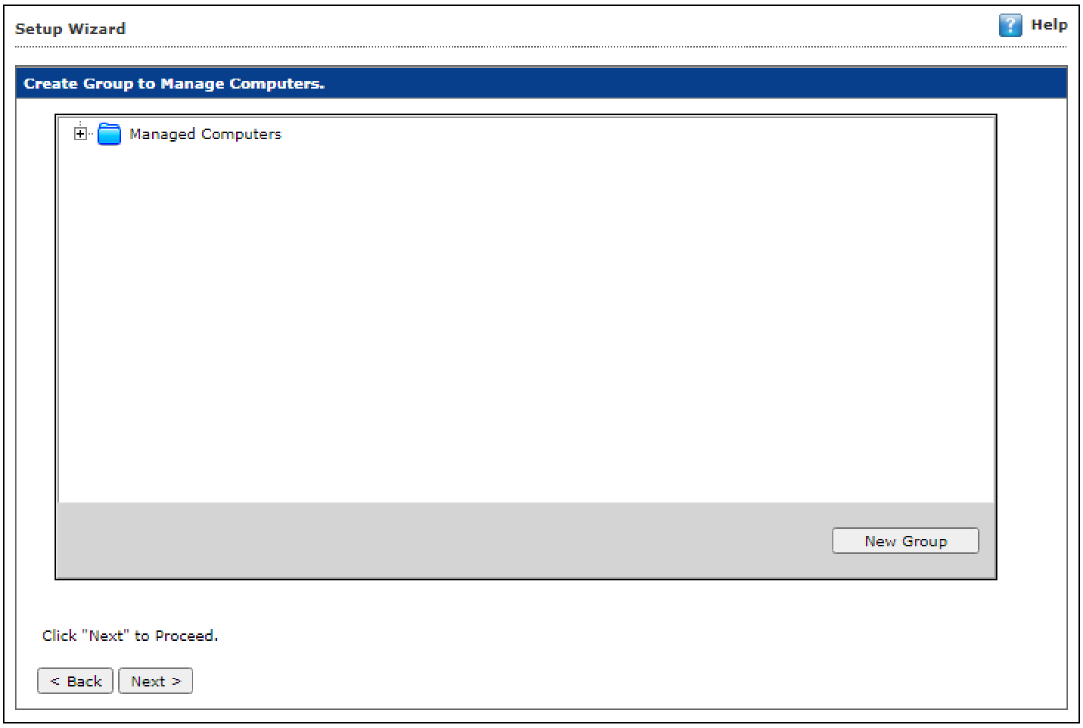
Setup Wizard

Welcome to the Setup Wizard

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

Click "Next" to Proceed.

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



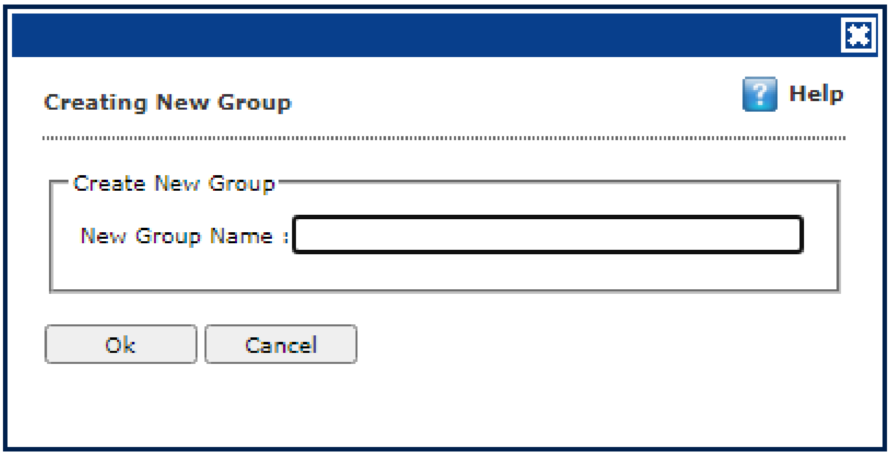
Setup Wizard

Create Group to Manage Computers.

Click "Next" to Proceed.

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

Creating New Group popup appears.

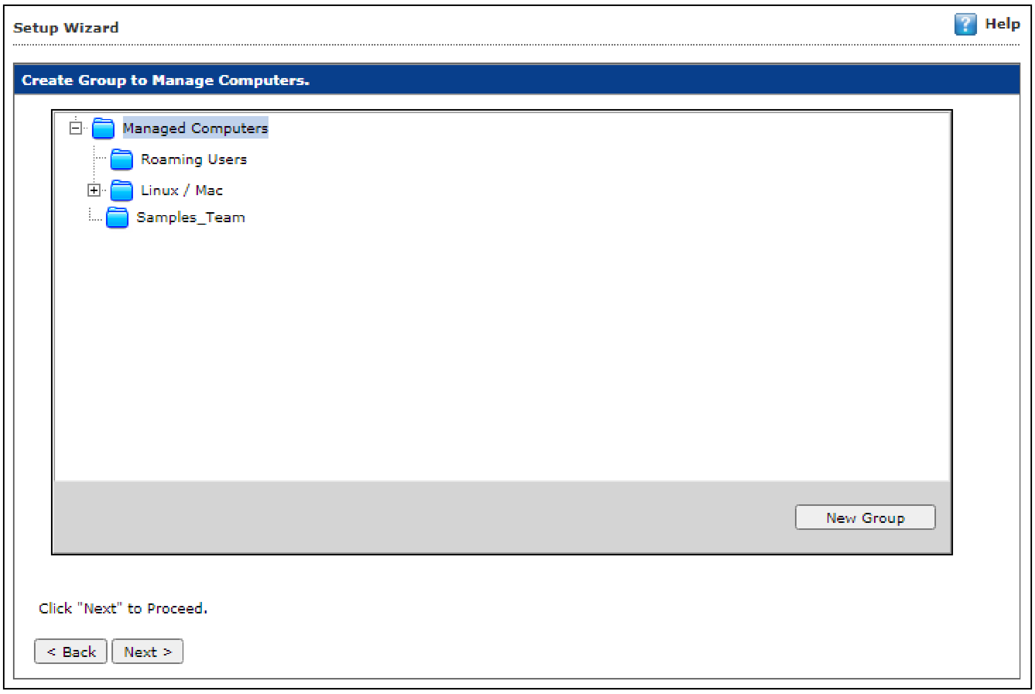


Creating New Group

Create New Group

New Group Name :

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



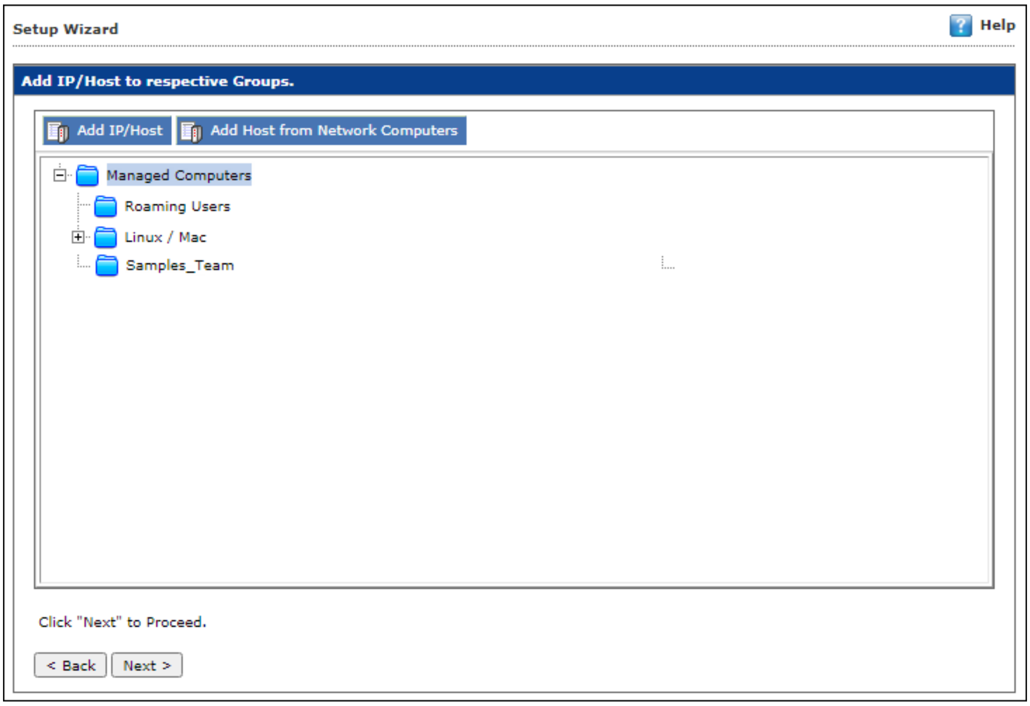
Setup Wizard

Create Group to Manage Computers.

Click "Next" to Proceed.

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

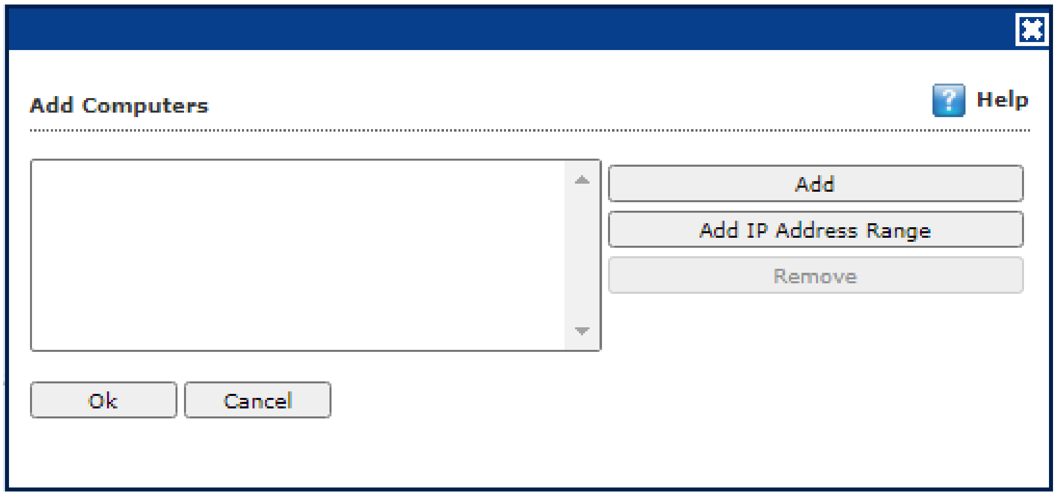
- IP Address/Host name
- Host from Network Computers



Adding computers via IP Address/Host Name

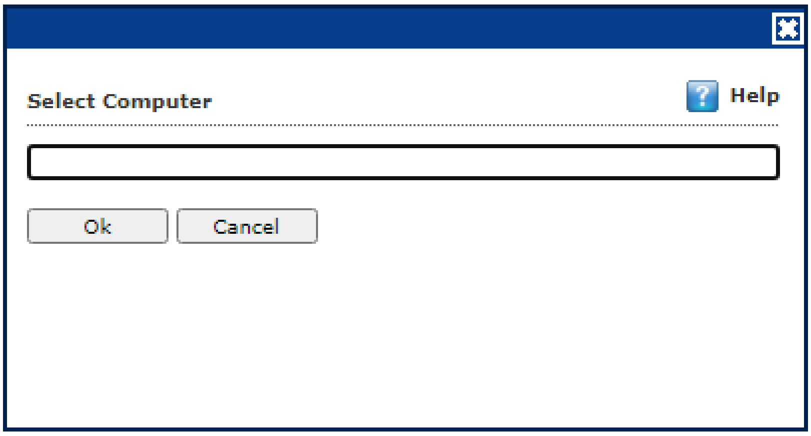
To add the computers through IP Address, follow the below steps:

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



2. Click **Add**.

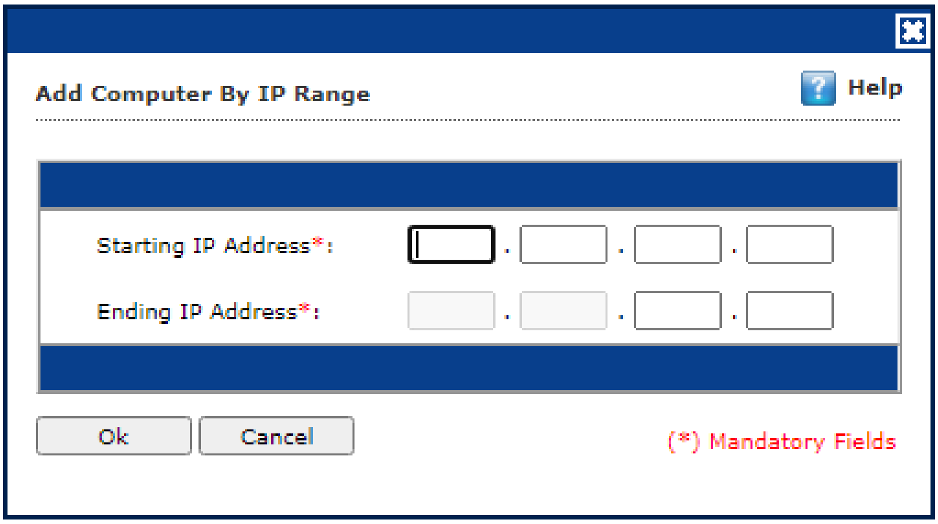
Select Computers popup appears.



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

   OR

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



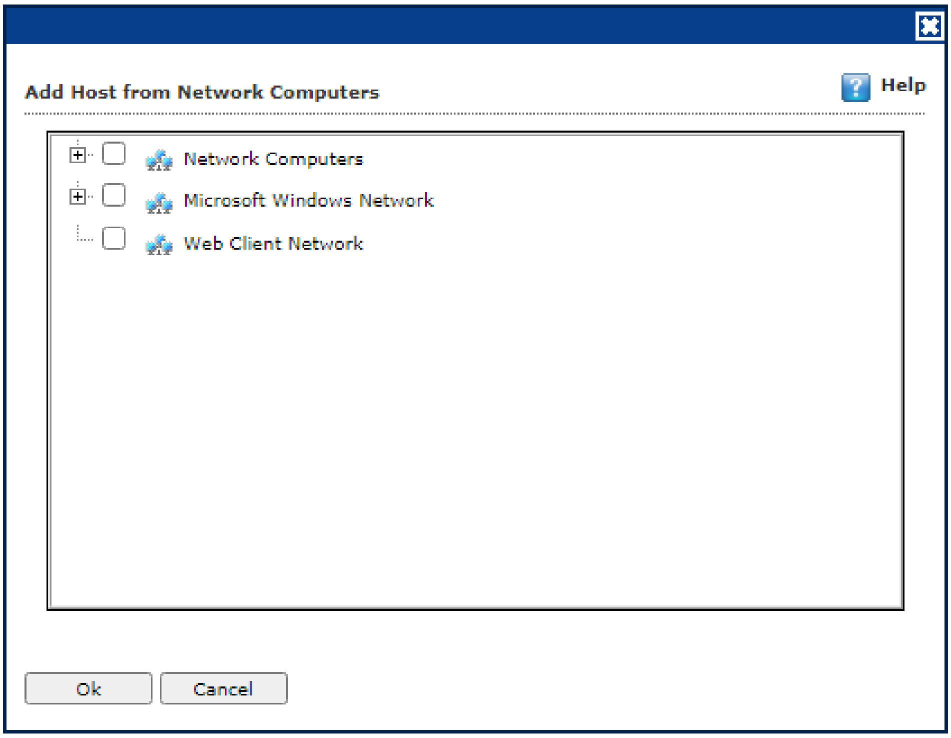
5. Enter the **Start** and **End IP Address**.
6. Click **Ok**.

The computers will be added in the group.

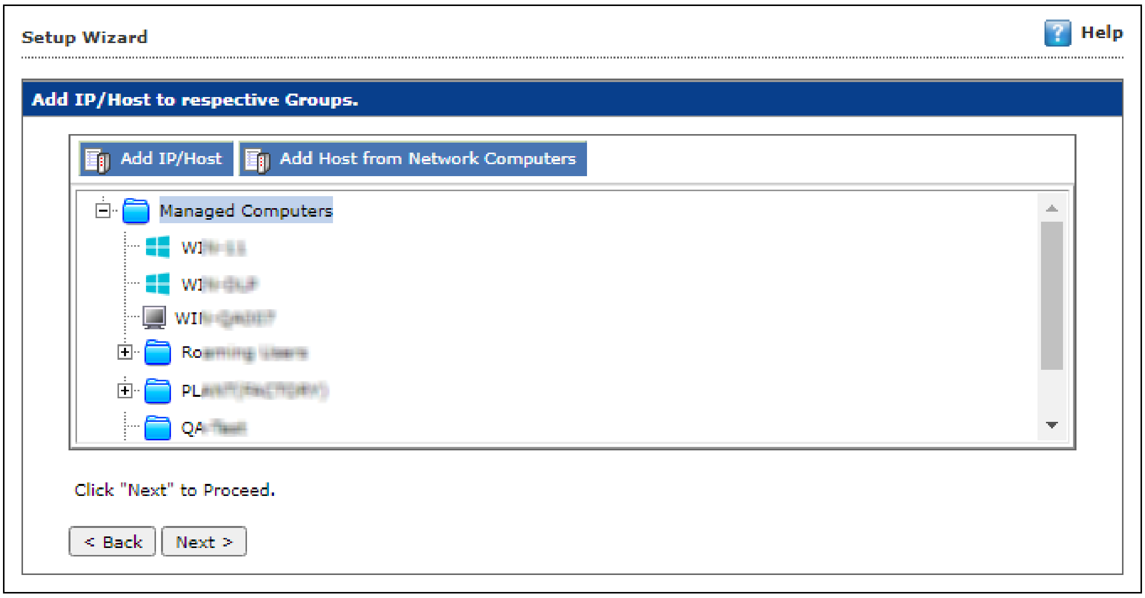
Adding Host Name from Network Computers

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

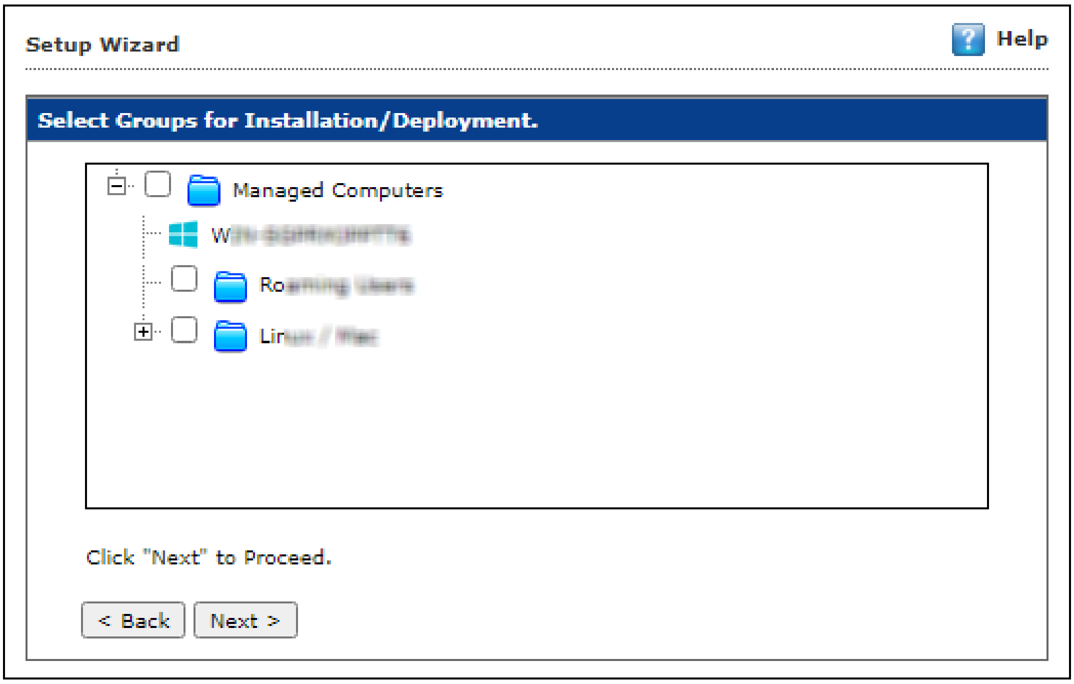
1. Select the group and click **Add Host from Network Computers**.
   Add Host from Network Computers window appears.



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



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

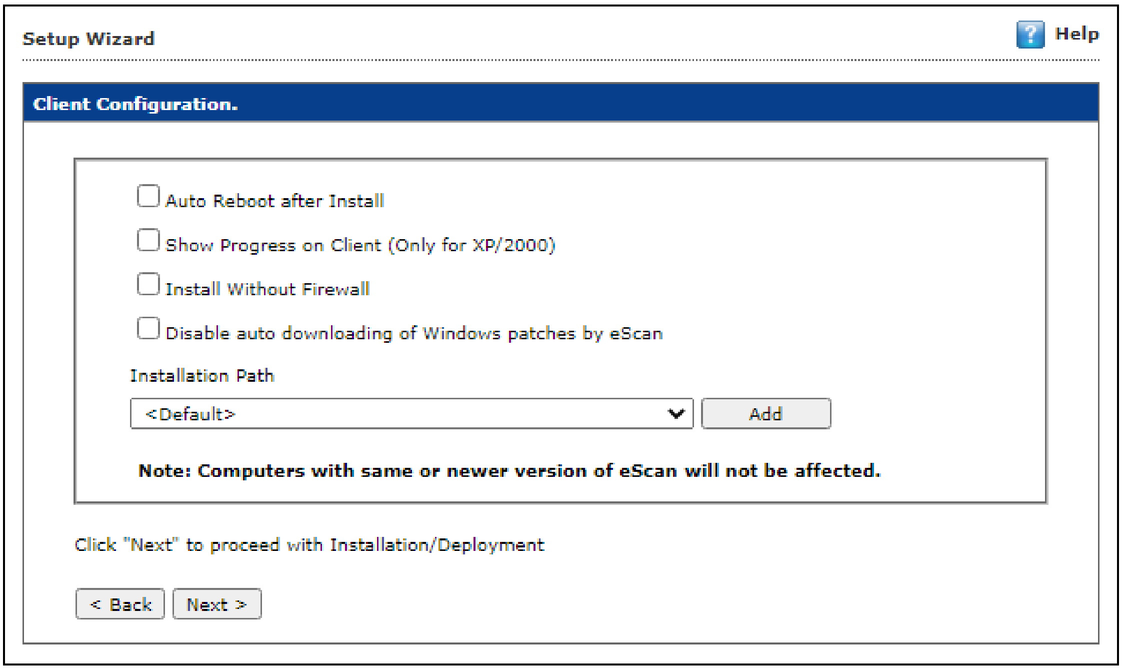


Setup Wizard

Select Groups for Installation/Deployment.

Click "Next" to Proceed.

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



Setup Wizard

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>

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

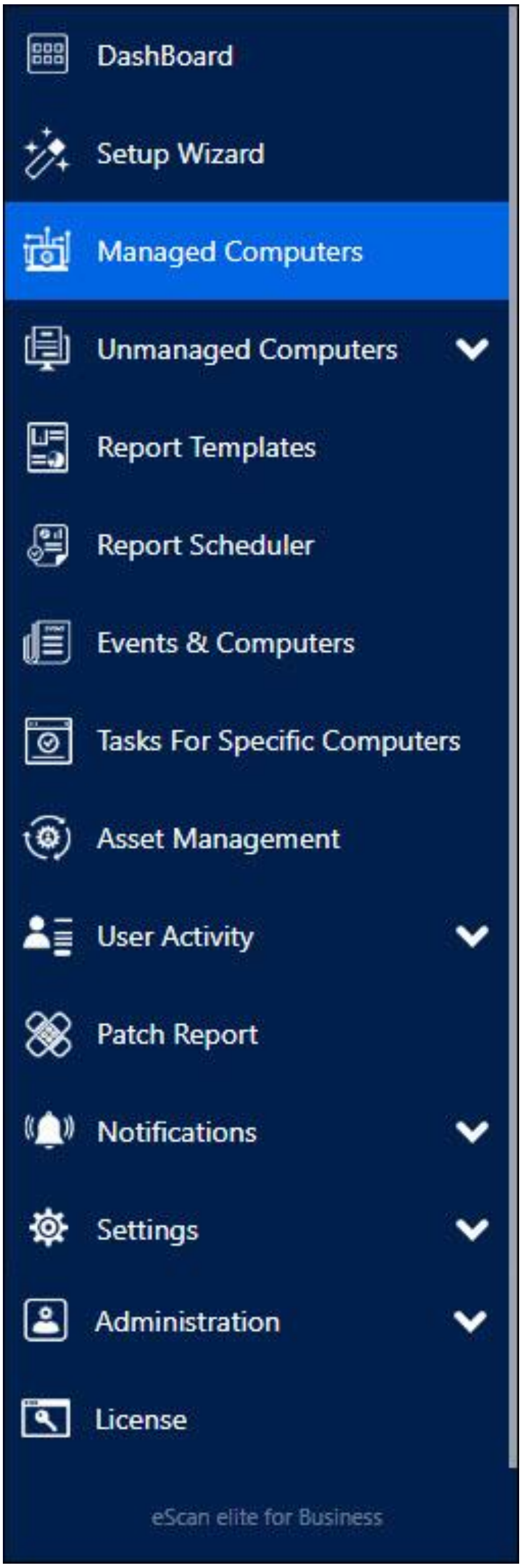
Click "Next" to proceed with Installation/Deployment

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

A window displays File transfer progress.

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

Navigation Panel



Dashboard

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

Setup Wizard

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

Managed Computers

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

Unmanaged Computers

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

Report Templates

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

Report Scheduler

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

Events and Computers

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

Tasks for Specific Computers

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

Asset Management

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

User Activity

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

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 options to enable different notifications when different actions/incidents occur on the endpoints. You may choose to be notified or not to be notified based on the significance of these actions in your business. To learn more, click here.

Settings

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

Administration

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

License

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

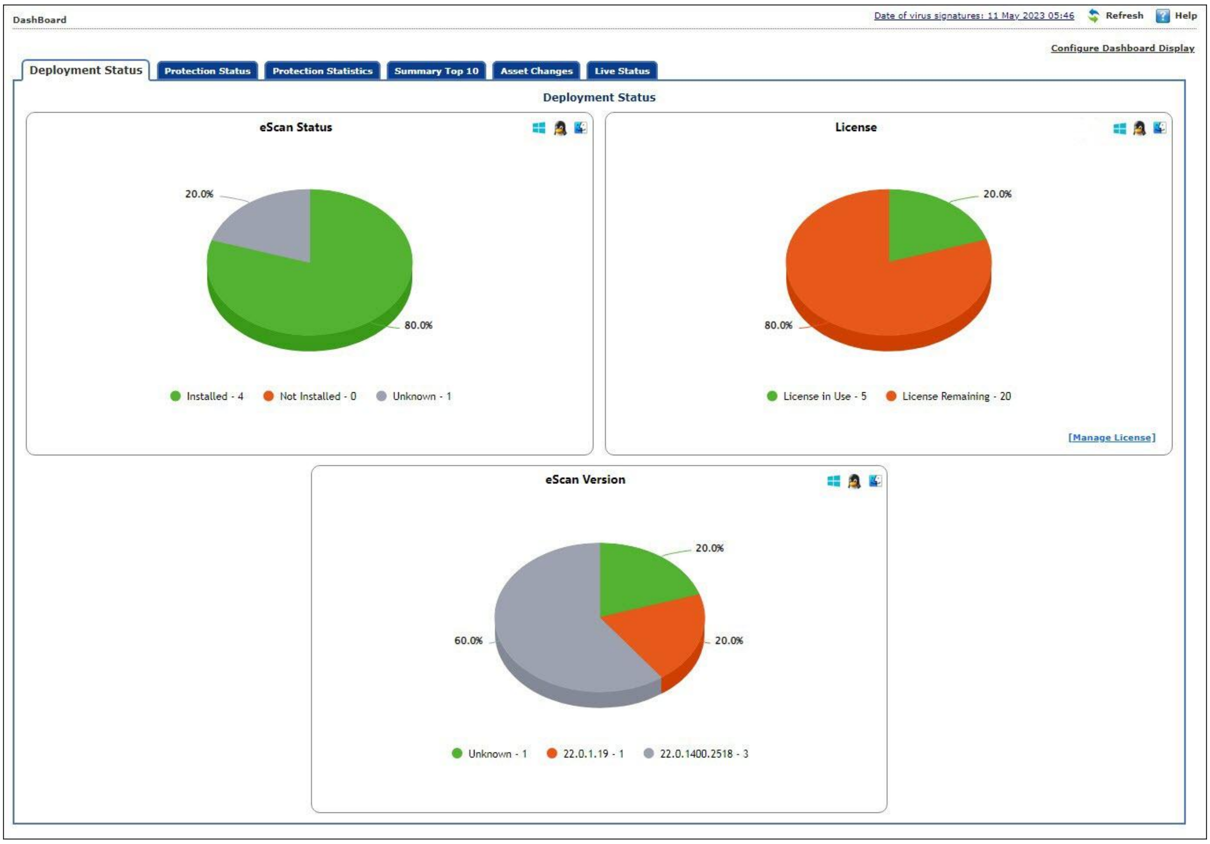
Dashboard

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

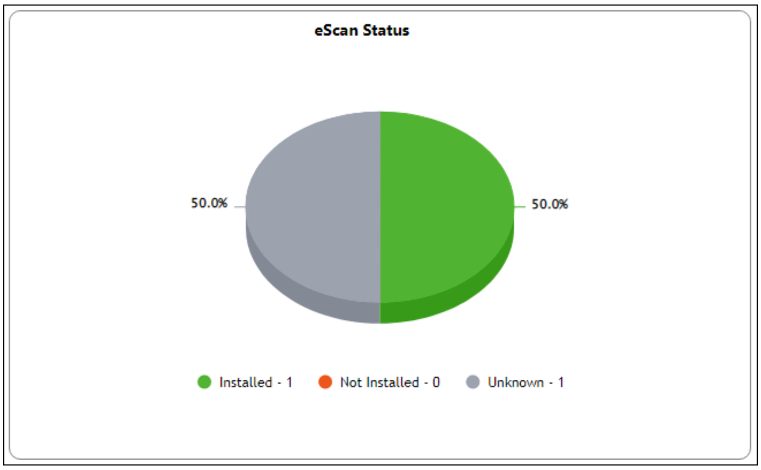
- **Deployment Status**
- **Protection Status**
- **Protection Statistics**
- **Summary Top 10**
- **Asset Changes**
- **Live Status**

Deployment Status

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

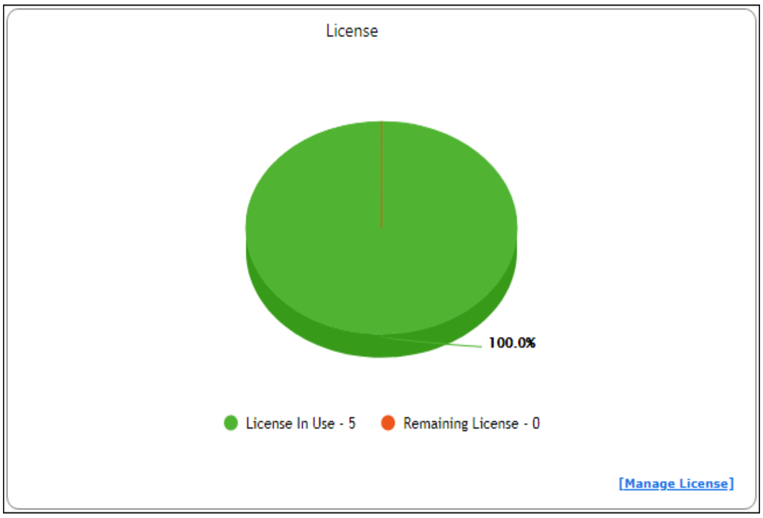


eScan Status



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)

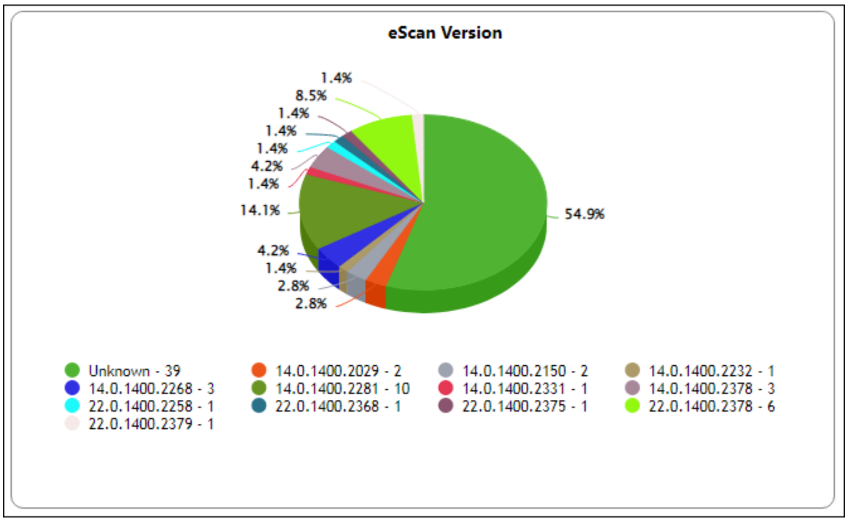
License



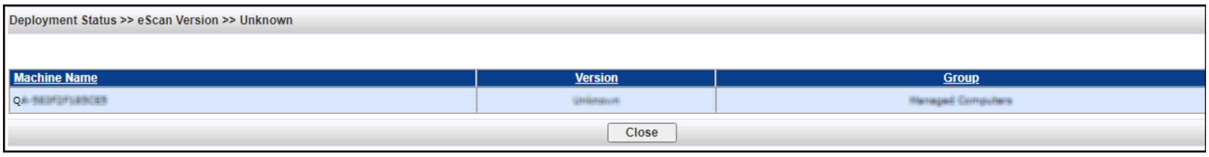
License in Use - It displays the number of licenses that are active.
Licenses Remaining - It displays the number of remaining licenses.

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.

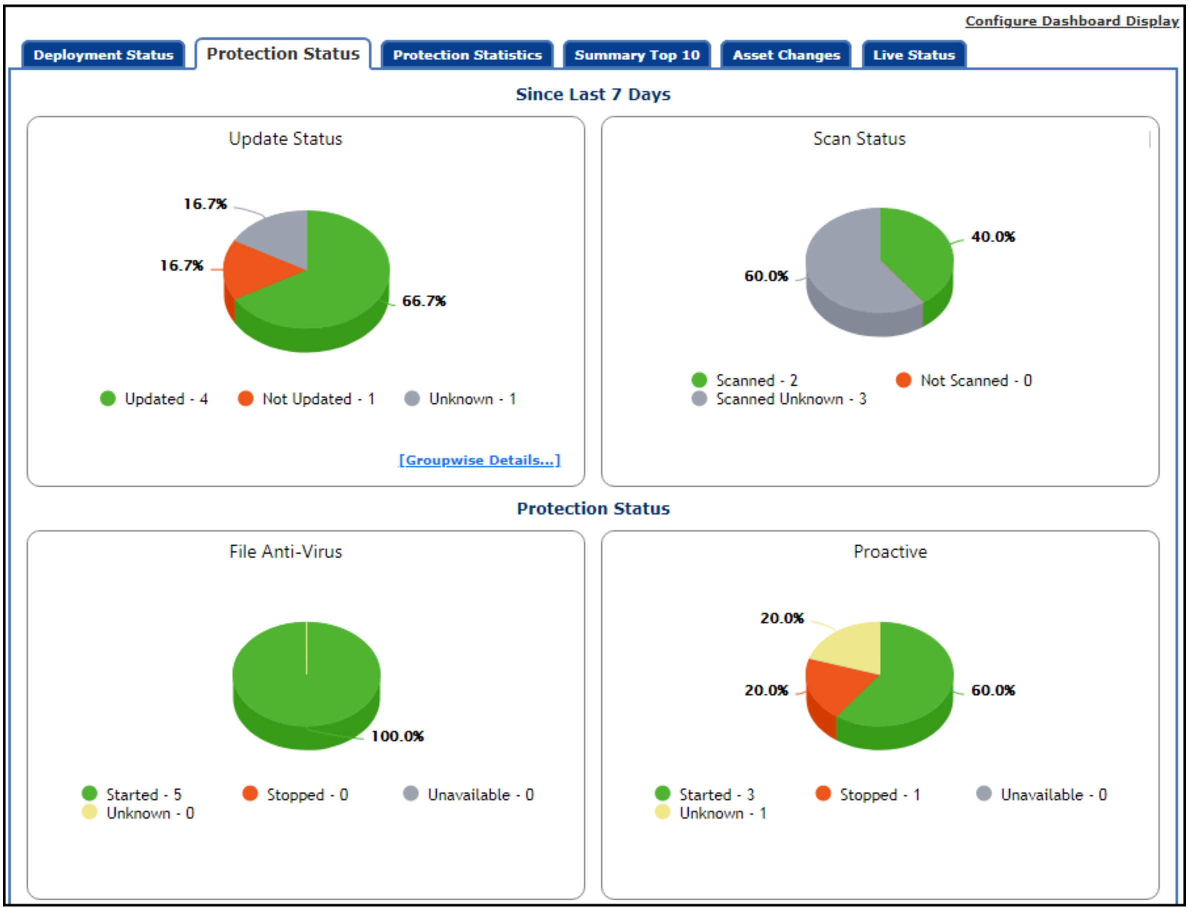

Deployment Status >> eScan Version >> Unknown

Machine Name	Version	Group
QA-[redacted]	[redacted]	[redacted]

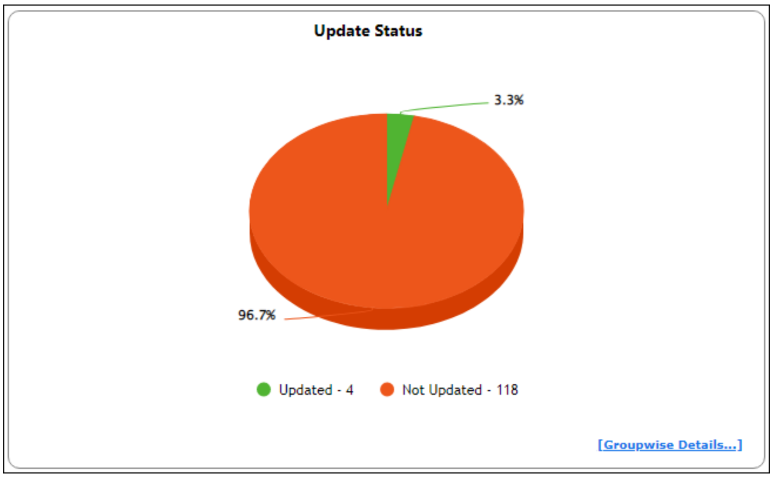
NOTE	Clicking underlined numerical displays detailed information for computers.

Protection Status

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

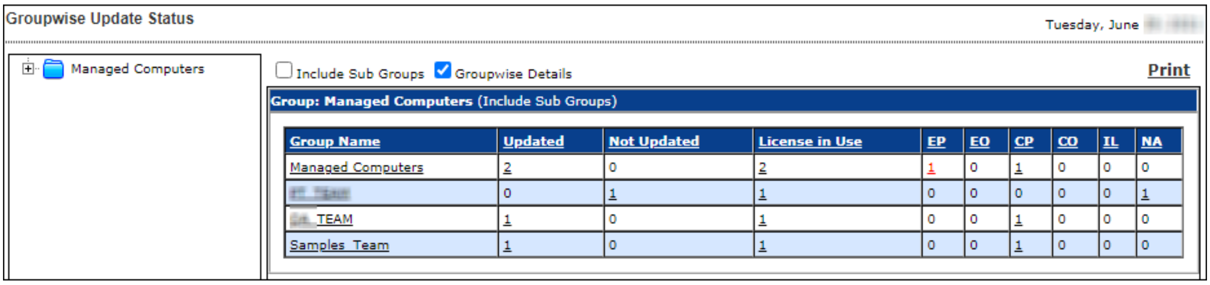


Update Status



Updated – It displays the number of computers on which virus signature database is updated.
Not Updated - It displays the number of computers on which virus signature database is not updated.

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



Groupwise Update Status

Tuesday, June [redacted]

Managed Computers

□ Include Sub Groups ☑ Groupwise Details

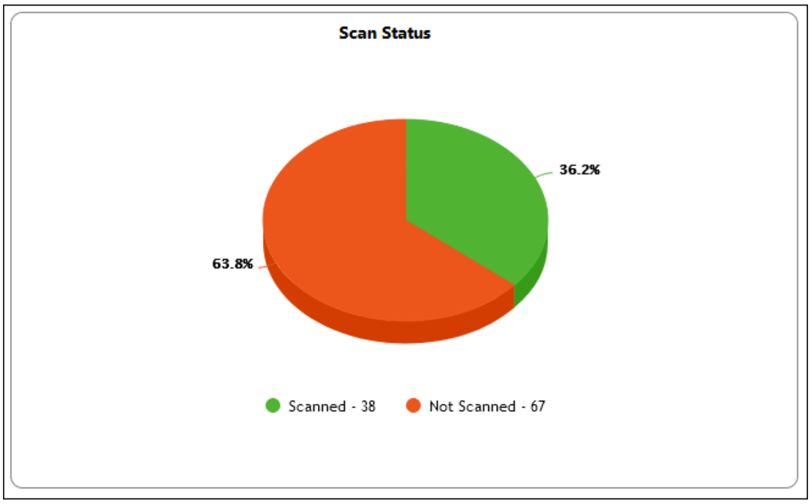
Print

Group: Managed Computers (Include Sub Groups)

Group Name	Updated	Not Updated	License in Use	EP	EO	CP	CO	IL	NA
Managed Computers	2	0	2	1	0	1	0	0	0
[redacted]	0	1	1	0	0	0	0	0	1
[redacted] TEAM	1	0	1	0	0	1	0	0	0
Samples_Team	1	0	1	0	0	1	0	0	0

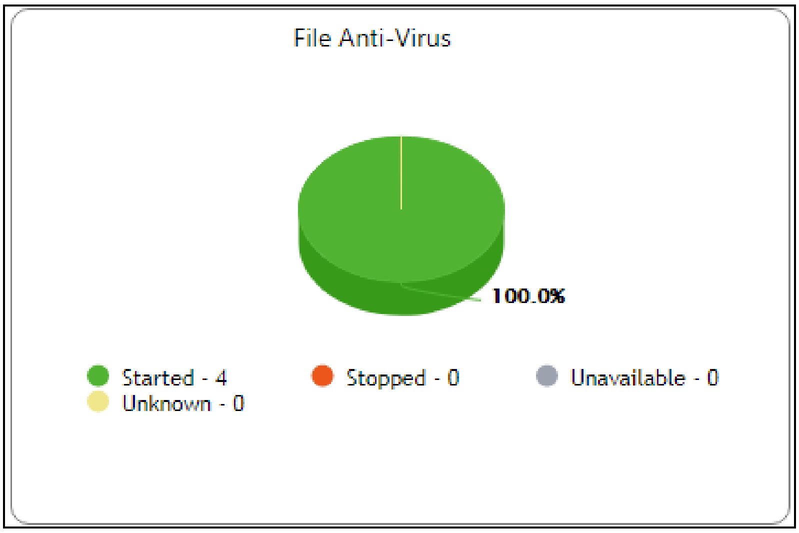
It displays the number of computers on which virus database is Updated, Not Updated and Licenses in Use as per the group.
Selecting **Include Sub Groups** checkbox will display the subgroups containing computers.

Scan Status



Scanned - It displays the number of computers that have been scanned in last 7 days for viruses and malware infections.
Not Scanned - It displays the number of computers that have not been scanned in last 7 days for virus and malware infections.

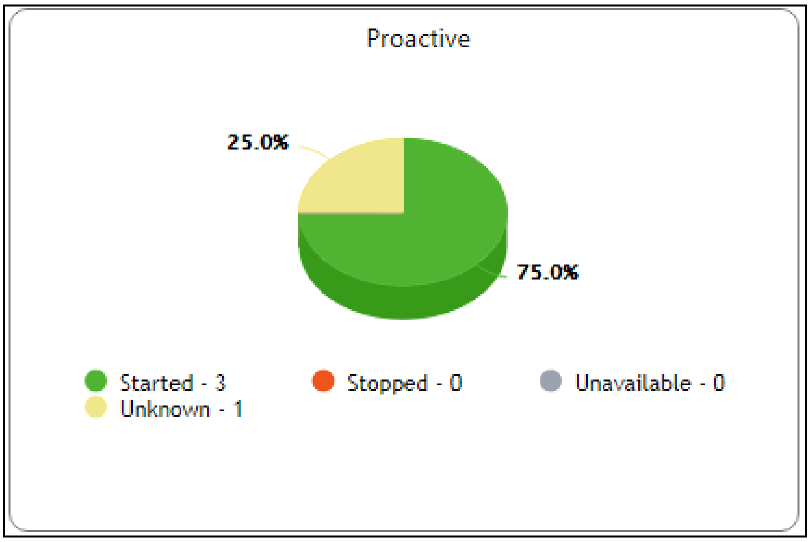
File Anti-Virus



Started – It displays the number of computers on which the File Anti-Virus module is in started state.
Stopped – It displays the number of computers on which the File Anti-Virus module is in stopped state.
Unavailable – It displays the number of computers where the File Anti-Virus module is unavailable.
Unknown – It displays the number of computers where the File Anti-Virus module status is unknown.

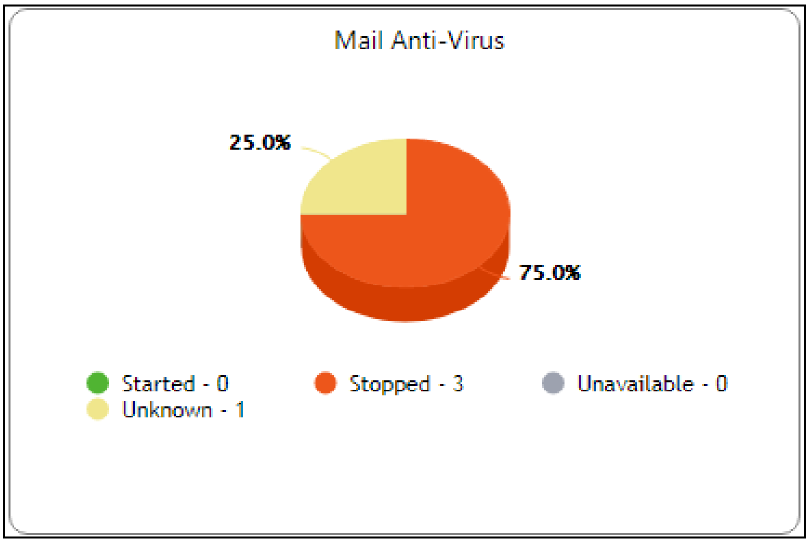
Proactive

This module is available only in computers with Windows OS.



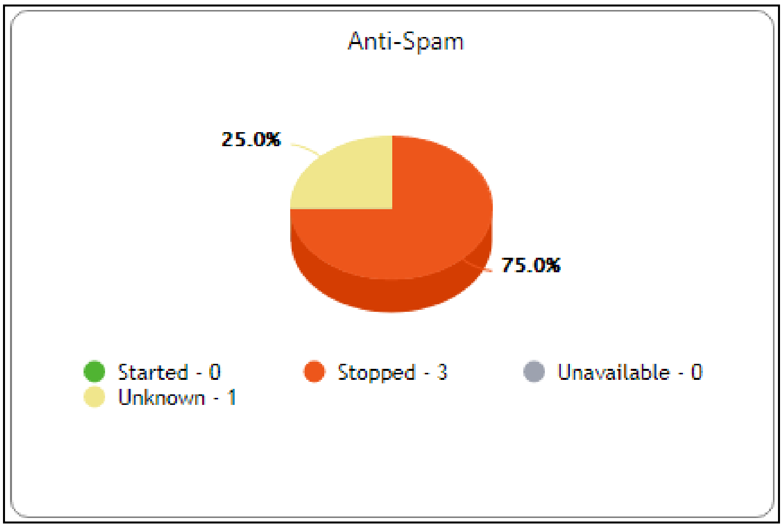
Started - It displays the number of computers on which Proactive scanning service is running.
Stopped - It displays the number of computers on which Proactive scanning service is stopped.
Unavailable – It displays the number of computers where Proactive scanning service is unavailable.
Unknown - It displays the number of computers on which the Proactive scanning service status is unknown.

Mail Anti-Virus



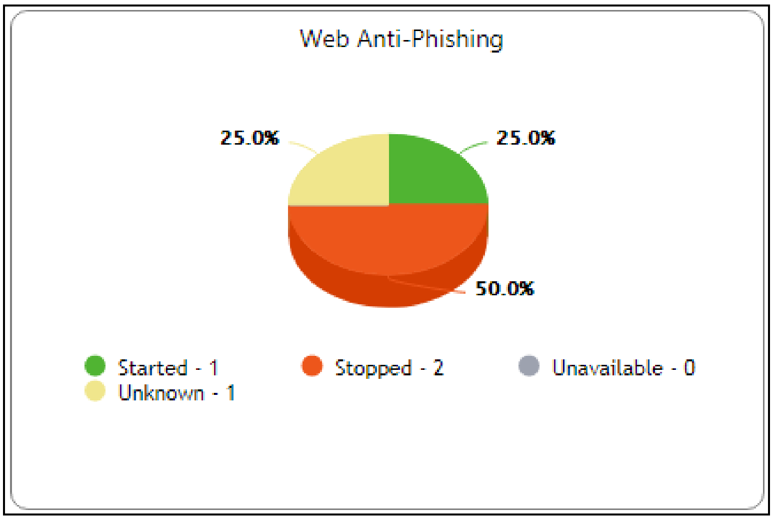
Started – It displays the number of computers on which the Mail Anti-Virus module is in started state.
Stopped – It displays the number of computers on which the Mail Anti-Virus module is in stopped state.
Unavailable – It displays the number of computers on which the Mail Anti-Virus module is unavailable.
Unknown – It displays the number of computers on which the Mail Anti-Virus module status is unknown.

Anti-Spam



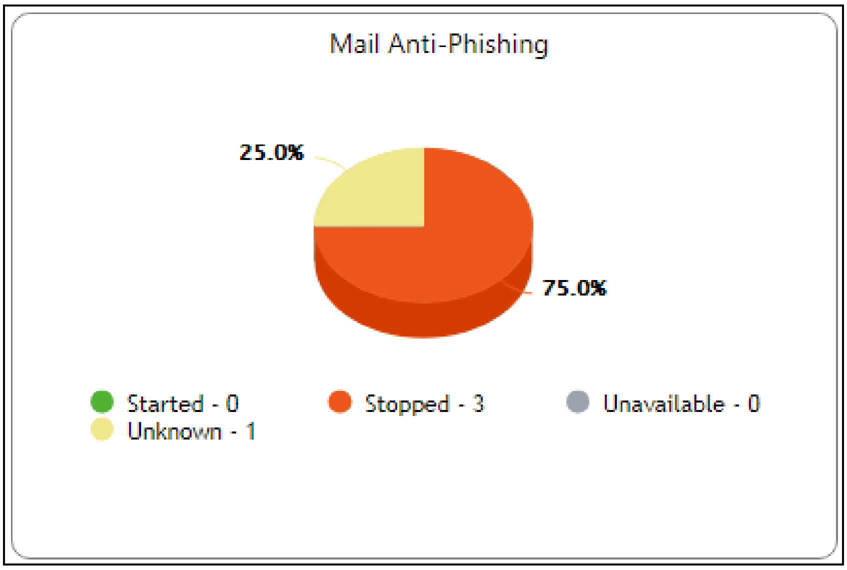
Started – It displays the number of computers on which the Anti-Spam module is in started state.
Stopped – It displays the number of computers on which the Anti-Spam module is in stopped state.
Unavailable – It displays the number of computers on which the Anti-Spam module is unavailable.
Unknown – It displays the number of computers on which the Anti-Spam module status is unknown.

Web Anti-Phishing



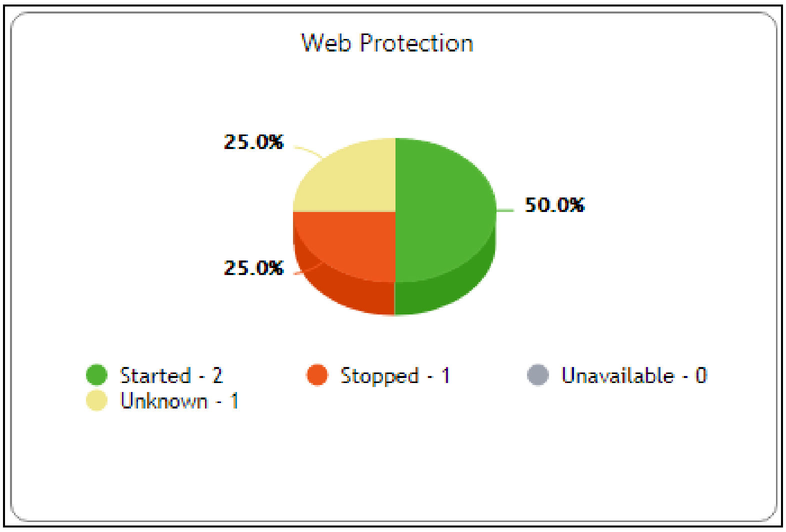
Started – It displays the number of computers on which the Web Anti-Phishing service is started.
Stopped – It displays the number of computers on which the Web Anti-Phishing service is stopped.
Unavailable - It displays the number of computers on which the Web Anti-Phishing service is unavailable.
Unknown – It displays the number of computers on which the Web Anti-Phishing service status is unknown.

Mail Anti–Phishing



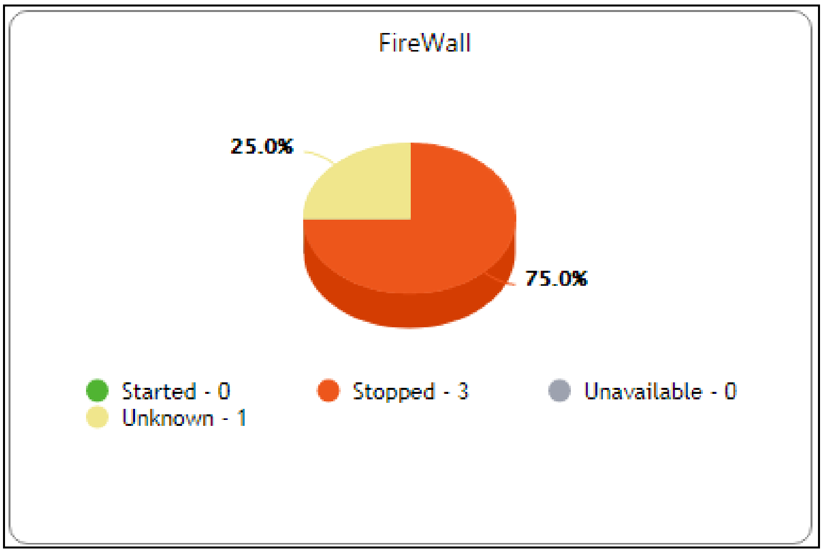
Started – It displays the number of computers on which the Mail Anti-Phishing service is enabled.
Stopped – It displays the number of computers on which the Mail Anti-Phishing service is disabled.
Unavailable – It displays the number of computers on which the Mail Anti-Phishing service is unavailable.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

Web Protection



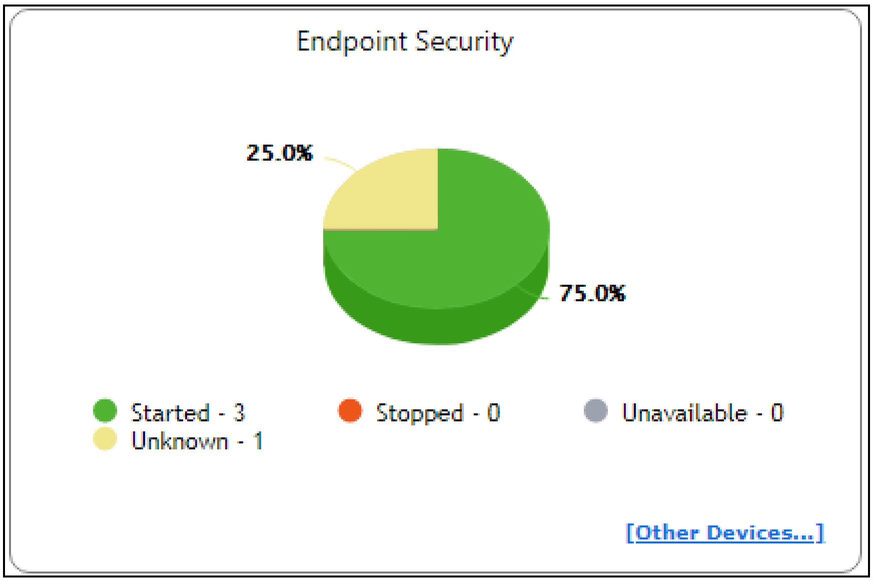
Started – It displays the number of computers on which the Web Protection module is in started state.
Stopped – It displays the number of computers on which the Web Protection module is in stopped state.
Unavailable – It displays the number of computers on which the Web Protection module is unavailable.
Unknown – It displays the number of computers on which the Web Protection module status is unknown.

Firewall



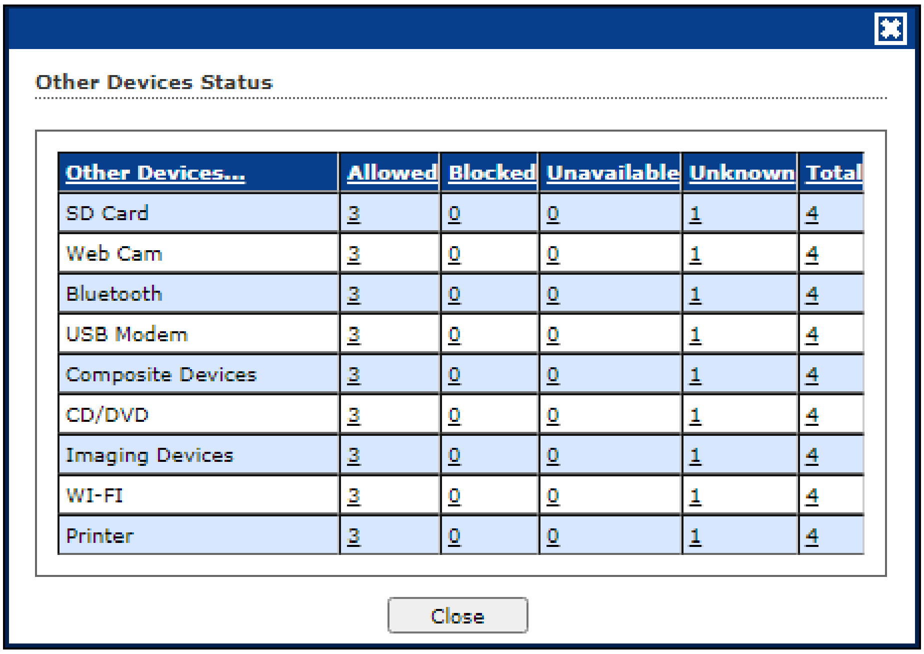
Started - It displays the number of computers on which the Firewall module is in started state.
Stopped - It displays the number of computers on which the Firewall module is in stopped state.
Unavailable - It displays the number of computers on which the Firewall module is unavailable.
Unknown - It displays the number of computers on which the Firewall module status is unknown.

Endpoint Security



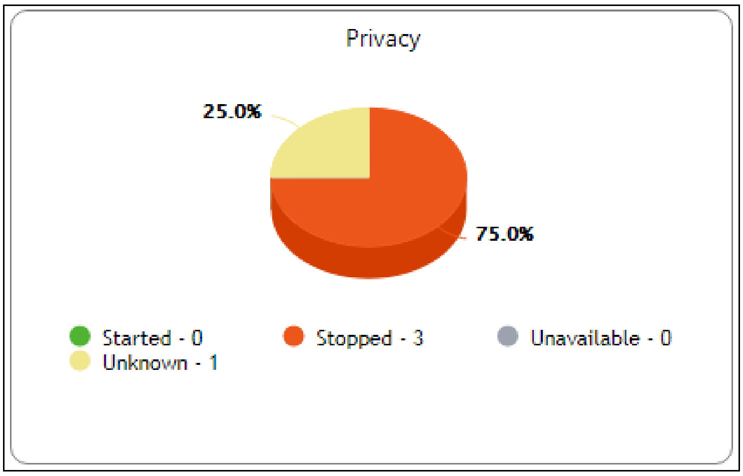
Started - It displays the number of computers on which the Endpoint Security module is in started state.
Stopped - It displays the number of computers on which the Endpoint Security module is in stopped state.
Unavailable – It displays the number of computers on which the Endpoint Security module is unavailable.
Unknown - It displays the number of computers on which the Endpoint Security module status is unknown.

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



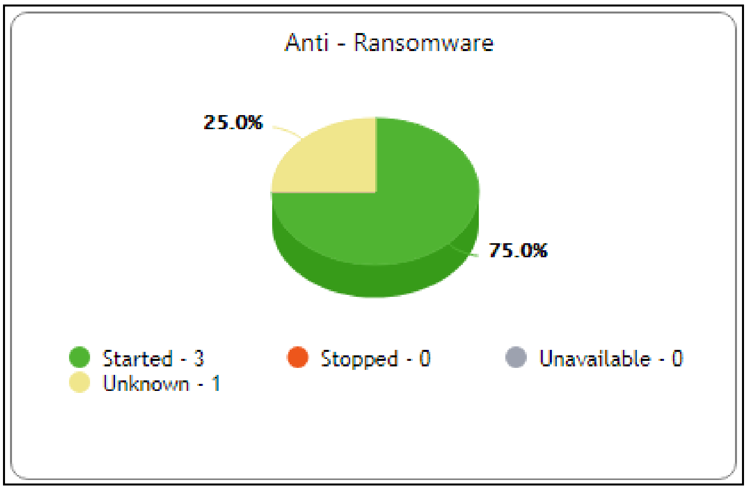
Other Devices...	Allowed	Blocked	Unavailable	Unknown	Total
SD Card	3	0	0	1	4
Web Cam	3	0	0	1	4
Bluetooth	3	0	0	1	4
USB Modem	3	0	0	1	4
Composite Devices	3	0	0	1	4
CD/DVD	3	0	0	1	4
Imaging Devices	3	0	0	1	4
WI-FI	3	0	0	1	4
Printer	3	0	0	1	4

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.

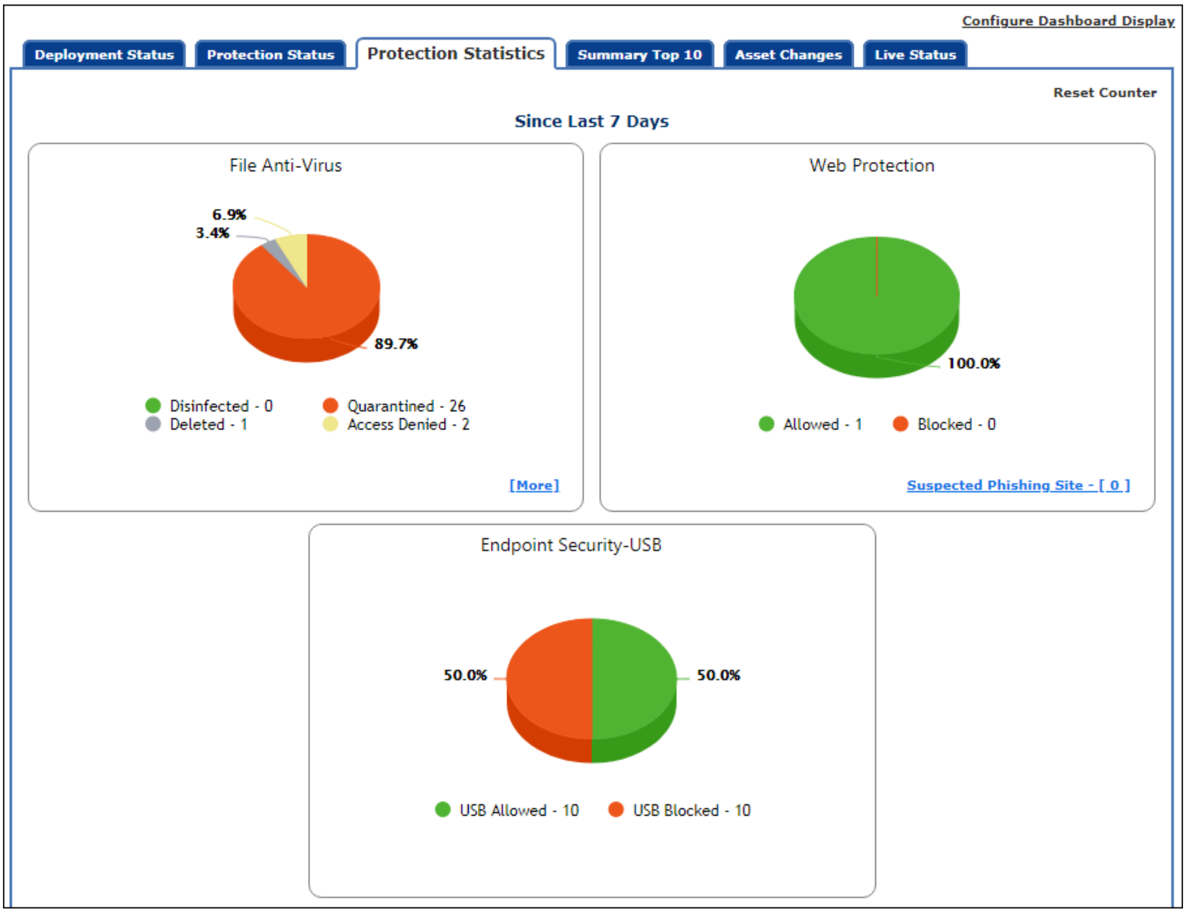
Anti – Ransomware



Started - It displays the number of computers on which the Anti – Ransomware module is in started state.
Stopped - It displays the number of computers on which the Anti – Ransomware module is in stopped state.
Unavailable – It display the number of computers on which the Anti – Ransomware module unavailable to system.
Unknown - It displays the number of computers on which the Anti – Ransomware module status is unknown.

Protection Statistics

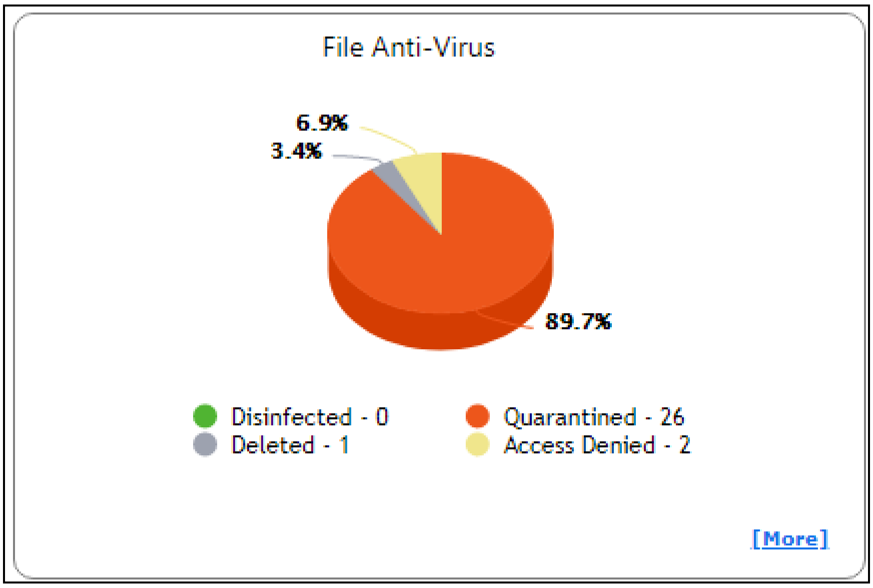
This tab displays activity statistics and action taken by all modules of eScan Client since last seven days in pie chart format.



Reset Counter

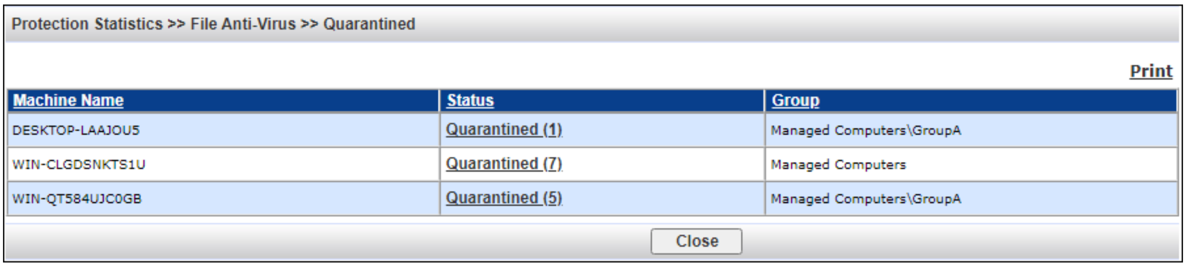
Clicking **Reset Counter** resets all the statistics to zero. This option proves useful after you have taken an action on infected files and want to scan for residual infection presence.

File Anti-Virus



Disinfected – It displays the number of files disinfected by File Anti-Virus module.
Quarantined – It displays the number of files quarantined by File Anti-Virus module.
Deleted - It displays the number of files deleted by File Anti-Virus module.
Access Denied - It displays Access was denied on file by File Anti-Virus module.

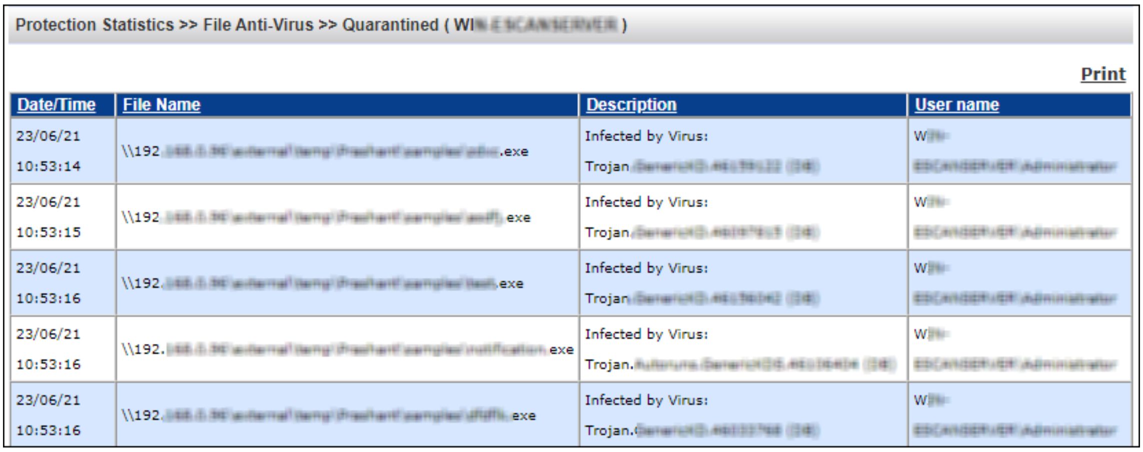
Clicking underlined numerical displays action taken on infected files amongst different computers and groups that computer belongs to.


Protection Statistics >> File Anti-Virus >> Quarantined

Print

Machine Name	Status	Group
DESKTOP-LAAJOU5	Quarantined (1)	Managed Computers\GroupA
WIN-CLGDSNKTS1U	Quarantined (7)	Managed Computers
WIN-QT584UJC0GB	Quarantined (5)	Managed Computers\GroupA

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

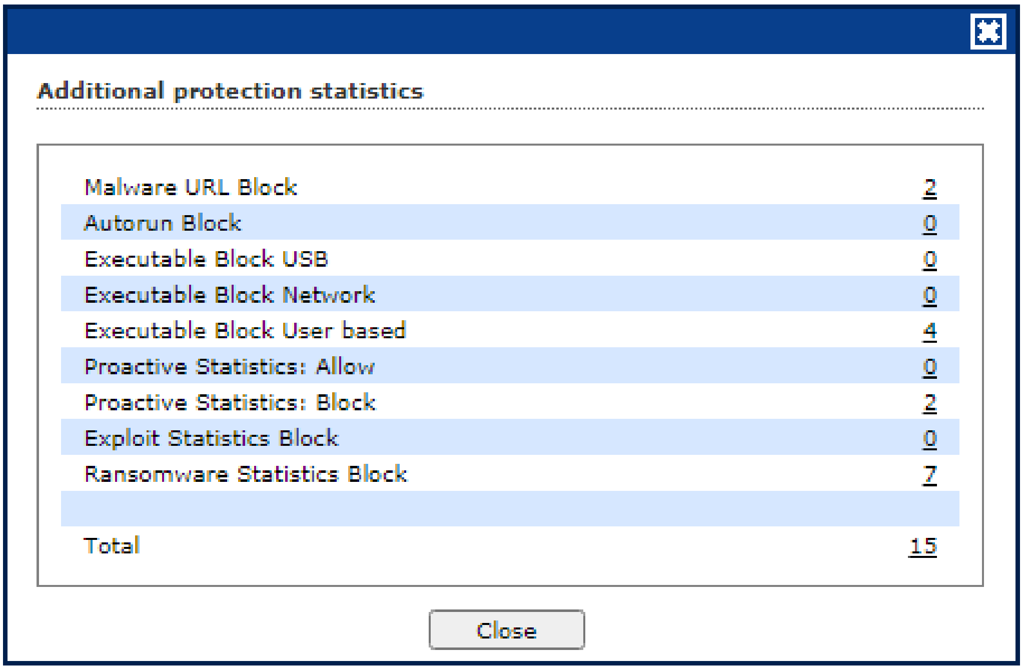


Protection Statistics >> File Anti-Virus >> Quarantined (WI[redacted])

Print

Date/Time	File Name	Description	User name
23/06/21 10:53:14	\\192.[redacted].exe	Infected by Virus: Trojan.[redacted]	W[redacted]
23/06/21 10:53:15	\\192.[redacted].exe	Infected by Virus: Trojan.[redacted]	W[redacted]
23/06/21 10:53:16	\\192.[redacted].exe	Infected by Virus: Trojan.[redacted]	W[redacted]
23/06/21 10:53:16	\\192.[redacted].exe	Infected by Virus: Trojan.[redacted]	W[redacted]
23/06/21 10:53:16	\\192.[redacted].exe	Infected by Virus: Trojan.[redacted]	W[redacted]

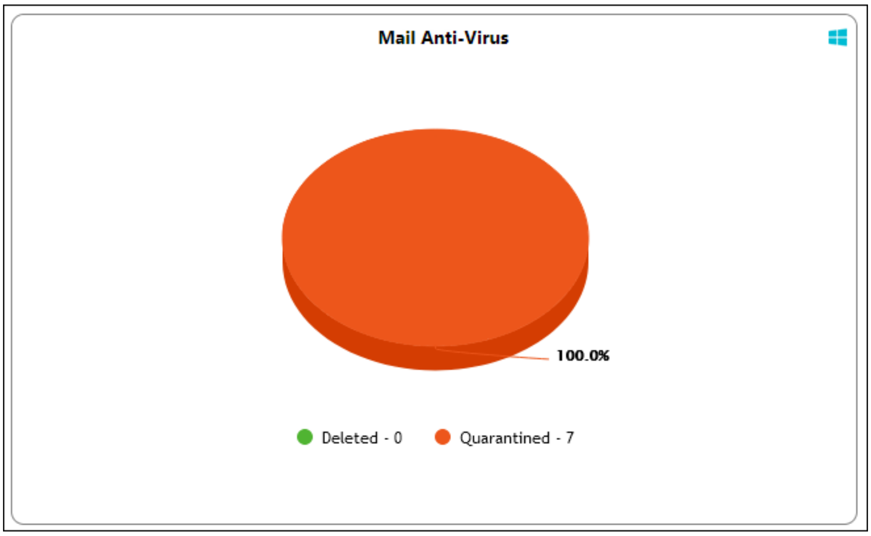
Clicking **[More]** displays additional protection statistics.



Additional protection statistics

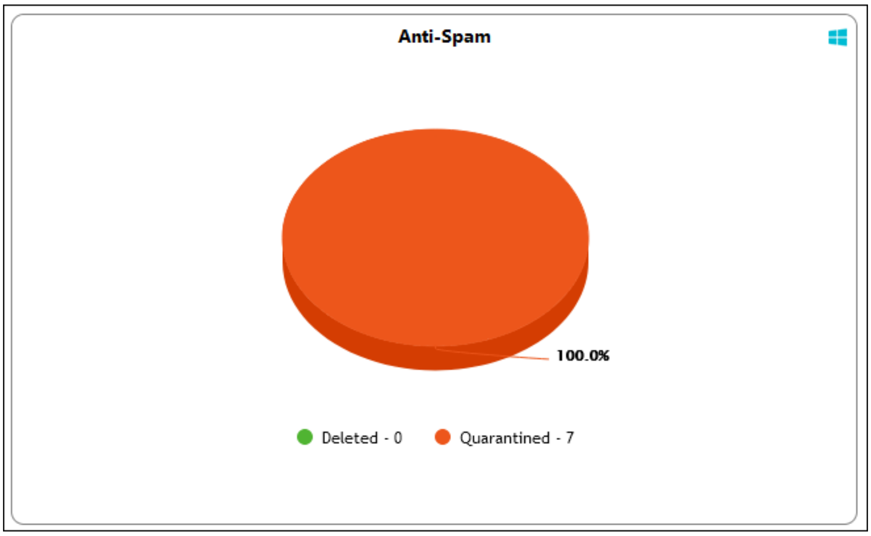
Malware URL Block	2
Autorun Block	0
Executable Block USB	0
Executable Block Network	0
Executable Block User based	4
Proactive Statistics: Allow	0
Proactive Statistics: Block	2
Exploit Statistics Block	0
Ransomware Statistics Block	7
Total	15

Mail Anti-Virus



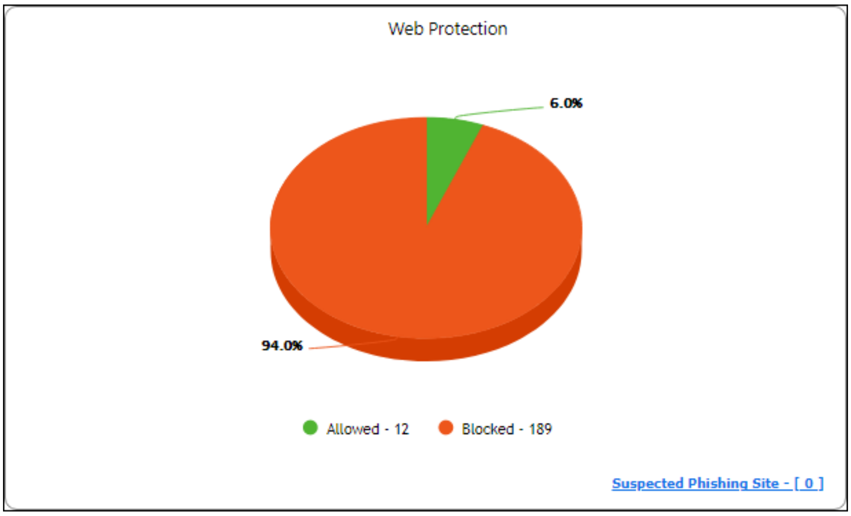
Deleted – It displays the number of files/emails deleted by Mail Anti-Virus module.
Quarantined – It displays the number of files/emails quarantined by Mail Anti-Virus module.

Anti-Spam



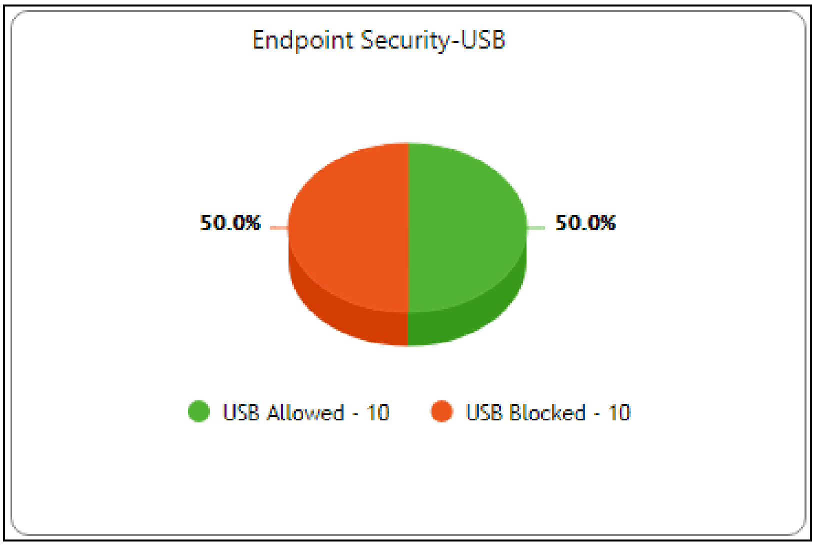
Deleted – It displays the number of mails deleted by Anti-Spam module.
Quarantined – It displays the number of mails quarantined by Anti-Spam module.

Web Protection



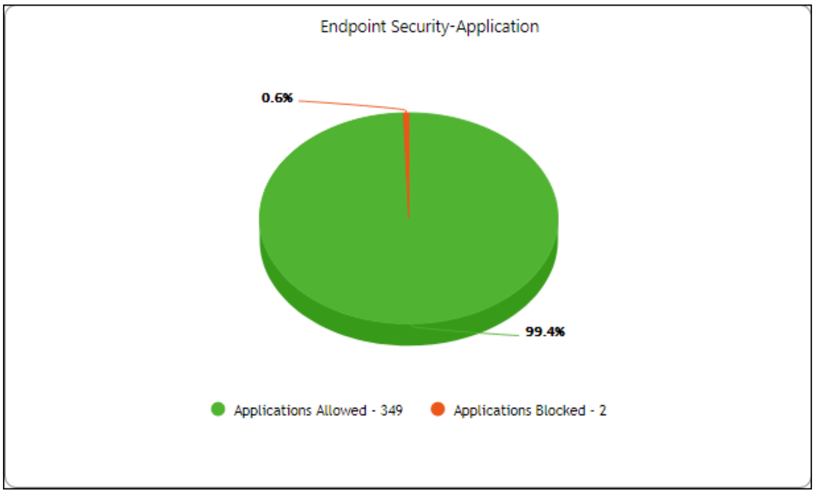
Allowed – It displays the number of websites to which access was allowed by Web Protection module.
Blocked – It displays the number of websites to which access was blocked by Web Protection module.
Suspected Phishing Site – It displays the number of systems on which suspected phishing sites were blocked. After clicking the numerical, Suspected Phishing Site window appears displaying System Name, Site Status, and Computer Group.
Clicking **Site Status** further displays Date, Time, Website name and action taken.

Endpoint Security-USB



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

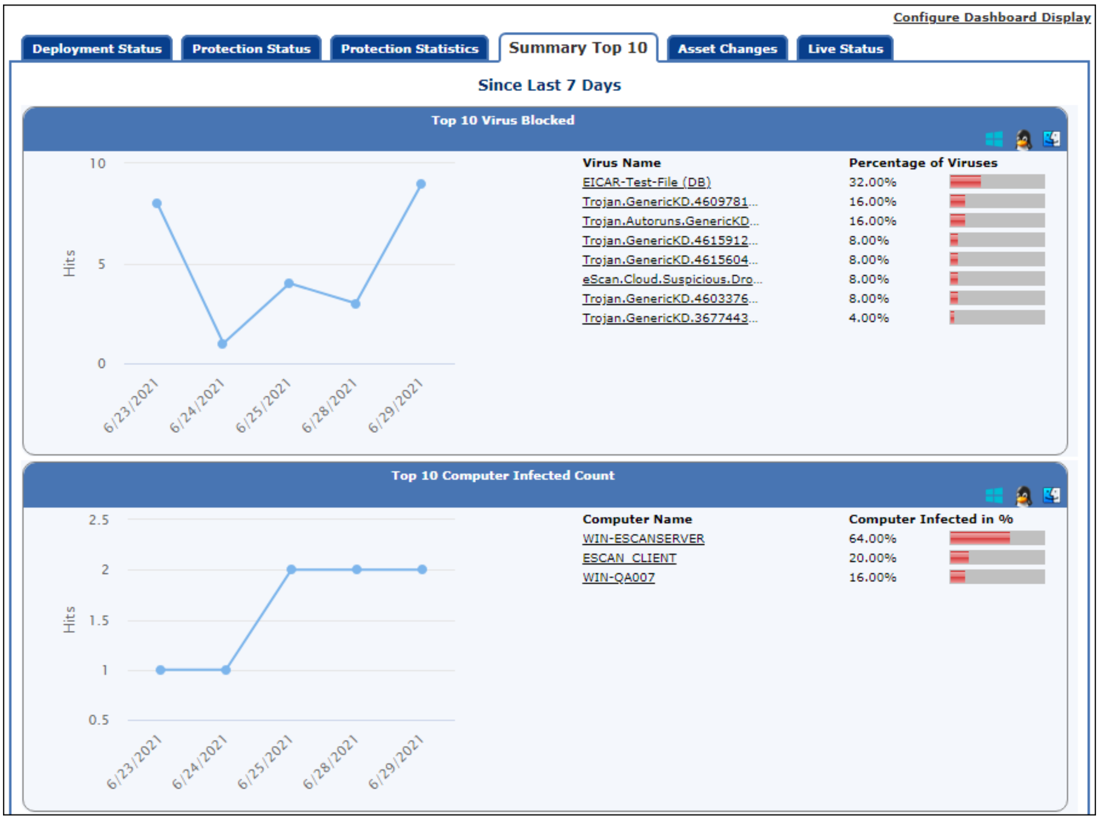
Endpoint Security-Application



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

Summary Top 10

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



Virus Name	Percentage of Viruses
EICAR-Test-File (DB)	32.00%
Trojan.GenericKD.4609781...	16.00%
Trojan.Autoruns.GenericKD...	16.00%
Trojan.GenericKD.4615912...	8.00%
Trojan.GenericKD.4615604...	8.00%
eScan.Cloud.Suspicious.Dro...	8.00%
Trojan.GenericKD.4603376...	8.00%
Trojan.GenericKD.3677443...	4.00%

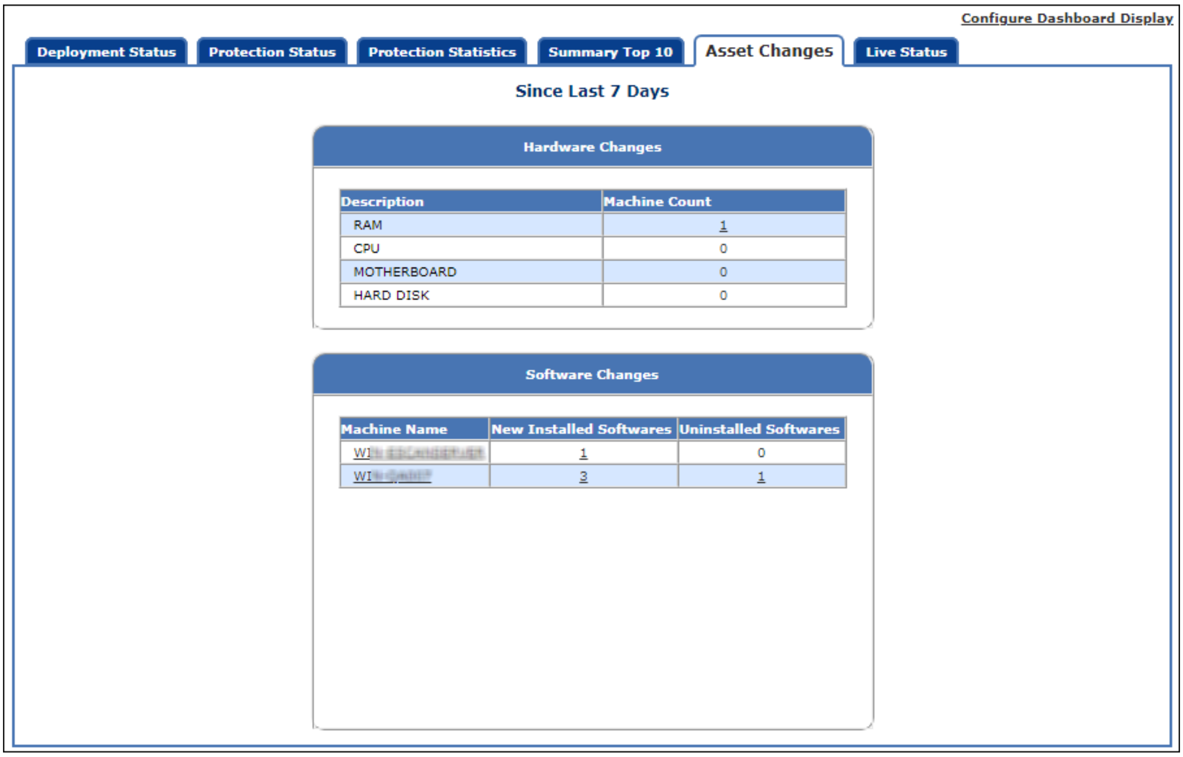
Computer Name	Computer Infected in %
WIN-ESCANSERVER	64.00%
ESCAN_CLIENT	20.00%
WIN-QA007	16.00%

The tab displays the summary for following parameters:

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

Asset Changes

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



Since Last 7 Days

Hardware Changes

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

Software Changes

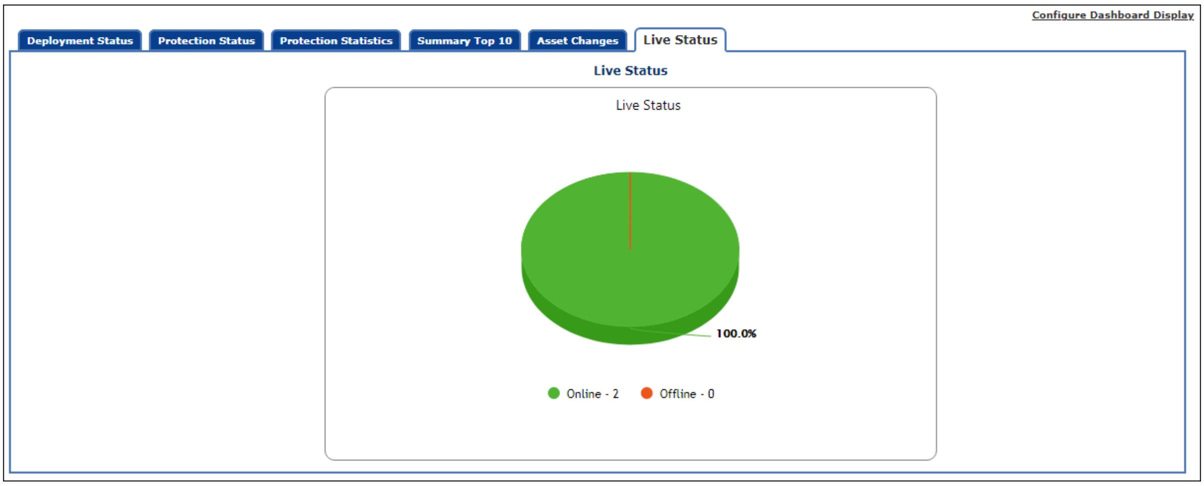
Machine Name	New Installed Softwares	Uninstalled Softwares
WI[redacted]	1	0
WI[redacted]	3	1

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.

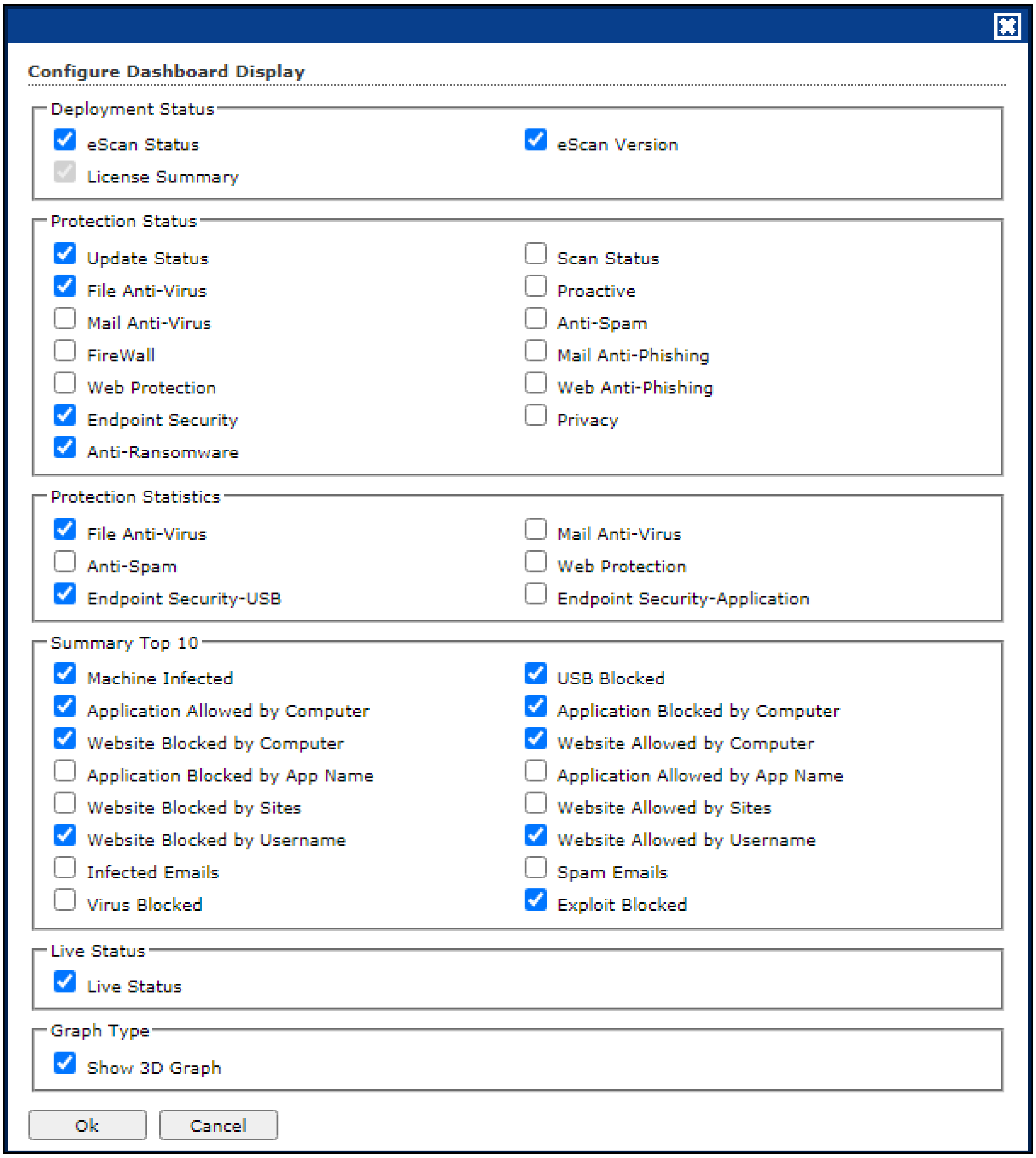


Clicking the numerical displays the computer's username, status, eScan Client version number, and the group under which it is categorized.

Configure the Dashboard Display

To configure the Dashboard display,

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



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
- ☑ 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

Live Status

- ☑ Live Status

Graph Type

- ☑ Show 3D Graph

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

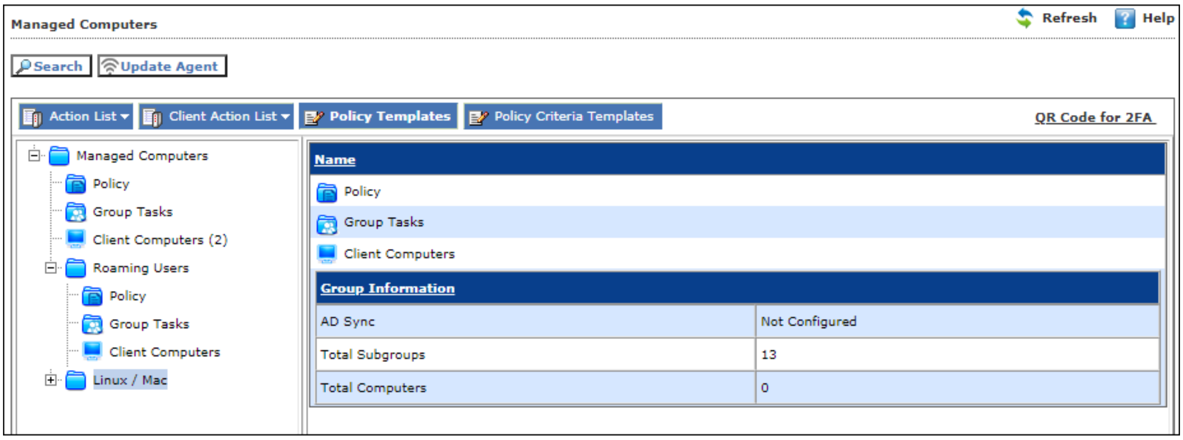
The tabs will be updated according to the changes.

Managed Computers

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

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

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



Name
Policy
Group Tasks
Client Computers

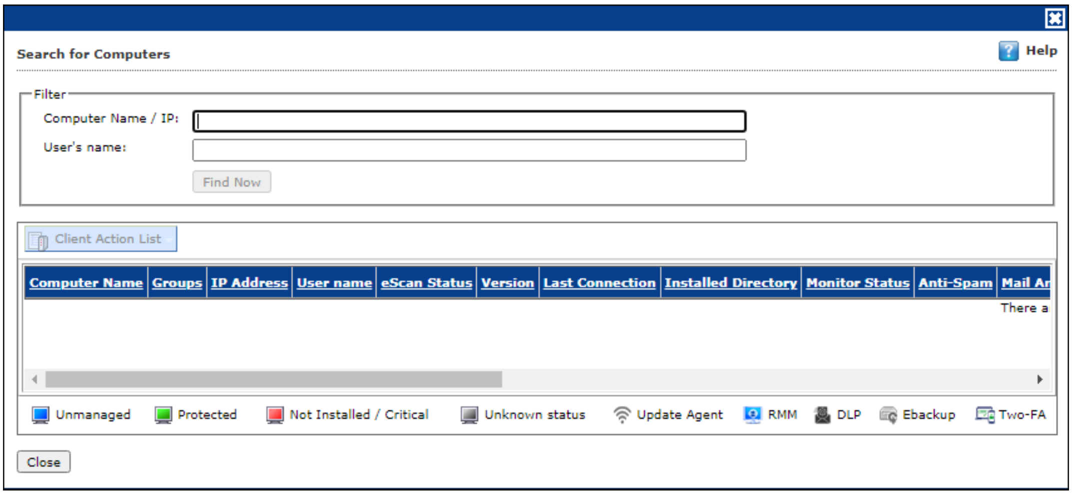
Group Information	
AD Sync	Not Configured
Total Subgroups	13
Total Computers	0

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.



Computer Name	Groups	IP Address	User name	eScan Status	Version	Last Connection	Installed Directory	Monitor Status	Anti-Spam	Mail Ar
										There a

Computer Name/IP

Enter a computer name or IP address.

Username

Enter a username.

Click **Find Now**.

The console will display the result.

Client Action List

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

Update Agent

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

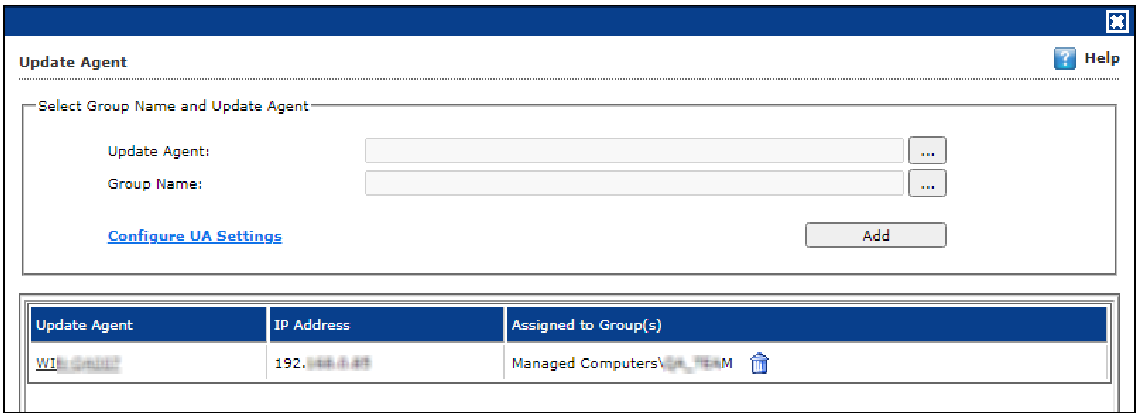
By default, eScan server distributes the virus definitions and policies to all the clients added in the web console. But, to reduce server's workload, you can create an Update Agent for the respective group(s). The Update Agent will receive virus definitions and policies from server and distribute it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

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

Adding an Update Agent

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

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



Update Agent

Select Group Name and Update Agent

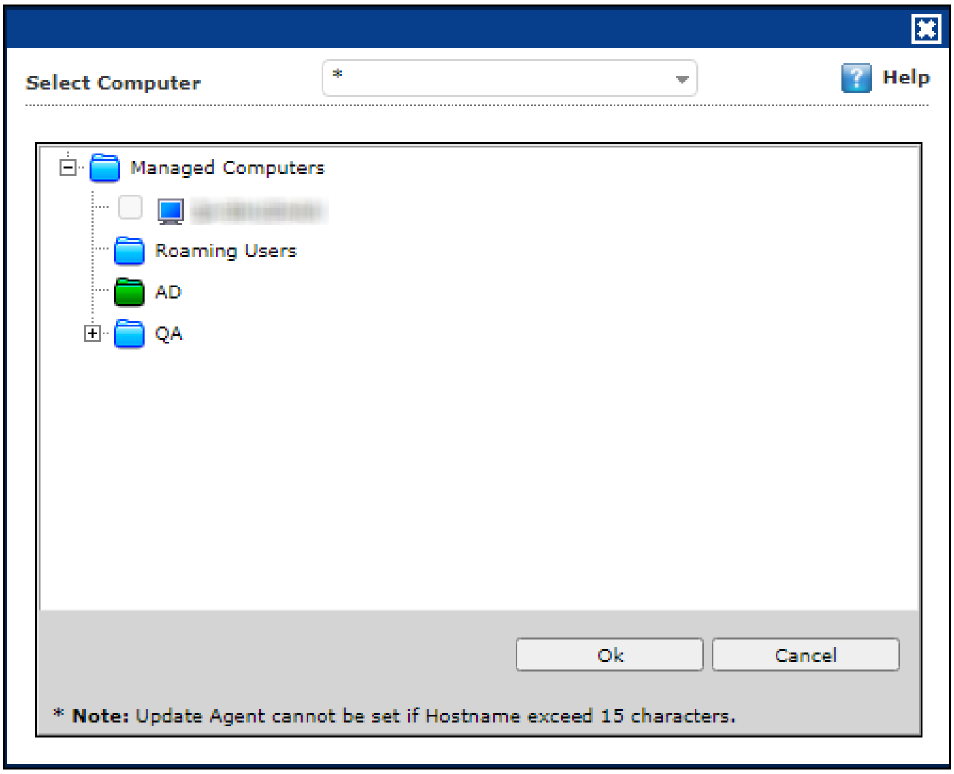
Update Agent: [ ] ...

Group Name: [ ] ...

Configure UA Settings

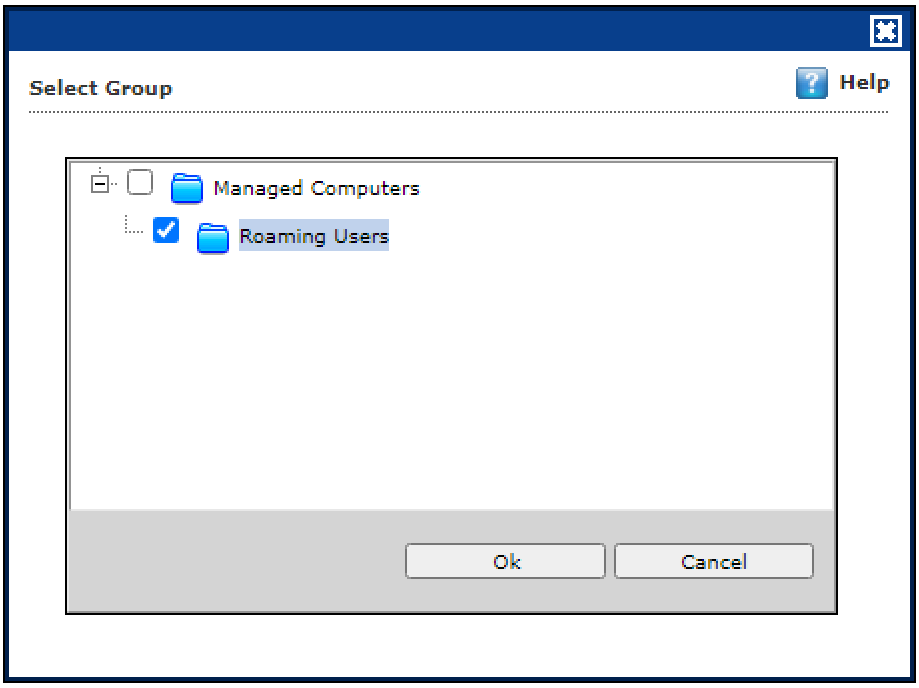
Update Agent	IP Address	Assigned to Group(s)
WI[redacted]	192.[redacted]	Managed Computers\[redacted]M

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



* **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**.**
   The computer will act as an Update Agent for selected group and provide updates to computers present in the group.

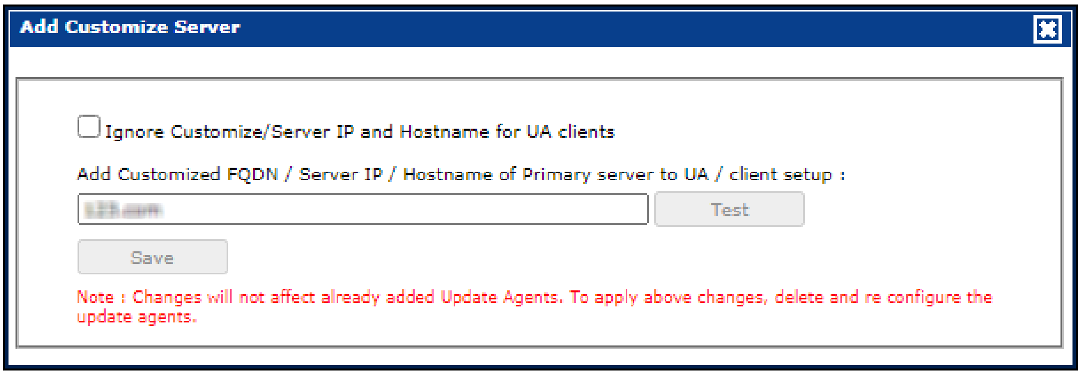


5. Select the Group and click **OK.**
6. Click **Add.**

The Update Agent will be set for the selected group.

Configuring UA Settings

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



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] Test

Save

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.

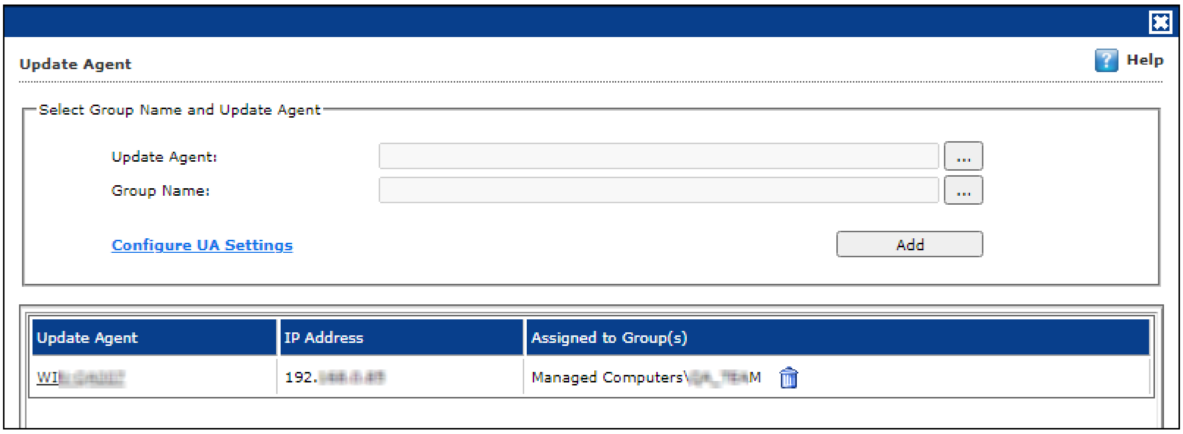
Add Customized FQDN / Server IP / Hostname of Primary server to UA / client setup
Enter the public address that has been assigned to the eScan Server through which clients can download the updates directly.

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

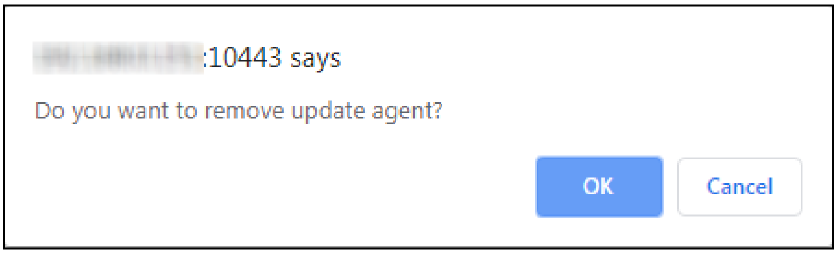
Update Agent: ...

Group Name: ...

Configure UA Settings

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

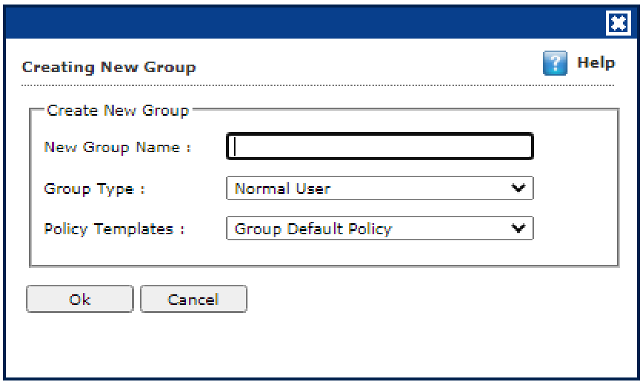
The Action List takes you action for a group. The drop-down contains following options:

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

Creating a Group

To create a group, follow the steps given below:

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



New Group Name :
Group Type : Normal User
Policy Templates : Group Default Policy

2. Enter a name for the group.
3. Click the **Group Type** drop-down and select a type.
4. Click the **Policy Templates** drop-down and select a policy for the group.
5. Click **OK**.

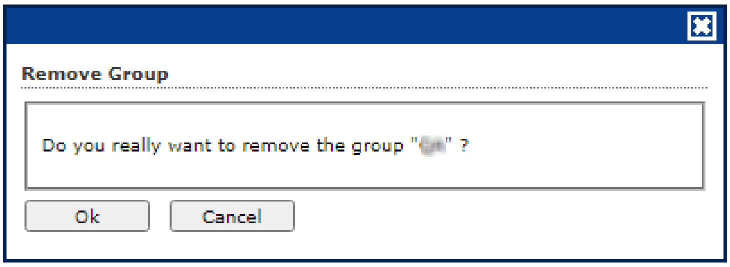
A new group will be created under the Managed Computers.

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

Removing a Group

To remove a group, follow the steps given below:

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



Remove Group

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

3. Click **OK**.

The group will be removed.

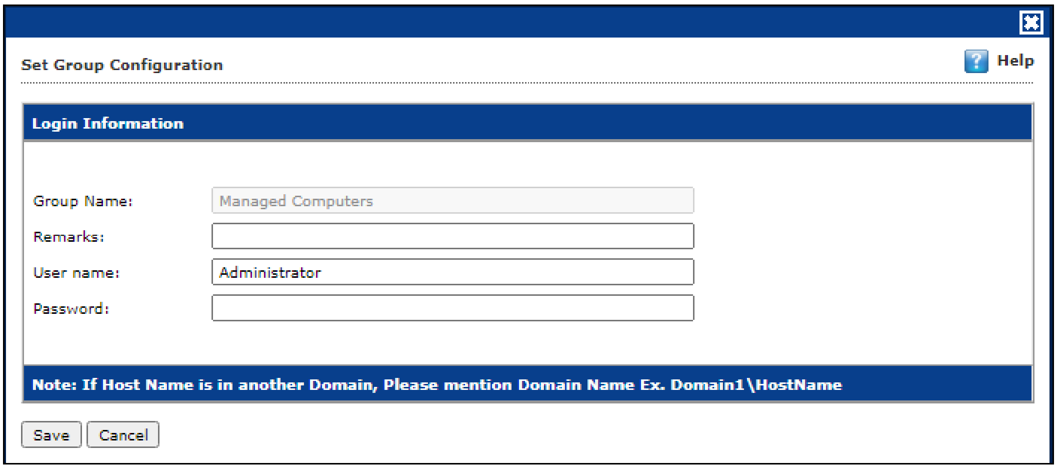
NOTE	A group will be removed only if it contains no computers.

Set Group Configuration

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

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

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



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.

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

Managing Installations

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

[**Conditions Apply**]
This section will give you an overview on following activities:

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

- **Remote Installation**: It lets you install eScan Client on all the computers in a selected group at once. You can initiate and monitor eScan Client installation using eScan Management Console. For more, click here.

- **Manual Installation**: In case remote installation fails, you can allow computer users to install eScan client manually on their computers. It does not require any remote assistance. For more, click here.

- **Installing eScan using agent**: Installation of agent ensures that you have Administrator rights on the computer and you can now remotely install eScan Client on that computer. For more, click here.

- **Installing other Software (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 force 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 Elite for Business; begin with checking if the basic system requirements are in place.
Configure the settings on the client computer according to the OS installed on it

- Windows XP Professional systems
- Windows XP Home
- Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11

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

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

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

For Windows XP Home

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

For Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11

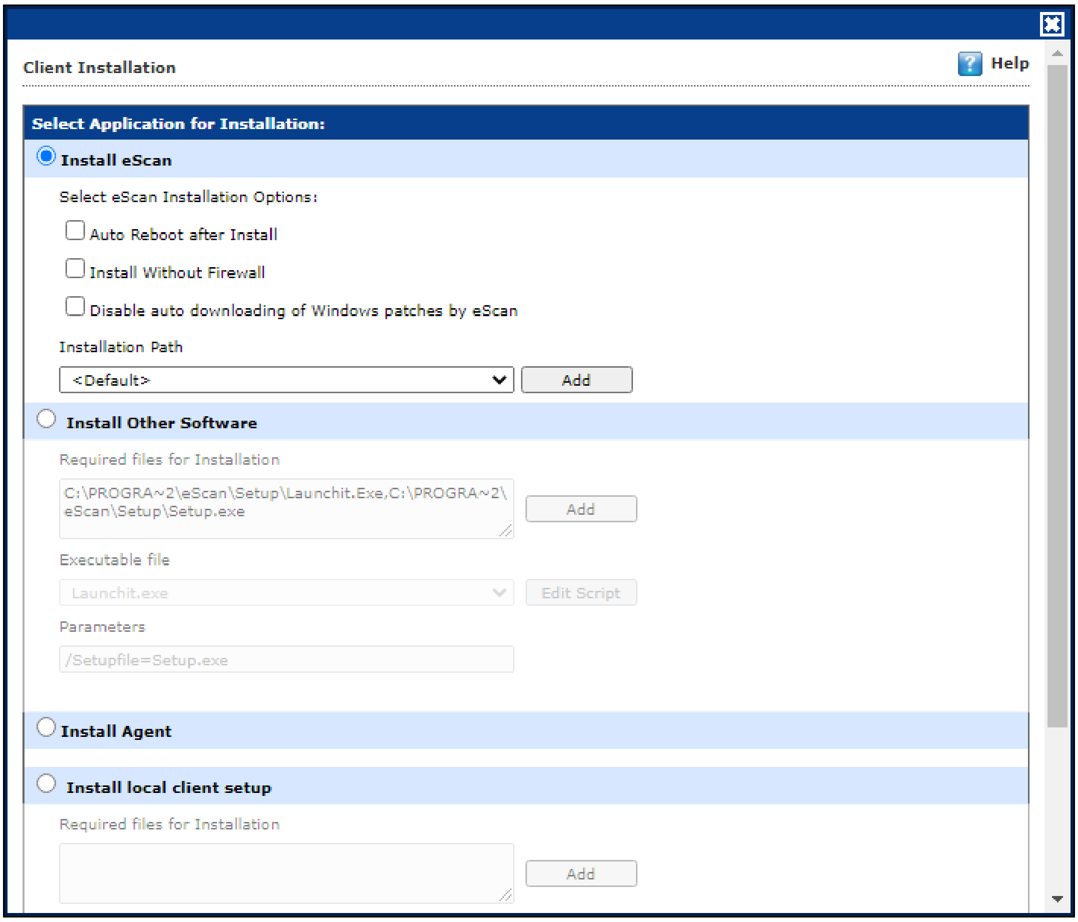
1. Launch **Run.**
2. Enter **secpol.msc**, and then click **OK**.
   Local Security Settings window appears.
3. On the navigation pane, click **Local Policies** folder, and then double-click **Security Options** folder.
   The security policy appears.
4. Double-click Network access: Sharing and security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

Deploy/Upgrade Client

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

Installing eScan Client on a Group

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



Client Installation

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

Required files for Installation

C:\PROGRA~2\eScan\Setup\Launchit.Exe,C:\PROGRA~2\eScan\Setup\Setup.exe

Executable file

Launchit.exe

Parameters

/Setupfile=Setup.exe

○ Install Agent

○ Install local client setup

Required files for Installation

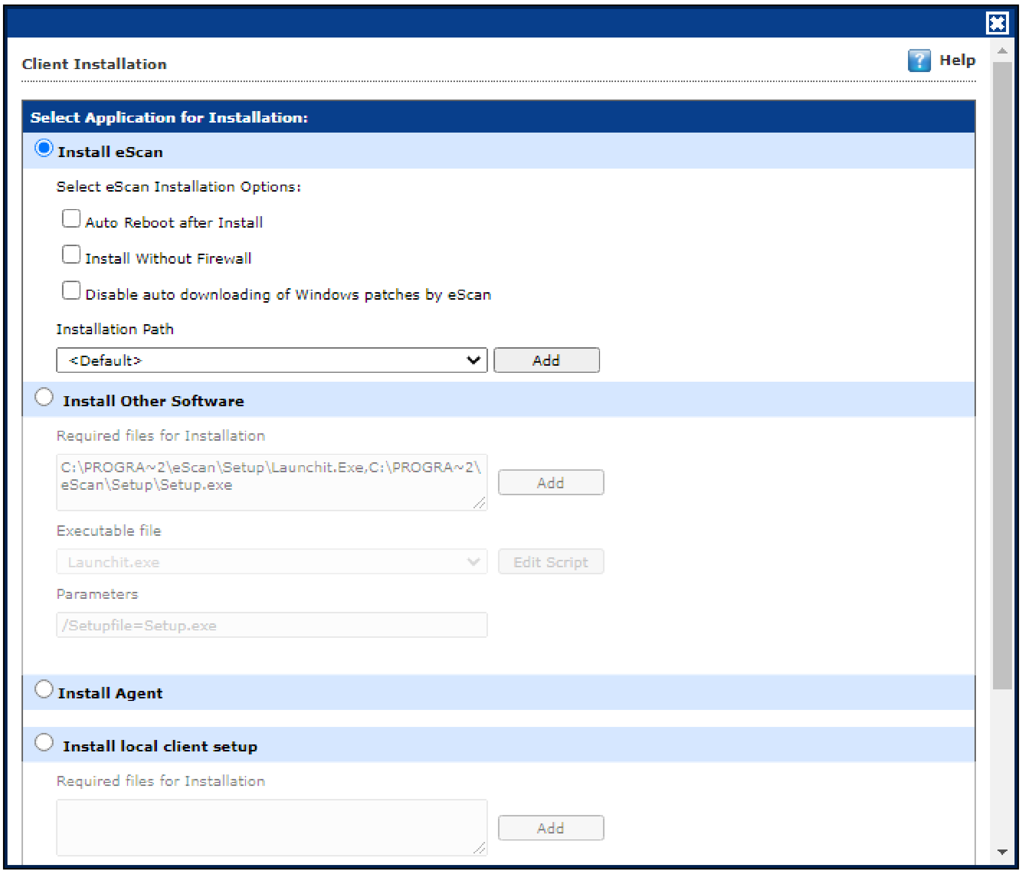
3. Select **Install eScan** option.
   By Default eScan is installed at the following Path on a Client computer.
   C:\Program Files\eScan (default path for 32-bit computer)
   OR
   C:\Program Files (x86)\eScan (default path for 64-bit computers).
4. To define a different installation path, click **Add**.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

A window displays File transfer progress.

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

Installing eScan Client on an Individual Computer in a Group

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



Client Installation

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

Required files for Installation: C:\PROGRA~2\eScan\Setup\Launchit.Exe,C:\PROGRA~2\eScan\Setup\Setup.exe

Executable file: Launchit.exe

Parameters: /Setupfile=Setup.exe

○ Install Agent

○ Install local client setup

Required files for Installation

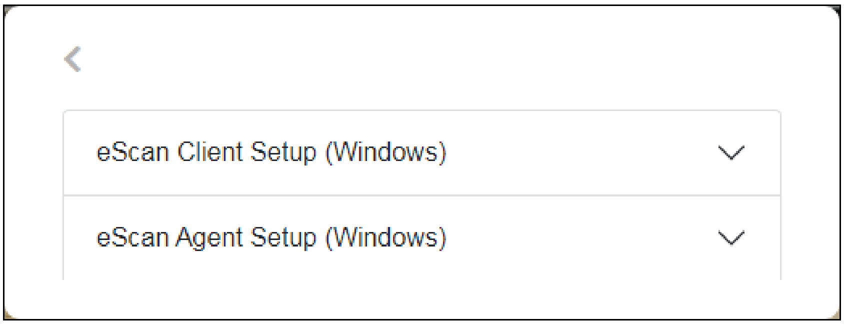
5. Select **Install eScan** option.
   By default eScan is installed at the following path on a Client computer.
   C:\Program Files\eScan (default path for 32-bit computer)
   OR
   C:\Program Files (x86)\eScan (default path for 64-bit computers).
6. To define a different installation path, click **Add**.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

A window displays File transfer progress.

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

Manual installation of eScan Client on network computer(s)

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



Installing eScan Client Using Agent

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

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

Remotely installing agent on Client computer(s)

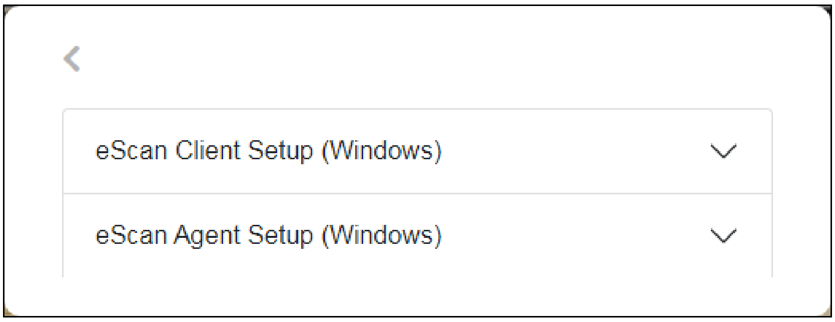
1. Click **Managed Computers**.
2. Select the computer(s) from a group.
3. Click **Client Action List** > **Deploy/Upgrade Client**.
4. Select **Install Agent** option and click **Install**.

eScan Agent will be installed on selected computers.

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)

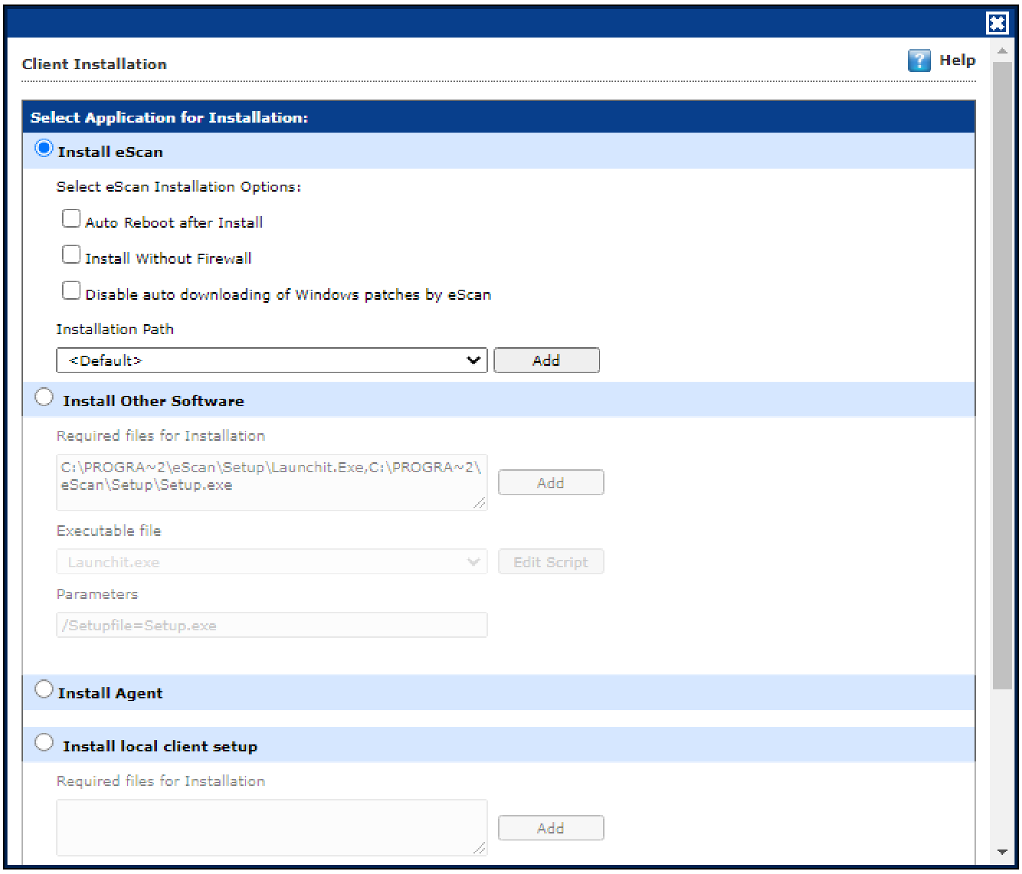
To manually install eScan Agent on computers, please send the link displayed on the **Login Page** > **Setup Links** of eScan Management Console to the users of the Client computer on mail.



Installing other Software (Third Party Software)

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

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



Client Installation

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

Required files for Installation: C:\PROGRA~2\eScan\Setup\Launchit.Exe,C:\PROGRA~2\eScan\Setup\Setup.exe

Executable file: Launchit.exe

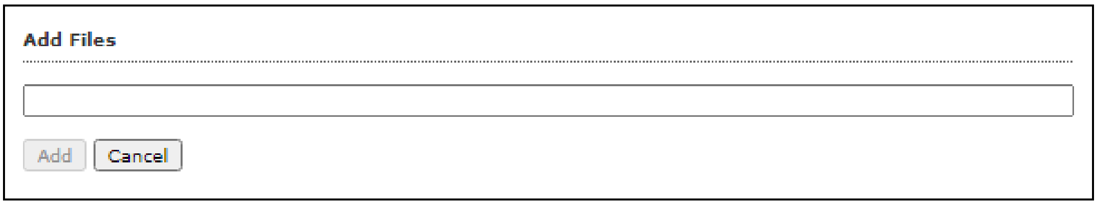
Parameters: /Setupfile=Setup.exe

○ Install Agent

○ Install local client setup

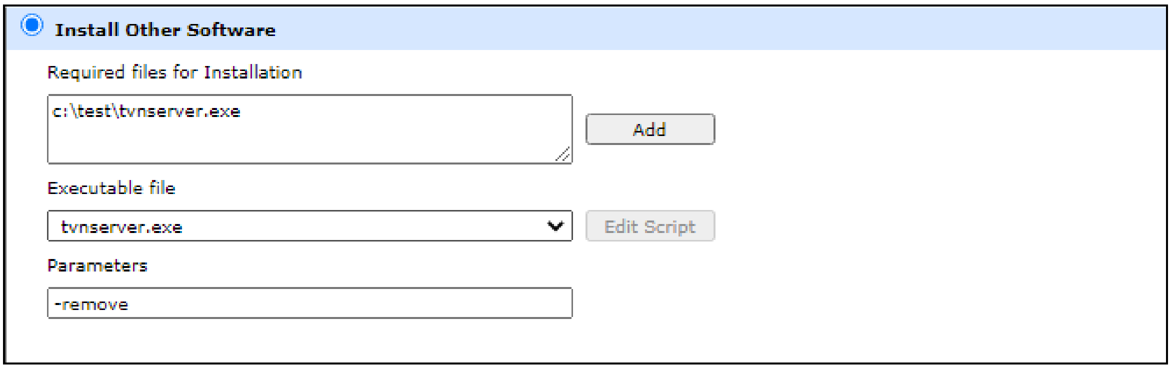
Required files for Installation

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**

Required files for Installation

c:\test\tvnserver.exe

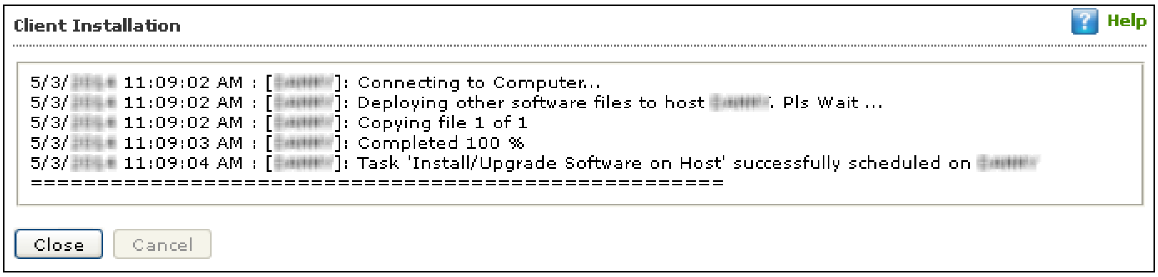
Executable file

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.



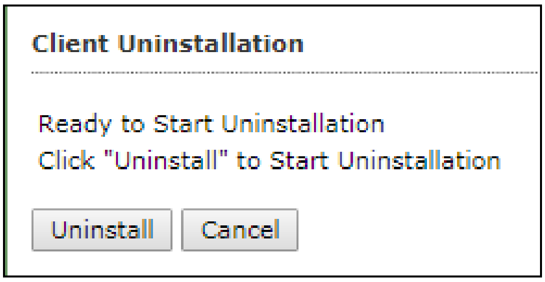
Client Installation

```
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]
====================================================
```

Uninstall eScan Client (Windows)

To uninstall eScan Client on all the computers in a group, follow the steps given below:

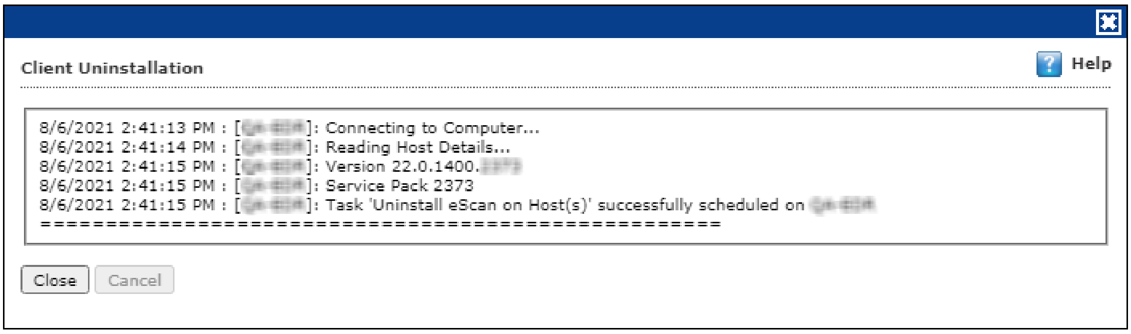
1. Select the group of computers for uninstallation.
2. Click **Action List** > **Uninstall eScan Client**.
   Client Uninstallation window appears.



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]
==================================================
```

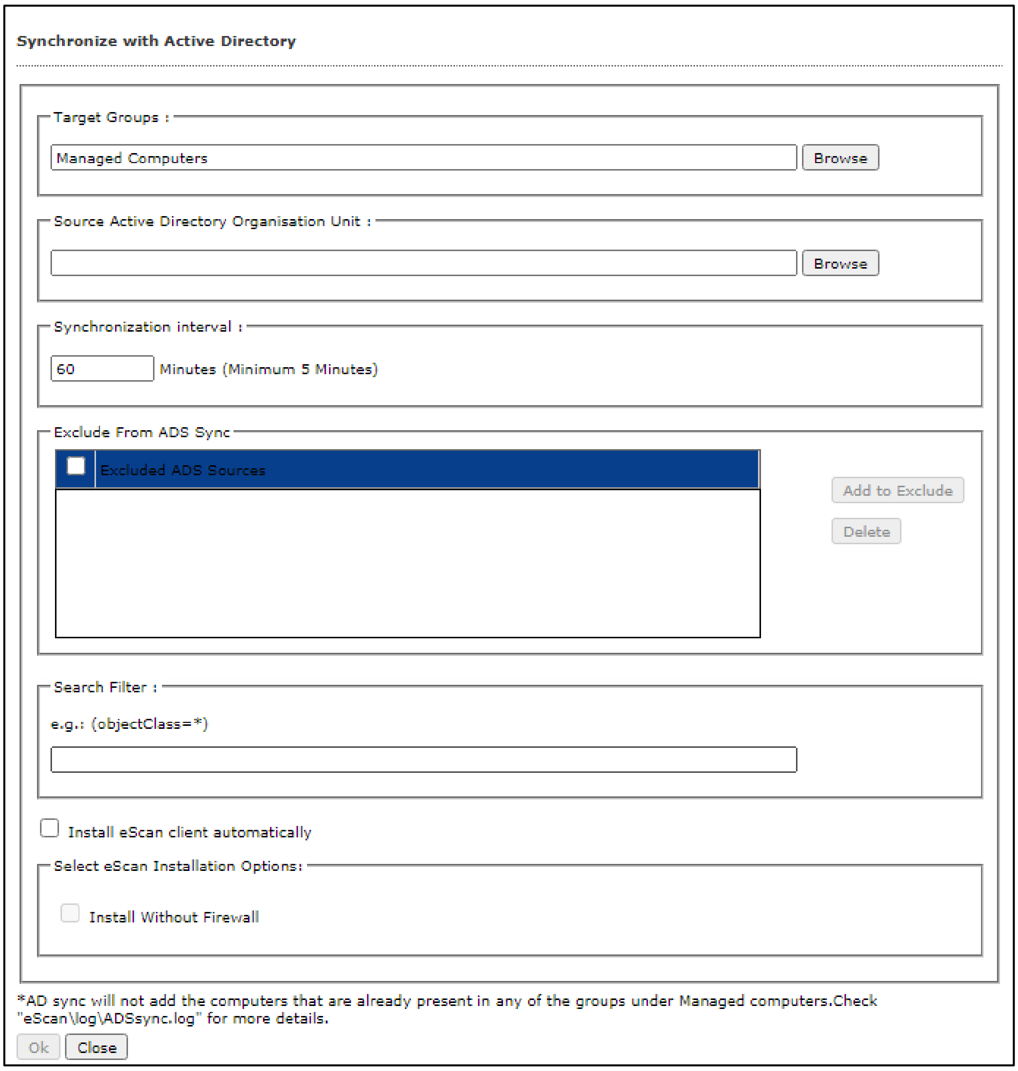
After the uninstallation process is over, click **Close**.

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**.

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

*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.

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

Source Active Directory Organization Unit
Click **Browse** and select an Active Directory.

Synchronization Interval
Enter the preferred duration (in minutes).

Exclude from ADS Sync
This field displays a list of excluded Active Directory sources.
To exclude a source, select the source and then click **Add to Exclude**.

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

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

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

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

3. After performing the necessary actions, click **OK**.

The group will be synchronized with the Active Directory.

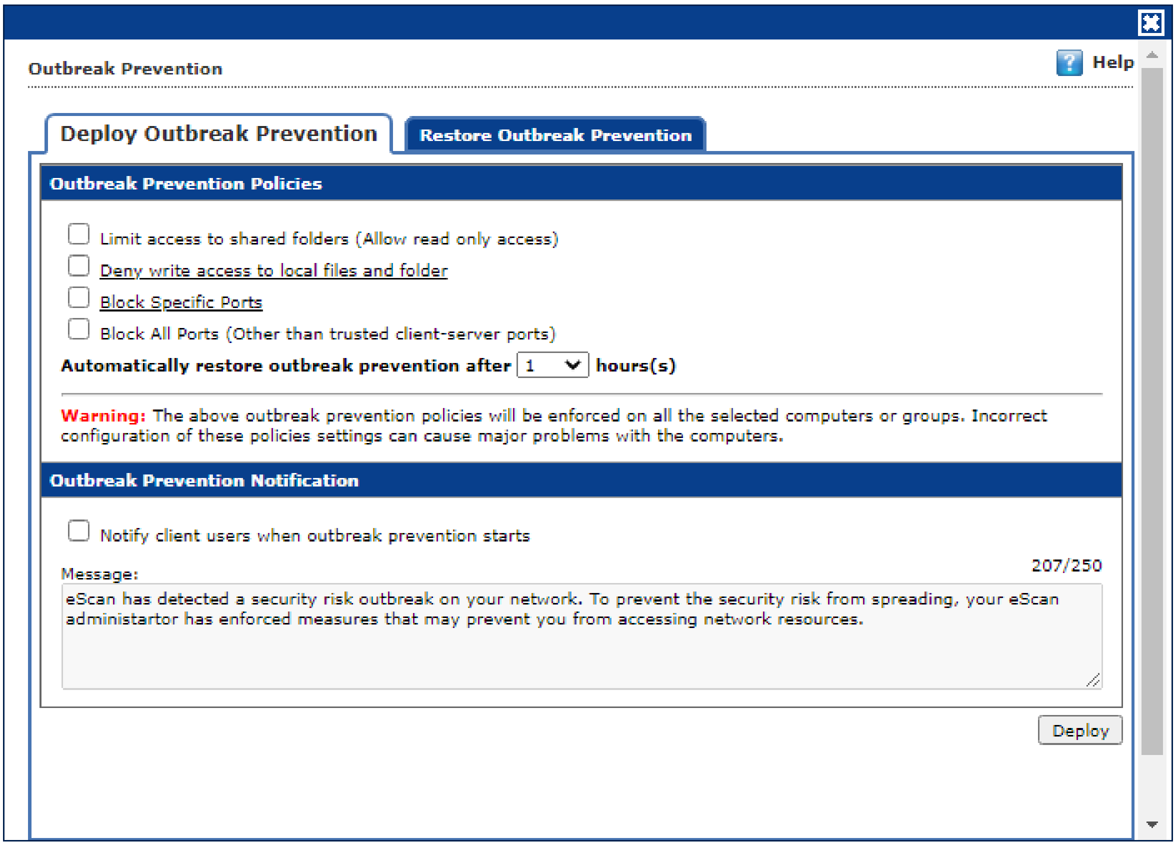
Outbreak Prevention

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

Deploying Outbreak Prevention

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

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



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

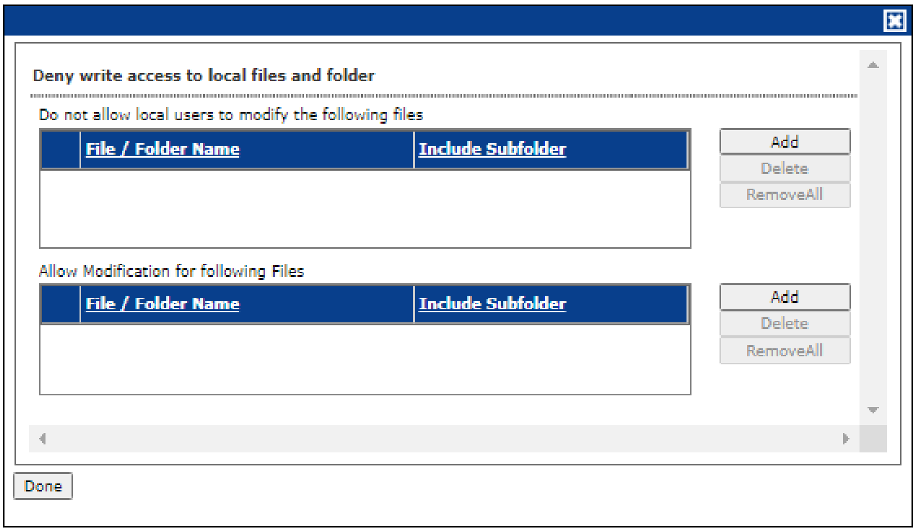
eScan has detected a security risk outbreak on your network. To prevent the security risk from spreading, your eScan administartor has enforced measures that may prevent you from accessing network resources.

Limit access to shared folders (Allow read only access)

Select this checkbox to limit the access of shared folder to read only. This will prevent infection to write into shared folder.

Deny write access to local files and folder

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



Deny write access to local files and folder

Do not allow local users to modify the following files

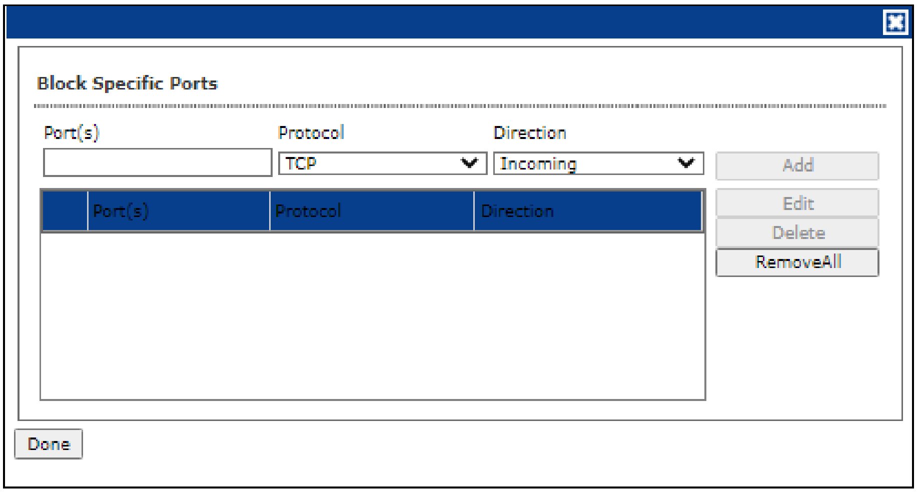
	File / Folder Name	Include Subfolder

Allow Modification for following Files

	File / Folder Name	Include Subfolder

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 Specific Ports

Port(s):
Protocol: TCP
Direction: Incoming

	Port(s)	Protocol	Direction

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.

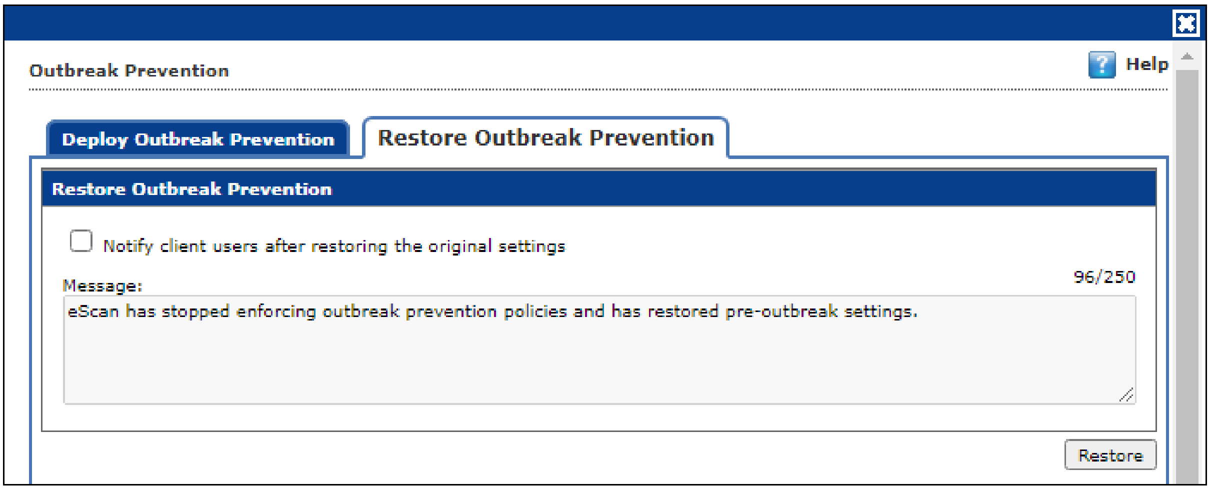
Outbreak Prevention Notification
To send a notification to client users after Outbreak Prevention is deployed, select the checkbox **Notify client users when outbreak prevention starts**. You can even write your own custom message for this feature in the Message field.

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

NOTE	The incorrect configuration of Outbreak Prevention can cause problems in computers.

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

□ Notify client users after restoring the original settings

Message: 96/250

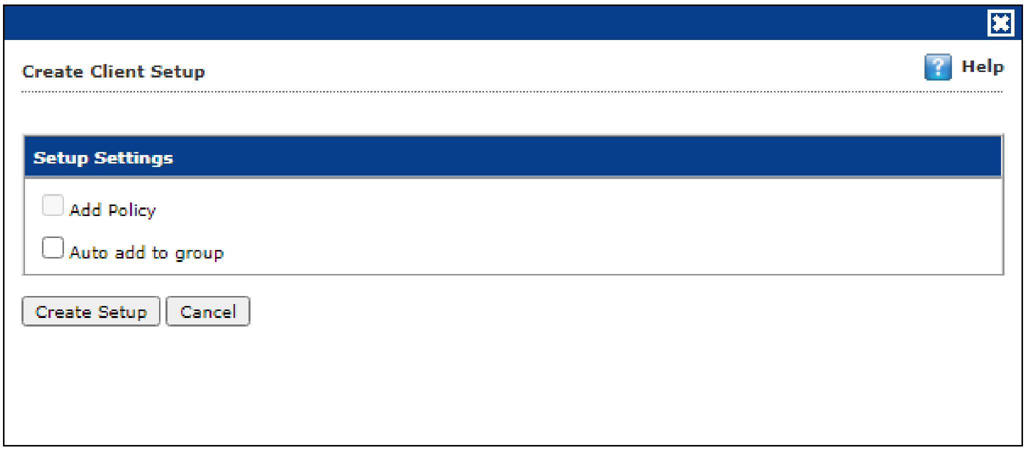
eScan has stopped enforcing outbreak prevention policies and has restored pre-outbreak settings.

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

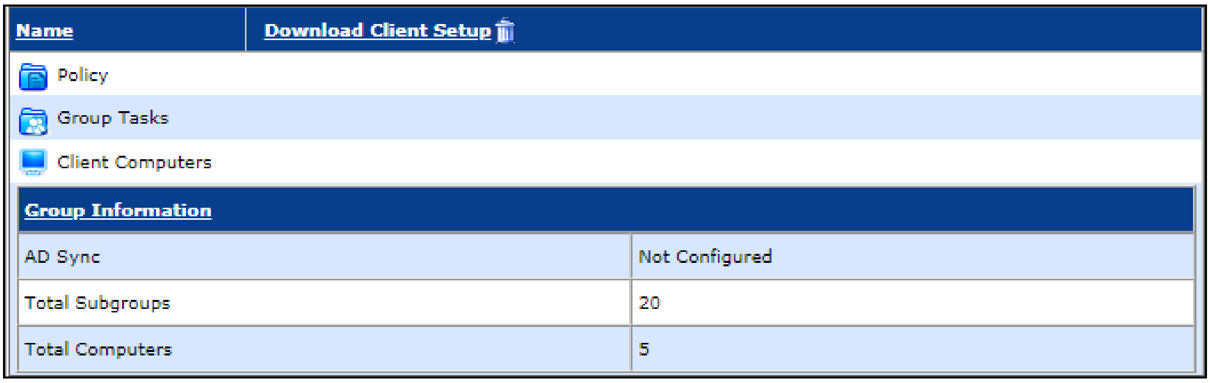
Setup Settings

□ Add Policy

□ Auto add to group

3. Select the necessary settings.
   - **Add Policy:** This option is enabled after the policy applied to client computers.
   - **Auto add to group:** This option will add the endpoint(s) to the respective group automatically after endpoint installation.
4. Click **Create Setup**.

The Client setup will be created and a download link will be displayed in right pane.



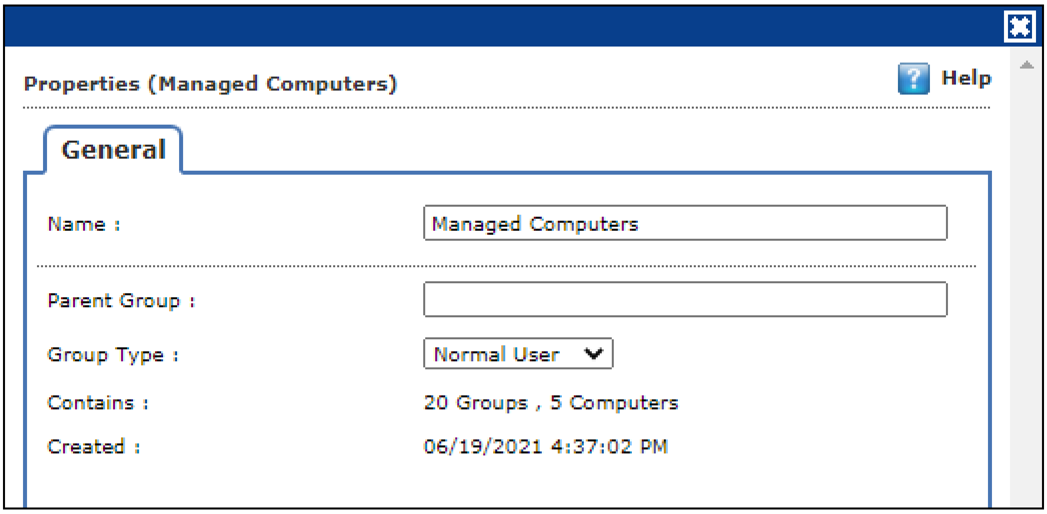
Name	Download Client Setup
Policy	
Group Tasks	
Client Computers	

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 (Managed Computers)

Name : Managed Computers

Parent Group :

Group Type : Normal User

Contains : 20 Groups , 5 Computers

Created : 06/19/2021 4:37:02 PM

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

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

Group Tasks

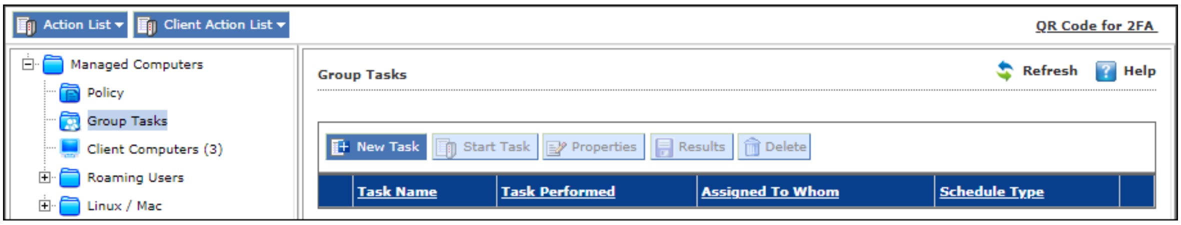
With the Group Tasks option, you can create a task, start a task, select a task and view its properties and results as well as delete an already created task. Tasks can include the following.

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

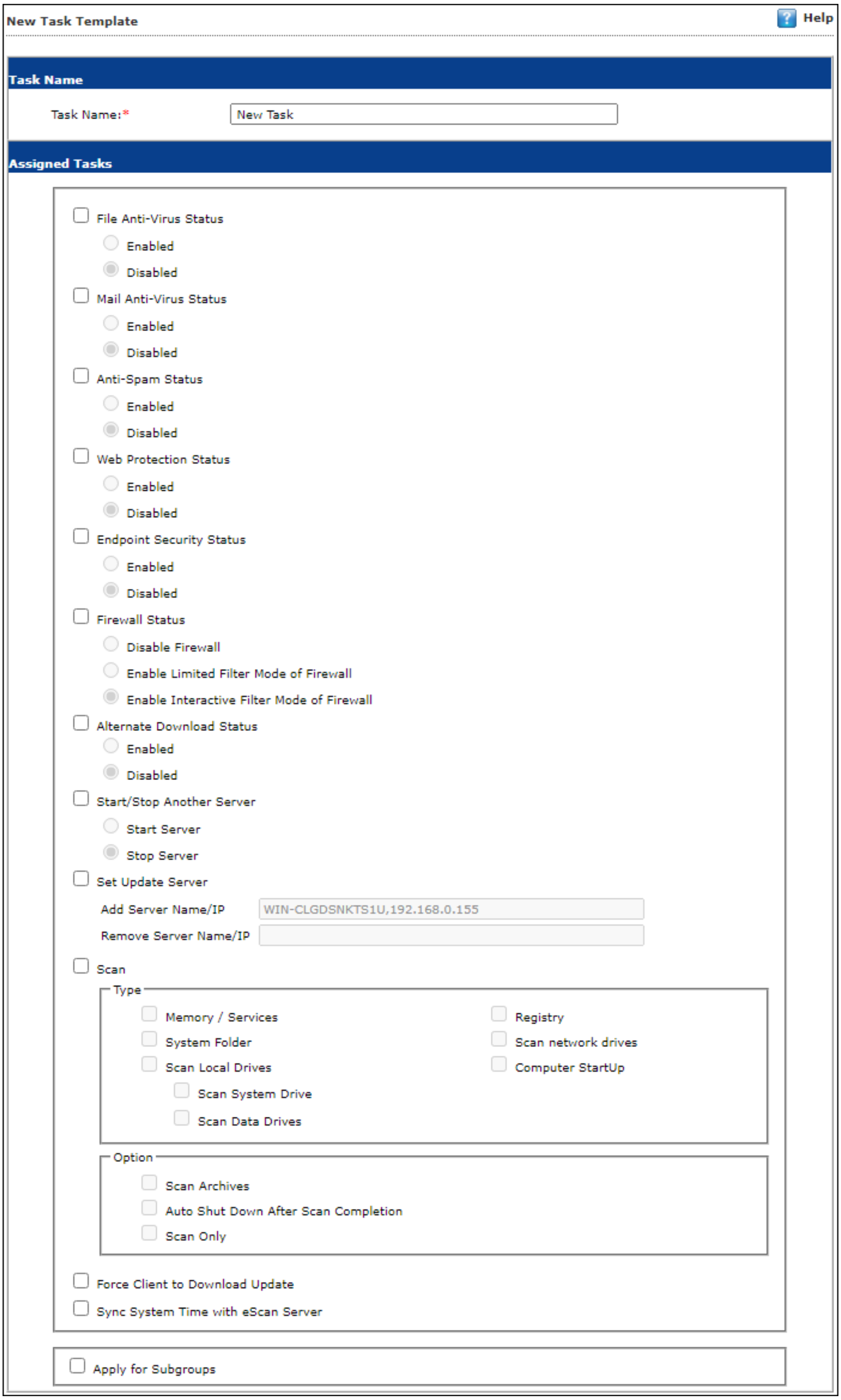
Creating a Group Task

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

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



New Task Template window appears.



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-CLGDSNKTS1U,192.168.0.155
Remove Server Name/IP

□ Scan

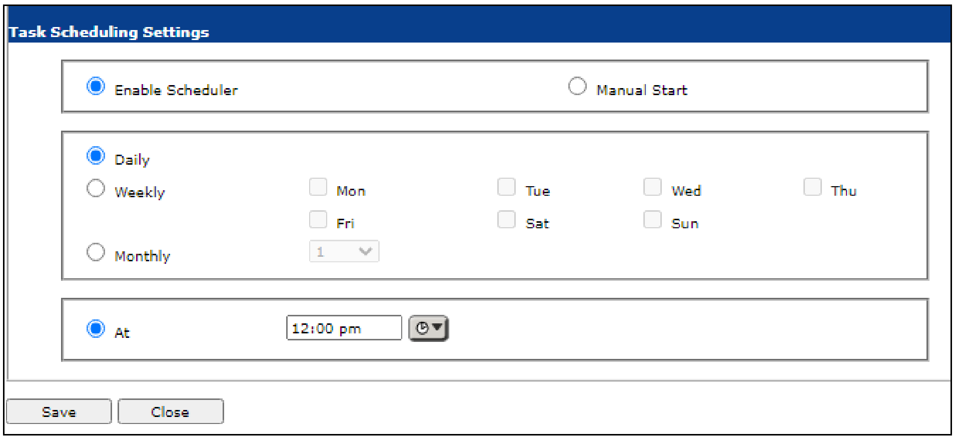
Type
□ Memory / Services
□ System Folder
□ Scan Local Drives
□ Scan System Drive
□ Scan Data Drives
□ Registry
□ Scan network drives
□ Computer StartUp

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

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

□ Apply for Subgroups

4. Enter the Task Name and configure the desired task settings.
5. Schedule the date and time for the execution of task.



Task Scheduling Settings

● Enable Scheduler ○ Manual Start

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

● At 12:00 pm

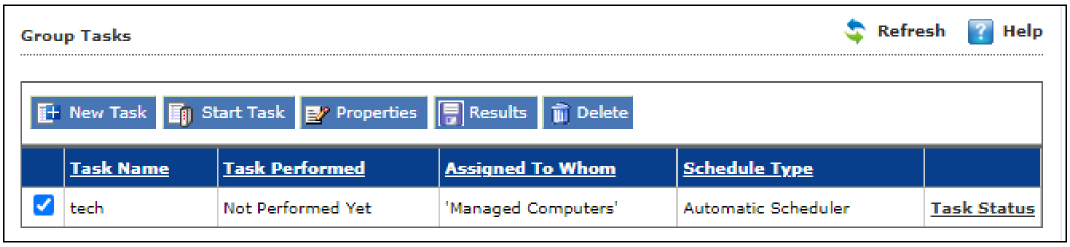
Save Close

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.



Group Tasks

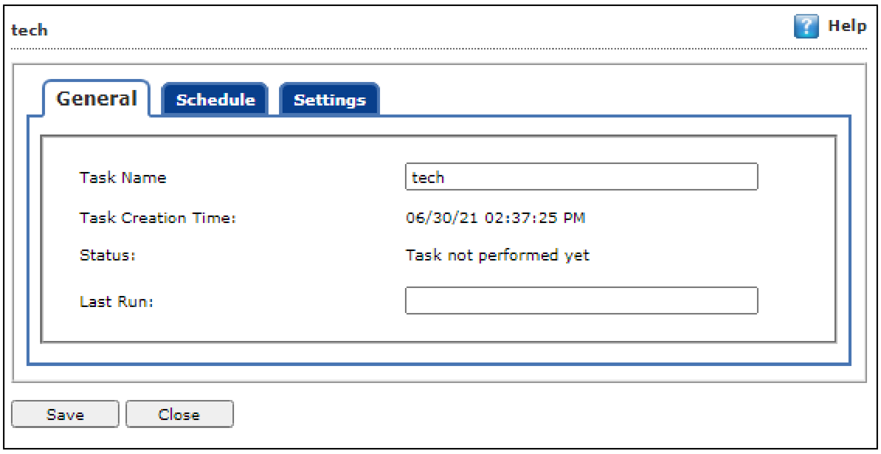
	Task Name	Task Performed	Assigned To Whom	Schedule Type	
☑	tech	Not Performed Yet	'Managed Computers'	Automatic Scheduler	Task Status

Start Task

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

Properties

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



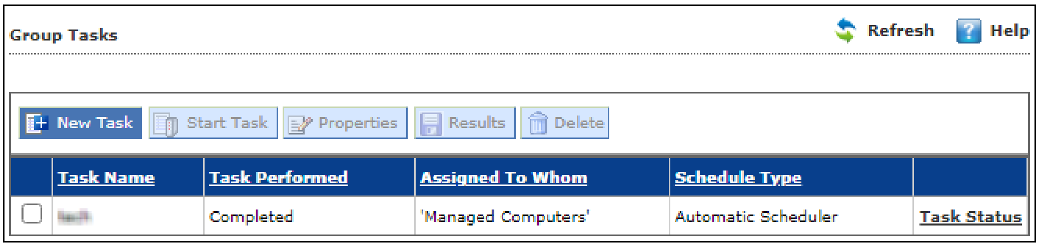
tech

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

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

Results

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



Group Tasks

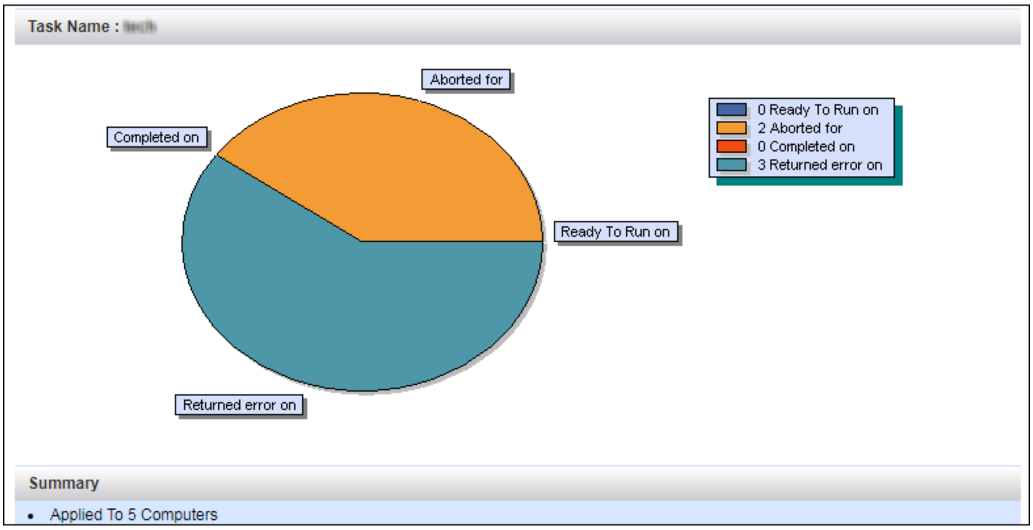
	Task Name	Task Performed	Assigned To Whom	Schedule Type	
☐	[redacted]	Completed	'Managed Computers'	Automatic Scheduler	Task Status

Delete Task

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

Task Status

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



Task Name : [redacted]

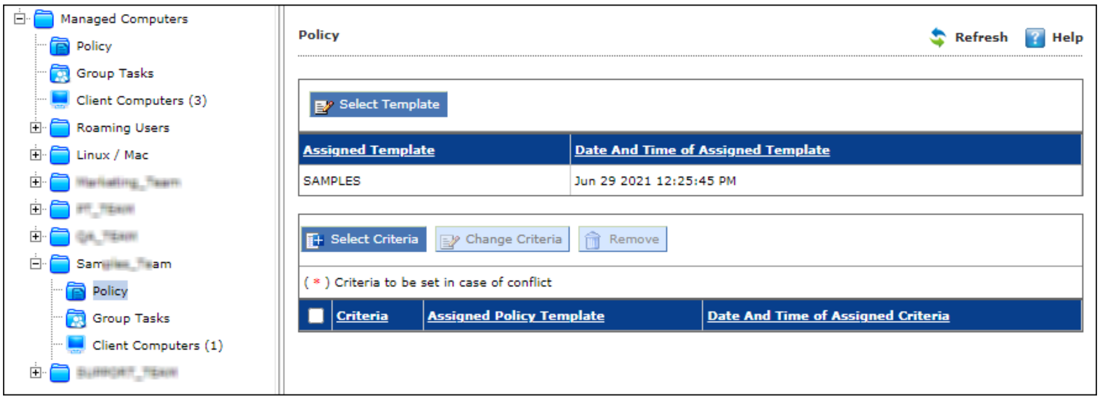
Summary

- 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.



- Managed Computers
  - Policy
  - Group Tasks
  - Client Computers (3)
  - Roaming Users
  - Linux / Mac
  - [redacted]
  - [redacted]
  - [redacted]
  - Sam[redacted]eam
    - Policy
    - Group Tasks
    - Client Computers (1)
  - [redacted]

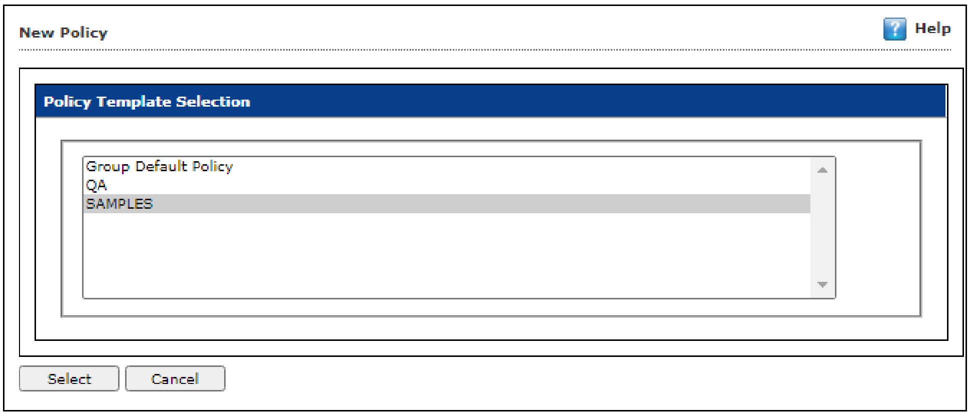
Policy

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.

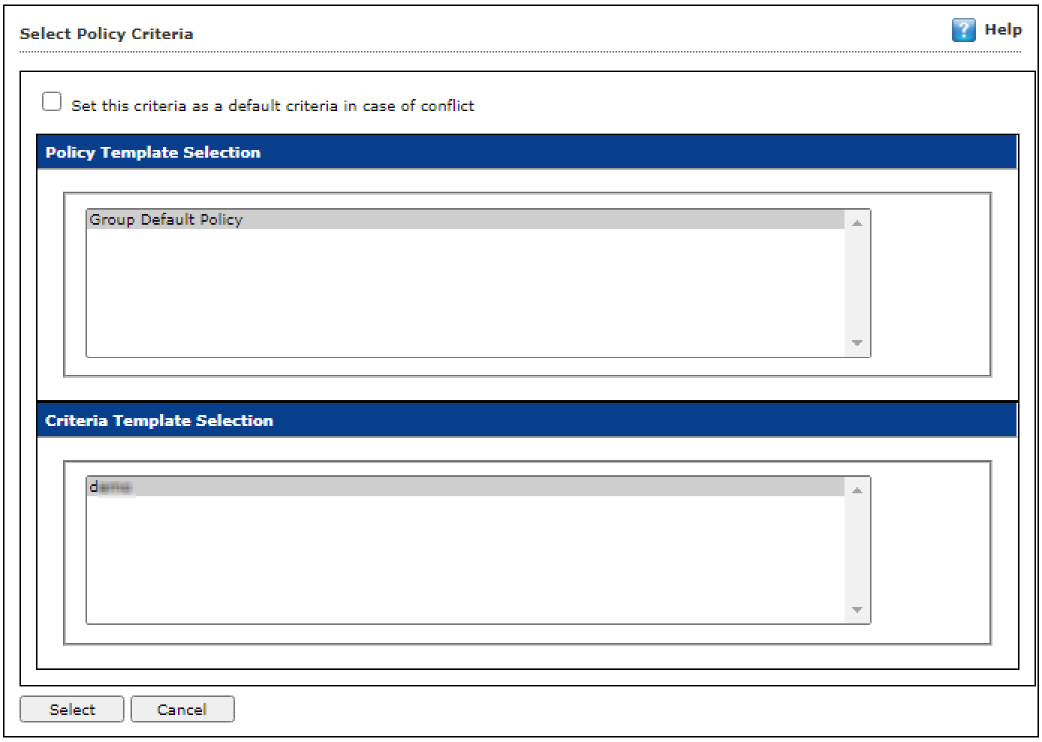


New Policy

Policy Template Selection

- Group Default Policy
- QA
- SAMPLES

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



Select Policy Criteria

□ Set this criteria as a default criteria in case of conflict

Policy Template Selection

Group Default Policy

Criteria Template Selection

[redacted]

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 and then click **Client Action List**.

The drop-down consists of following options:

- **Set Host Configuration**
- **Deploy/Upgrade Client**
- **Uninstall eScan Client**
- **Move to Group**
- **Remove from Group**
- **Refresh Client**
- **Connect to Client (RMM)**
- **Assign Policy Template**
- **Show Critical Events**
- **Export**
- **Show Installed Softwares**
- **Force Download**
- **Forensic-Port/Communication**
- **On Demand Scanning**
- **Send Message**
- **Outbreak Prevention**
- **Delete All Quarantine Files**
- **Create OTP**
- **Pause Protection**
- **Resume Protection**
- **Properties**

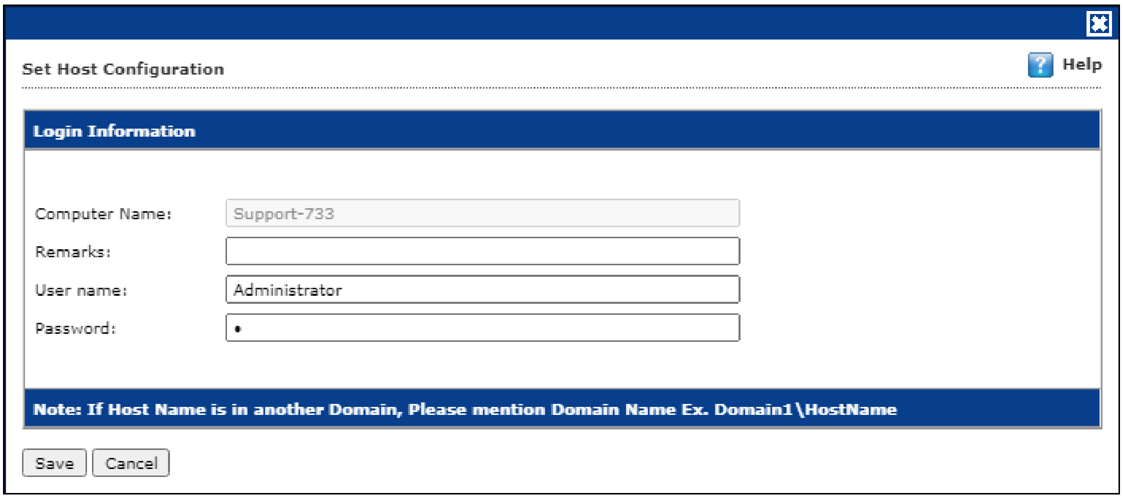
The Client Action List contains few options similar to Action List. These options perform same, except they perform the action only for selected computer(s).

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: Support-733
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**.

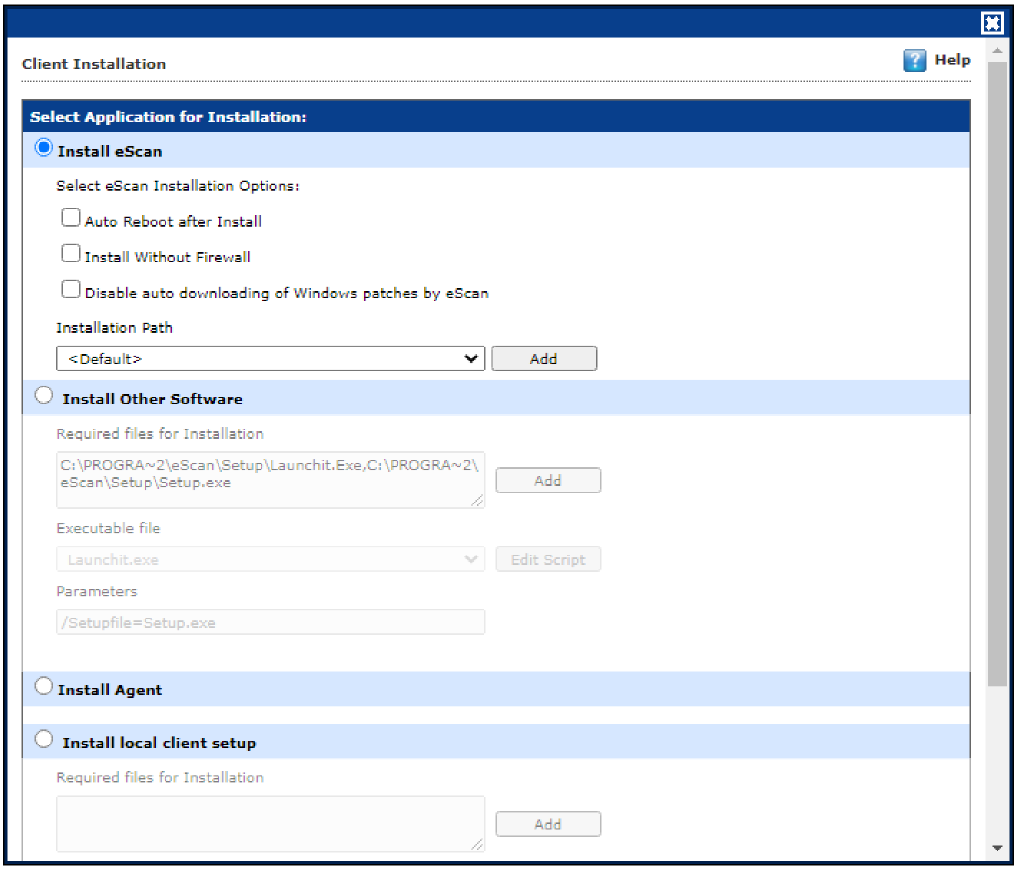
The Host will be configured as per new settings.

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



Client Installation

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

Required files for Installation

C:\PROGRA~2\eScan\Setup\Launchit.Exe,C:\PROGRA~2\eScan\Setup\Setup.exe

Executable file

Launchit.exe

Parameters

/Setupfile=Setup.exe

○ Install Agent

○ Install local client setup

Required files for Installation

3. Select **Install eScan** option.
   By Default eScan is installed at the following Path on a Client computer.
   C:\Program Files\eScan (default path for 32-bit computer)

   OR

   C:\Program Files (x86)\eScan (default path for 64-bit computers).
4. To define a different installation path, click **Add**. (Skip this step if default path chosen).
5. Click **Install**.

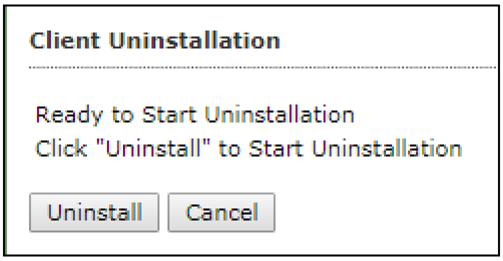
A window displays File transfer progress.

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

Uninstall eScan Client

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

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

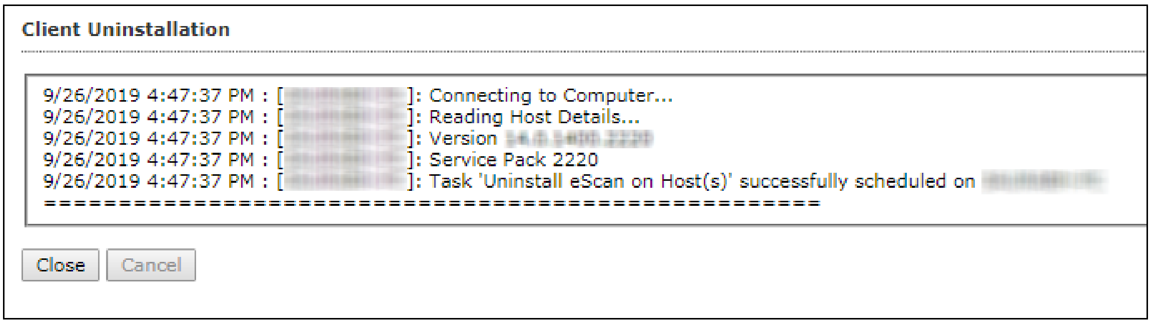


Client Uninstallation

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 [redacted]
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**.

Move to Group

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

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

The computers will be moved to the selected group.

Remove from Group

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

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

The computers will be removed from the group.

Refresh Client

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

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

The Client status will be refreshed.

Connect to Client (RMM)

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

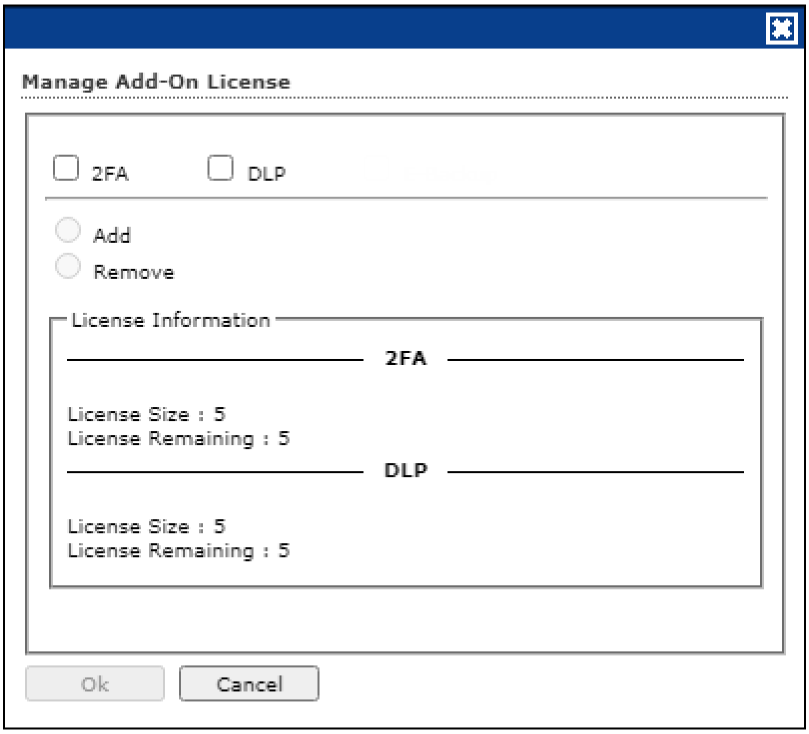
1. Go to **Managed Computers**.
2. Select the client computer which you want to connect to RMM.
3. Click **Client Action List > Connect to Client (RMM)**.
4. Read the disclaimer thoroughly and then click **Accept.**
   Your default browser opens eScan Remote Access window (Google Chrome, Mozilla Firefox, MS Edge, etc.).

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

Manage Add-On License

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

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



Manage Add-On License

□ 2FA □ DLP

○ Add
○ Remove

License Information

2FA

License Size : 5
License Remaining : 5

DLP

License Size : 5
License Remaining : 5

Ok | Cancel

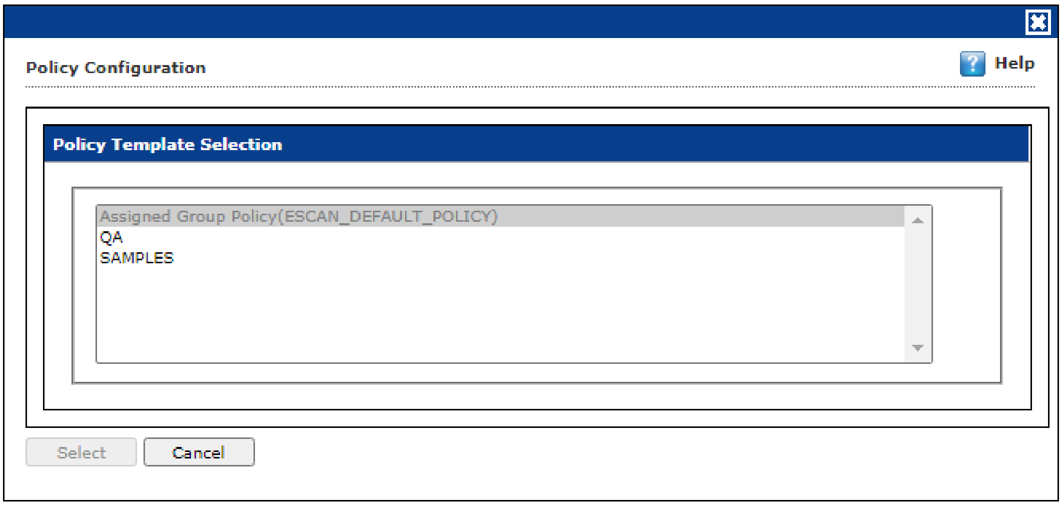
4. Select **Add** to add a client computer to 2FA, DLP, and E-Backup licenses or **Remove** to remove the added client computer and then click **OK**.

The computer gets added or removed from 2FA, DLP, and E-Backup licenses as per your preferred option.

Assign Policy Template

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

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



Policy Configuration

Policy Template Selection

Assigned Group Policy(ESCAN_DEFAULT_POLICY)
QA
SAMPLES

4. Select the policy template and click **Select** to add.

The computer get assign with the selected policy template.

Show Critical Events

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

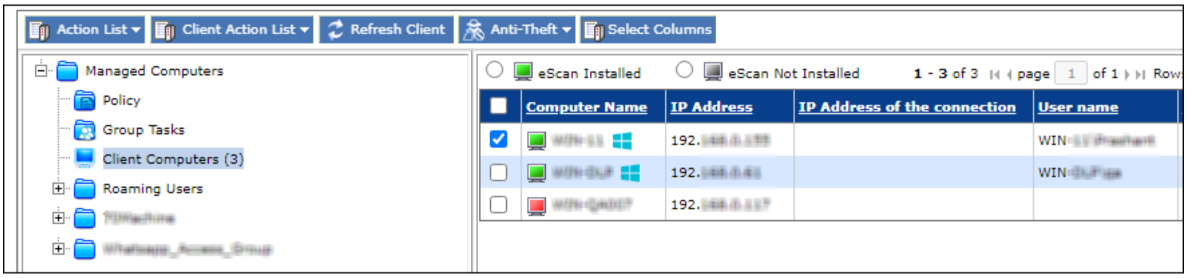
1. Go to **Managed Computers**.
2. Select the client computer which you want to assign policy template.
3. Click **Client Action List** > **Show Critical Events**.

This will display the list of all the critical events of the computer that can also be exported as a report.

Export

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

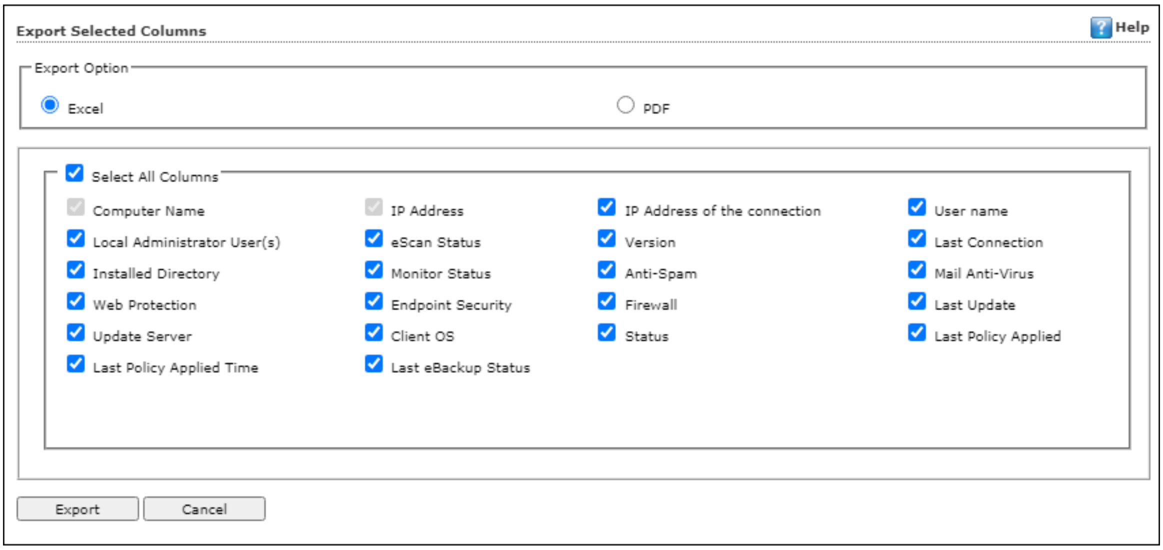
1. In the Managed Computers folder tree, select a group and then click **Client Computers**.
   The right pane displays the list of computers in the group and their detailed information.



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

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**.

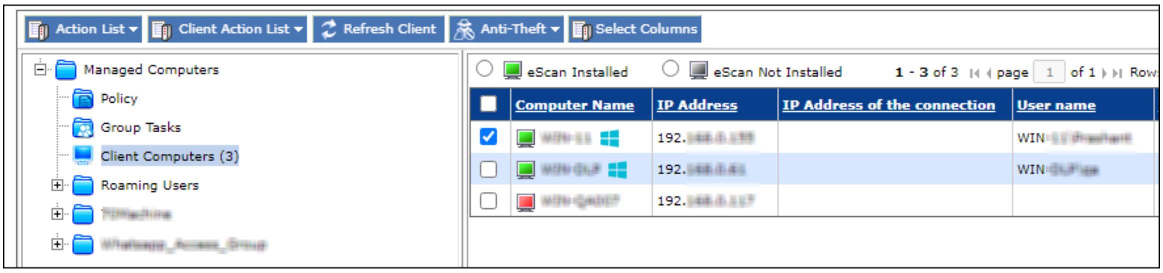
The report will be exported as per your preferences.

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.

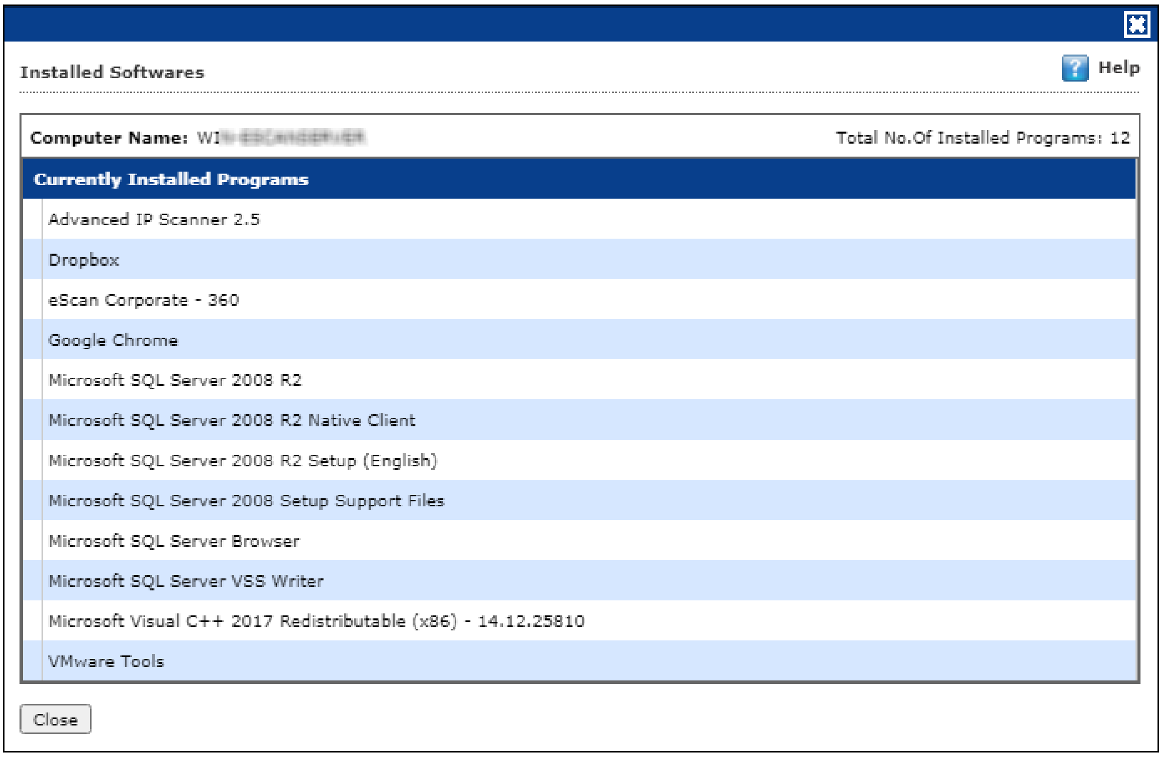


Managed Computers
Policy
Group Tasks
Client Computers (3)
Roaming Users
[redacted]
[redacted]

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

☐	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

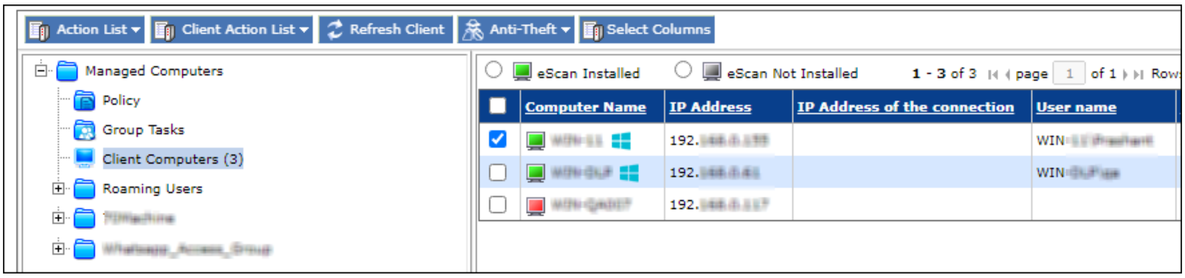
Computer Name: WI[redacted] Total No.Of Installed Programs: 12

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

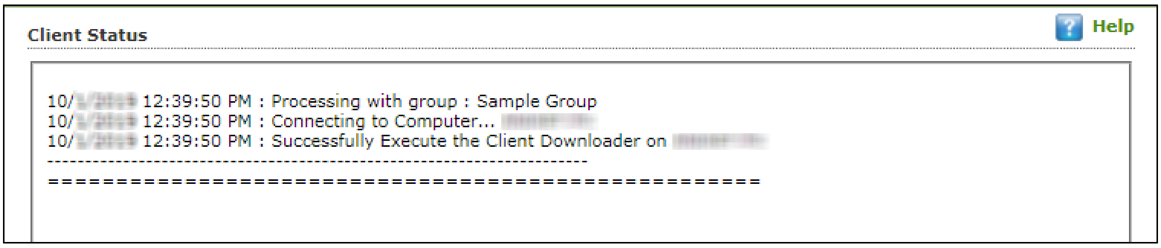
The Force Download feature forces a client computer to download Policy Template modifications (if any) and update virus signature database. To activate this feature, follow the steps given below:

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



□	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.

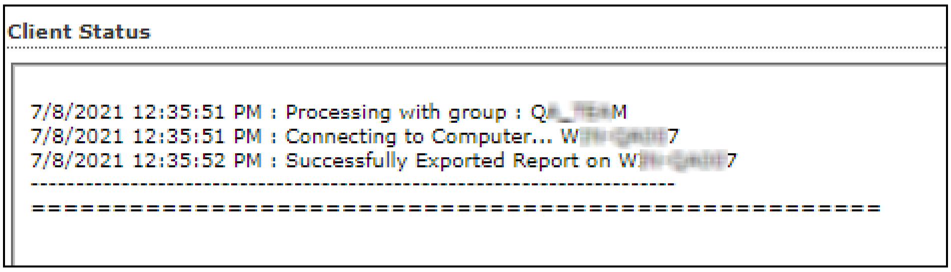


Client Status

```
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]
-------------------------------------------------------------------------
=====================================================
```

Forensic-Port/Communication

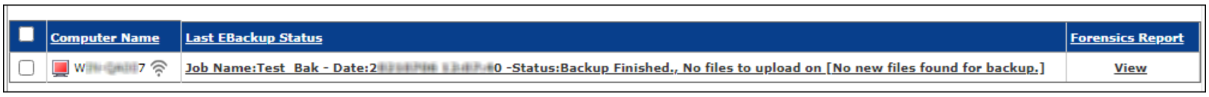
This option generates the Forensic report of the service running on certain port during a particular period for analysis. To generate the report, select the client computer and click **Client Action List** > **Forensic Port/Communication** option.



Client Status

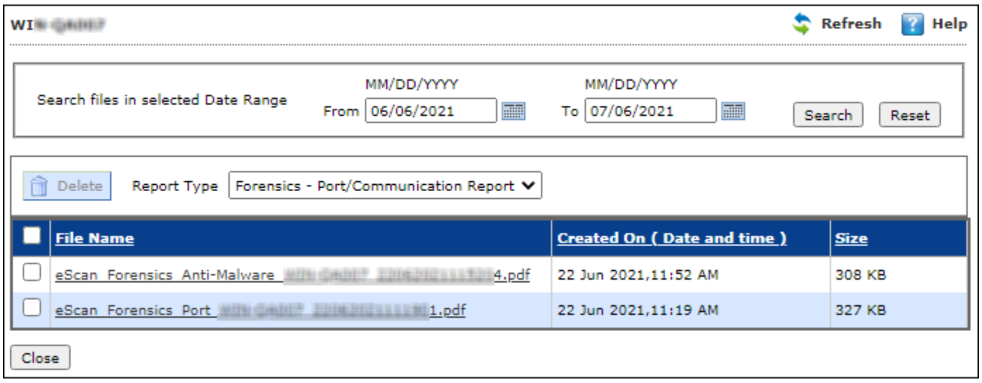
```
7/8/2021 12:35:51 PM : Processing with group : Q[redacted]M
7/8/2021 12:35:51 PM : Connecting to Computer... W[redacted]7
7/8/2021 12:35:52 PM : Successfully Exported Report on W[redacted]7
----------------------------------------------------------------------
=====================================================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

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



☐	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

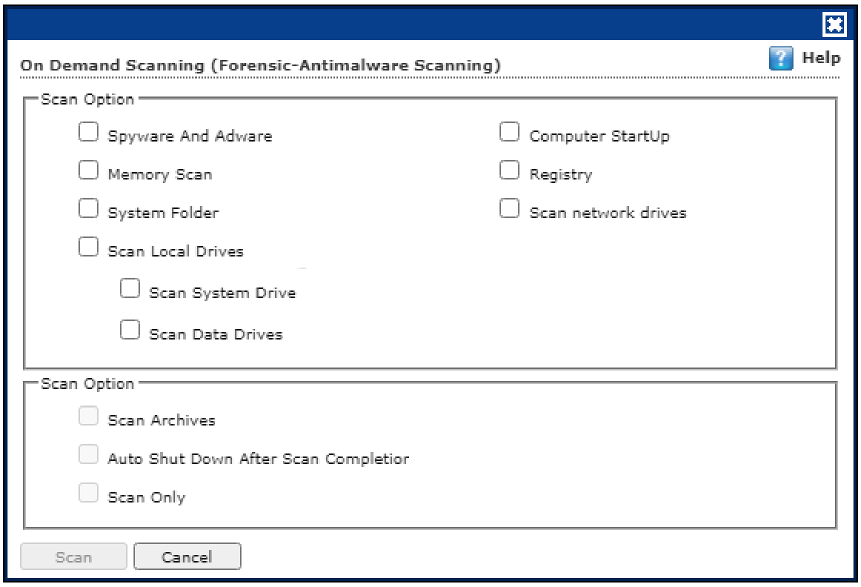
Report Type: Forensics - Port/Communication Report

☐	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

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

□ Spyware And Adware
□ Memory Scan
□ System Folder
□ Scan Local Drives
□ Scan System Drive
□ Scan Data Drives
□ Computer StartUp
□ Registry
□ Scan network drives

Scan Option

□ Scan Archives
□ Auto Shut Down After Scan Completior
□ Scan Only

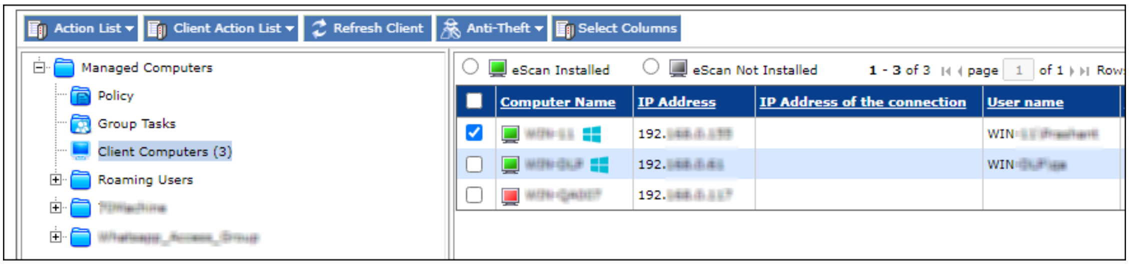
4. Select the preferred scan options and then click **Scan**.

The On Demand Scan for selected client computer begins.

Send Message

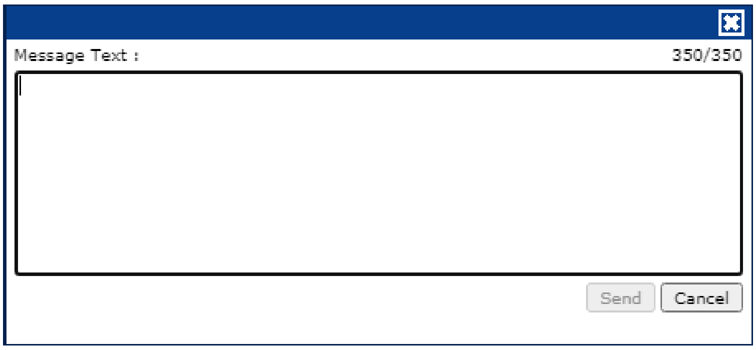
The Send Message feature lets you send a message to computers. To send message to computers, follow the steps given below:

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.



□	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 computer.

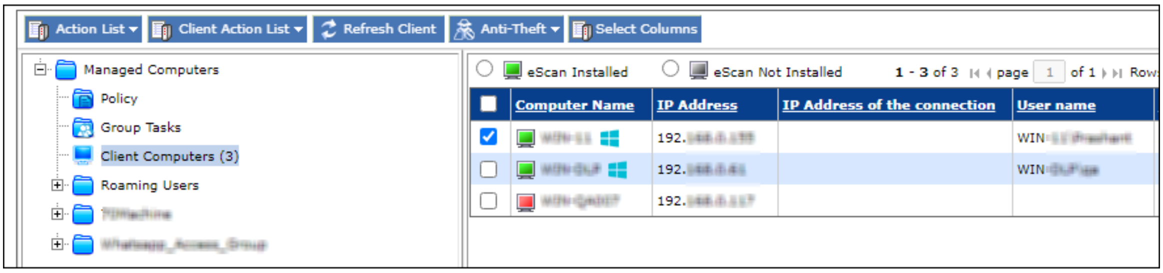
Outbreak Prevention

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. Click here, to learn more about deployment and restoring of Outbreak Prevention.

Delete All Quarantine Files

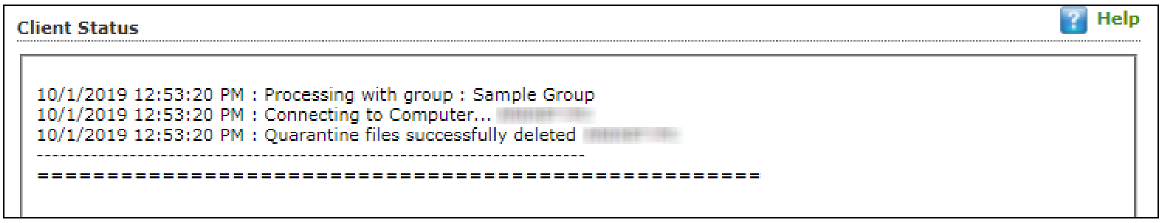
The Delete All Quarantine Files feature lets you delete all quarantine files stored on a computer. To delete all quarantine files on computers, follow the steps given below:

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 computer 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]
----------------------------------------------------------------------
======================================================
```

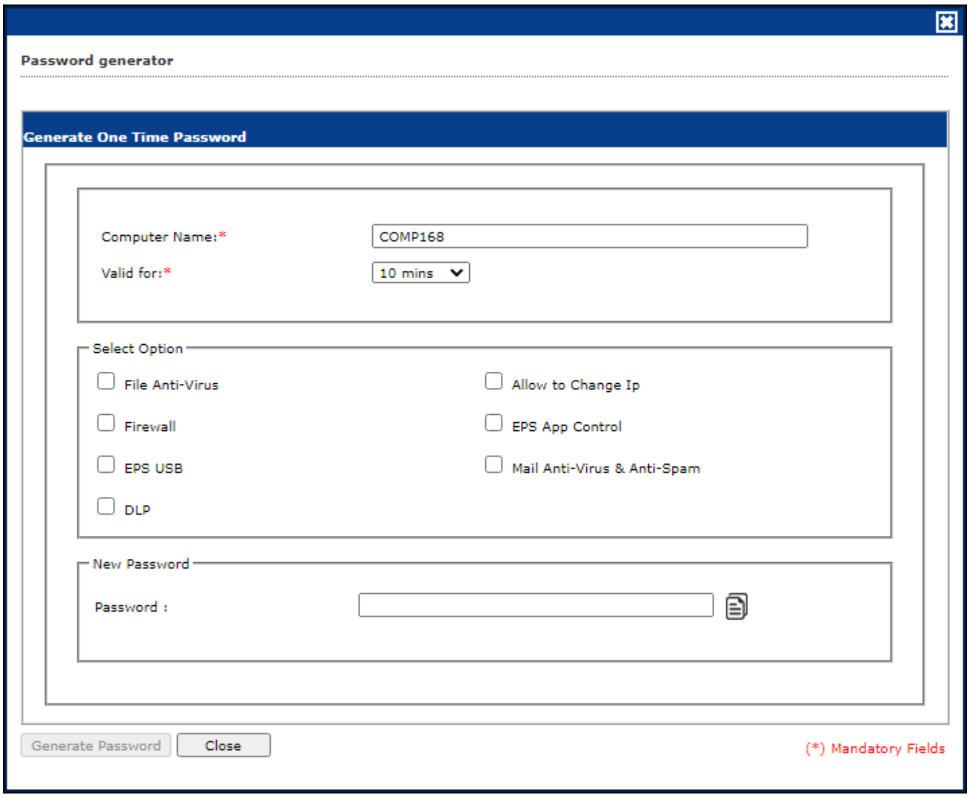
Create OTP

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 to disable USB block policy on specific computer. The administrator can define policy disable duration ranging from 10 minutes to an hour without violating existing policy.

Generating an OTP

To generate an OTP, follow the steps given below:

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



Password generator

Generate One Time Password

Computer Name:* COMP168

Valid for:* 10 mins

Select Option

□ File Anti-Virus

□ Firewall

□ EPS USB

□ DLP

□ Allow to Change Ip

□ EPS App Control

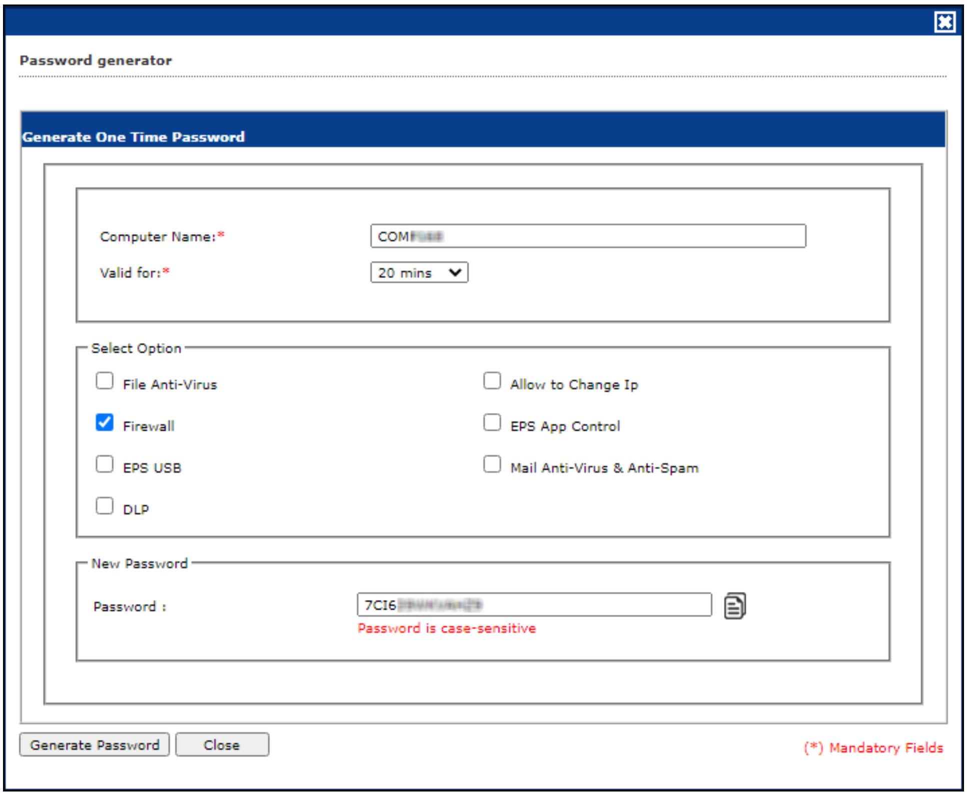
□ Mail Anti-Virus & Anti-Spam

New Password

Password :

(*) Mandatory Fields

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



Password generator

Generate One Time Password

Computer Name:* COM[redacted]

Valid for:* 20 mins

Select Option

□ File Anti-Virus

☑ Firewall

□ EPS USB

□ DLP

□ Allow to Change Ip

□ EPS App Control

□ Mail Anti-Virus & Anti-Spam

New Password

Password : 7CI6[redacted]

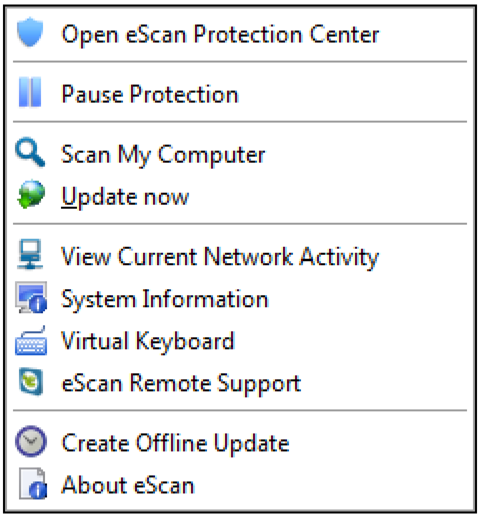
Password is case-sensitive

(*) Mandatory Fields

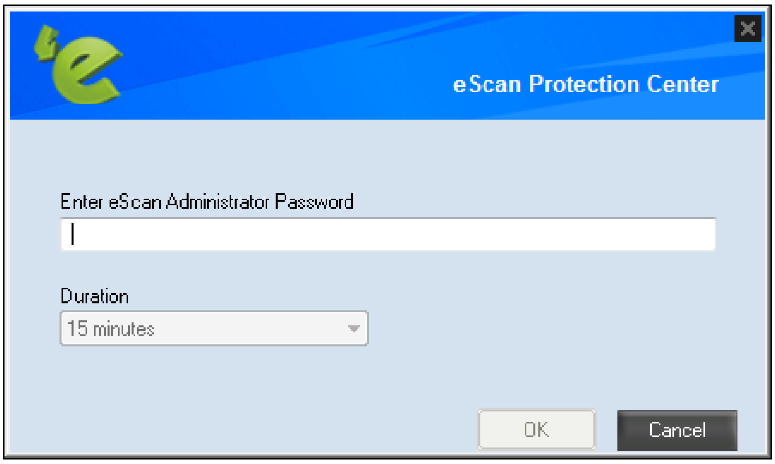
Entering an OTP

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

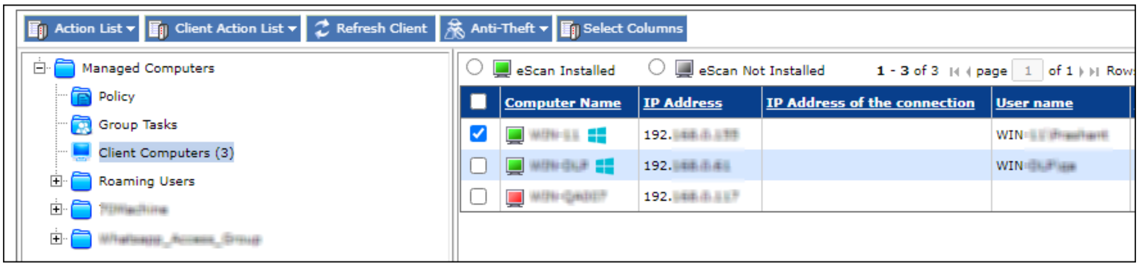
3. Enter an OTP in the field.
4. Click **OK**.

The selected module will be disabled for set duration.

Pause Protection

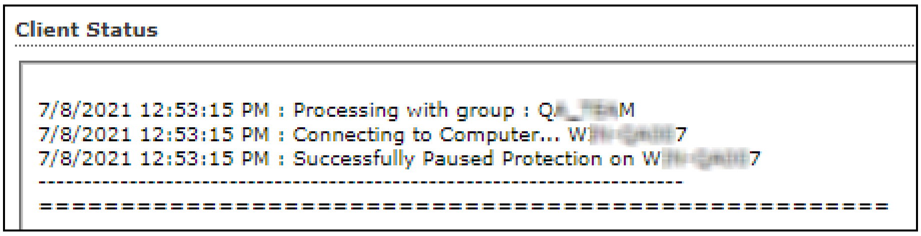
The Pause Protection feature lets you pause the protection for computers.
To pause the protection for computers, follow the steps given below:

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



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

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



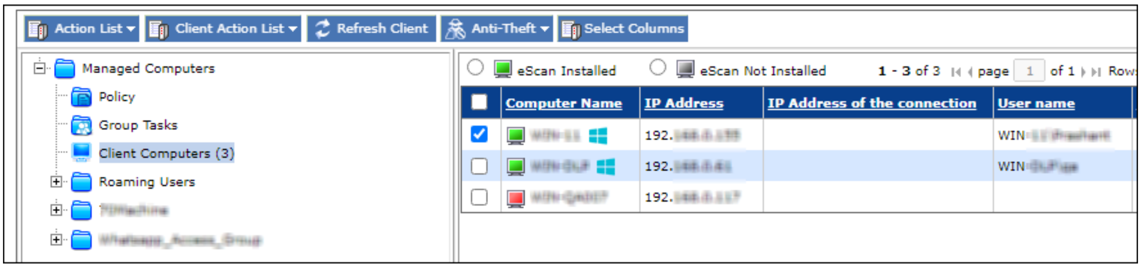
Client Status

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

Resume Protection

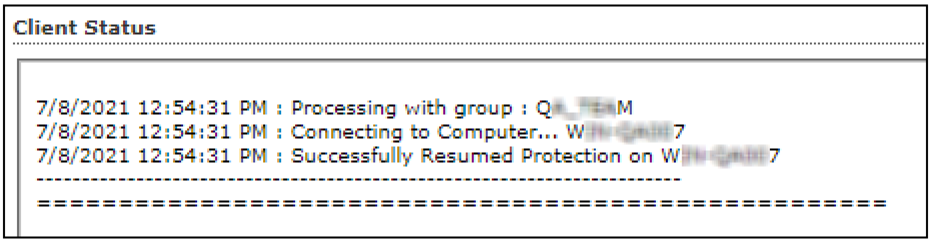
The Resume Protection feature lets you resume protection for computers whose protection is paused. To resume protection for computers, follow the steps given below:

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
☑	[illegible]	192.[illegible]		WIN-[illegible]
☐	[illegible]	192.[illegible]		WIN-[illegible]
☐	[illegible]	192.[illegible]		

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



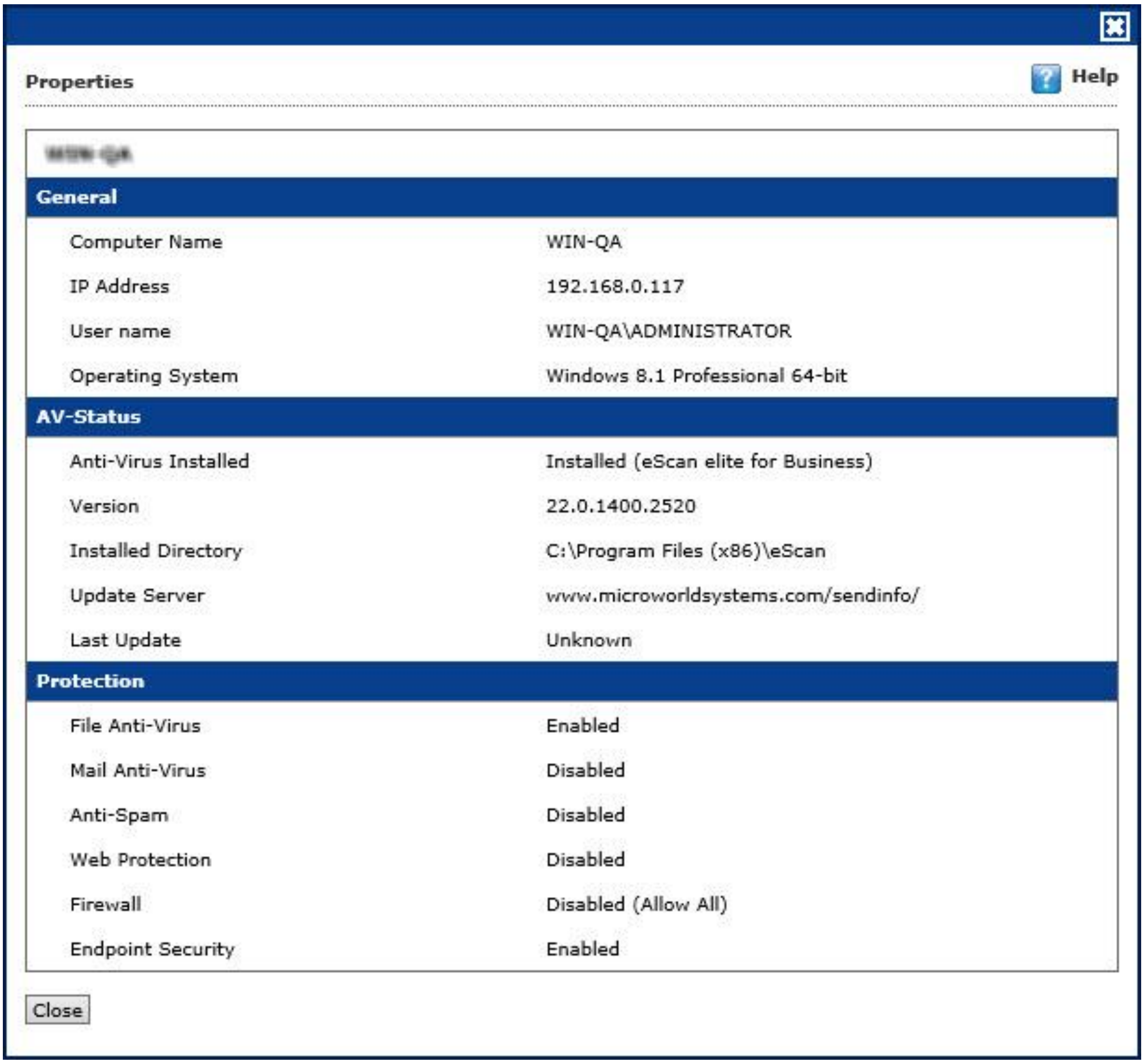
Client Status

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



Properties

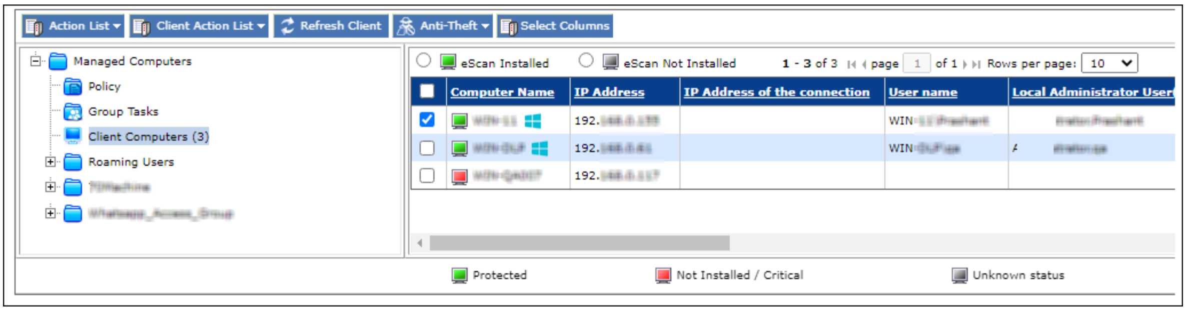
[redacted]

General	
Computer Name	WIN-QA
IP Address	192.168.0.117
User name	WIN-QA\ADMINISTRATOR
Operating System	Windows 8.1 Professional 64-bit
AV-Status	
Anti-Virus Installed	Installed (eScan elite for Business)
Version	22.0.1400.2520
Installed Directory	C:\Program Files (x86)\eScan
Update Server	www.microworldsystems.com/sendinfo/
Last Update	Unknown
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.

Anti-Theft

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



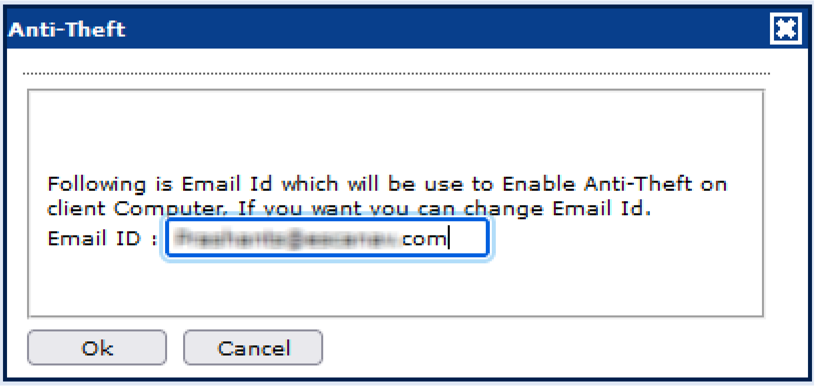
☐	Computer Name	IP Address	IP Address of the connection	User name	Local Administrator User
☑	[redacted]	192.[redacted]		WIN-[redacted]	[redacted]
☐	[redacted]	192.[redacted]		WIN-[redacted]	[redacted]
☐	[redacted]	192.[redacted]			

🟩 Protected 🟥 Not Installed / Critical ▨ Unknown status

Anti-Theft Options

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

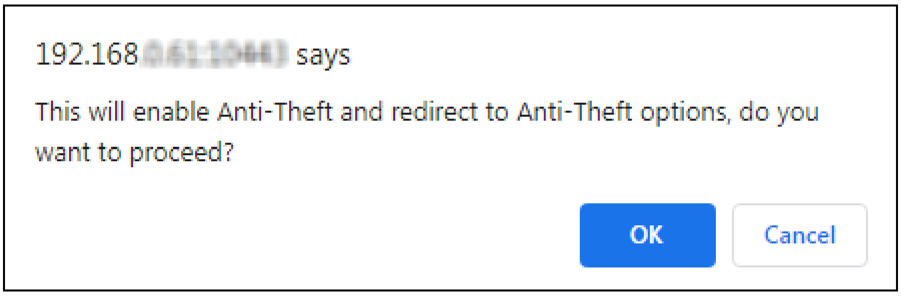
1. Go to **Managed Computers**.
2. Select the desired computers to add in Anti-theft Portal.
3. Click **Anti-Theft** > **Anti-Theft Options**.
4. Enter the **Email ID** then Click **OK.**
   The computer will add in Anti-Theft Portal.



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

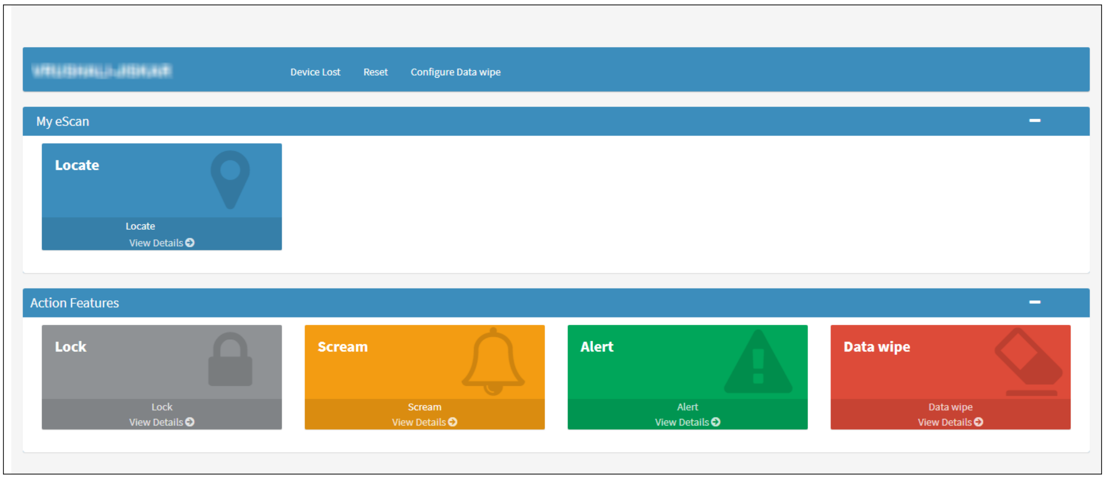
A confirmation prompt appears.



192.168[redacted] says

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

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



[redacted] Device Lost Reset Configure Data wipe

My eScan

Locate
Locate
View Details

Action Features

Lock
Lock
View Details

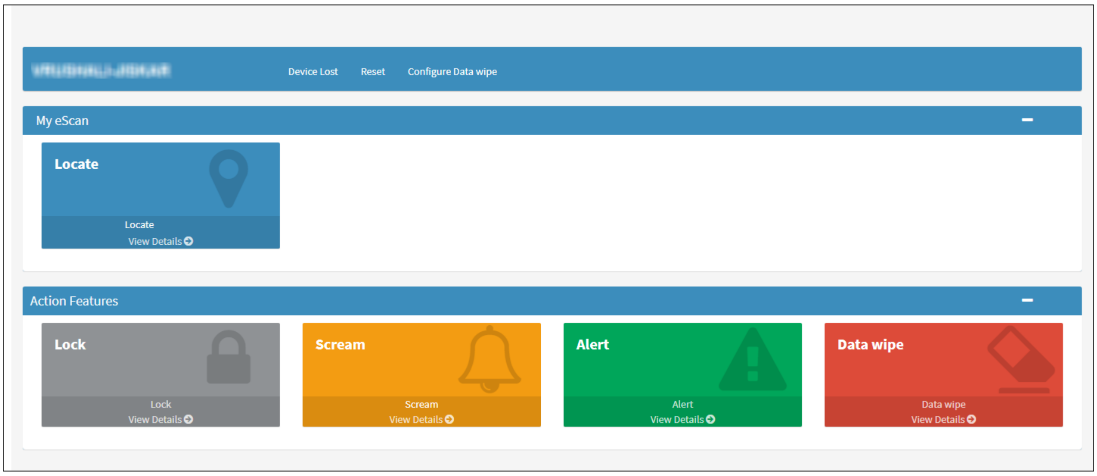
Scream
Scream
View Details

Alert
Alert
View Details

Data wipe
Data wipe
View Details

Anti-Theft Portal

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



[redacted] Device Lost Reset Configure Data wipe

My eScan

Locate
Locate
View Details

Action Features

Lock
Lock
View Details

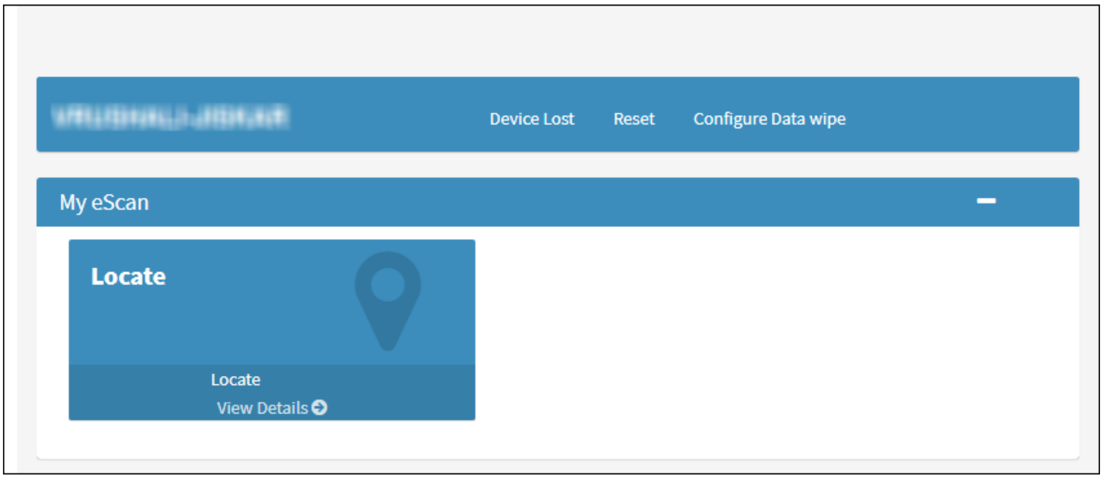
Scream
Scream
View Details

Alert
Alert
View Details

Data wipe
Data wipe
View Details

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

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

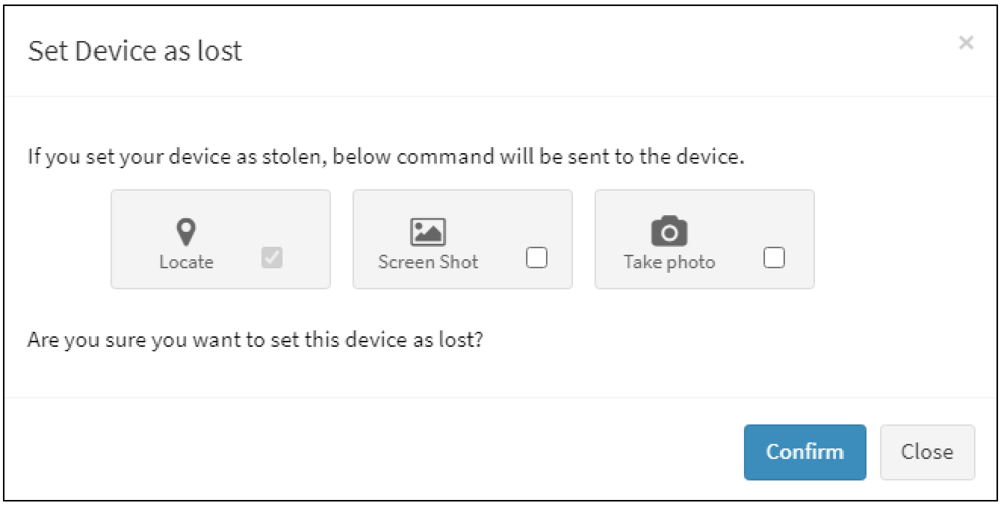


[redacted] Device Lost Reset Configure Data wipe

My eScan

Locate
Locate
View Details

2. 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.

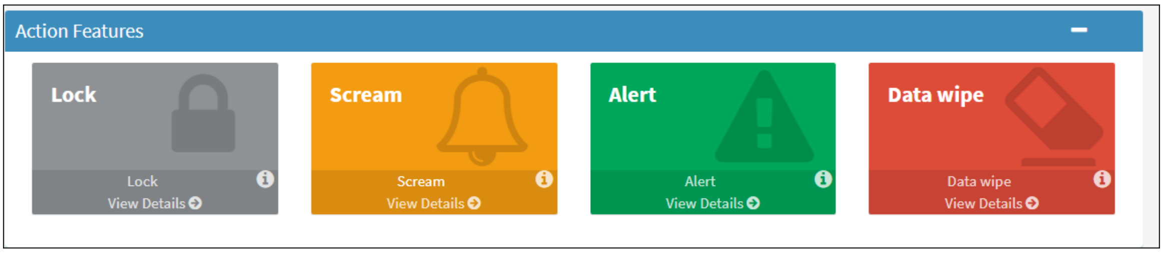
Are you sure you want to set this device as lost?

- **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:
  1) Click **Locate**, the status will change to Request Pending; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to locate the system is in progress.
  2) **View Details** displays the Last Location of your system on a map. It also shows details of last two successful executions of the Locate command.

- **Screenshot**: This option will take a screen shot of the system whenever it is synced to the server.
  1) Click **Screenshot**, the status will change to Request Pending; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to take a screenshot is in progress.
  2) **View Details** displays the last two screenshots from the successful execution of the screenshot command.

- **Take Photo**: This option will allow you to take a snapshot of the current user of the system from the webcam on clicking the **Camera** option on the anti-theft portal.
  1) Click **Camera**, the status will change to Request Pending; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to take a snapshot is in progress.
  2) **View Details** displays the last two snapshots taken from your system.

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



Action Features

Lock
Lock
View Details

Scream
Scream
View Details

Alert
Alert
View Details

Data wipe
Data wipe
View Details

- **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 recovred. Click **Alert** option to remotely send a message to your lost system. Type in your message in the **send message** section and click **Confirm**.

- **Data wipe**: The Data Wipe feature will delete all the selected files and folders that have been added to the list to be deleted from the portal. Click **Data Wipe** option to remotely wipe all the selected files and folders or only delete the cookies and click **Confirm**. Select the **Delete Cookies** checkbox to delete cookies or select the **Data wipe** checkbox to wipe the data and click on **Confirm**.

Disable Anti-Theft

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

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

The Anti-Theft will be disable on selected computer.

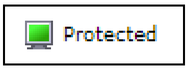
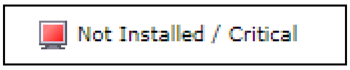
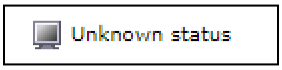
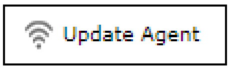
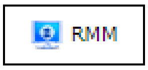
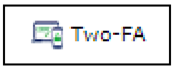
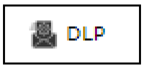
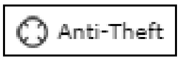
Refresh Client

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

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

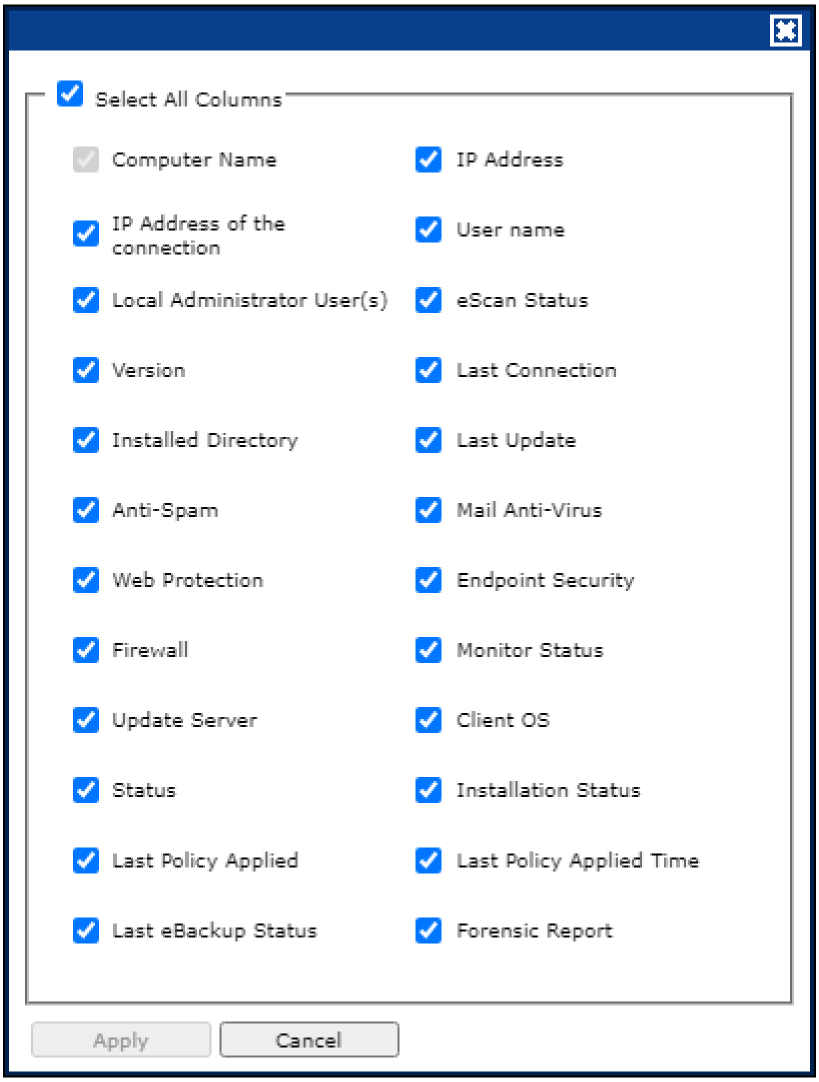
The Client will be refreshed.

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.
 Anti-Theft	This status is displayed when a computer is added to Anti-Theft Portal.

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 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.

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.

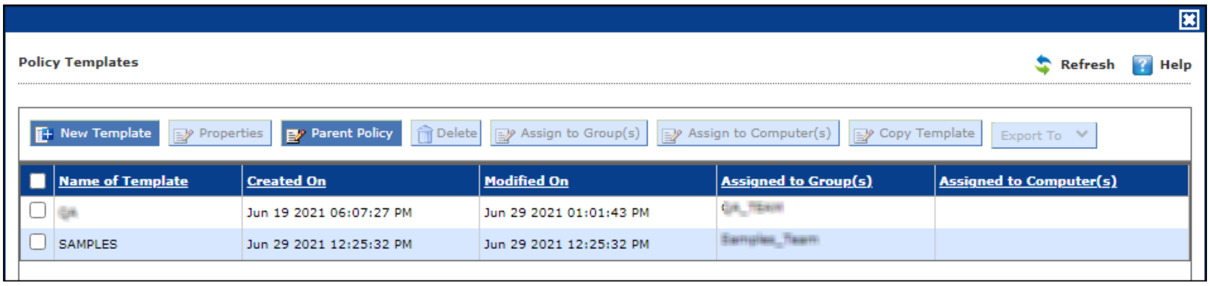
Schedule Update
Schedule Update policy lets you schedule eScan database updates. To learn more, click here.

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

Creating Policy Template for a group/specific computer

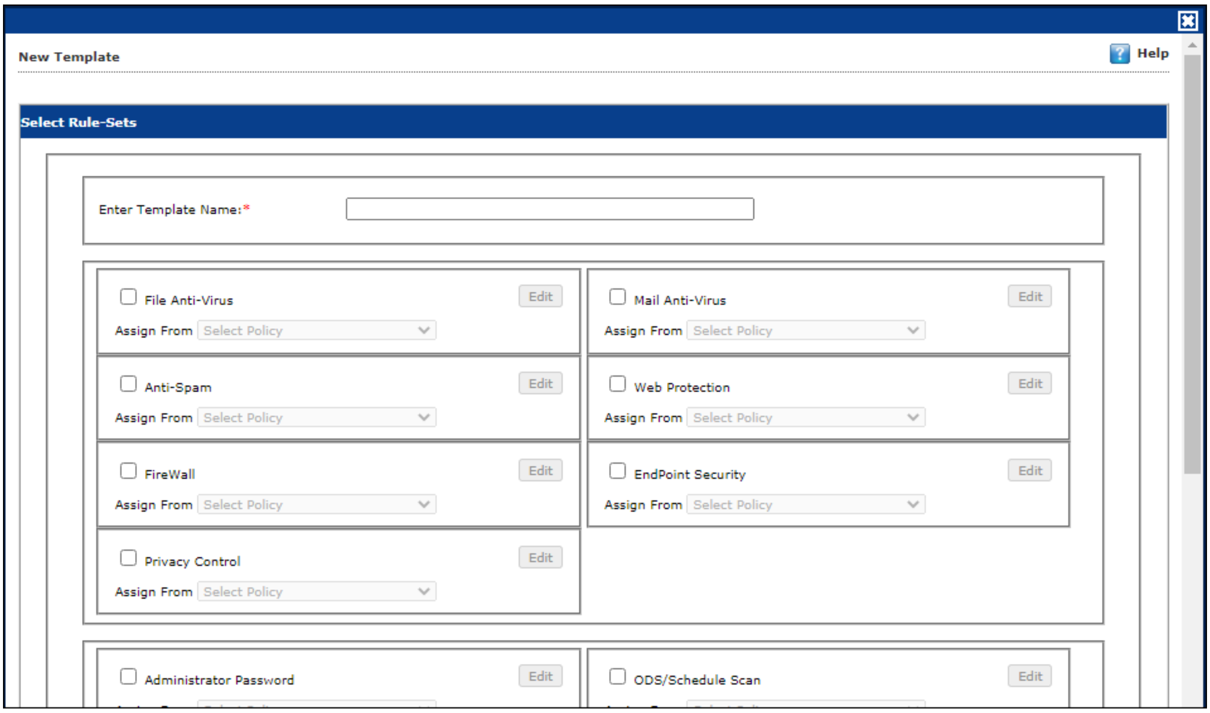
To create a Policy template for a group, follow the steps given below:

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 computers.



New Template
Help

Select Rule-Sets

Enter Template Name:*

□ File Anti-Virus Edit
Assign From Select Policy

□ Mail Anti-Virus Edit
Assign From Select Policy

□ Anti-Spam Edit
Assign From Select Policy

□ Web Protection Edit
Assign From Select Policy

□ FireWall Edit
Assign From Select Policy

□ EndPoint Security Edit
Assign From Select Policy

□ Privacy Control Edit
Assign From Select Policy

□ Administrator Password Edit

□ ODS/Schedule Scan Edit

4. Enter name for Template.
5. To edit a module, select it and then click **Edit**.
6. Make a changes and Click **Save**.

The Policy Template will be saved.

Configuring eScan Policies for Windows Computers

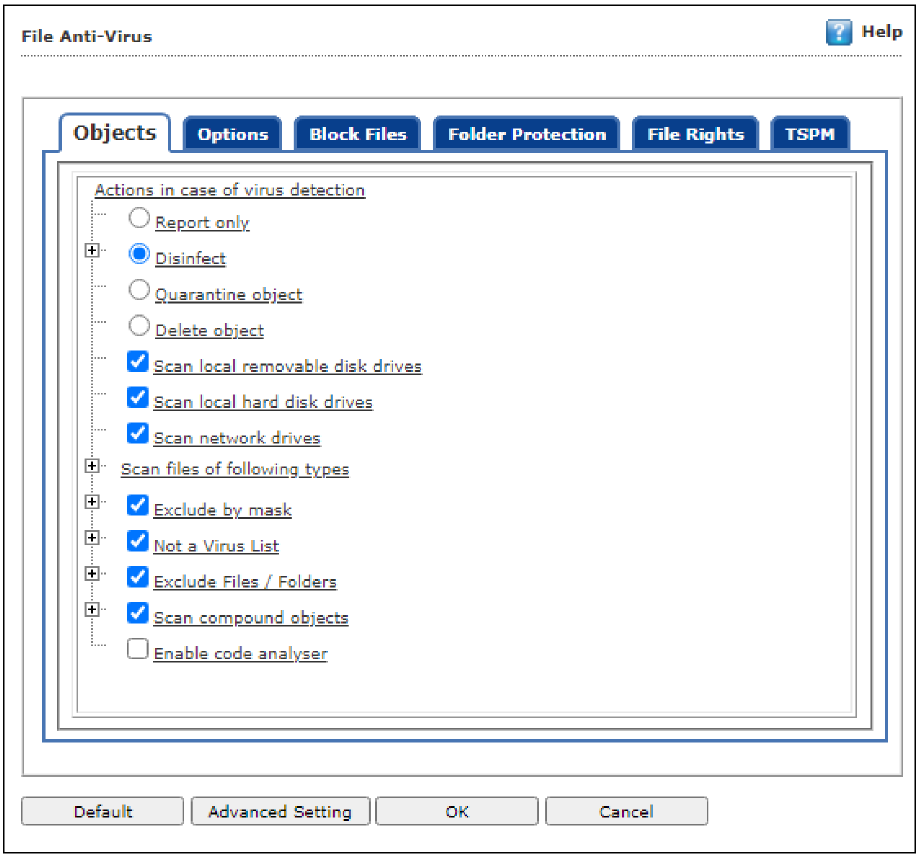
Each module of a policy template can be further edited to meet your requirements.

File Anti-Virus

File Anti-Virus module displays following tabs:

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

Objects



File Anti-Virus

Actions in case of virus detection

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

Actions in case of virus detection
This section lists the different actions that File Anti-Virus can perform when it detects virus infection.

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

Disinfect [Default]
Tries to disinfect the detected object and If disinfection is impossible it will **Quarantine Object** or **Delete 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**.**

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 requirement 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.

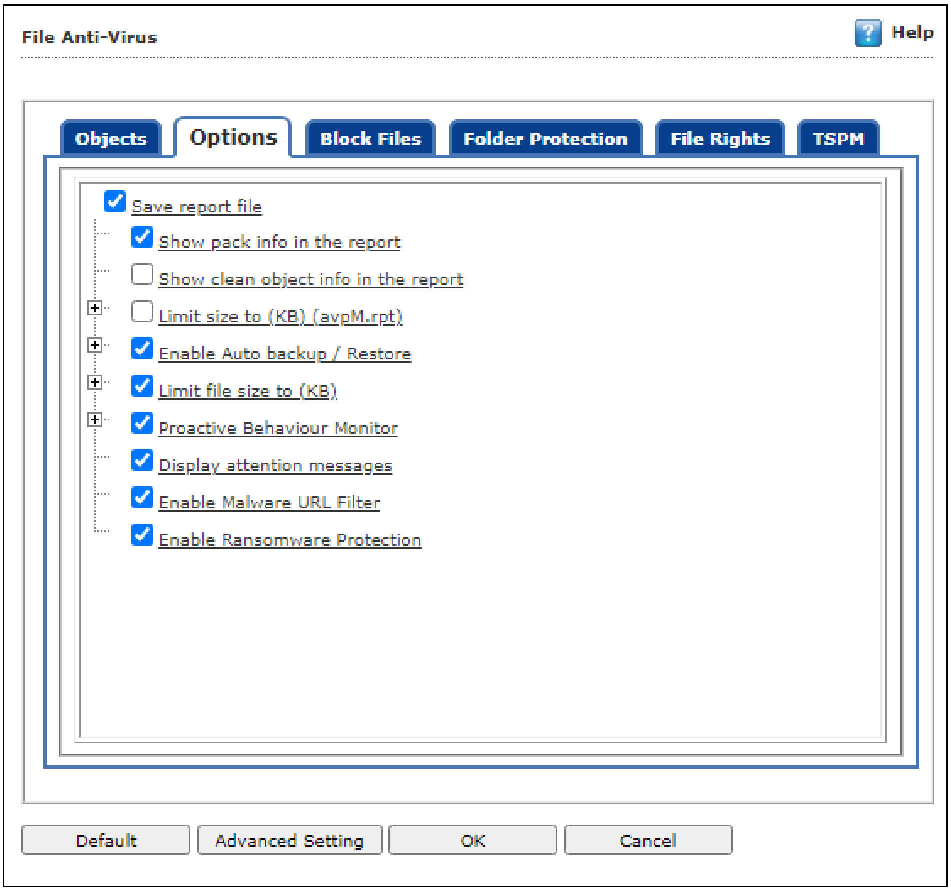
Exclude Files/Folders [Default]
Select this checkbox if you want File Anti-Virus to exclude all the listed files, folders, and sub folders while it is monitoring or scanning folders. The files/folders added to this list will be excluded from real-time scan as well as on demand scan. You can add or delete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

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.

Options

The Options tab lets you configure following options:



☑ 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 given textbox.

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 do the following settings:

Do not backup files above size (KB)
This option lets you prevent File Anti-Virus from creating backup of files that are larger than the file size that you have specified. The default value is 32768 kb.

Minimum disk space (MB)
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 mark the files in the database that you want to exclude from being blocked. To whitelist a file/folder, click **Whitelist** and then click **Add from DB**.
- **Block List**
  Block listing allows to you mark the files from the white list that should be blocked.

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

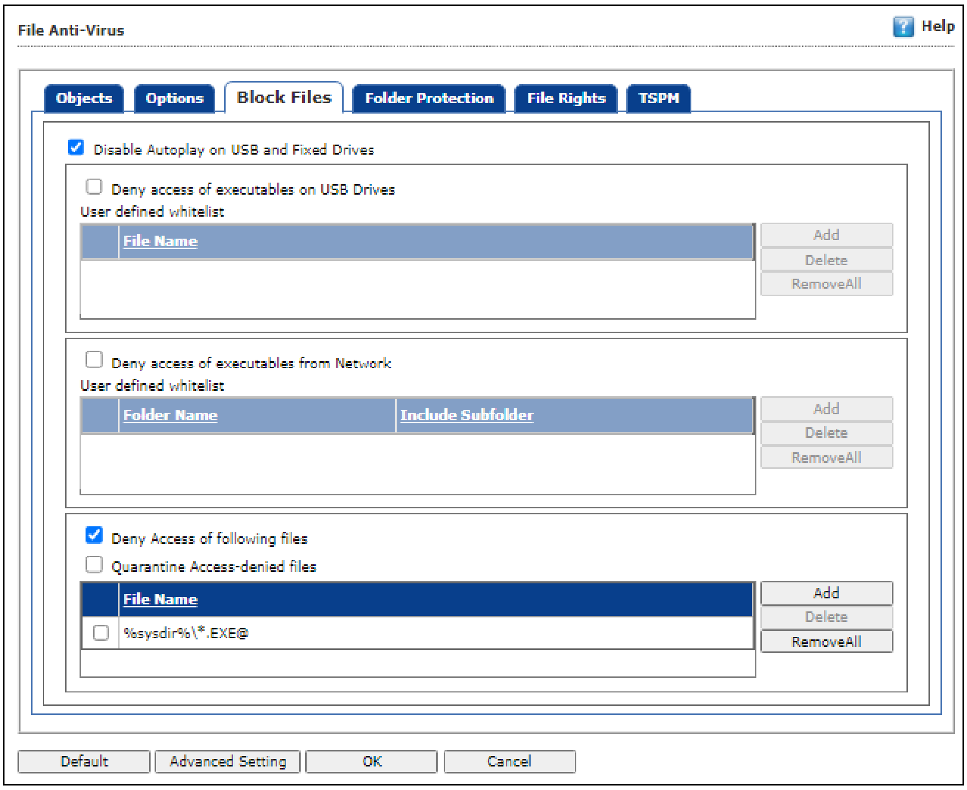
Display attention messages [Default]
When this option is selected, eScan displays an alert consisting the path and name of the infected object and the action taken by the File Anti-Virus module.

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

Block Files

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



☑ 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@

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

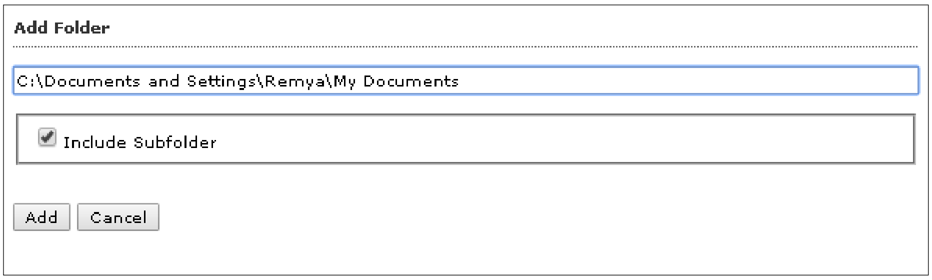
Select this checkbox if you want eScan to prevent executables stored on USB drives from being accessed.

Deny access of executables 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**.



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.

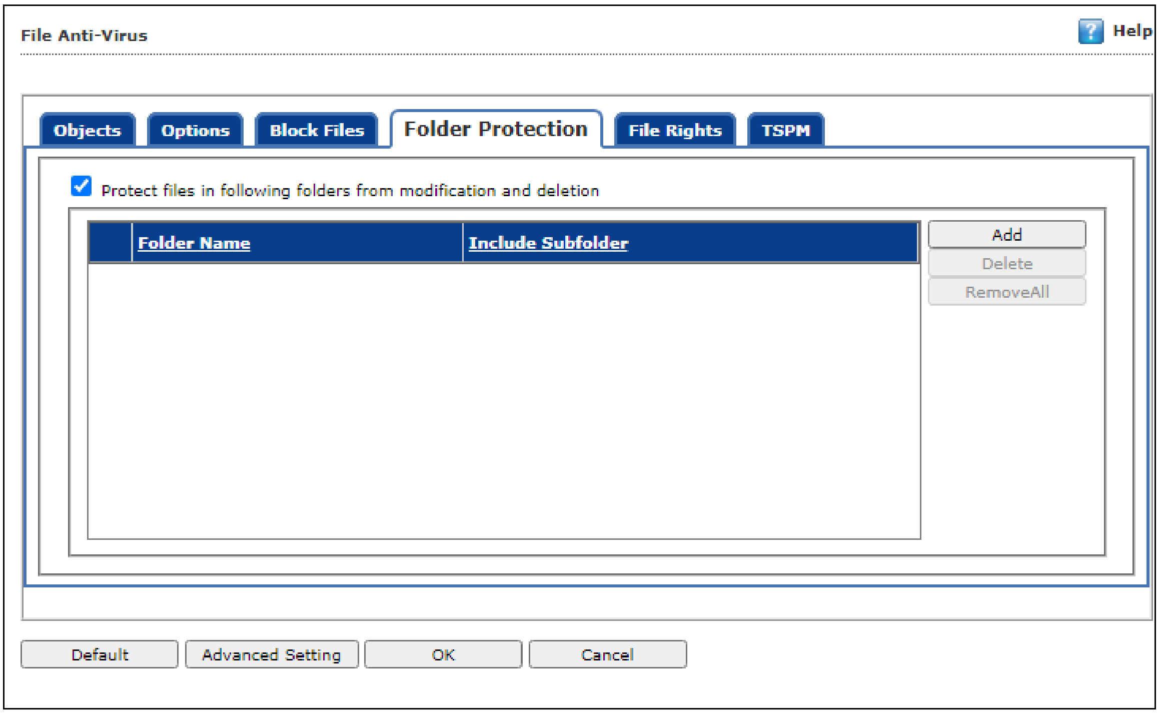
Deny Access of following files [Default]
Select this checkbox if you want eScan to prevent the files in the list from running on the computers.

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:



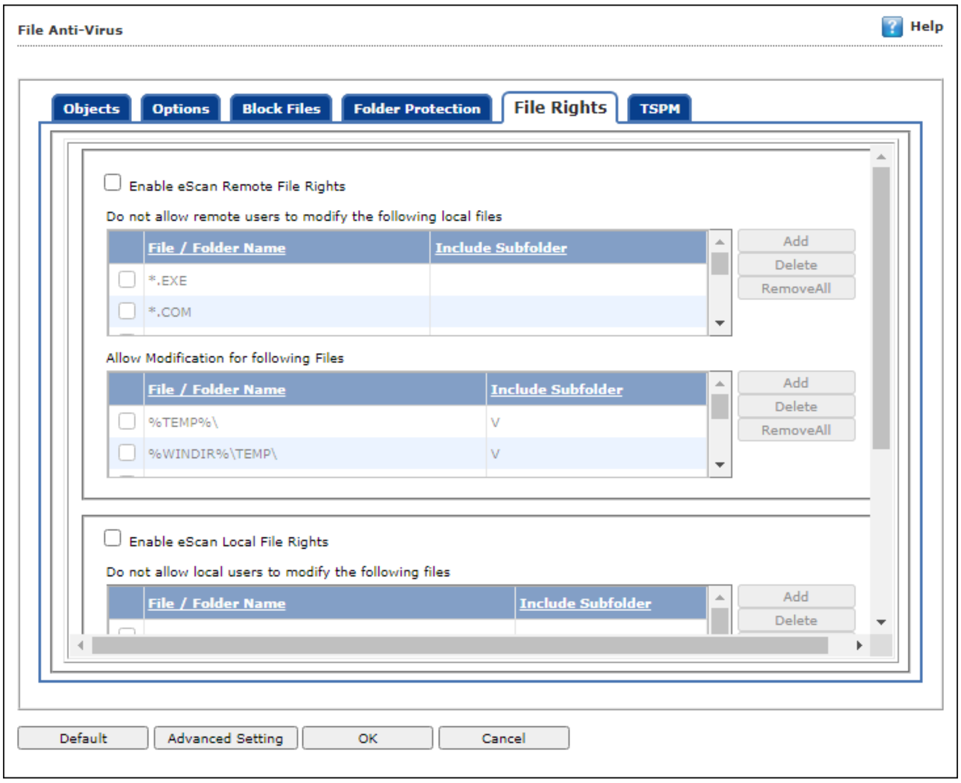
☑ Protect files in following folders from modification and deletion

	Folder Name	Include Subfolder

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



File Anti-Virus

□ 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

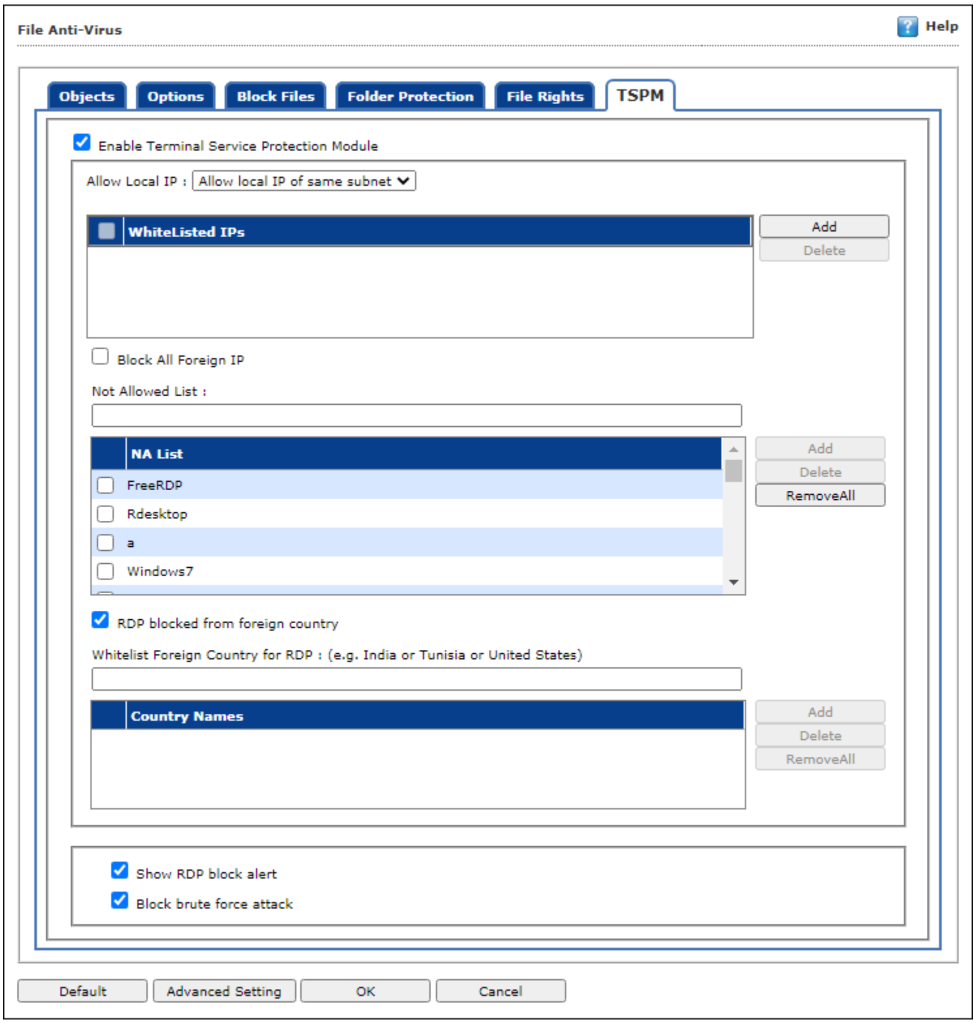
The files/folders added to this list cannot be modified by the local users.

Allow Modification for following Files

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

TSPM

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

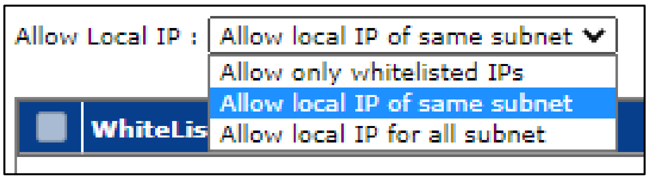
☑ Block brute force attack

Enable Terminal Service Protection Module [Default]

Select this checkbox to activate TSPM module.

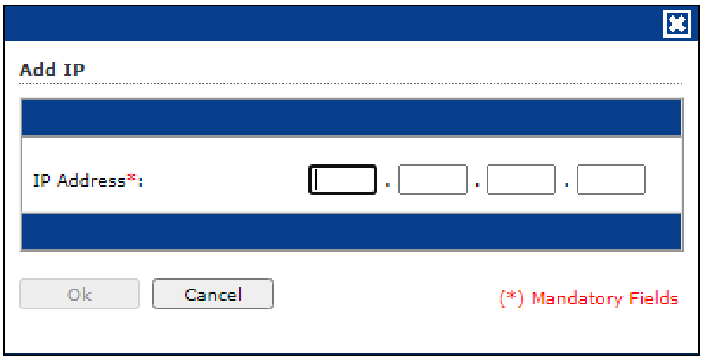
Allow Local IP

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.**
To delete the IP address from list, select the IP address and click **Delete**.

- ○ **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 [Default]:** Select this option to allow the local IPs that belongs to same subnet.
- **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 address 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 at once, 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.

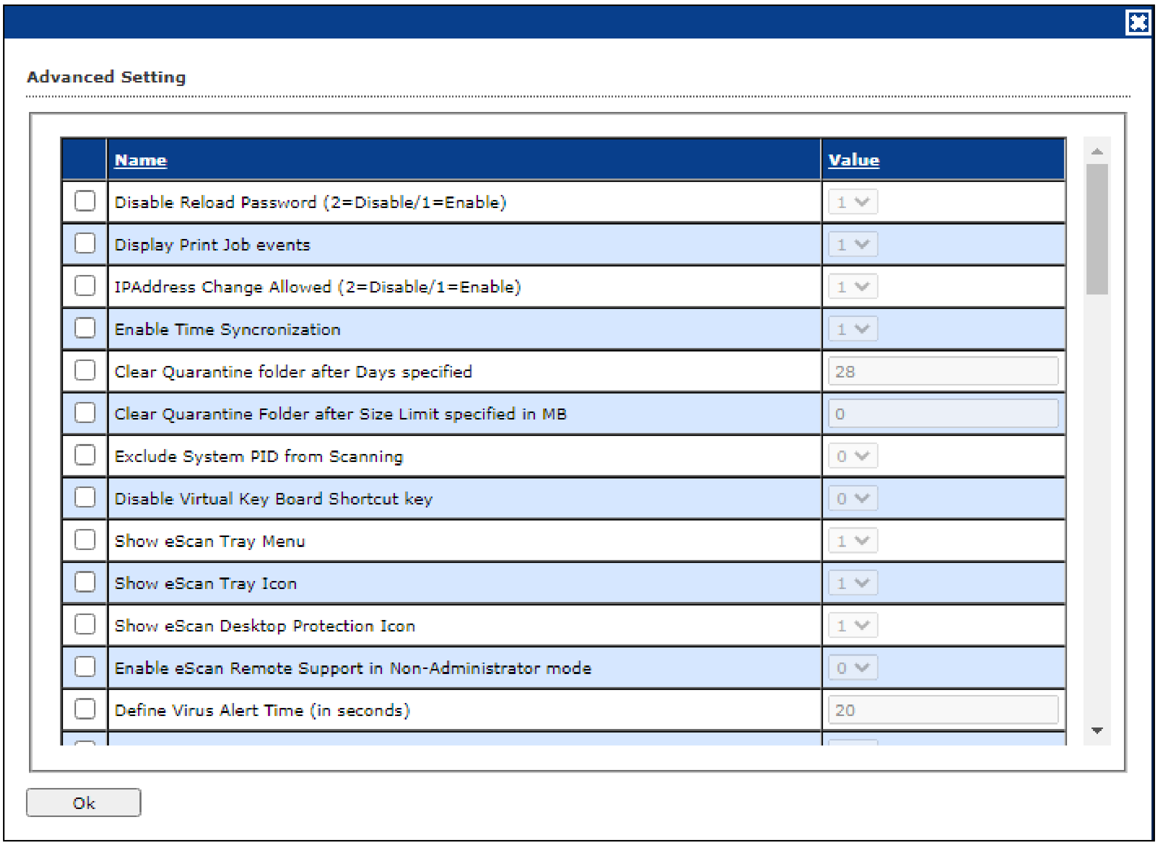
Show RDP block alert [Default]
This checkbox allows eScan to alert the user in case of any RDP connection is blocked.

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

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

Advanced Settings

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



Advanced Setting

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

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 keys for using Virtual Keyboard on Managed Computers.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

Enable Winsock Protection (Require Restart) (1 = Enable/0 = Disable)
Selecting this option lets you restarts Winsock protection. By default, this option is enabled.

Block Gmail (Except corporate ones) (1 = Enable/0 = Disable)
Selecting this option lets you enable/disable block Gmail.

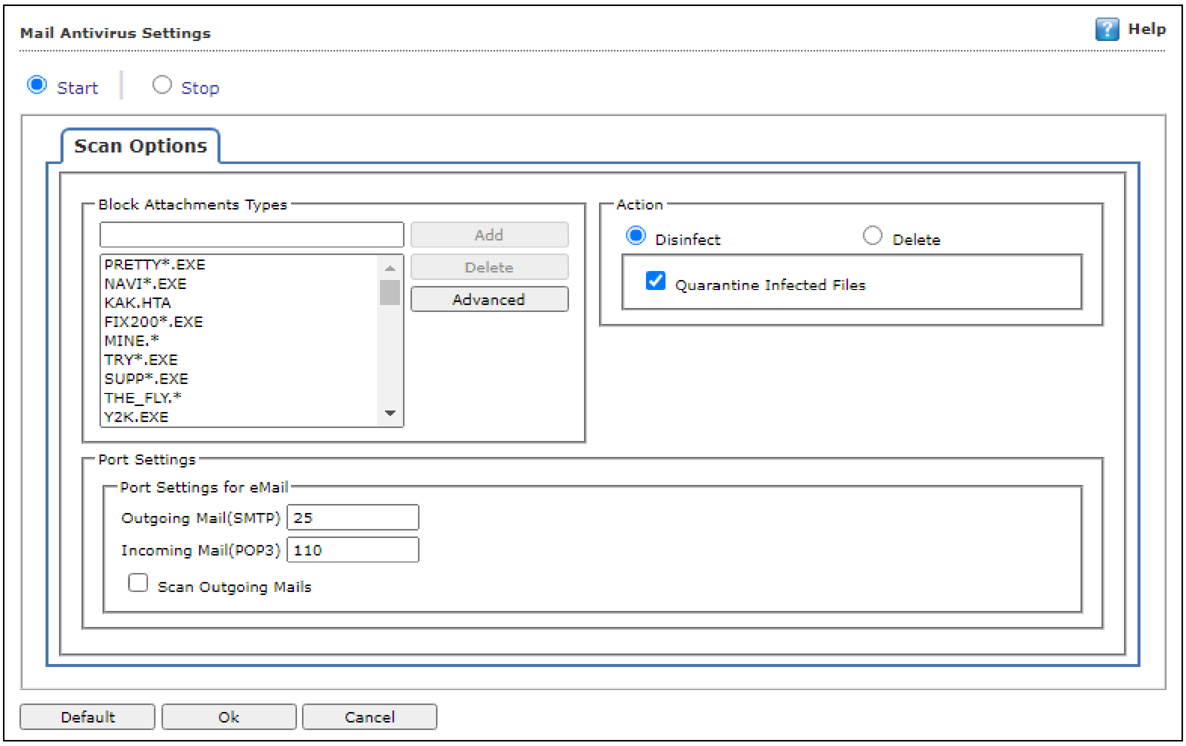
Block Registry Editor (1 = Enable/0 = Disable)
Selecting this option lets you enable/disable block Registry Editor.

Block PowerShell (1 = Enable/0 = Disable)
Selecting this option lets you enable/disable block PowerShell.

Block MS Office (0 = Disable /1-All/2-All except Outlook)
Selecting this option lets you enable/disable block MS Office.

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 requirement. 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.

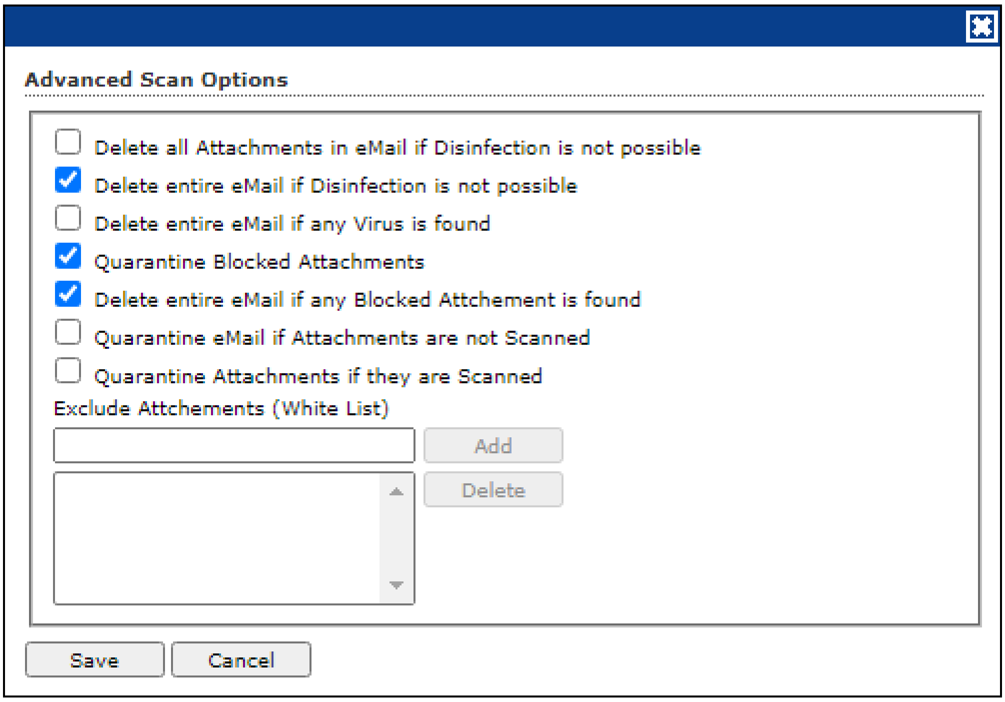
Incoming Mail (POP3) [Default: 110]
You need to specify a port number for POP3.

Scan Outgoing Mails
Select this checkbox if you want Mail Anti-Virus to scan outgoing emails as well.

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

Advanced

Clicking **Advanced** tab 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.

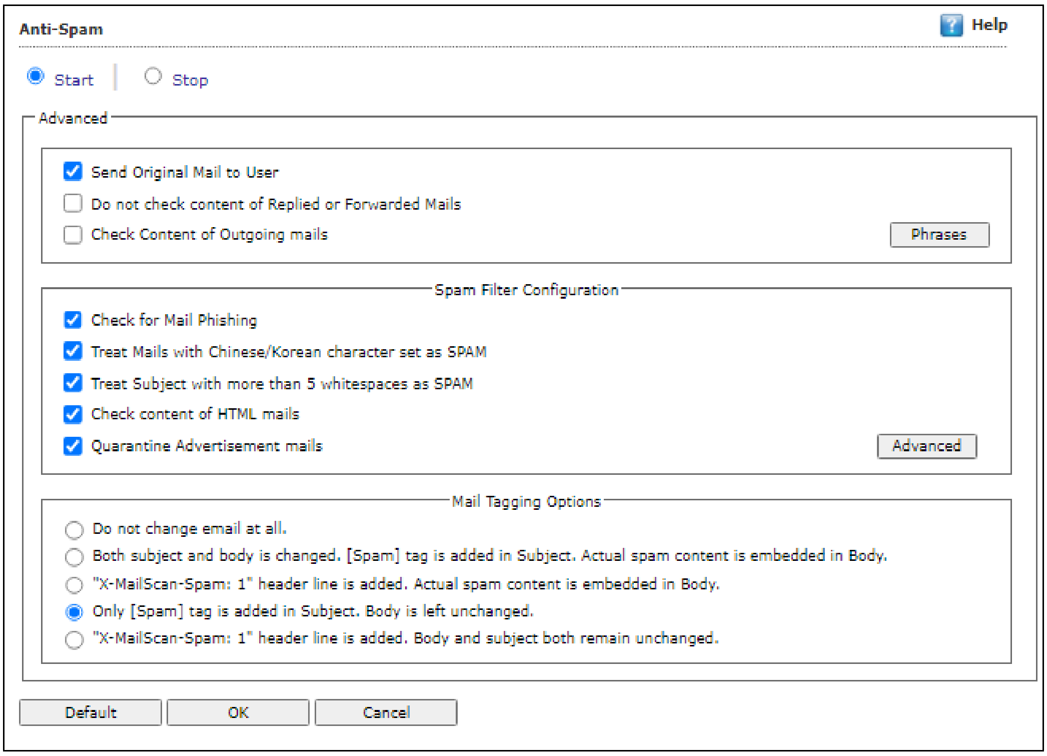
Quarantine email if attachments are not scanned
Select this checkbox to quarantine an entire email if it contains an attachment not scanned by Mail Anti-Virus.

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 *.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]

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

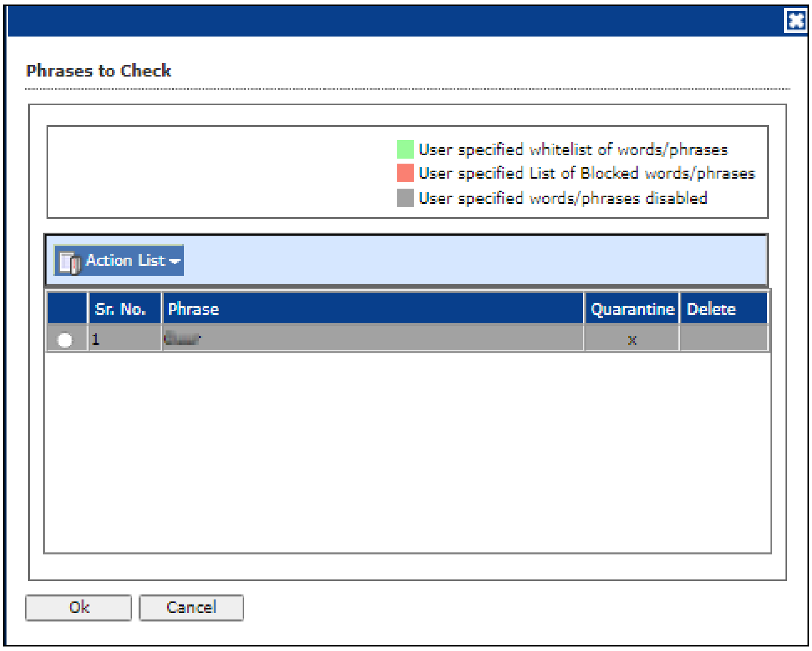
Select this checkbox, if you want to ensure that eScan does not check the contents of emails that you have either replied or forwarded to other recipients.

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.



Phrases to Check

🟩 User specified whitelist of words/phrases
🟥 User specified List of Blocked words/phrases
▨ User specified words/phrases disabled

	Sr. No.	Phrase	Quarantine	Delete
○	1	[illegible]	x	

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.

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]

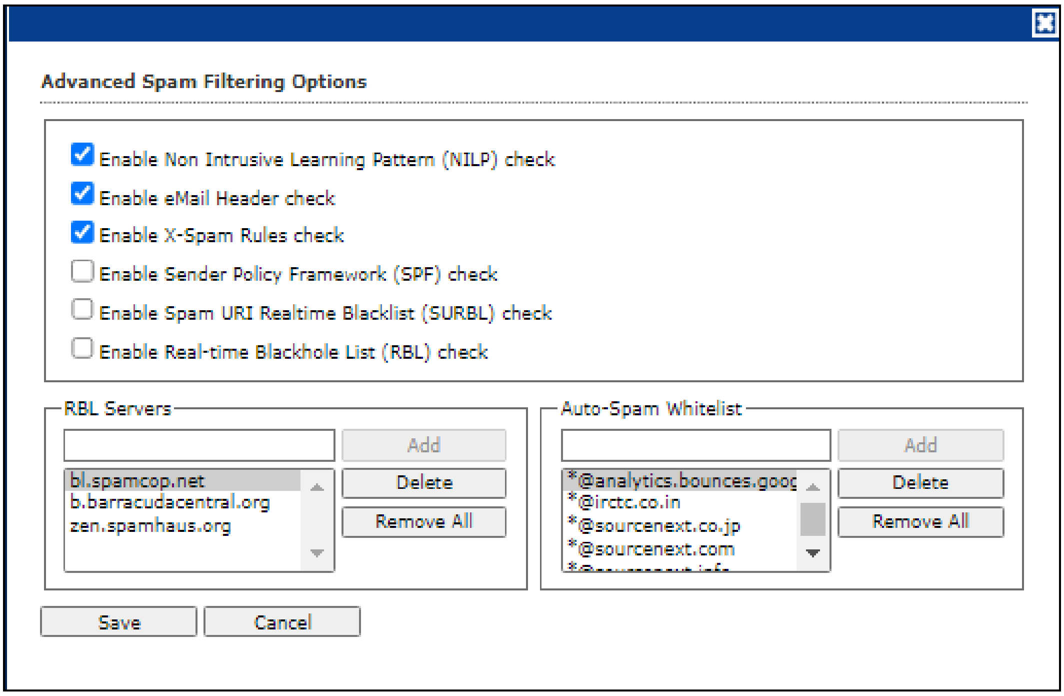
Select this option if you want Anti-Spam to scan emails in HTML format along with text content.

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
zen.spamhaus.org

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

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

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

Enable email Header check [Default]

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

Enable X Spam Rules check [Default]

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

Enable Sender Policy Framework (SPF) check
SPF is a world standard framework adopted by eScan to prevent hackers from forging sender addresses. It acts as a powerful mechanism for controlling phishing mails. Select this 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.

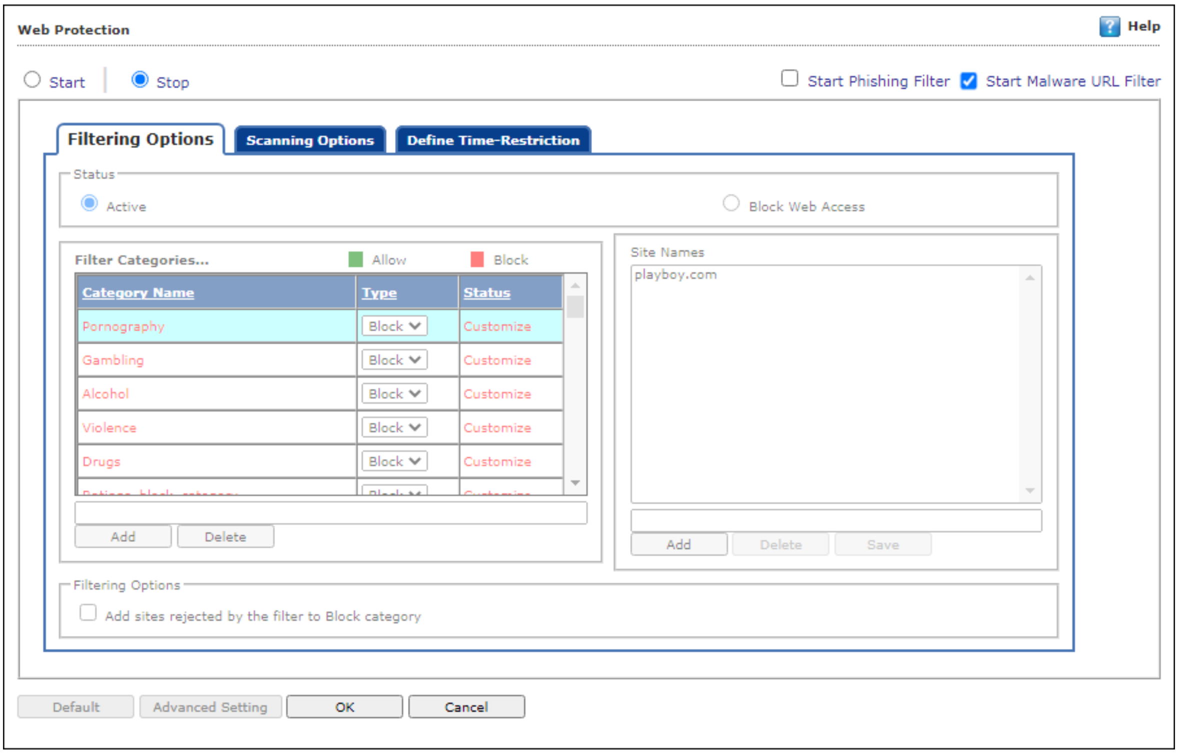
Only [Spam] tag is added in Subject: Body is left unchanged [Default]
This option lets you add the [Spam] tag only in the subject of the email, which has been identified as spam.

"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.

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

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
Ratings_block_category	Block	Customize

Site Names: playboy.com

Filtering Options: □ Add sites rejected by the filter to Block category

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 [Allow]

It represents an allowed websites category.

Red [Block]

It represents a blocked websites category.
The filter categories used in this section include categories like Pornography, Gambling, Chat, Alcohol, Violence, Drugs, Ratings_block_category, Websites Allowed, etc. You can also add or delete filter categories depending on your requirement.

Category Name

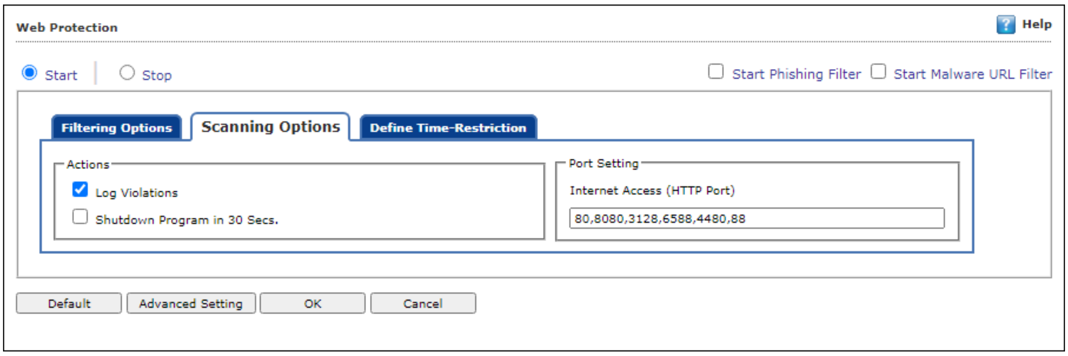
This section shows the **Words/Phrases** list. It lists the words or phrases present in the selected category. In addition, the section displays the **Site Names** list, which lists the websites belonging to the selected category. You can also add or delete filter categories depending on your requirement.

Filtering Options

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

Scanning Options

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



Web Protection

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

Actions
☑ Log Violations
□ Shutdown Program in 30 Secs.

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

Actions

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

Log Violations [Default]

This 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

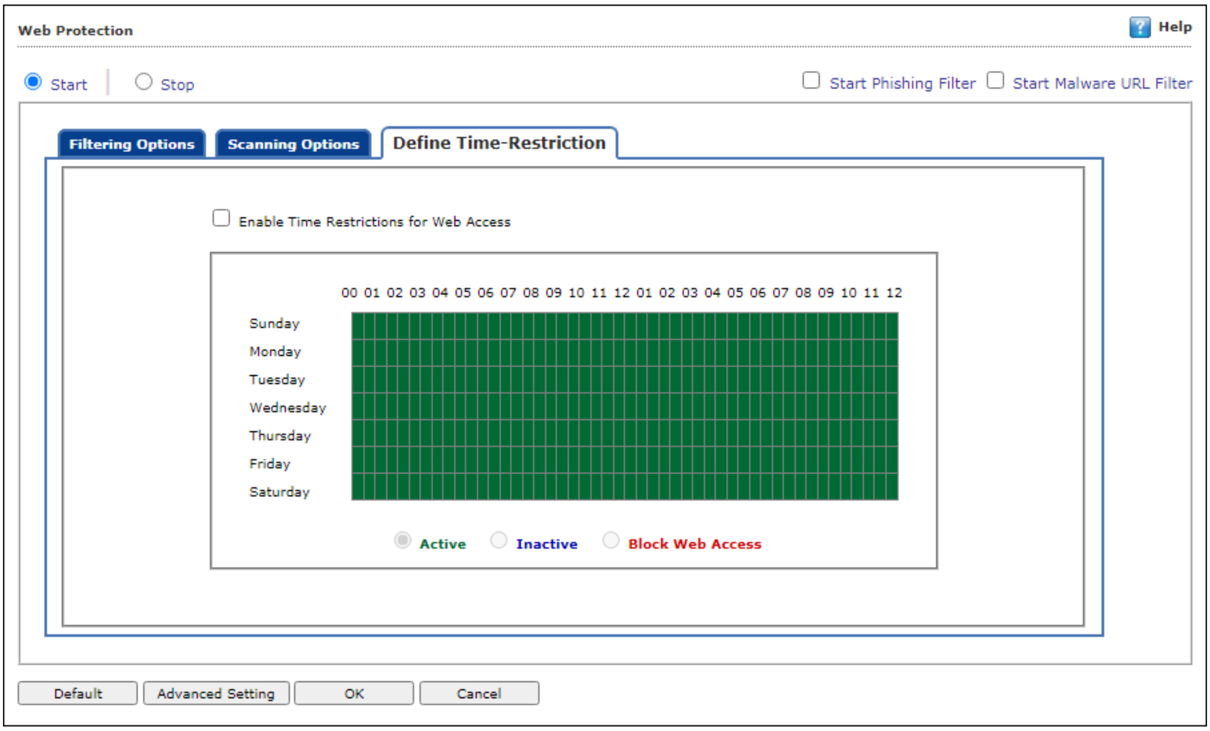
This section lets you specify the port numbers that eScan should monitor for suspicious traffic.

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.

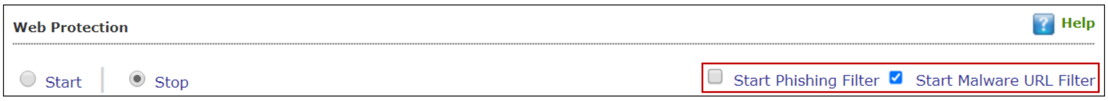
Block Web Access

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.

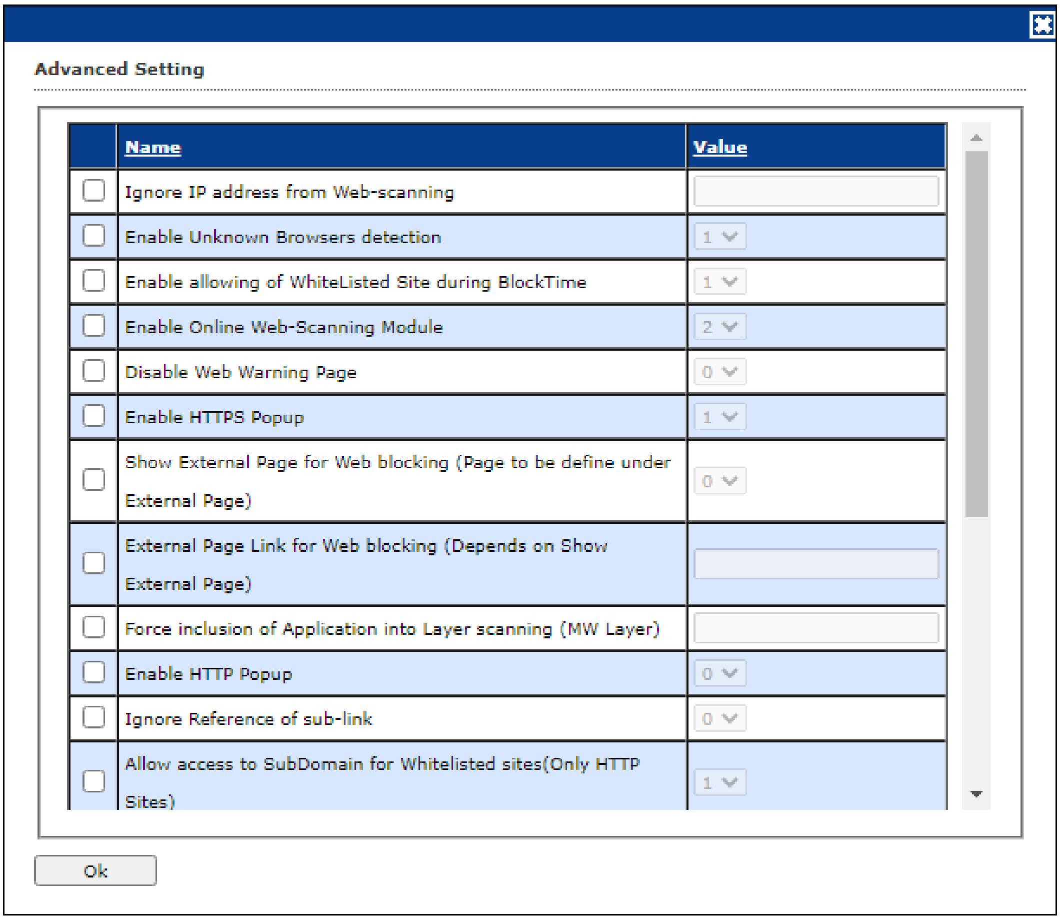


Web Protection Help

○ Start | ● Stop □ Start Phishing Filter ☑ Start Malware URL Filter

Advanced Settings

Clicking **Advanced** displays Advanced Settings.



Advanced Setting

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

Ignore IP address from Web-scanning

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

Enable Unknown Browser detection

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 blocks HTTP Traffic on Web Browser.

Allow website list (Depends on "Block HTTP Traffic only on Web Browser")
Select this option to enter the website name need to be allowed.

Block Microsoft EDGE Browser (1 = Enable/0 = Disable)
Select this option to enable/disable blocking Microsoft Edge browser.

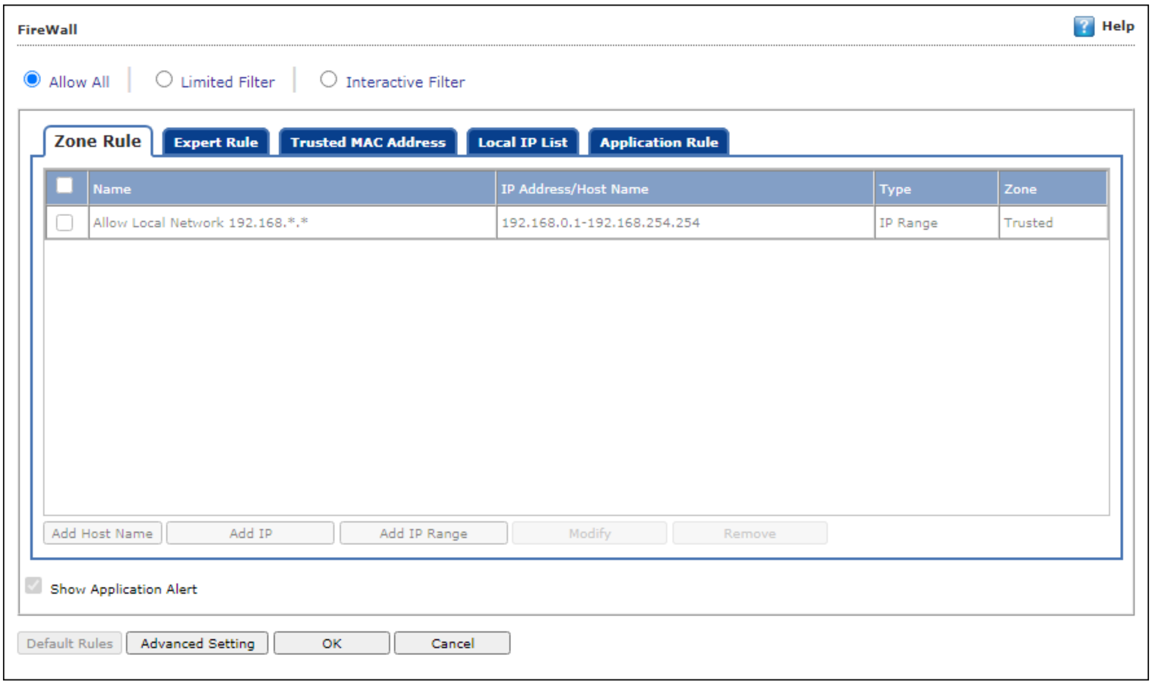
Enable Web Protection using Filter driver (1 = Enable/0 = Disable)
Select this option to enable/disable web protection using filter driver.

Force Disable Web Protection using Filter driver (1 = Enable/0 = Disable)
Select this option to force enable/disable web protection using filter driver.

WFP Exclude IP List (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

□	Name	IP Address/Host Name	Type	Zone
□	Allow Local Network 192.168.*.*	192.168.0.1-192.168.254.254	IP Range	Trusted

☑ Show Application Alert

The Firewall feature of eScan protects your data when you:

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

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

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

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

Following tabs are available:
Zone Rule
Expert Rule
Trusted MAC Address
Local IP List
Application Rule

Zone Rule

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

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

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

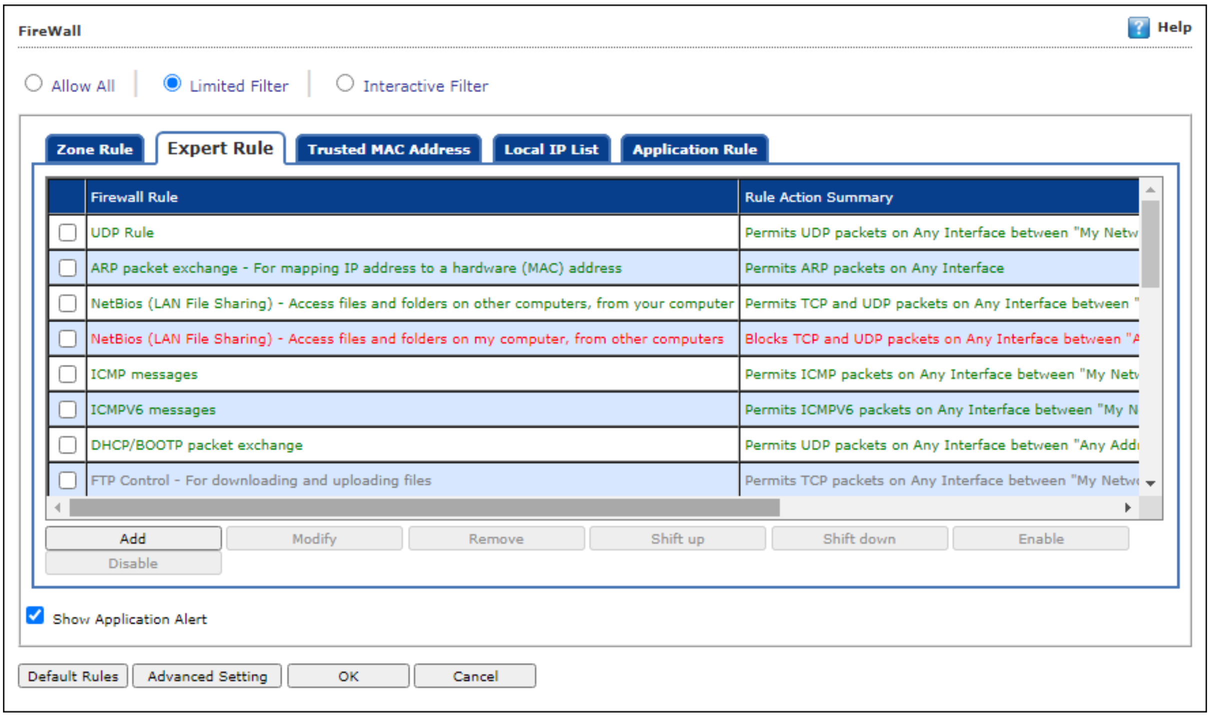
Add IP Range – This option lets you add an IP range to be added in the zone rule. After clicking **Add IP Range**, add the IP Range (i.e. a range of IP that the zone rules should be applied), select the zone (Trusted/Blocked) and enter a name for the zone rule. Click **OK** to create the zone rule.

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

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

Expert Rule

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



FireWall

○ Allow All | ● Limited Filter | ○ Interactive Filter

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

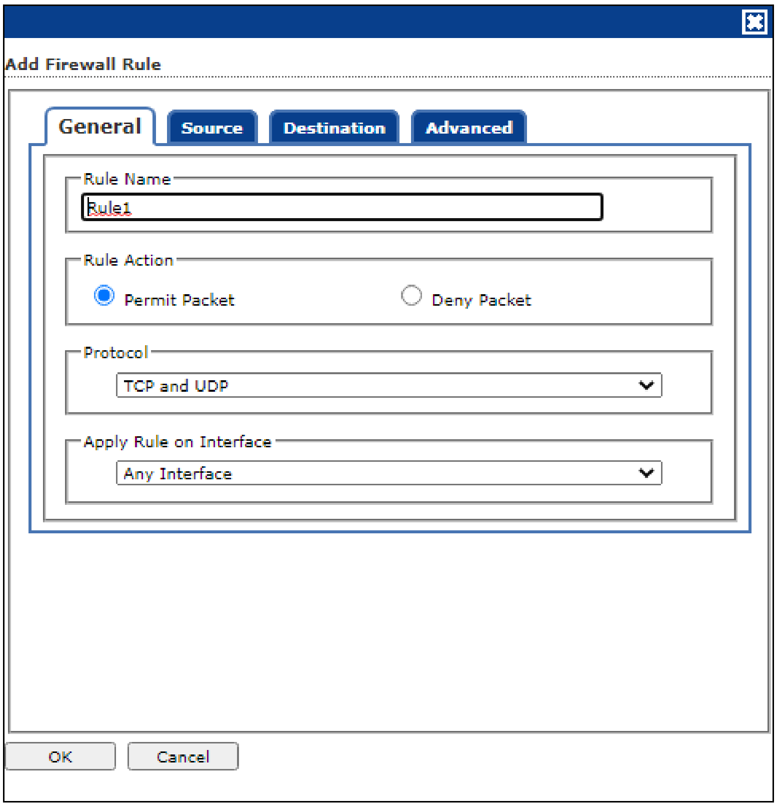
	Firewall Rule	Rule Action Summary
□	UDP Rule	Permits UDP packets on Any Interface between "My Netw
□	ARP packet exchange - For mapping IP address to a hardware (MAC) address	Permits ARP packets on Any Interface
□	NetBios (LAN File Sharing) - Access files and folders on other computers, from your computer	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 Addı
□	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

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

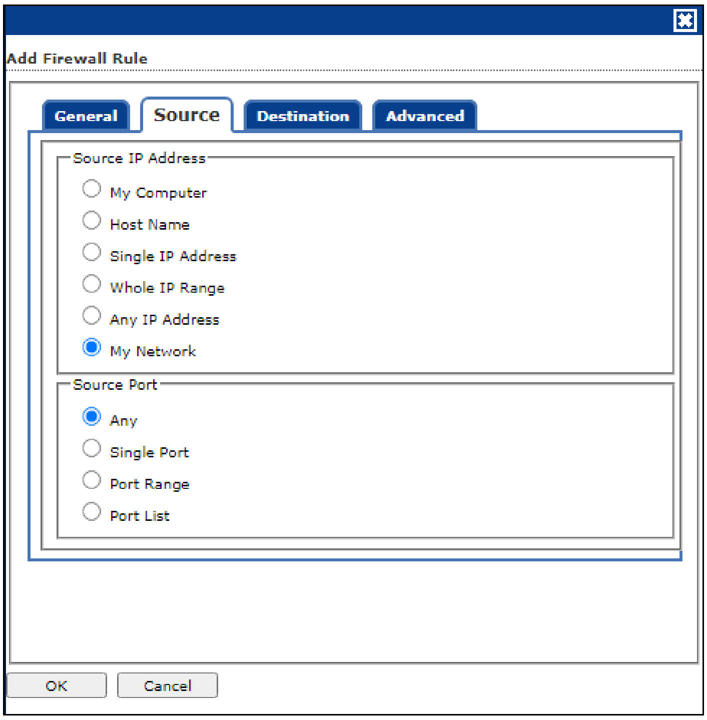
General tab

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 which 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 traffic originating from your computer.
- **Host Name –** The rule will be applied for the traffic originating from the computer as per the host name specified.
- **Single IP Address –** The rule will be applied for the 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 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 traffic originating from ANY IP address.
- **My Network –** The rule will be applied for the traffic originates to your network.

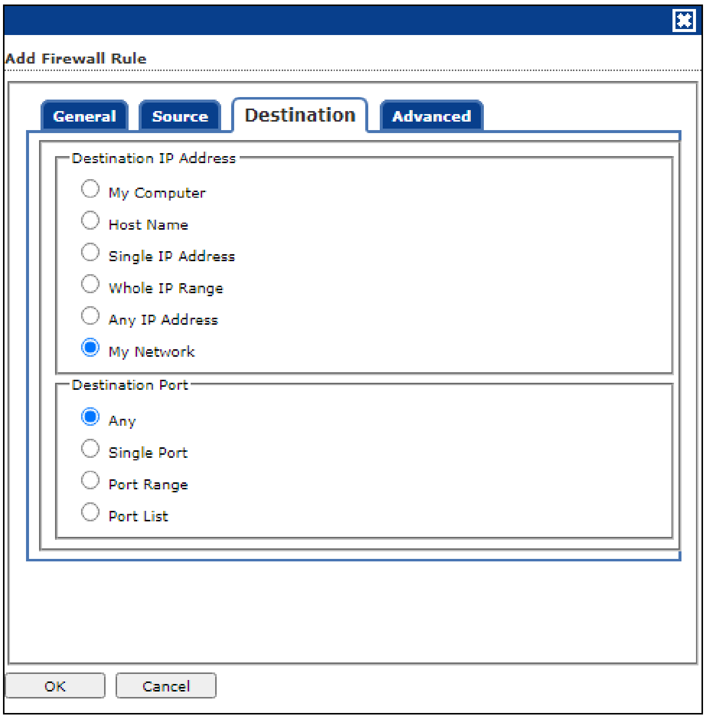
Source Port –

- **Any –** When this option is selected, the rule gets applied for traffic originating from any port.
- **Single Port –** When this option is selected, the rule gets applied for the 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 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 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 destination network traffic.



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 traffic to your computer.
- **Host Name –** The rule will be applied for the traffic to the computer as per the host name specified.
- **Single IP Address –** The rule will be applied for the 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 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 traffic to ANY IP Addresses.
- **My Network –** The rule will be applied for the traffic to your network.

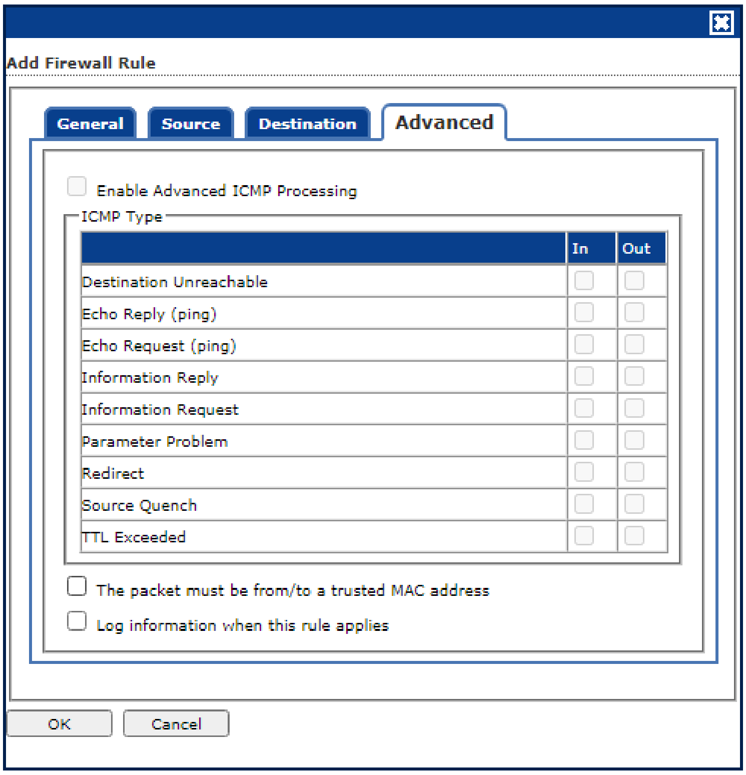
Destination Port –

- **Any –** After selecting this option, the rule will be applied for the traffic to any port.
- **Single Port –** After selecting this option, the rule will be applied for the 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 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 traffic to the ports as per specified in the list.

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

Advanced tab

This tab contains advance setting for Expert Rule.



Add Firewall Rule

□ Enable Advanced ICMP Processing

ICMP Type

	In	Out
Destination Unreachable	□	□
Echo Reply (ping)	□	□
Echo Request (ping)	□	□
Information Reply	□	□
Information Request	□	□
Parameter Problem	□	□
Redirect	□	□
Source Quench	□	□
TTL Exceeded	□	□

□ The packet must be from/to a trusted MAC address

□ Log information when this rule applies

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

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

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

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

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

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

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

Trusted MAC Address

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

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]

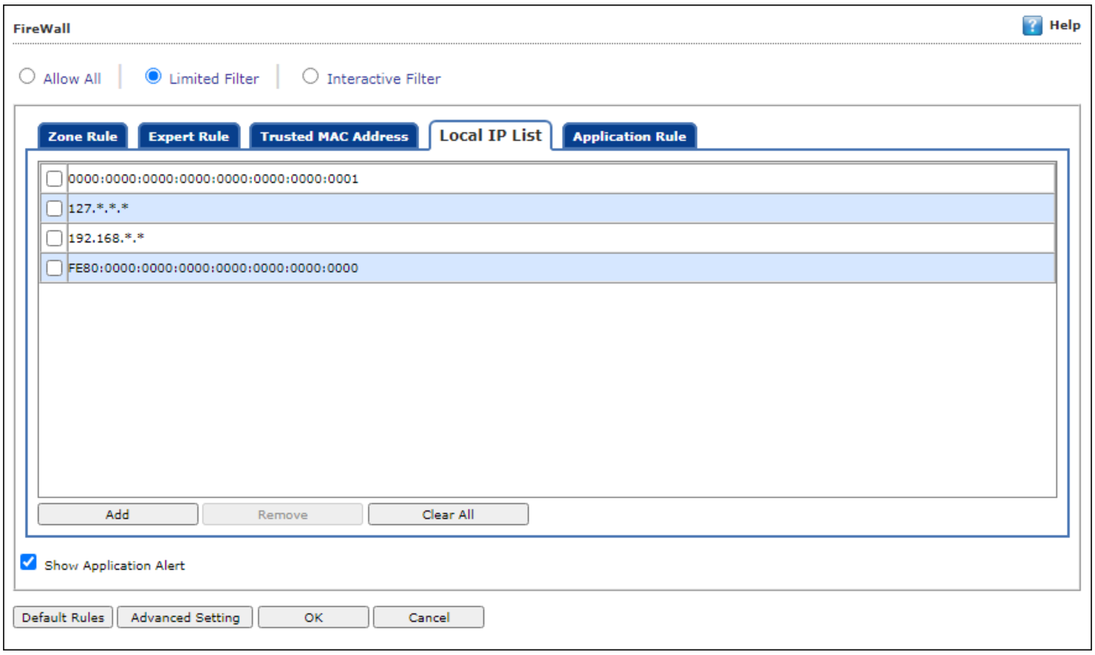
Edit – To modify/change the MAC Address, click **Edit**.

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

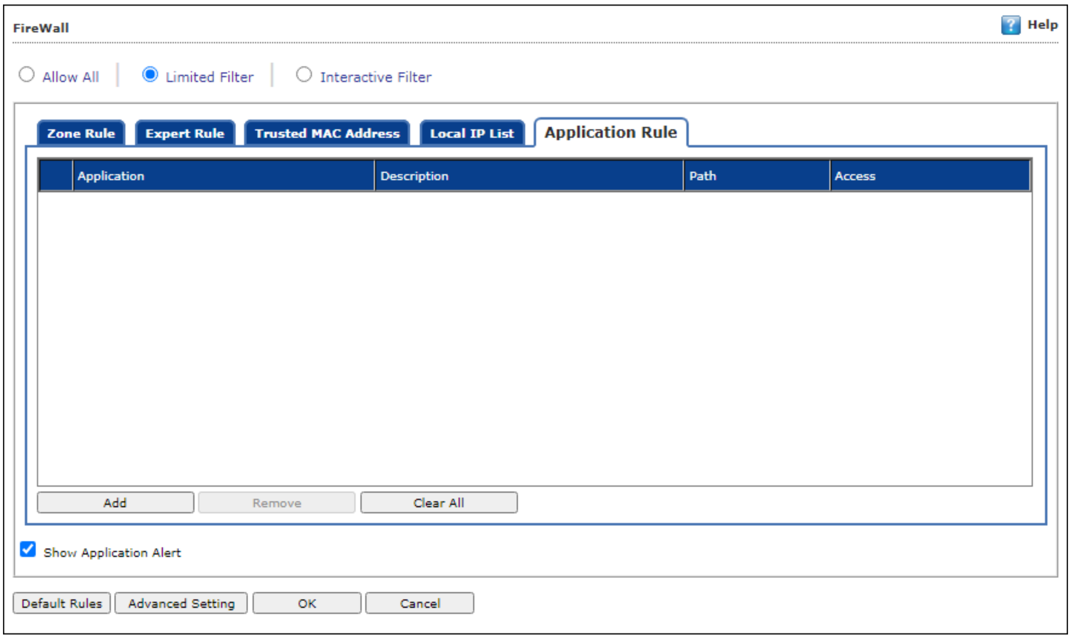
Add – To add a local IP address, click **Add**.

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

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

Application Rule

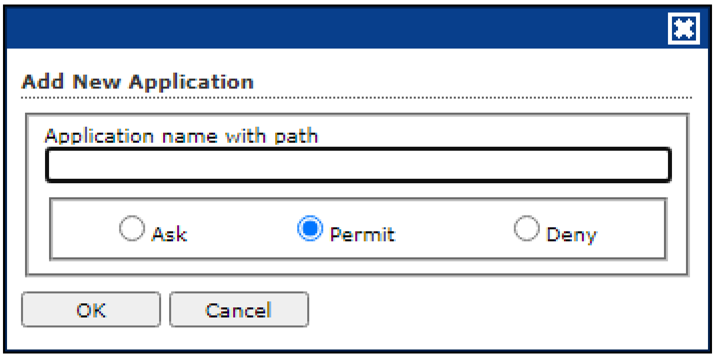
In this section you can define the permissions for different application. The application can be set to Ask, Permit or Deny mode.



Defining permission for an application

To define permission for an application,

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



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

The permission for the application will be defined.

Removing permission of an application

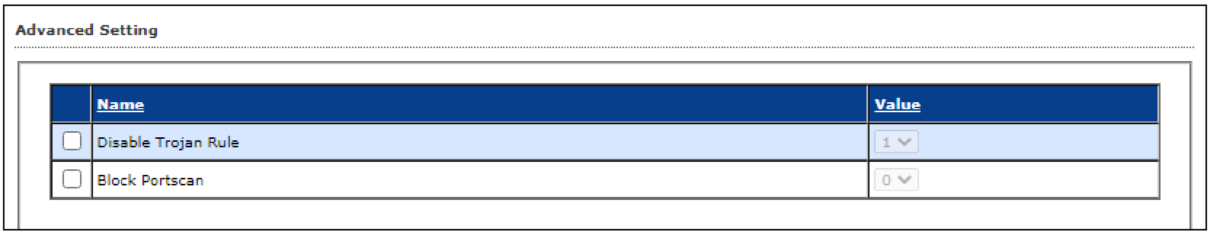
Select an application and then click **Remove**. The application will no longer have the permission.

Clear All – This option will clear/delete all the information stored by the Firewall cache.

Other Options:

- **Show Application Alert** – Selecting this checkbox will display an eScan Firewall Alert displaying the blocking of any application as defined in the Application Rule.

- **Default Rules -** This button will load/reset the rules to the Default settings present during the installation of eScan. This will remove all the settings defined by user.
- **Advanced Settings**: This button allows you to configure the advanced settings such as block port scan and disable Trojan rule.

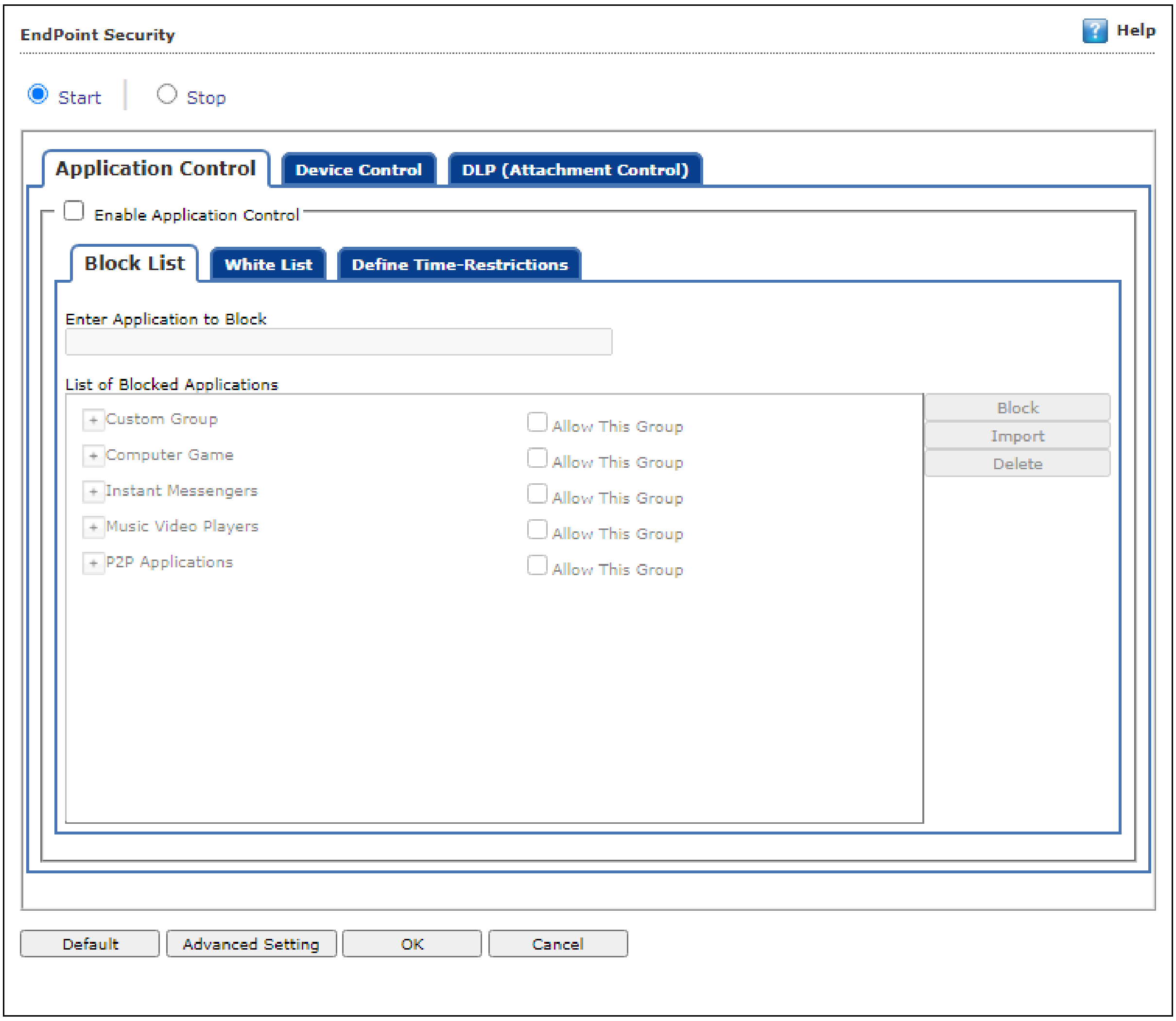


Advanced Setting

	Name	Value
□	Disable Trojan Rule	1
□	Block Portscan	0

Endpoint Security

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



EndPoint Security

● Start | ○ Stop

□ Enable Application Control

Enter Application to Block

List of Blocked Applications

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

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

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

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

Application Control

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

Enable Application Control

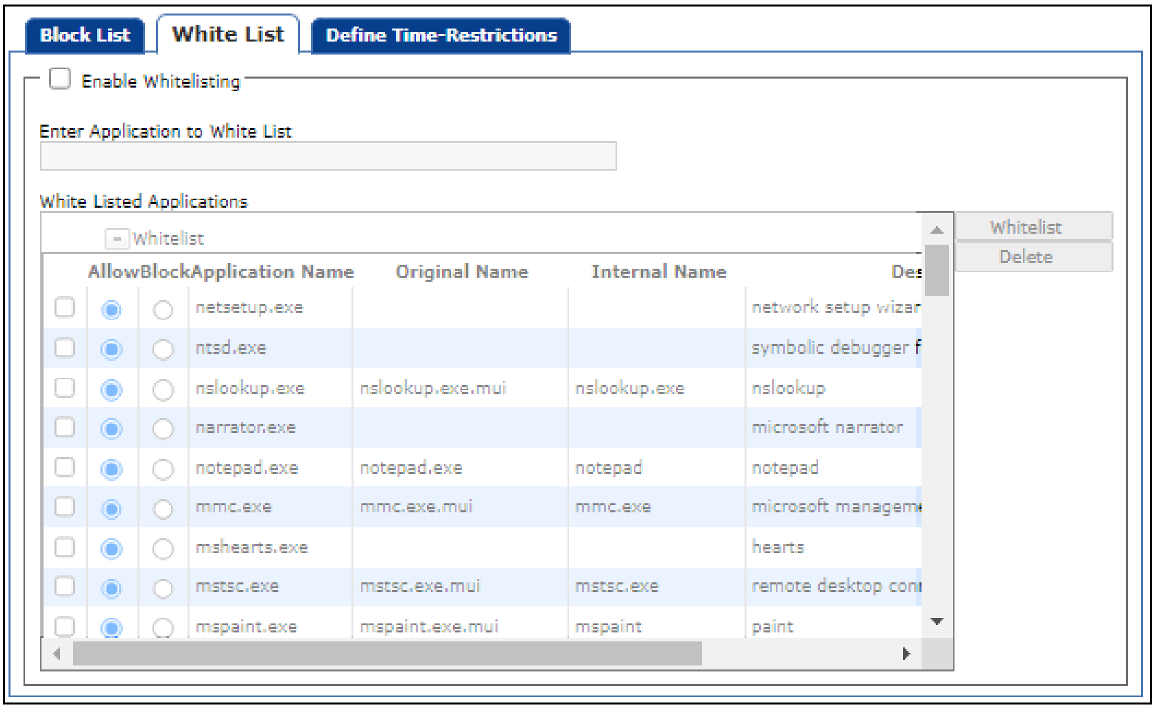
Select this option if you want to enable the Application Control feature of the Endpoint Security module.

Block List

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

List of Blocked Applications

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



□ Enable Whitelisting

Enter Application to White List

White Listed Applications

⊟ Whitelist

	Allow	Block	Application Name	Original Name	Internal Name	Des
□	●	○	netsetup.exe			network setup wizar
□	●	○	ntsd.exe			symbolic debugger f
□	●	○	nslookup.exe	nslookup.exe.mui	nslookup.exe	nslookup
□	●	○	narrator.exe			microsoft narrator
□	●	○	notepad.exe	notepad.exe	notepad	notepad
□	●	○	mmc.exe	mmc.exe.mui	mmc.exe	microsoft managem
□	●	○	mshearts.exe			hearts
□	●	○	mstsc.exe	mstsc.exe.mui	mstsc.exe	remote desktop con
□	●	○	mspaint.exe	mspaint.exe.mui	mspaint	paint

White List

Enable White Listing

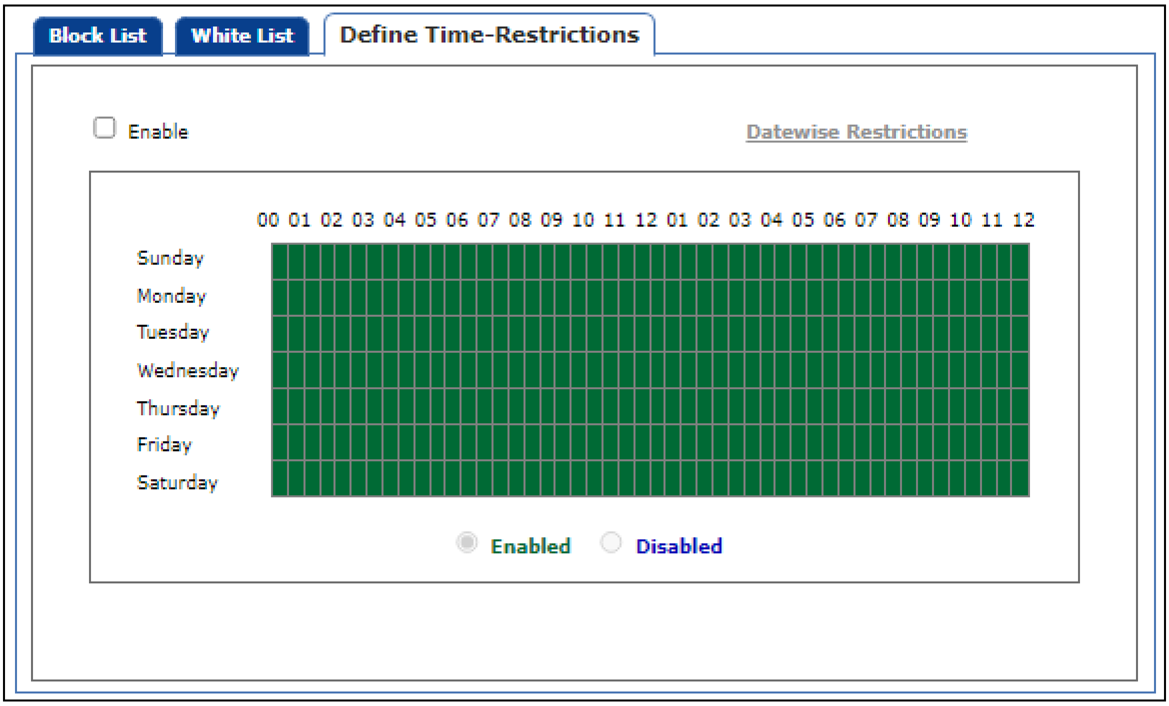
Select this checkbox to enable the whitelisting feature of the Endpoint Security module.

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 categories, select the **Block** option.



□ Enable

Datewise Restrictions

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

● Enabled ○ Disabled

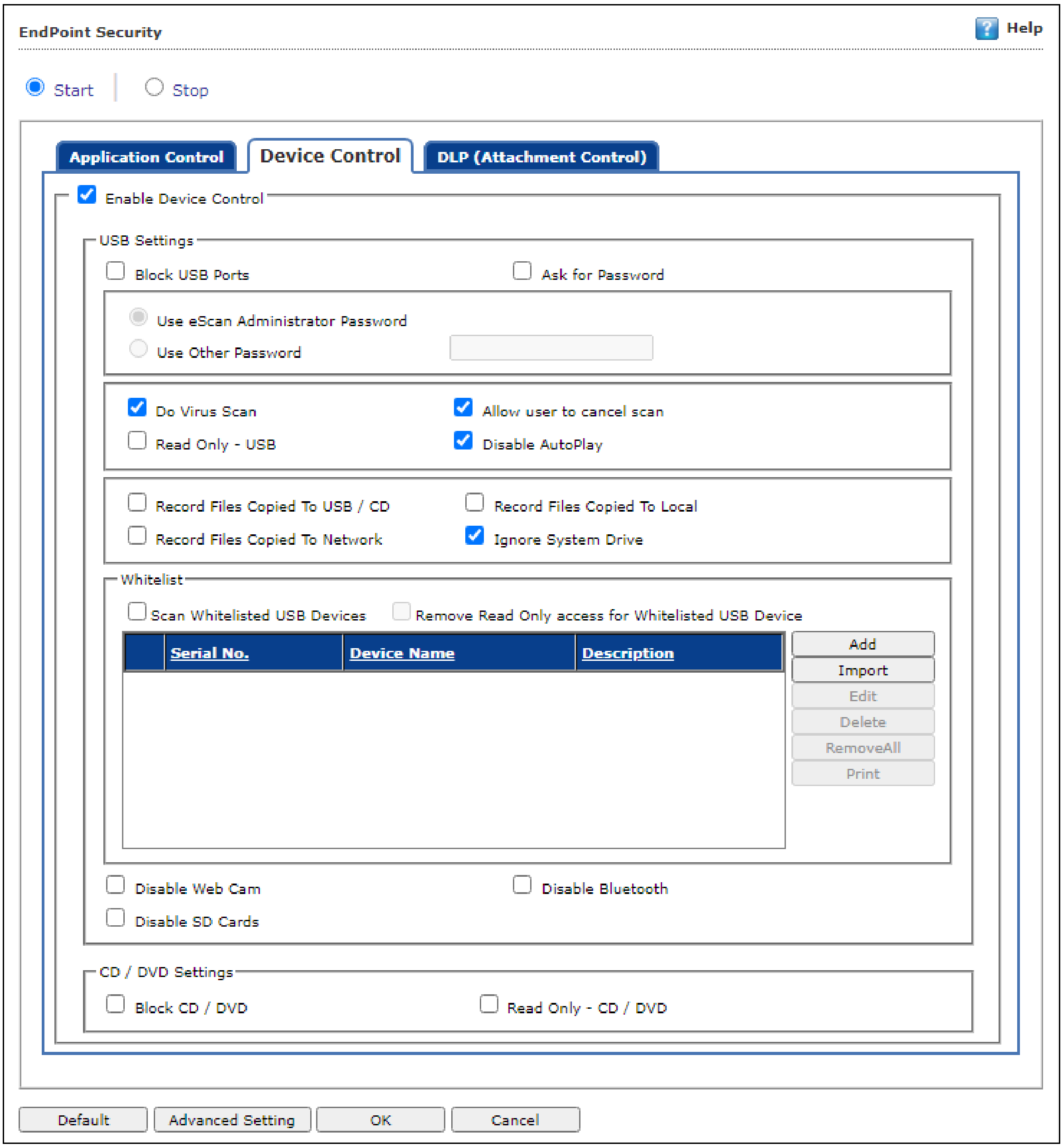
Define Time Restrictions
This feature lets you define time restriction when you want to allow or block access to the applications based on specific days and between pre-defined hours during a day.
For example, the administrator can block computer games, instant messengers, for the whole day but allow during lunch hours without violating the Application Control Policies.

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

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

Device Control

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



EndPoint Security — Help

● Start | ○ Stop

Application Control | Device Control | DLP (Attachment Control)

☑ Enable Device Control

USB Settings

☐ Block USB Ports ☐ Ask for Password

○ Use eScan Administrator Password
○ Use Other Password

☑ Do Virus Scan ☑ Allow user to cancel scan
☐ Read Only - USB ☑ Disable AutoPlay

☐ Record Files Copied To USB / CD ☐ Record Files Copied To Local
☐ Record Files Copied To Network ☑ Ignore System Drive

Whitelist

☐ Scan Whitelisted USB Devices ☐ Remove Read Only access for Whitelisted USB Device

	Serial No.	Device Name	Description

☐ Disable Web Cam ☐ Disable Bluetooth
☐ Disable SD Cards

CD / DVD Settings

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

You can configure the following settings:

Enable Device Control [Default]
Select this option if you want to monitor all the USB storages devices connected to your endpoint. This will enable all the options on this tab.

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

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

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

Record Files Copied To USB/CD
Select this option if you want eScan to create a record of the files copied from the system to USB drive.

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

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

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

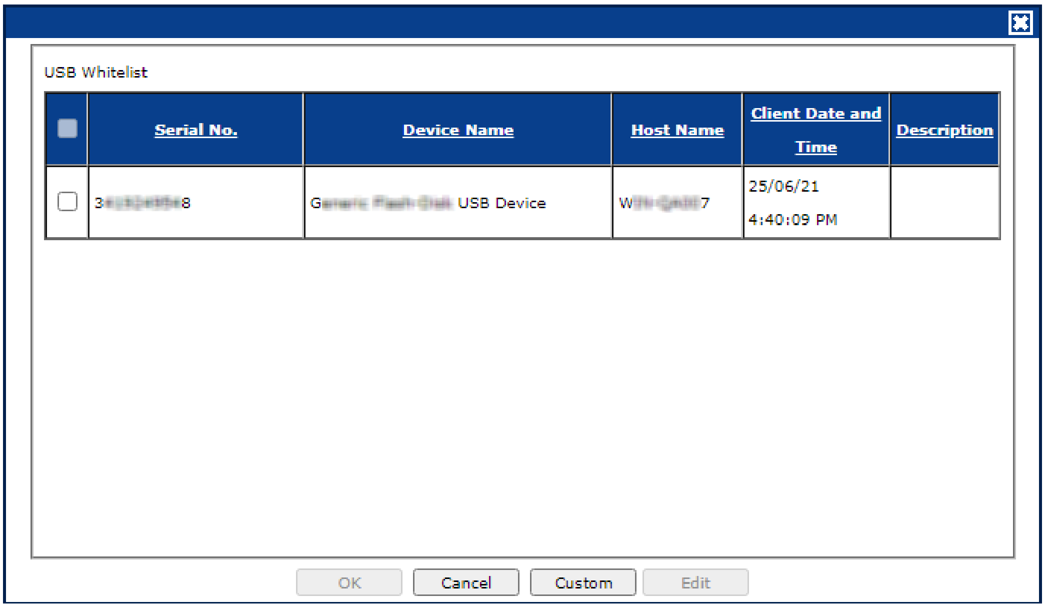
Whitelist
eScan provides a greater level of endpoint security by prompting you for a password whenever you connect a USB drive. To disable password protection for a specific device, you can add it along with its serial number to the whitelist. The next time you connect the device it will not ask for a password but will directly display the files or folders stored on the device. This section displays the serial

number and device name of each of the whitelisted devices in a list. You can add devices to this list by clicking **Add**. The Whitelist section displays the following button.

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

Remove Read Only access for Whitelisted USB Device
Select this option to remove the read-only access for the whitelisted USB Device.

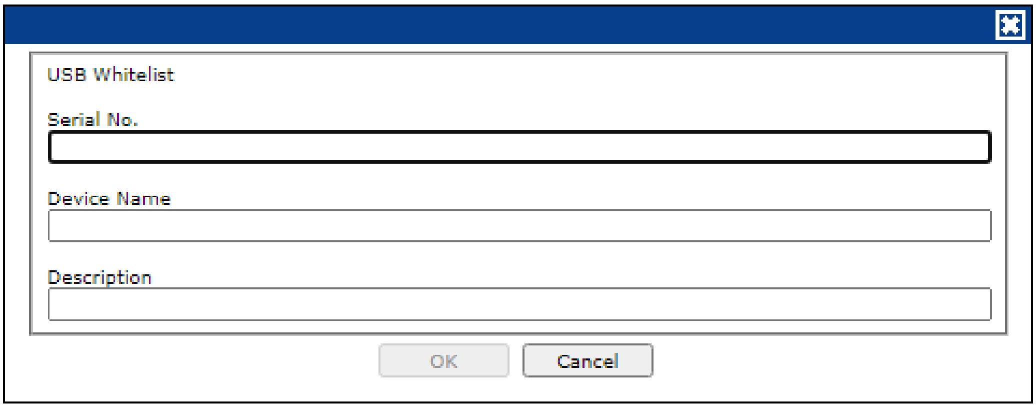
Add
Click **Add** to whitelist USB devices.
USB Whitelist window appears.



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



USB Whitelist

Serial No.

Device Name

Description

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

Import
To whitelist USB devices from a CSV file, click **Import**.
Click **Choose File** to import the file with the list.
The list should be in following format:
Serial No 1, Device Name 1, Device Description 1(Optional)
Serial No 2, Device Name 2
Eg: SDFSD677GFQW8N6CN8CBN7CXVB, USB Drive 2.5, Whitelist by
xyzDFRGHHRS54456HGDF347OMCNAK, Flash Drive 2.2

Disable Web Cam: Select this option to disable Webcams.

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

Disable Bluetooth: Select this option to disable Bluetooth.

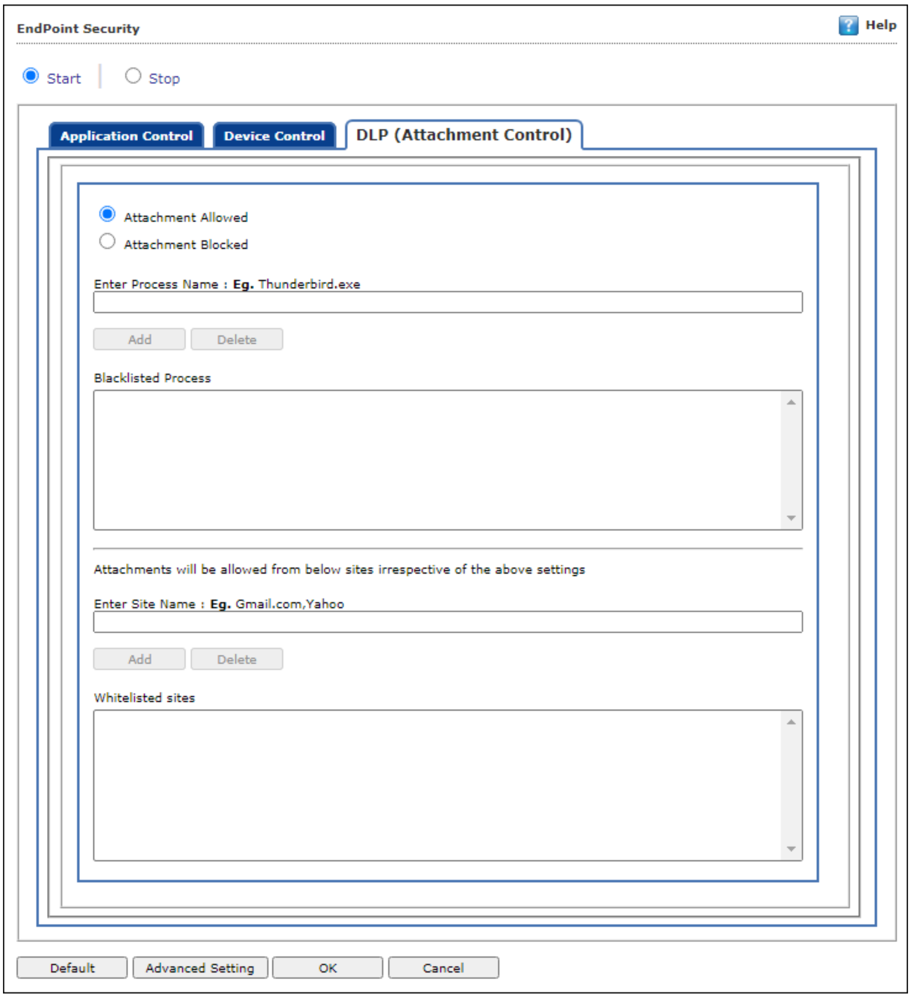
CD/DVD Settings

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.

DLP (Attachment Control)

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



EndPoint Security

● Start ○ Stop

Application Control | Device Control | DLP (Attachment Control)

● Attachment Allowed

○ Attachment Blocked

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

Add | Delete

Blacklisted Process

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

Enter Site Name : **Eg.** Gmail.com,Yahoo

Add | Delete

Whitelisted sites

Attachment Allowed [Default]

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

Attachment Blocked

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

Configure Extension/Group based Whitelisting

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

Enter Process Name

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

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.

Enter Site Name

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

Whitelisted Sites

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

Attachment / Email report

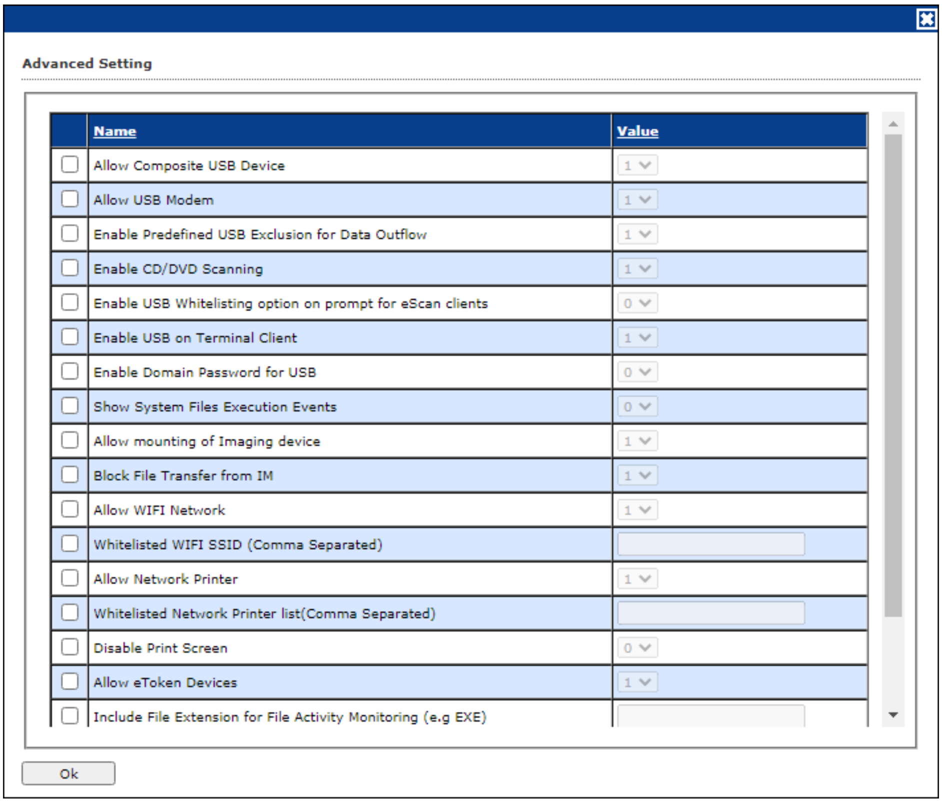
Report for Attachment Allowed [Default]

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.

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

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

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

Show System Files Execution Events
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.

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.

Disable Print Screen
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).

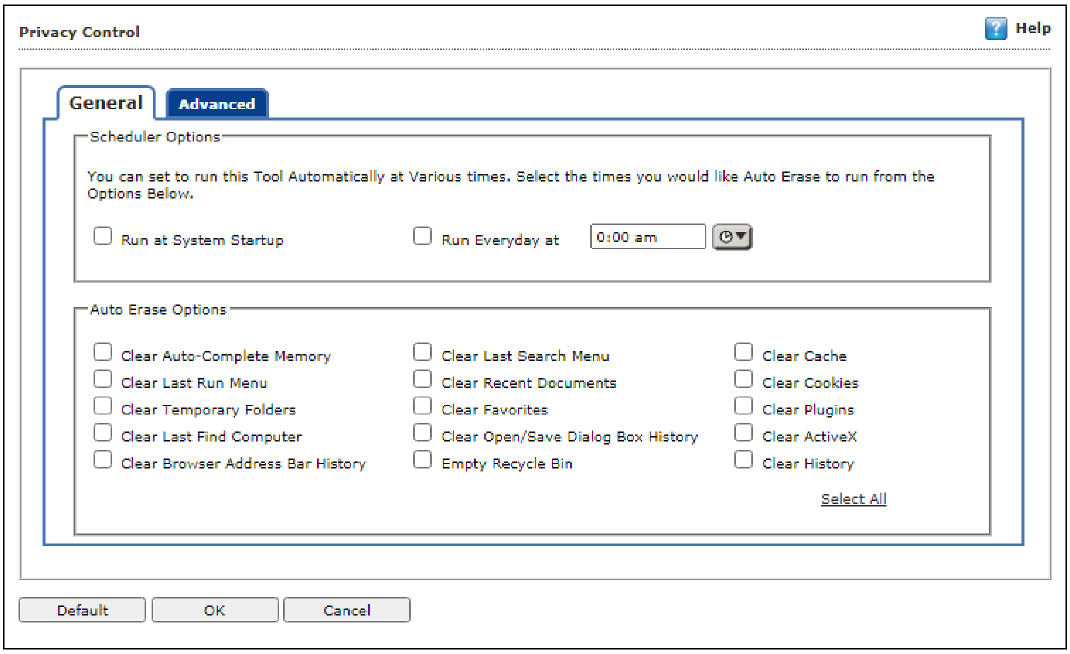
Auto Whitelist BitLocker encrypted USB Devices
Select this option to allow/block auto whitelist BitLocker encrypted USB devices.

Ask Password for whitelisted Devices only
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 sites and web pages you have accessed while browsing. This page provides you with options for configuring the module.



Privacy Control

Help

General | Advanced

Scheduler Options

You can set to run this Tool Automatically at Various times. Select the times you would like Auto Erase to run from the Options Below.

□ Run at System Startup □ Run Everyday at 0:00 am

Auto Erase Options

□ Clear Auto-Complete Memory
□ Clear Last Run Menu
□ Clear Temporary Folders
□ Clear Last Find Computer
□ Clear Browser Address Bar History
□ Clear Last Search Menu
□ Clear Recent Documents
□ Clear Favorites
□ Clear Open/Save Dialog Box History
□ Empty Recycle Bin
□ Clear Cache
□ Clear Cookies
□ Clear Plugins
□ Clear ActiveX
□ Clear History

Select All

Default | OK | Cancel

It consists following tabs:

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

General tab

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

Scheduler Options

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

Run at System Startup

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

Run Every day at

It auto-executes the Privacy Control module at specified times and performs the desired auto erase functions. You can specify the time within the hours and minutes boxes.

Auto Erase Options

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

Clear Auto Complete Memory

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

Clear Last Run Menu

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

Clear Temporary Folders

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

Clear Last Find Computer

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

Clear Browser Address Bar History

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

Clear Last Search Menu

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

Clear Recent Documents

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

Clear Favorites

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

Clear Open/Save Dialog box History

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

Empty Recycle Bin

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

Clear Cache

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

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

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

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

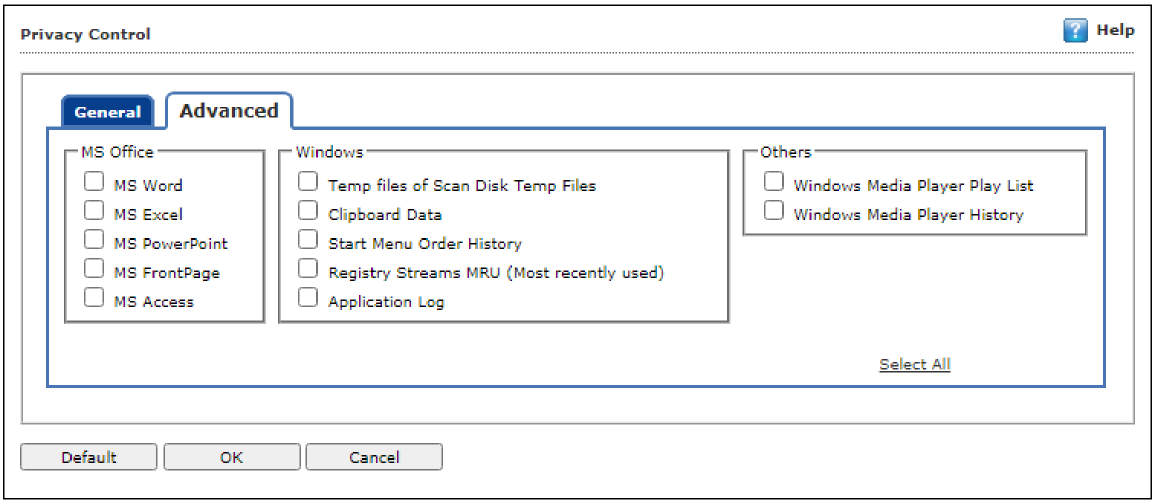
Clear History
When you select this checkbox, Privacy Control clears the history of all the websites that you have visited.

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

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

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

Windows
The respective unwanted files like temp files will be cleared.

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

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

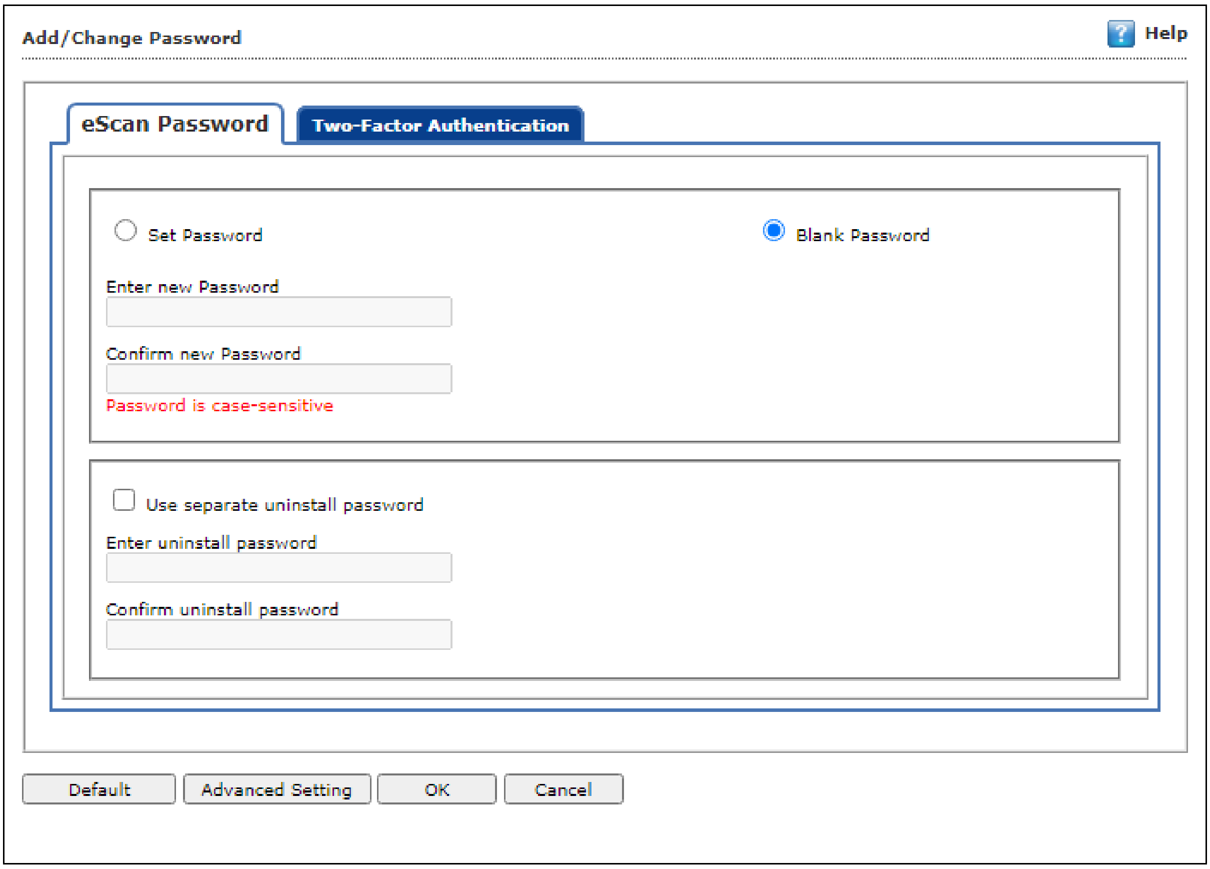
NOTE	Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.

Administrator Password

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

eScan Password

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



○ Set Password

● Blank Password

Enter new Password

Confirm new Password

Password is case-sensitive

□ Use separate uninstall password

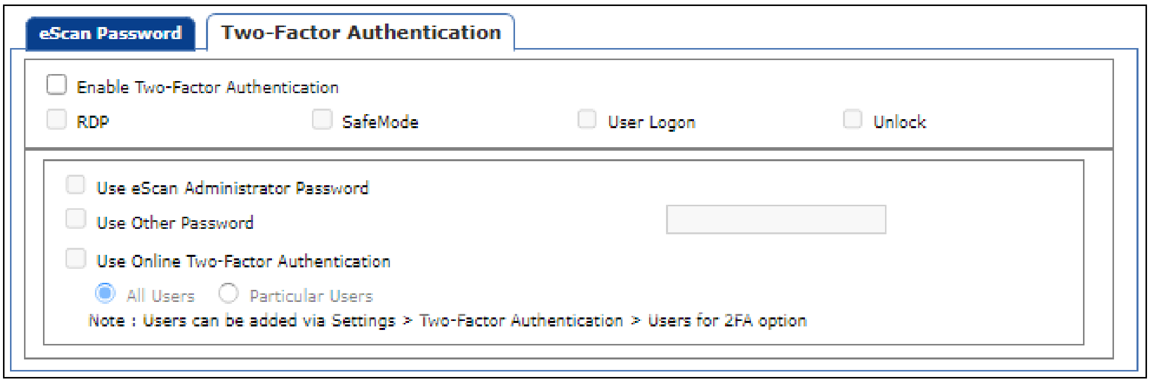
Enter uninstall password

Confirm uninstall password

There is also an option to set a uninstall password. An uninstallation password prevents personnel from uninstalling eScan client from their endpoint. Upon selecting **Uninstall** option, eScan asks them for uninstall password. To set an uninstall password, select checkbox **Use separate uninstall password**.

Two-Factor Authentication

Your default system authentication (login/password) is Single-Factor Authentication which is considered insecure as it may put your organization's data at high risk of compromise. The Two-Factor Authentication, also more commonly known as 2FA, adds an extra layer of protection to your basic system logon. The 2FA feature requires personnel to enter an additional passcode after entering the system login password. So, even if an unauthorized person knows your system credentials, the 2FA feature secures a system against unauthorized logons.



□ Enable Two-Factor Authentication

□ RDP □ SafeMode □ User Logon □ Unlock

□ Use eScan Administrator Password

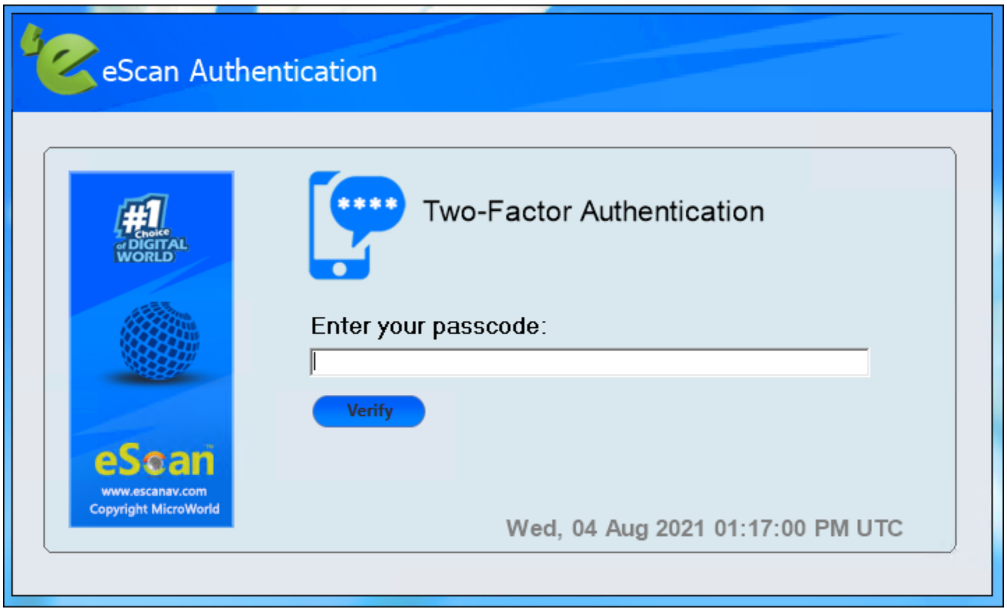
□ Use Other Password

□ Use Online Two-Factor Authentication

● All Users ○ Particular Users

Note : Users can be added via Settings > Two-Factor Authentication > Users for 2FA option

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



Enter your passcode:

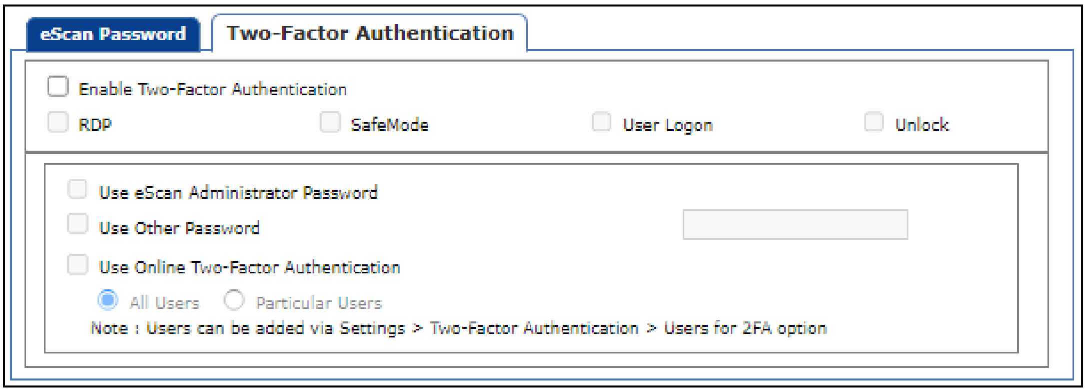
Wed, 04 Aug 2021 01:17:00 PM UTC

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

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

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

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



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 following all login scenarios:

RDP

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

Safe Mode

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

User Logon

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

Unlock

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

Password Types

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.

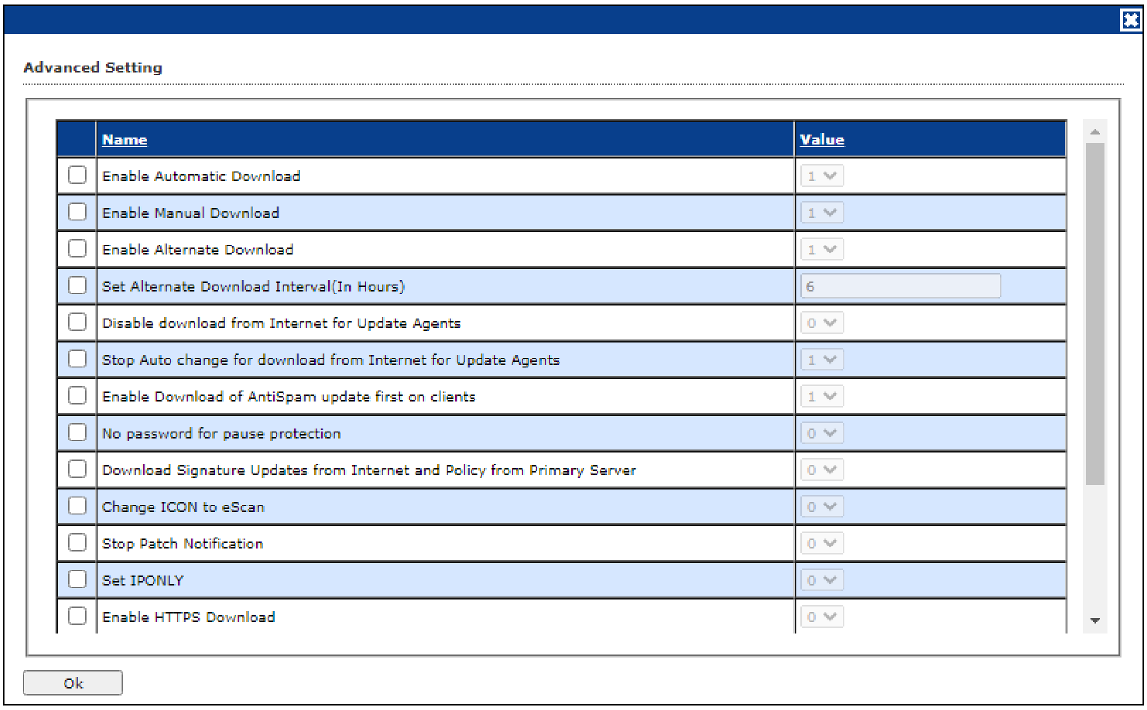
To use this feature, follow the steps given below:

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.

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

Advanced Setting

Clicking **Advanced Setting** displays Advance setting.



Advanced Setting

	Name	Value
□	Enable Automatic Download	1
□	Enable Manual Download	1
□	Enable Alternate Download	1
□	Set Alternate Download Interval(In Hours)	6
□	Disable download from Internet for Update Agents	0
□	Stop Auto change for download from Internet for Update Agents	1
□	Enable Download of AntiSpam update first on clients	1
□	No password for pause protection	0
□	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.

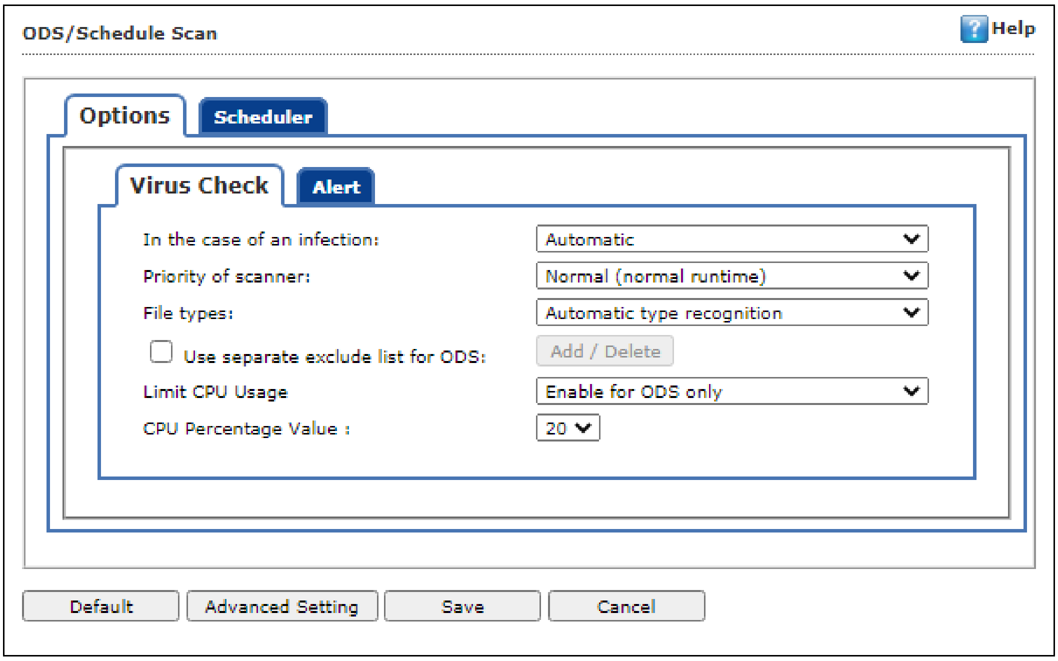
No password for pause protection
Selecting this option lets you pause the eScan protection without entering password.

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.

It consists following tabs:

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



ODS/Schedule Scan

In the case of an infection: Automatic

Priority of scanner: Normal (normal runtime)

File types: Automatic type recognition

□ Use separate exclude list for ODS: Add / Delete

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,

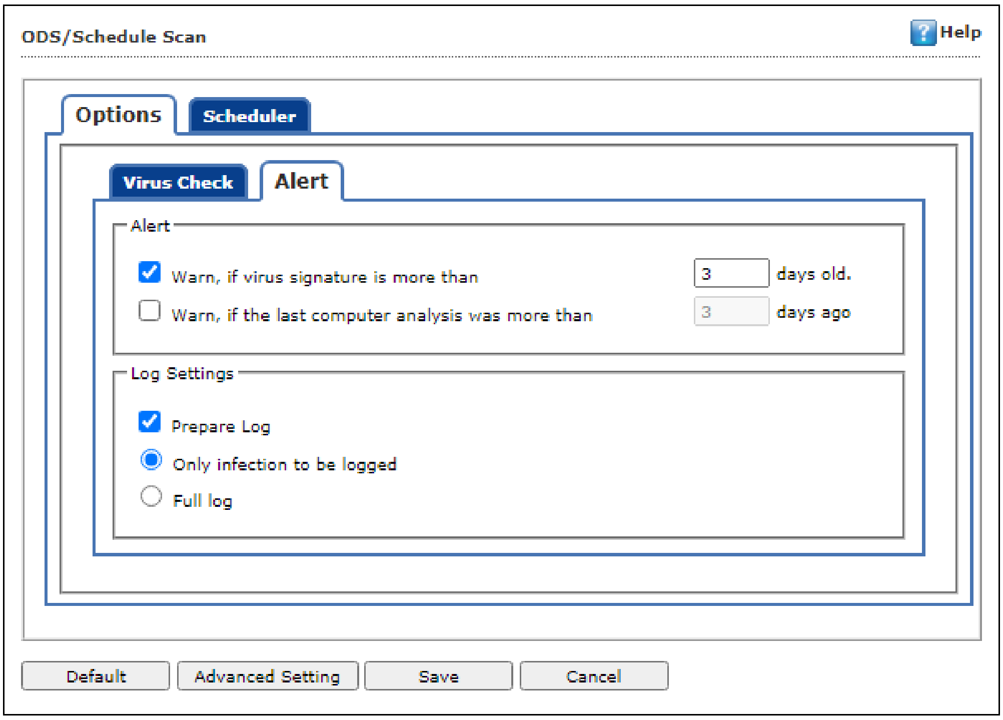
1. Specify the following field details.
   - **In the case of an infection**: Select an appropriate option from the drop-down list. For example, Log only, Delete infected file, and [Default] Automatic.
   - **Priority of scanner**: Select an appropriate option from the drop-down list. For example,
     - ○ High (short runtime)
     - ○ Normal (normal runtime) [Default]
     - ○ Low (long runtime)
   - **File types**: Select an appropriate option from the drop-down list. For example, \[Default\] Automatic type recognition and only program files.

- **Use separate exclude list for ODS**: Select this option to add a list of file/folders that should be excluded from scan.
- **Limit CPU Usage**: Select an appropriate option from the drop-down list. For example, \[Default\] Enable for ODS only.
- **CPU Percentage Value**: select the preferred value (between 10-80) in percentage of CPU Usage.

2. Click **Save**.

Alert 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

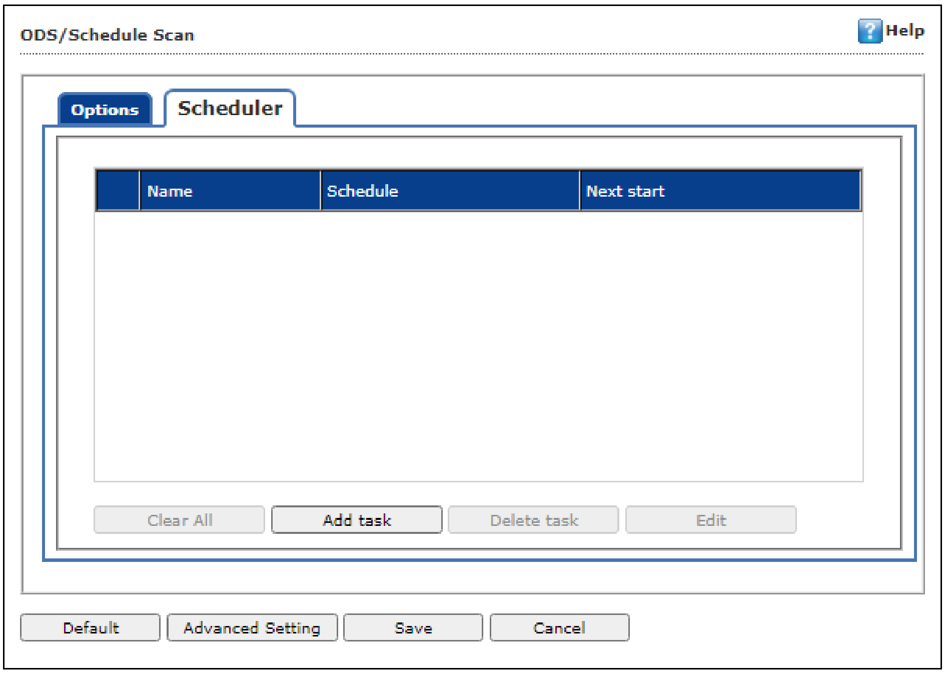
○ Full log

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 provided 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 provided 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**.

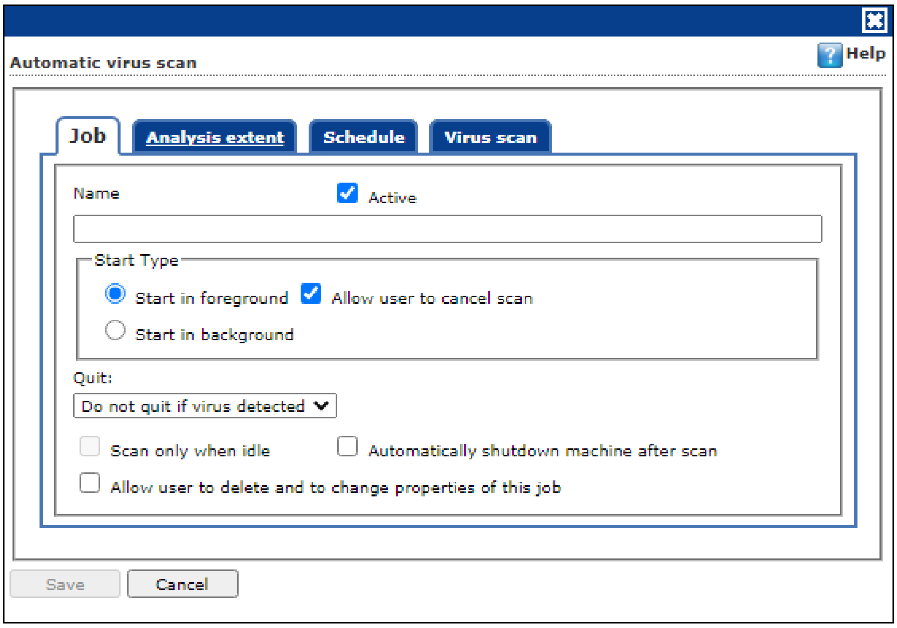
Scheduler

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



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

Add Task



Name ☑ Active

Start Type

● Start in foreground ☑ Allow user to cancel scan

○ Start in background

Quit: Do not quit if virus detected

□ Scan only when idle □ Automatically shutdown machine after scan

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

Automatic Virus Scan lets you do following activities:

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

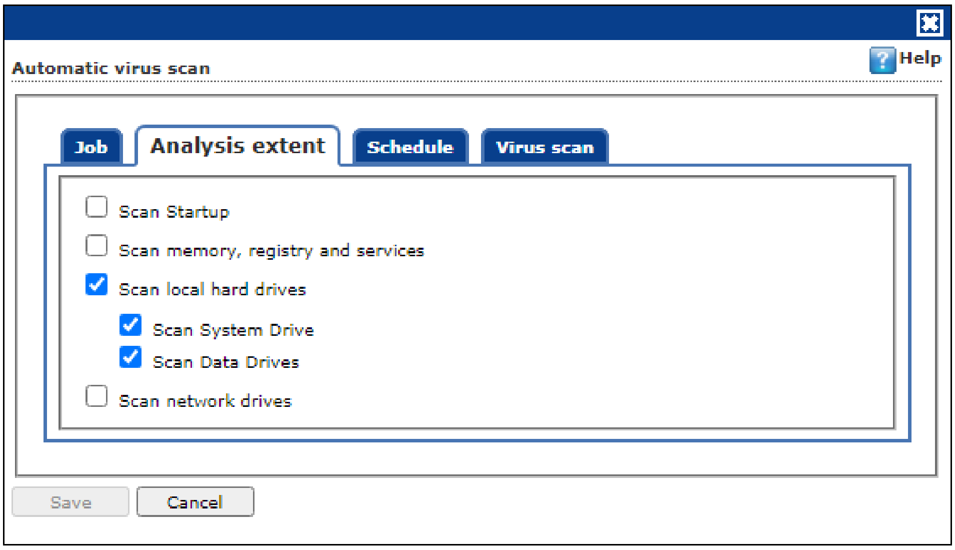
a) Job

It lets you create the job details for virus scanning.

1. Click the **Job** tab.
2. Specify the following field details.
   - **Name**: Enter a name for the task.
   - **Active [Default]**: Select this 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.
   - **Allow user to cancel scan [Default]**: Select this option to allow the user to cancel the scanning process of the USB device.
   - **Quit**: Select an appropriate option from the drop-down list. For example, \[Default\] Do not quit if virus is detected.
   - **Scan only when idle**: Select this checkbox, if you want to scan only in idle mode.
   - **Automatically shutdown machine after scan**: Select this checkbox, if you want to shutdown the system automatically after scan completed.
   - **Allow user to delete and to change properties of this job**: Select this checkbox, to allow user to configure the properties of Job.
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

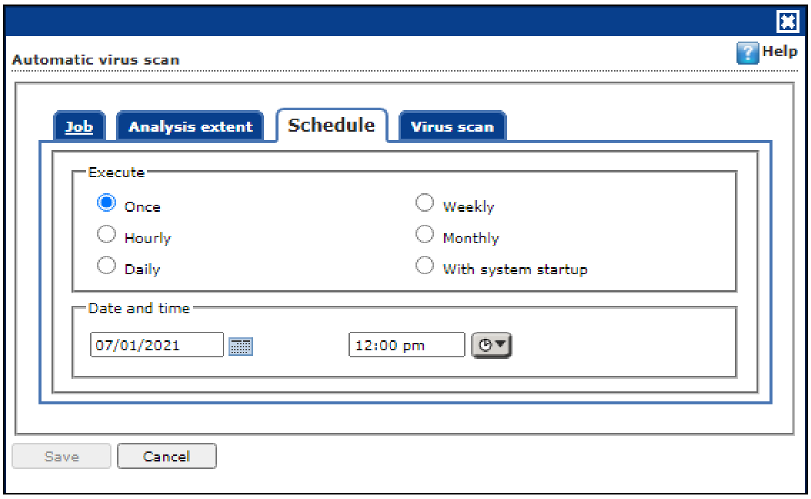
□ Scan network drives

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 **Scan local hard drives [Default]** 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) Schedule

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



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

Date and time: 07/01/2021 12:00 pm

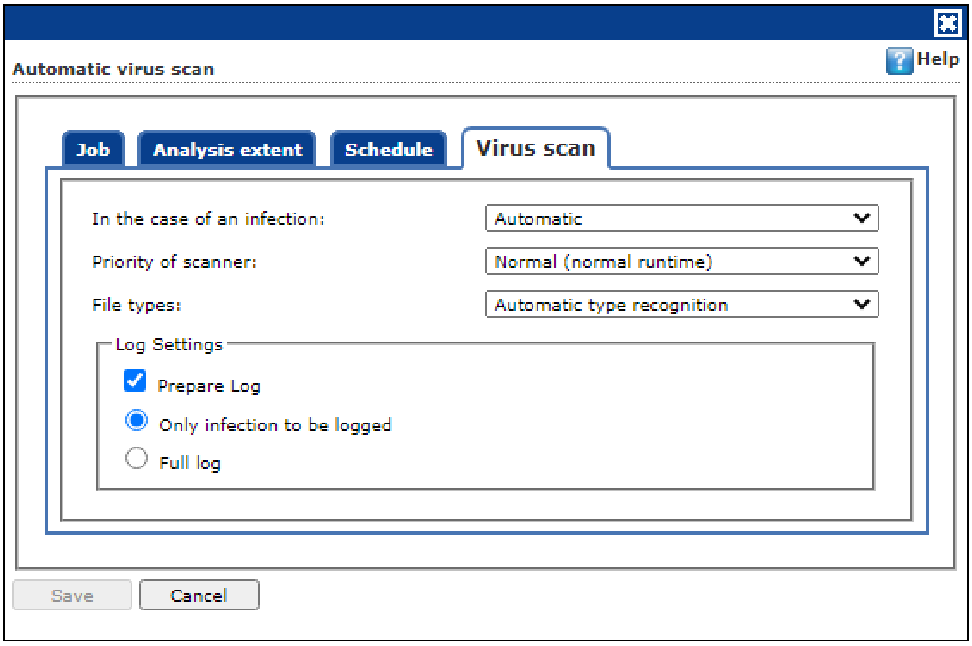
1. Click **Schedule** tab.
2. Under **Execute** section, select an appropriate option. For example, [Default] once, weekly, hourly, and so on.
3. Under **Date and time** section, click the **Calendar** icon.
   The calendar appears.
4. Select an appropriate date from the calendar.

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

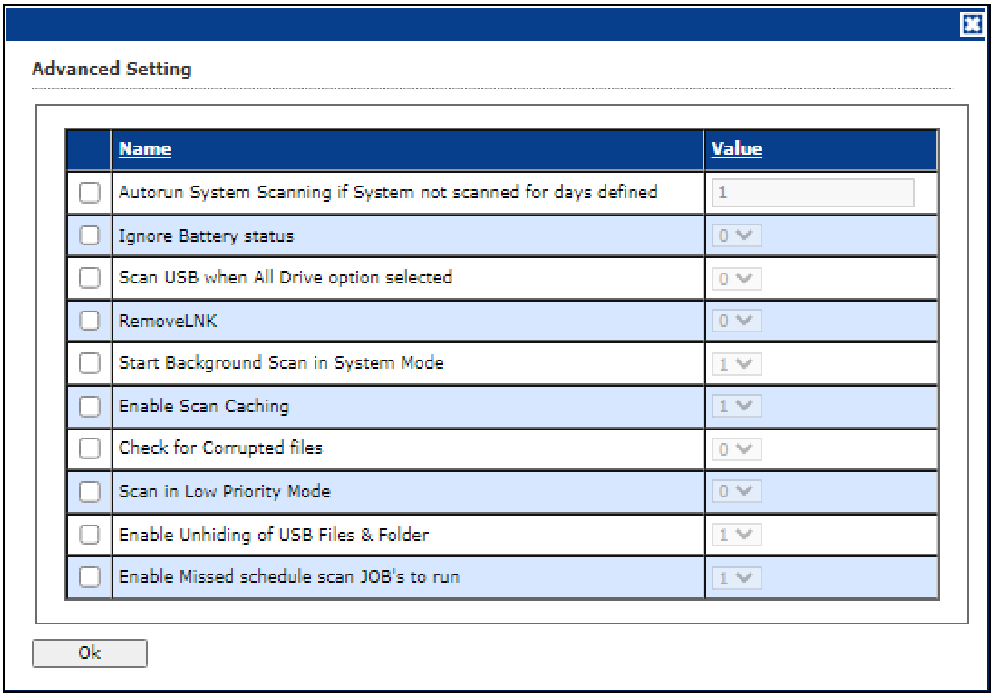
1. Click the **Virus Scan** tab.
2. Specify the following field details:
    - **In the case of an infection**: Select an appropriate option from the drop-down list. For example, Log only, Delete infected file, and [Default] Automatic.
    - **Priority of scanner**: Select an appropriate priority from 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 **Prepare Log [Default]** 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.

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

Advanced Settings



Advanced Setting

	Name	Value
□	Autorun System Scanning if System not scanned for days defined	1
□	Ignore Battery status	0
□	Scan USB when All Drive option selected	0
□	RemoveLNK	0
□	Start Background Scan in System Mode	1
□	Enable Scan Caching	1
□	Check for Corrupted files	0
□	Scan in Low Priority Mode	0
□	Enable Unhiding of USB Files & Folder	1
□	Enable Missed schedule scan JOB's to run	1

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 (1 = Enable/0= Disable)
This option scan computer, even when Laptop is on Battery Mode.

Scan USB when All Drive option selected (1 = Enable/0= Disable)
Select this option to scan USB when all drive option selected.

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

Start Background Scan in System Mode (1 = Enable/0= Disable)
This option starts background scans when systems switch to system mode.

Enable Scan Caching (1 = Enable/0= Disable)
It lets you Enable/Disable automatic caching of files.

Check for Corrupted files (1 = Enable/0= Disable)
It lets you Enable/Disable checking of corrupted files during scan.

Scan in Low Priority Mode (1 = Enable/0= Disable)
It lets you Enable/Disable Scan in Low Priority Mode.

Enable Unhiding of USB Files & Folder (1 = Enable/0= Disable)
It lets you Enable/Disable unhiding of USB files & folder.

Enable Missed schedule scan JOB's to run (1 = Enable/0= Disable)
It lets you Enable/Disable missed schedule scan JOB's to run.

MWL (MicroWorld WinSock Layer)

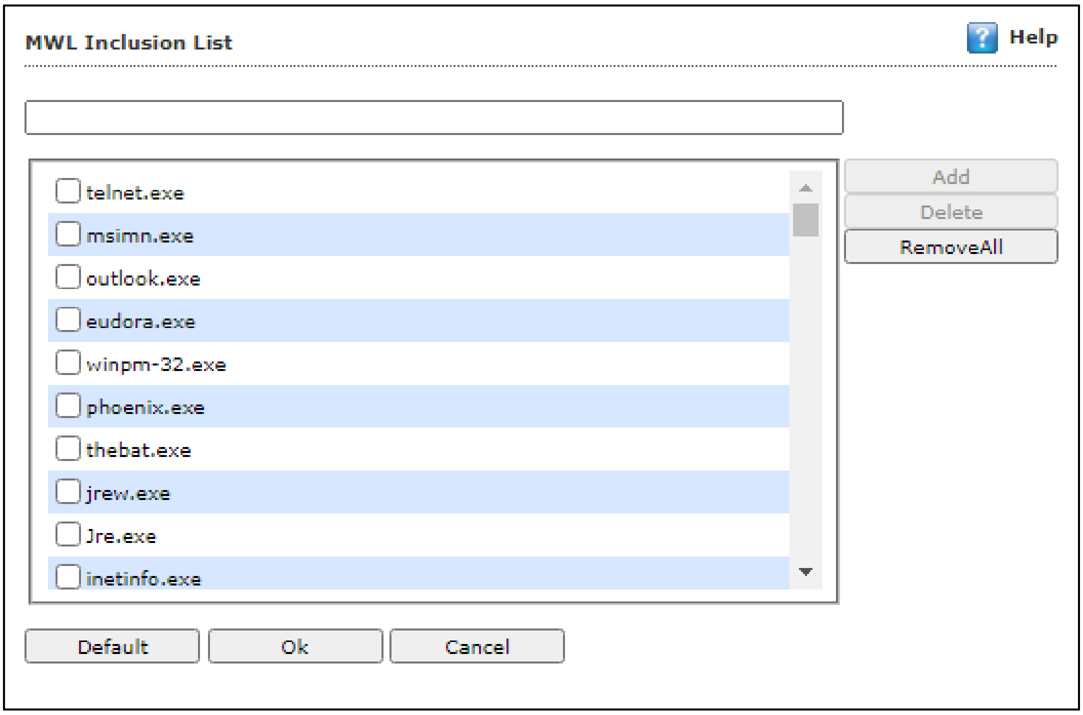
eScan's "MicroWorld-WinSock Layer" (MWL) is a revolutionary concept in scanning Internet traffic on a real-time basis. It has changed the way the world deals with Content Security threats. Unlike the other products and technologies, MWL tackles a threat before it reaches your applications. MWL is technically 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.

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**.

The executable file will be added to the Inclusion List.

Delete files from Inclusion List

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

1. Select executable files, and then click **Delete**.
   A confirmation prompt appears.
2. Click **OK**.

The executable file will be deleted from the Inclusion List.

Remove all files from Inclusion List

To remove all executable files from the Inclusion List,

1. Click **Remove All**.
   A confirmation prompt appears.
2. Click **OK**.

All executable files will be removed from the Inclusion List.

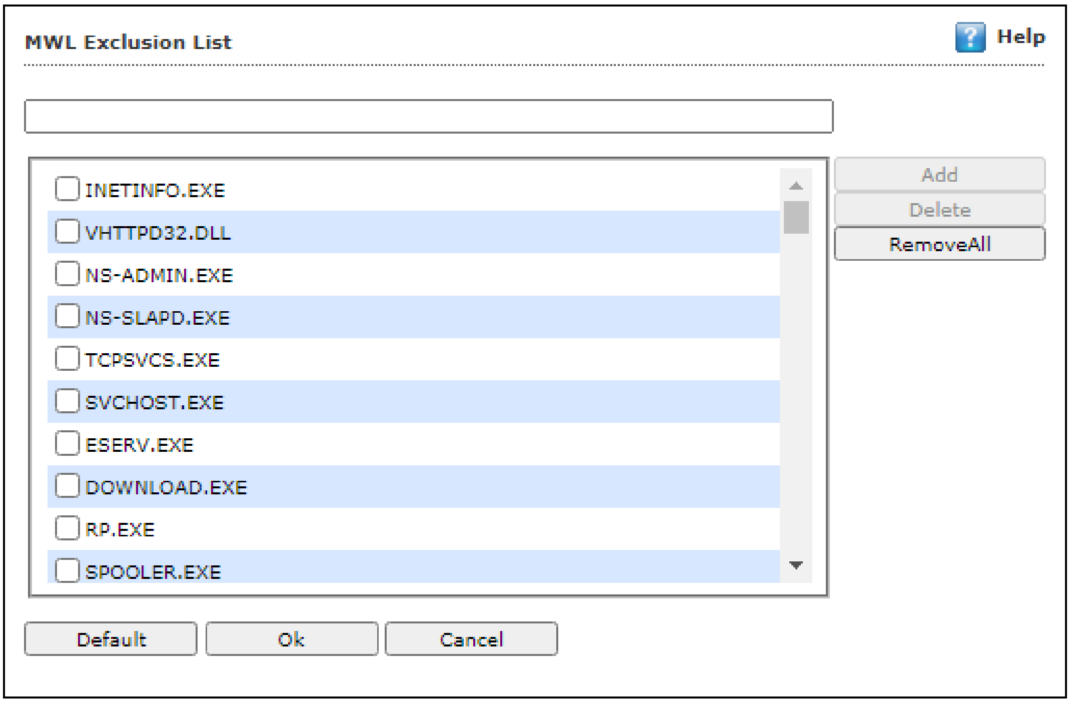
! **NOTE**	Click **Default** to apply default settings, done during eScan installation. It loads and resets the values to the default settings.

MWL Exclusion List

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

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

Help

□ 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**.

The executable file will be added to the Exclusion List.

Deleting files from Exclusion List

To delete executable files from the Exclusion List,

1. Select the appropriate file checkbox, and then click **Delete**.
   A confirmation prompt appears.
2. Click **OK**.

The executable file gets deleted from the Exclusion List.

Removing all files from Exclusion List

To remove all executable files from the Exclusion List,

1. Click **Remove All**.
   A confirmation prompt appears.

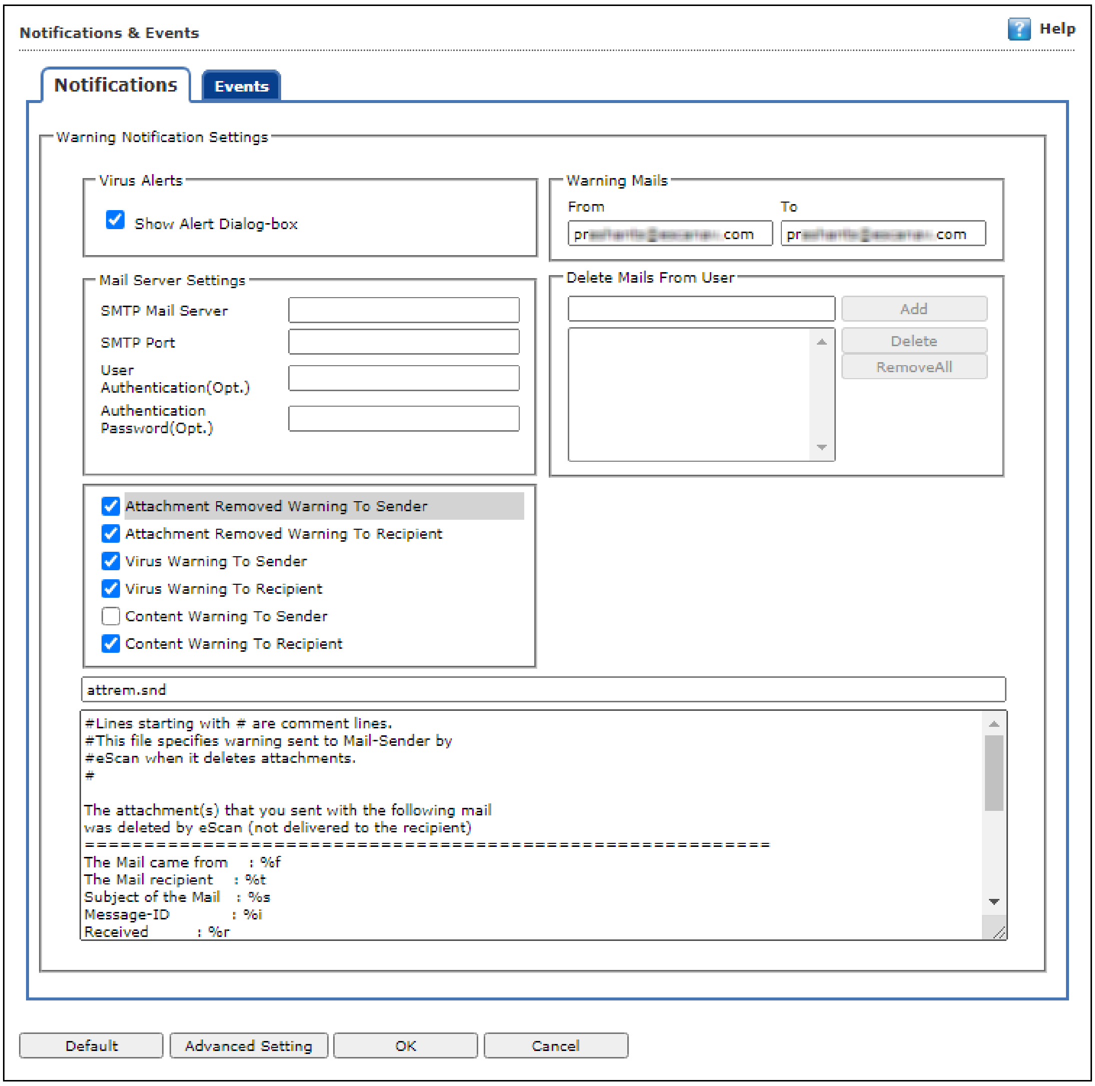
2. Click **OK**.

All executable files get removed from the Exclusion List.

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

Notifications and Events

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.



Warning Notification Settings

Virus Alerts

☑ Show Alert Dialog-box

Warning Mails

From	To
pr[redacted].com	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. 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**.

Mails Server Settings

Here you can configure the mail server settings for all the email notifications. The option sends a warning notification to the user through mail server setting.

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.

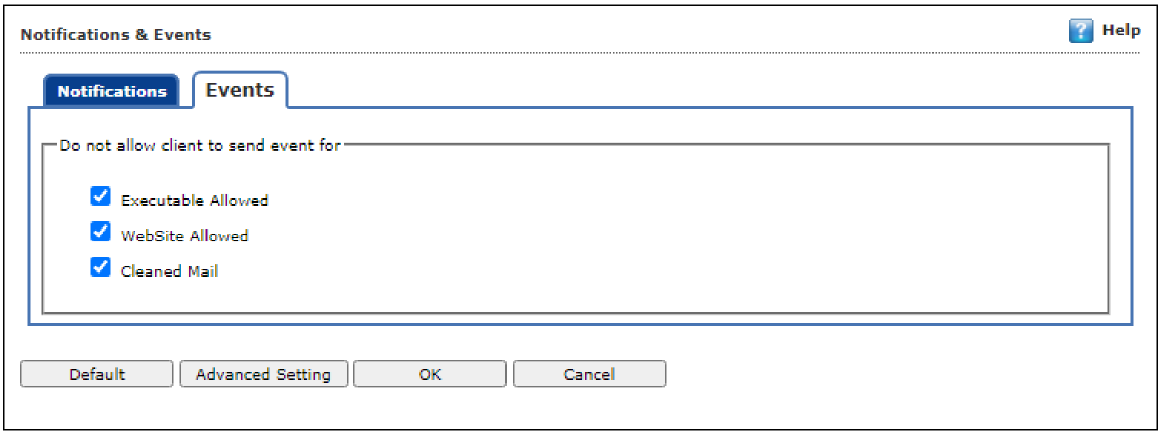
Delete Mails from User
You can configure eScan to automatically delete emails that have been sent by specific users. For this, you need to add the email addresses of such users to the **Delete Mails From User** field. The **Add**, **Delete**, and **Remove All** buttons appear as dimmed. After you enter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

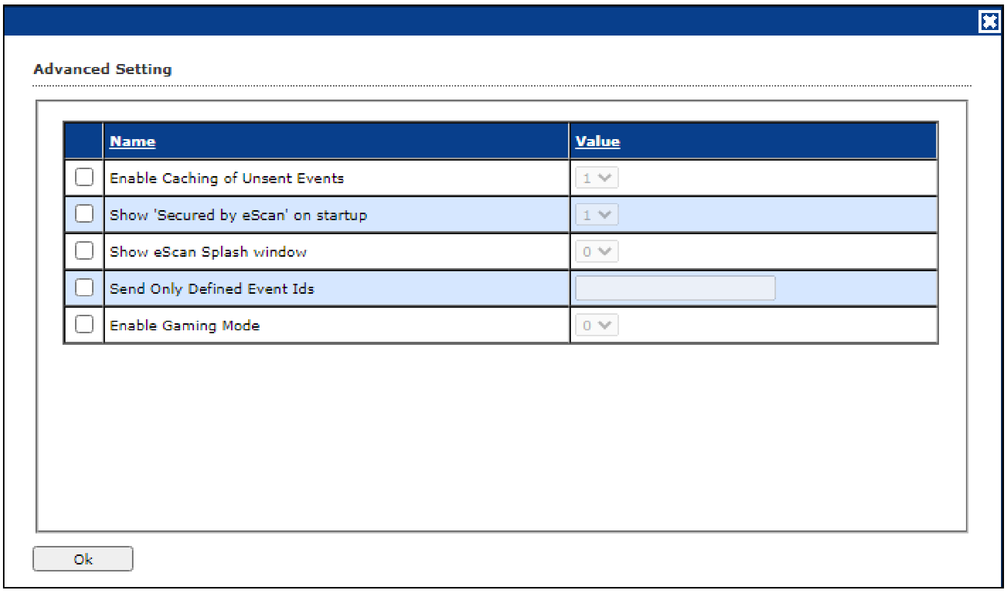


Do not allow client to send event for

☑ Executable Allowed
☑ WebSite Allowed
☑ Cleaned Mail

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

Advanced Settings



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 Unsent Events (1 = Enable/0= Disable)
It lets you Enable/Disable automatic caching of unsent events.

Show 'Secured by eScan' on startup (1 = Enable/0= Disable)
It lets you Enable/Disable the display of 'Secured by eScan' at the startup of the computers.

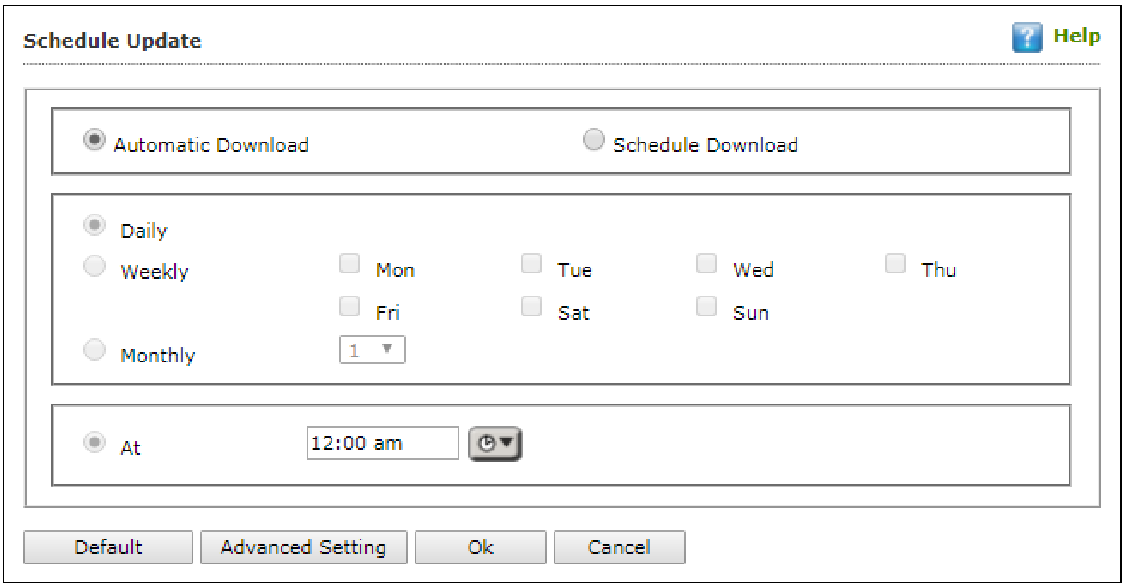
Show eScan Splash window (1 = Enable/0= Disable)
It lets you Enable/Disable display of eScan Splash Window.

Send Only Defined Event Ids
It lets you send only the defined events such as File Antivirus IDs, Mail Antivirus IDs, and more.

Enable Gaming Mode (1 = Enable/0 = Disable)
It lets you Enable/Disable the gaming mode on the computer.

Schedule Update

The Schedule Update lets you schedule eScan database updates.



Schedule Update

● Automatic Download ○ Schedule Download

○ Daily

○ Weekly □ Mon □ Tue □ Wed □ Thu

□ Fri □ Sat □ Sun

○ Monthly 1

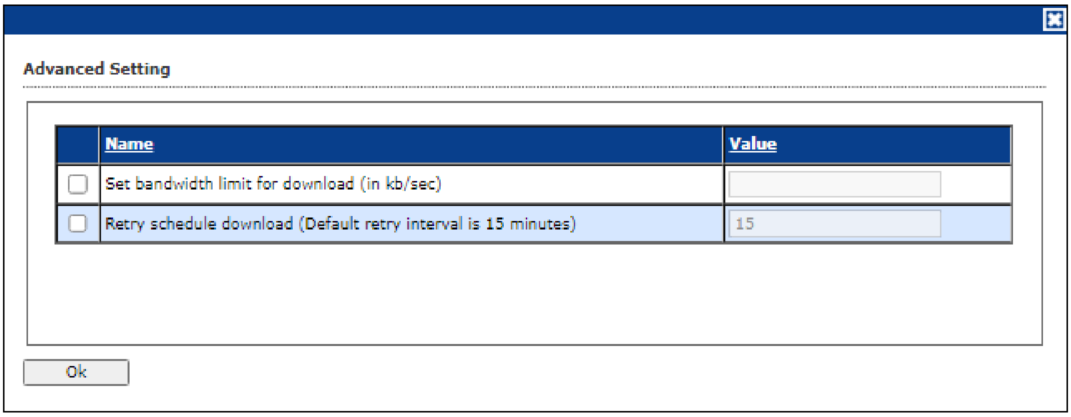
○ At 12:00 am

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

-OR-

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

Advanced Settings



Advanced Setting

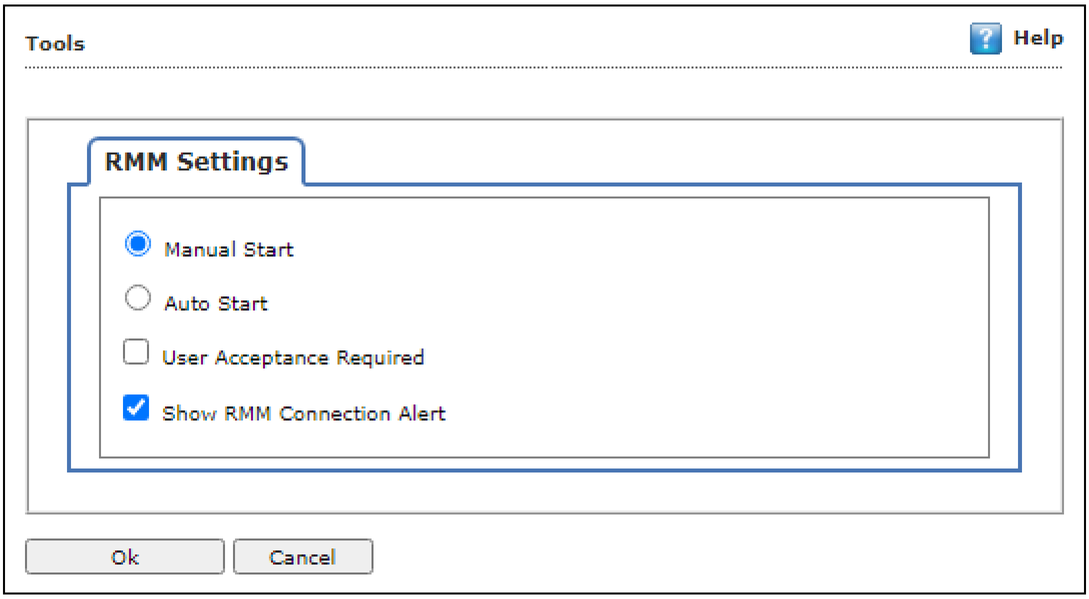
	Name	Value
□	Set bandwidth limit for download (in kb/sec)	
□	Retry schedule download (Default retry interval is 15 minutes)	15

Set bandwidth limit for download (in kb/sec)
It lets you define bandwidth limit for download on managed computers.

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

Tools

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



● Manual Start
○ Auto Start
□ User Acceptance Required
☑ Show RMM Connection Alert

RMM Settings

The RMM settings let you configure default connection settings for connecting to client computers. You will get the following configuration options:

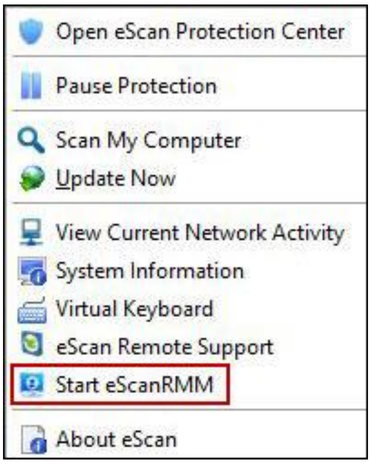
- **Manual Start**: If this option is selected by default, client endpoint users have to manually start the RMM service to establish a RMM connection.
- **Auto Start**: If this option is selected, RMM service will be started automatically and all client endpoints will be connected to your main eScan server.
- **User Acceptance Required**: If this checkbox is selected, a pop-up appears on client endpoint for RMM connection acceptance. If left unselected, pop-up doesn't appear and you get direct access to the client endpoint.
- **Show RMM Connection Alert**: 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.

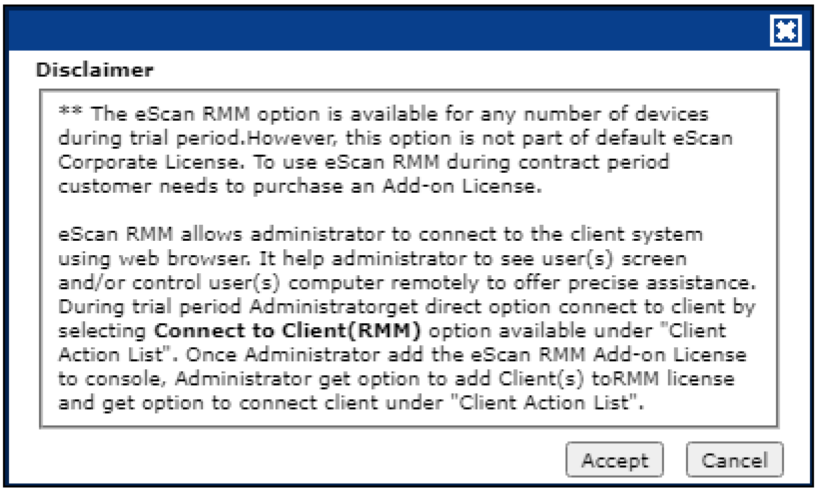
RMM - Manual Start

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.



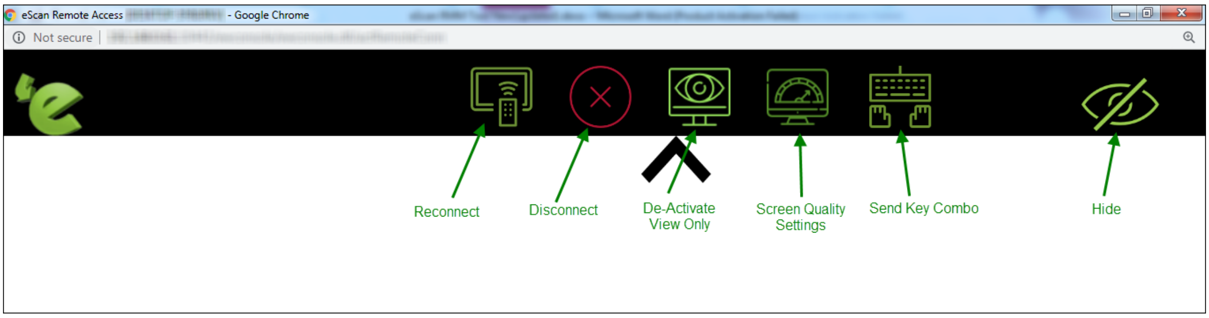
Disclaimer

** 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.

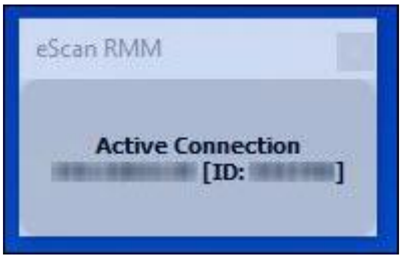
eScan RMM allows administrator to connect to the client system using web browser. It help administrator to see user(s) screen and/or control user(s) computer remotely to offer precise assistance. During trial period Administratorget direct option connect to client by selecting **Connect to Client(RMM)** 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.

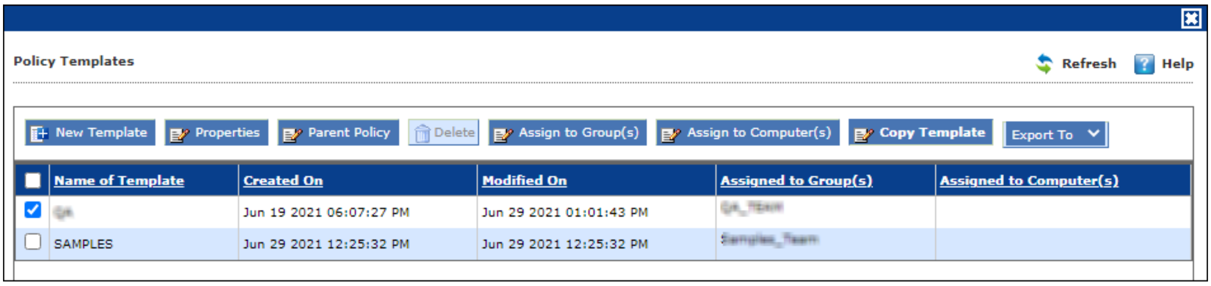
Assigning Policy Template to a group

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

Method 1

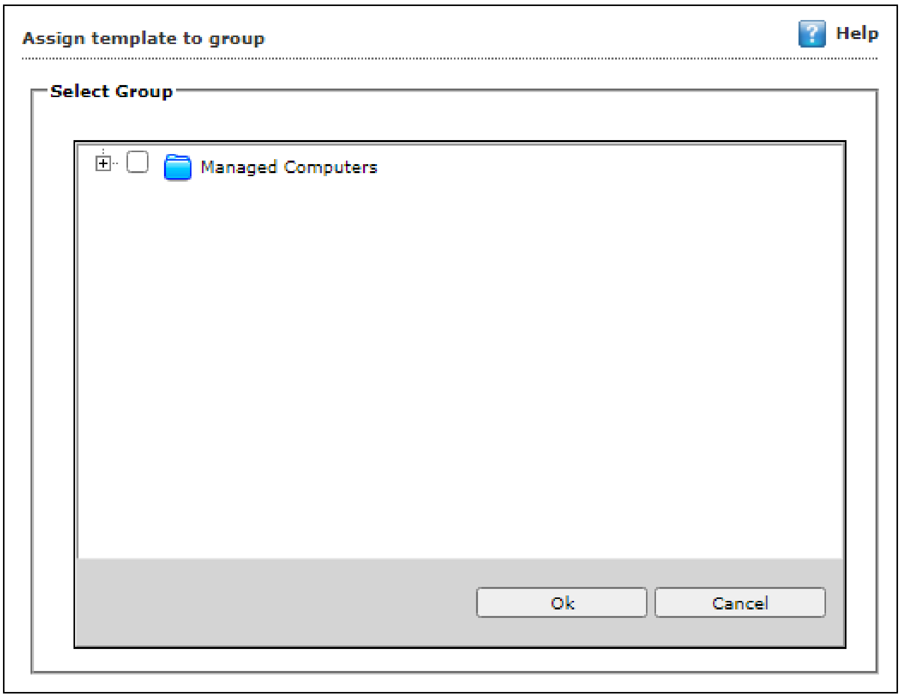
To assign a Policy to a group,

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.

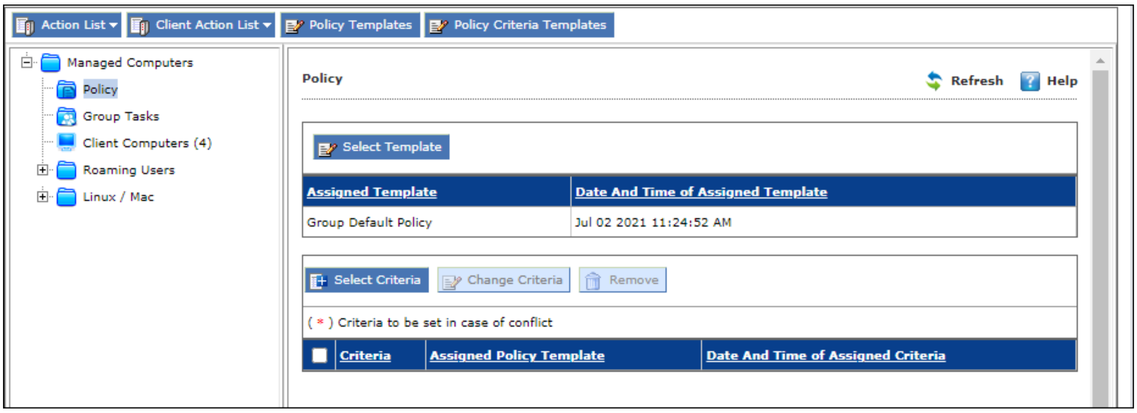


4. Select the group(s) and then click **OK**.
   The policy will be assigned to the selected group(s).

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.

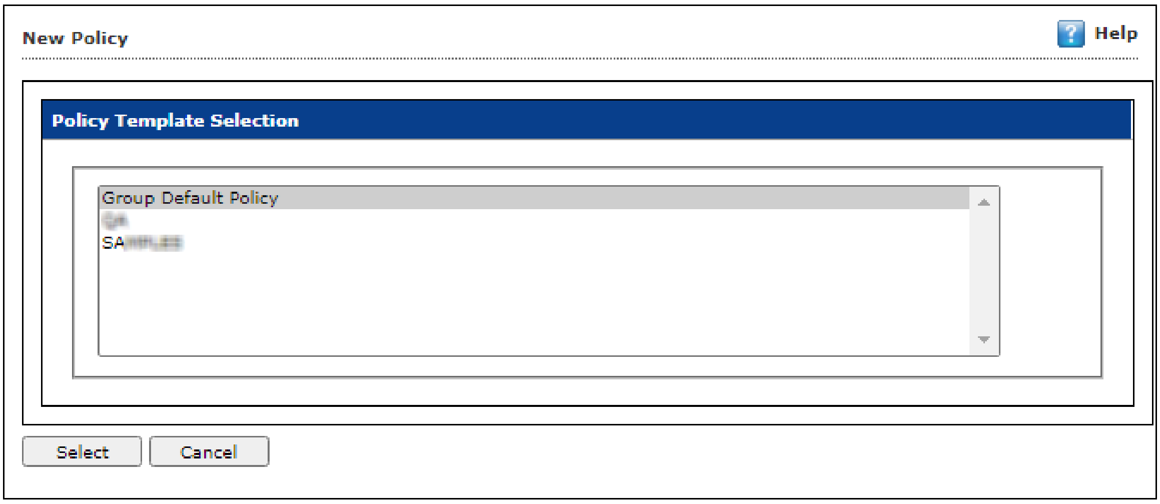


Assigned Template	Date And Time of Assigned Template
Group Default Policy	Jul 02 2021 11:24:52 AM

(*) 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.



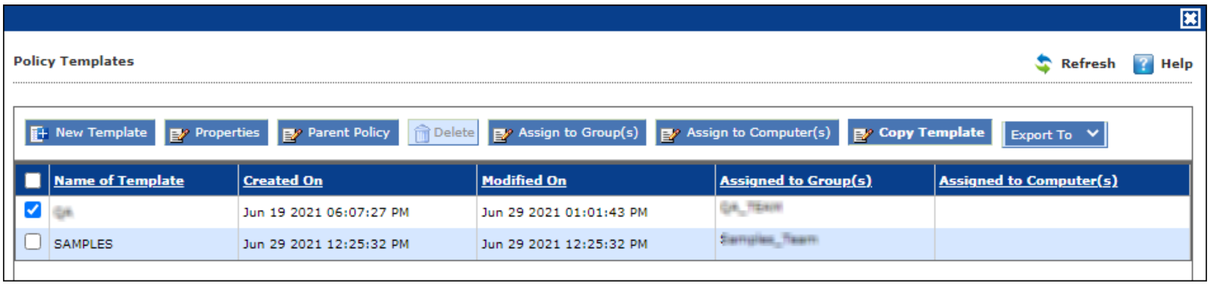
Group Default Policy
[redacted]
SA[redacted]

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

Assigning Policy Template to Computer(s)

To assign a policy template to computers,

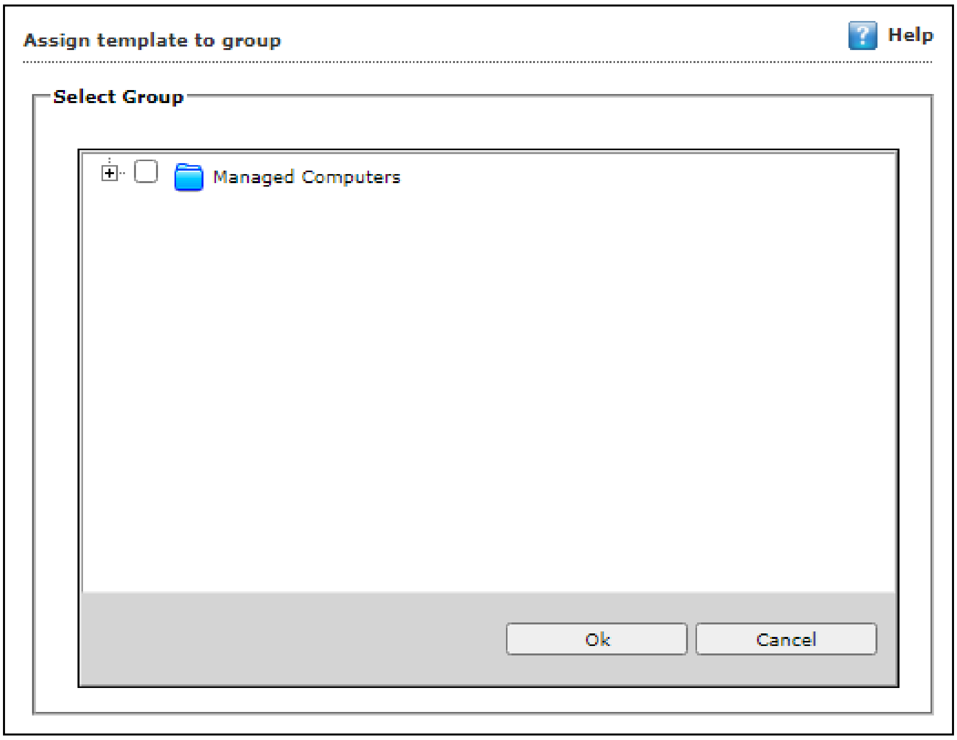
1. In the **Policy Templates** window, select a policy.



Policy Templates

☐	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
☑	[redacted]	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)**.
   Assign Template to computer window appears.



Assign template to group

Select Group

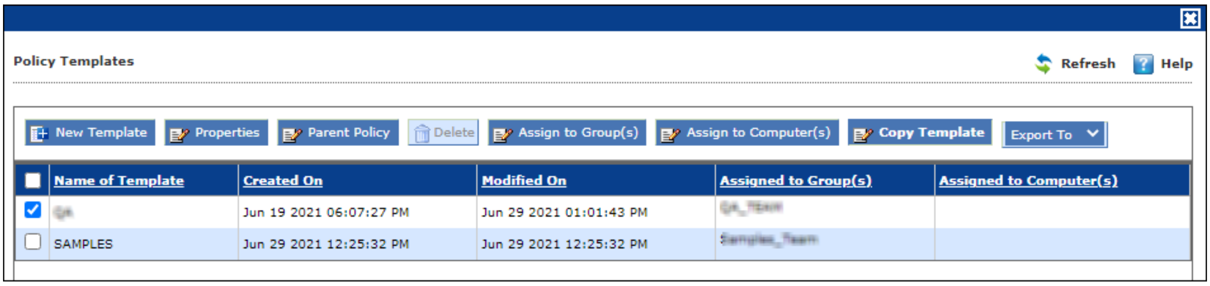
☐ Managed Computers

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

Copy a Policy Template

To copy a Policy Template,

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



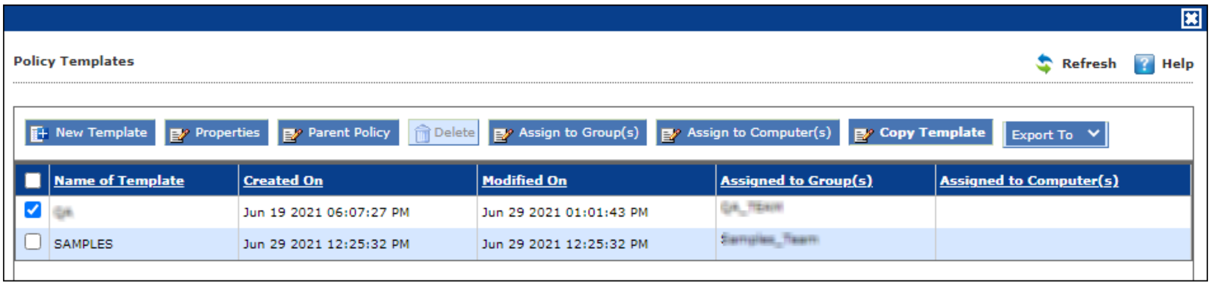
□	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
☑	[redacted]	Jun 19 2021 06:07:27 PM	Jun 29 2021 01:01:43 PM	[redacted]	
□	SAMPLES	Jun 29 2021 12:25:32 PM	Jun 29 2021 12:25:32 PM	[redacted]	

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

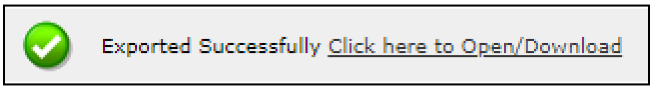
To copy a Policy Template,

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



□	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.

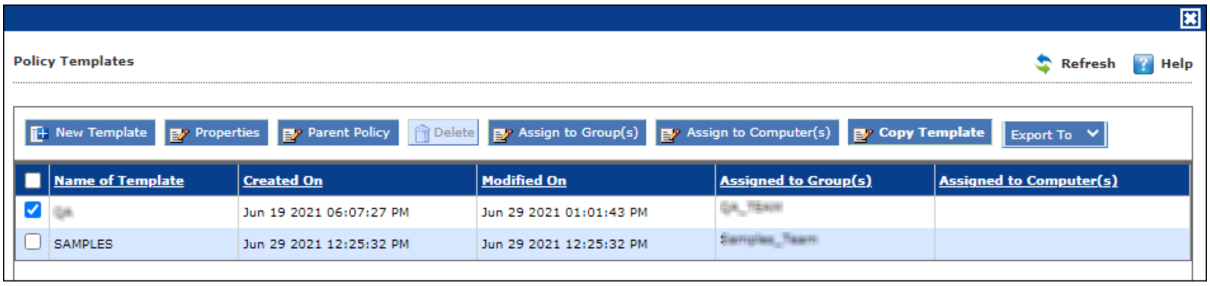


Exported Successfully Click here to Open/Download

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:

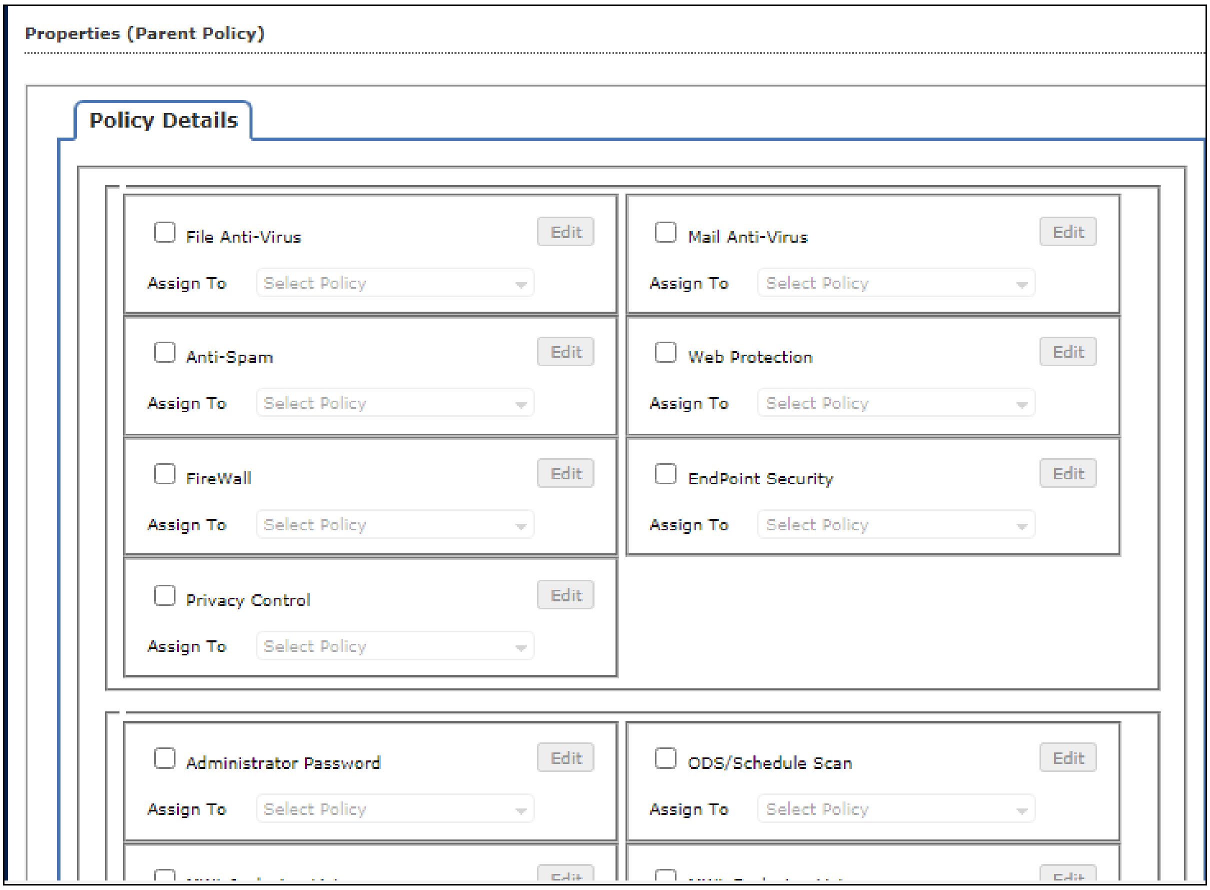
1. In the Managed Computers screen, click **Policy Templates**.
   Policy Templates window appears.
2. In the Policy Template window, click **Parent Policy**.



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]	

Properties (Parent Policy) window appears displaying all the policies.

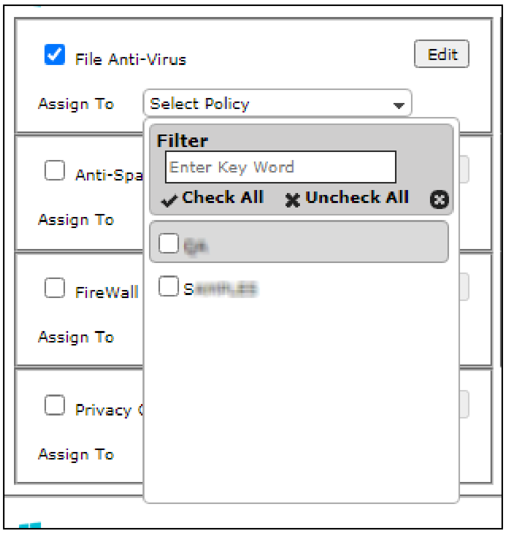


Properties (Parent Policy)

Policy Details

☐ 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.



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.

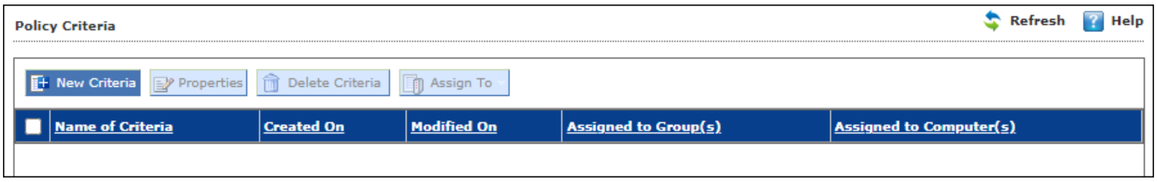
Policy Criteria Templates

This button allows to add criteria template based on the endpoints conditions.

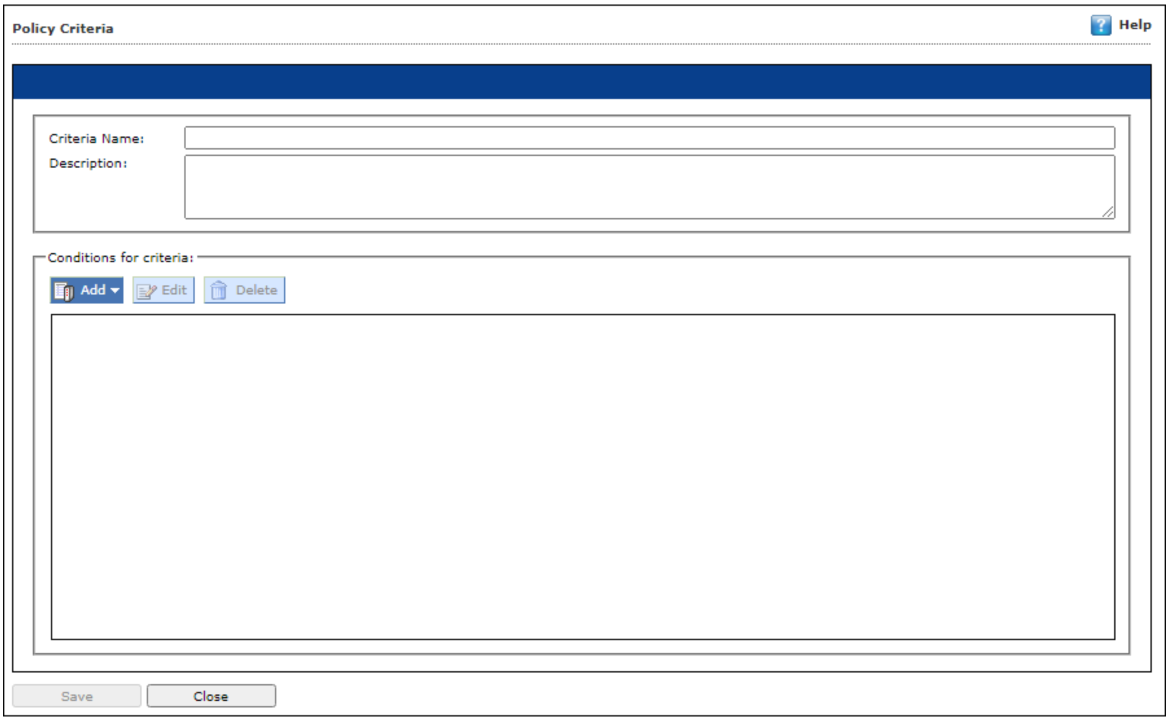
Adding a Policy Criteria Template (AND condition)

To define Policy Criteria Template, follow the steps given below:

1. In the Managed Computers screen, click **Policy Criteria Templates**.
   Policy Criteria screen appears.

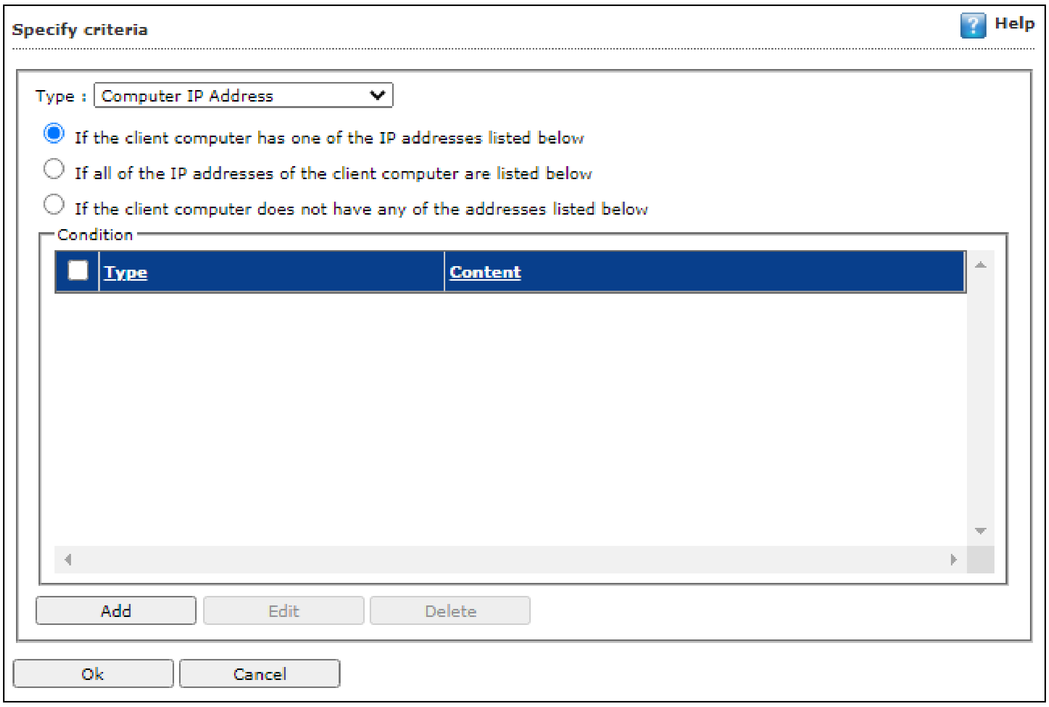


2. Click **New Criteria**.
   Policy Criteria screen displays parameter for creation.



3. Enter **Name** and **Description**.
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

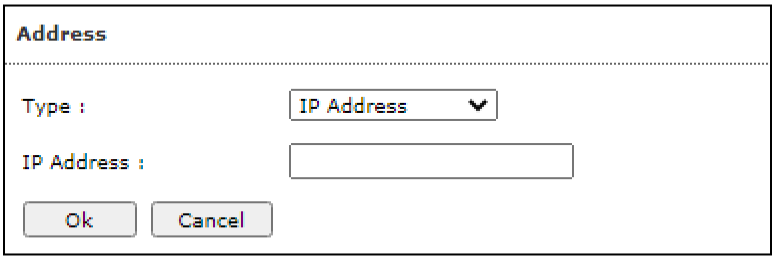
6. Click the **Type** drop-down. It displays following options:
   - Computer IP Address
   - Management Server Connection
   - Users
   - Machine Name

Depending upon the option, the conditions and settings may vary.

Computer IP Address

This option let you display list of computer IP address connected to client computer.

1. Select the appropriate condition.
2. Click **Add**.
   Address window appears.



Address

Type : IP Address

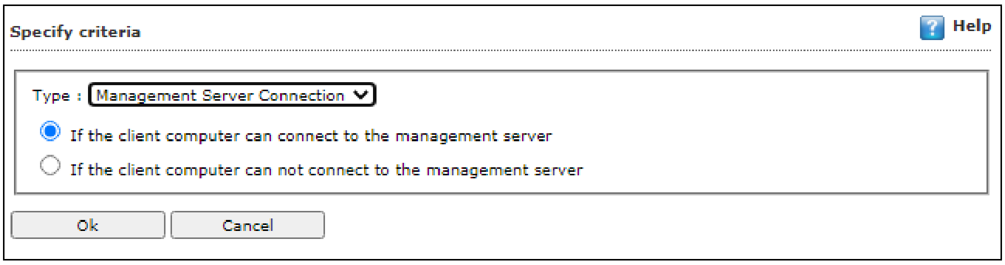
IP Address :

3. Enter the IP address.
4. Click **OK**.
   The Policy Criteria Template for an IP Address will be saved.

Edit – Clicking **Edit** lets you edit the IP address of the policy template from the list.
Delete – Clicking **Delete** lets you delete the IP address of the policy template from the list.

Management Server Connection

It display the client computer connect to the management server.



Specify criteria

Help

Type : Management Server Connection

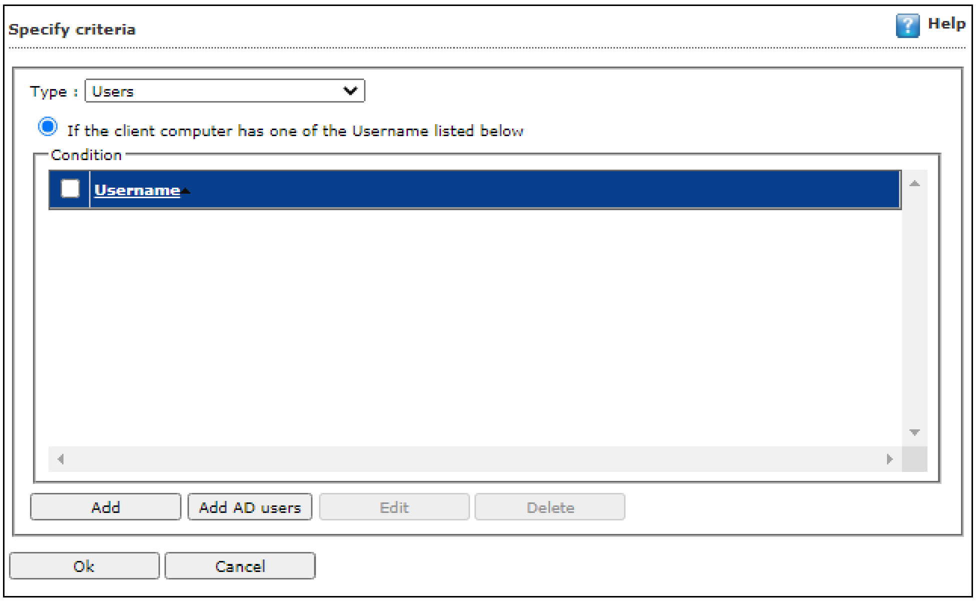
● If the client computer can connect to the management server

○ 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

This option shows the list of username connected with client computer.



Specify criteria

Help

Type : Users

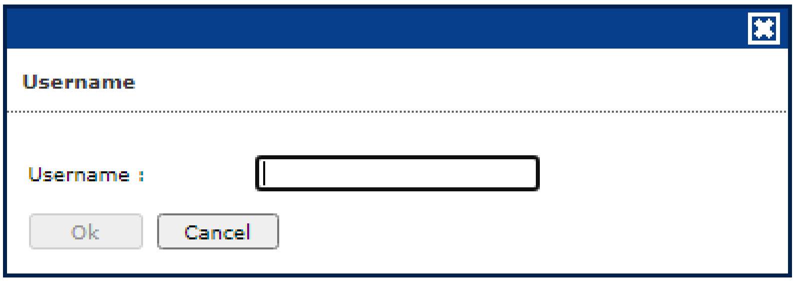
● If the client computer has one of the Username listed below

Condition

□	Username

Adding Local Users

1. To add local users, click **Add**.
   Username window appears.



Username

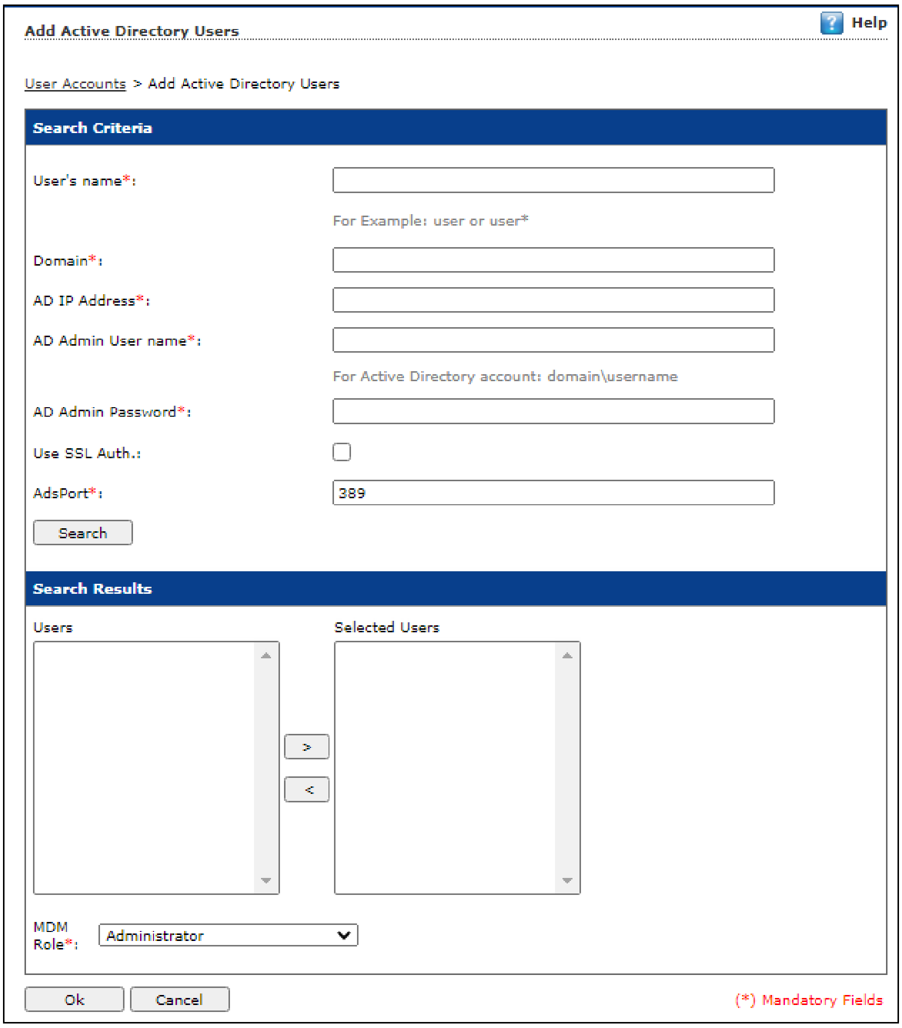
Username :

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 Users — Help

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

Search Results

Users — Selected Users

MDM Role*: Administrator

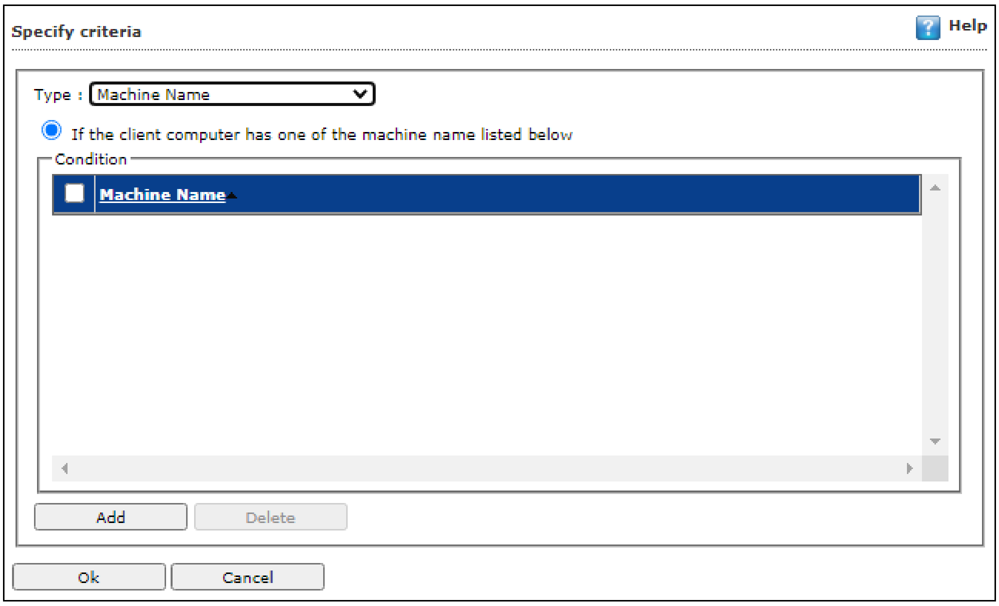
Ok — Cancel — (*) Mandatory Fields

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 <.
5. Click **OK**.
   The Policy Criteria Template for Users will be saved.

Edit – Clicking **Edit** lets you edit user details of the policy template from the list.
Delete – Clicking **Delete** lets you delete user of the policy template from the list.

Machine Name

This option show list of machine name connected to the client computer.



Specify criteria

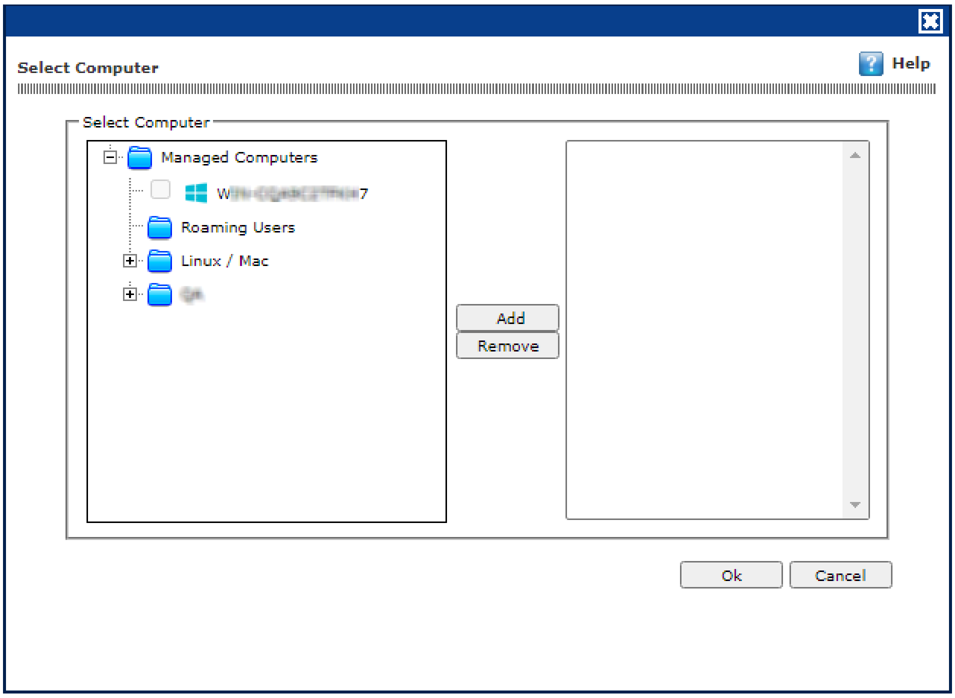
Help

Type : Machine Name

● If the client computer has one of the machine name listed below

Condition

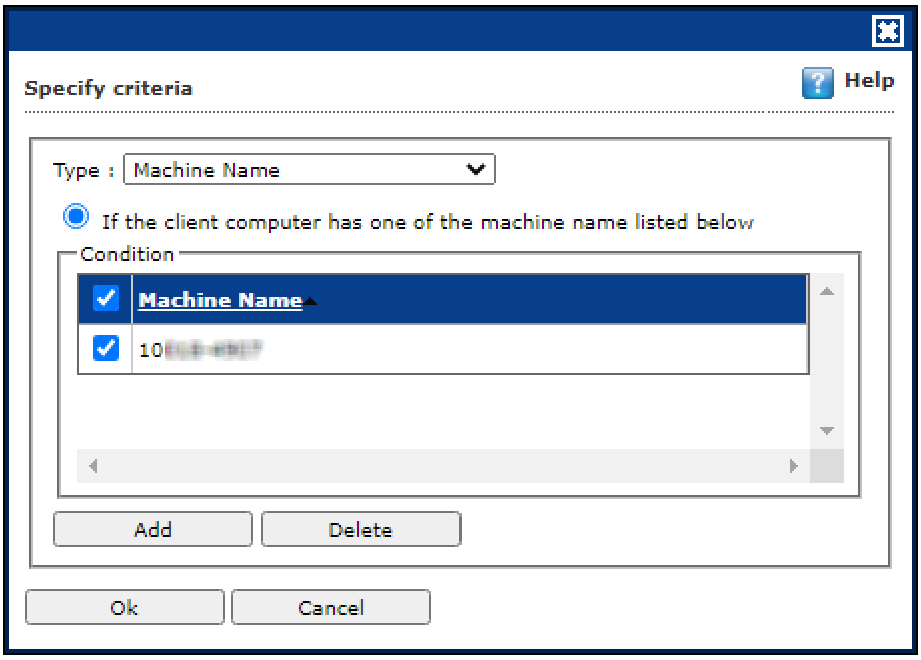
1. Click **Add**.
   Select Computer screen appears displaying all managed computers.



Select Computer

Help

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.



Specify criteria

Type : Machine Name

● If the client computer has one of the machine name listed below

Condition

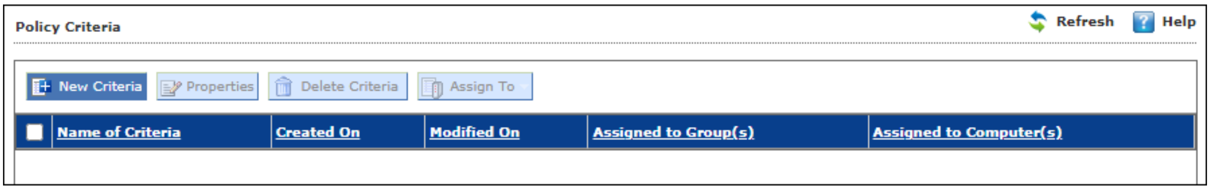
☑	Machine Name
☑	10[redacted]

3. Select the Machine Name. This enable **Delete** button.
4. Click **Delete**.
   The machine will be deleted.

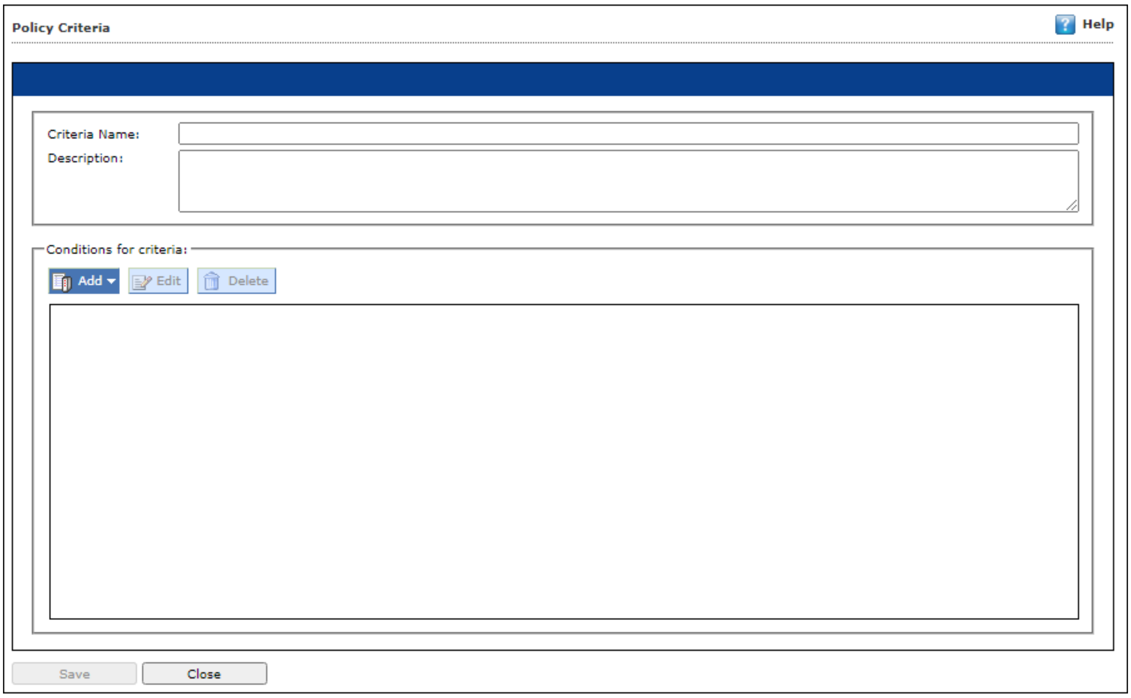
Adding a Policy Criteria Template (OR condition)

To define Policy Criteria Template, follow the steps given below:

1. In the Managed Computers screen, click **Policy Criteria Templates**.
   Policy Criteria screen appears.



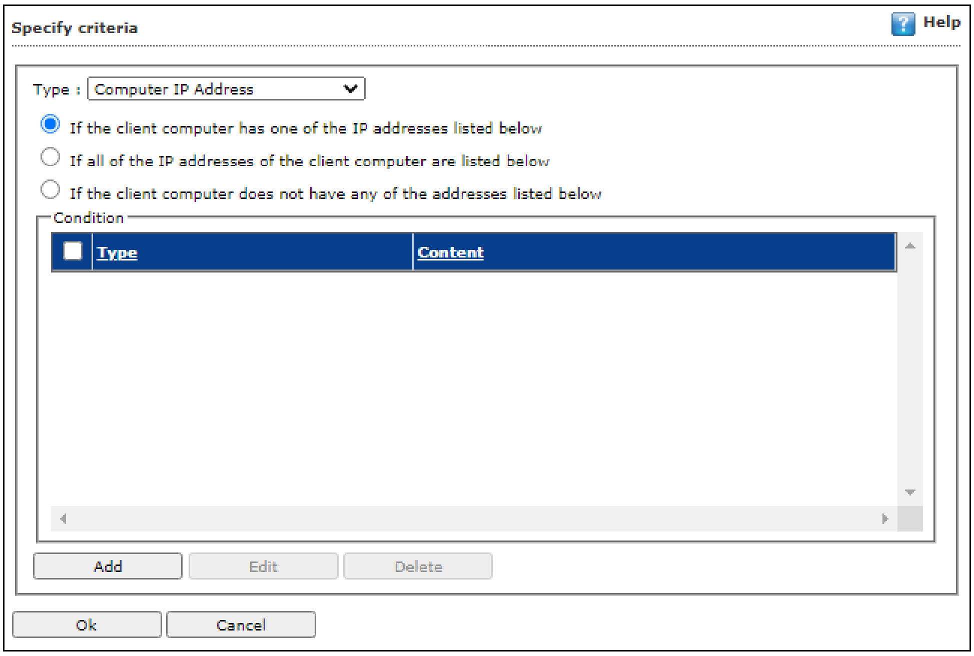
2. Click **New Criteria**.
   Policy Criteria screen displays parameter for creation.



3. Enter **Name** and **Description**.
4. Click **Add** drop-down.
5. Click Add **OR Condition**.

NOTE	Before creating **OR Condition** in policy criteria, ensure that **AND Condition** is created in the policy criteria template.

Specify Criteria screen appears.


Specify criteria
Help
Type : Computer IP Address
● If the client computer has one of the IP addresses listed below
○ If all of the IP addresses of the client computer are listed below
○ If the client computer does not have any of the addresses listed below
Condition
□ Type
Content
Add
Edit
Delete
Ok
Cancel

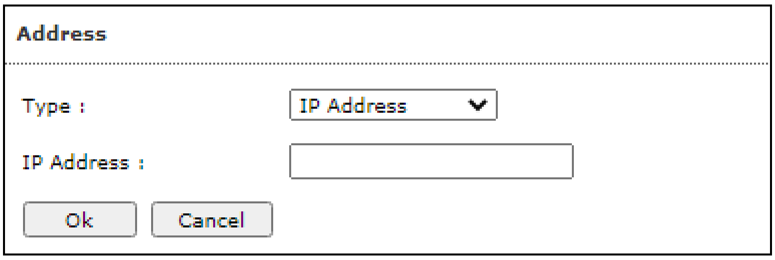
6. Click the **Type** drop-down. It displays following options:
   - Computer IP Address
   - Management Server Connection
   - Users
   - Machine Name

Depending upon the option, the conditions and settings may vary.

Computer IP Address

This option let you display list of computer IP address connected to client computer.

1. Select the appropriate condition.
2. Click **Add**.
   Address window appears.

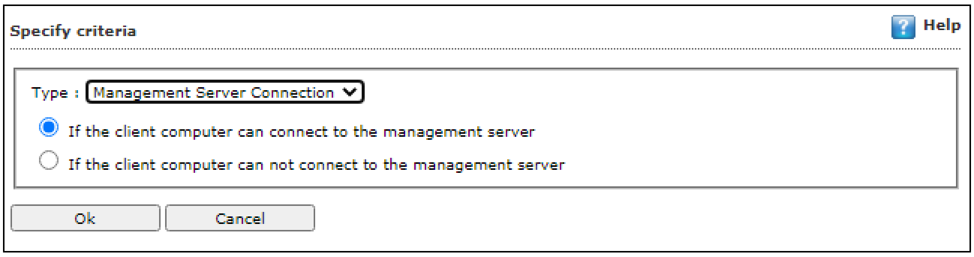


3. Enter the IP address.
4. Click **OK**.
   The Policy Criteria Template for an IP Address will be saved.

Edit – Clicking **Edit** lets you edit the IP address of the policy template from the list.
Delete – Clicking **Delete** lets you delete the IP address of the policy template from the list.

Management Server Connection

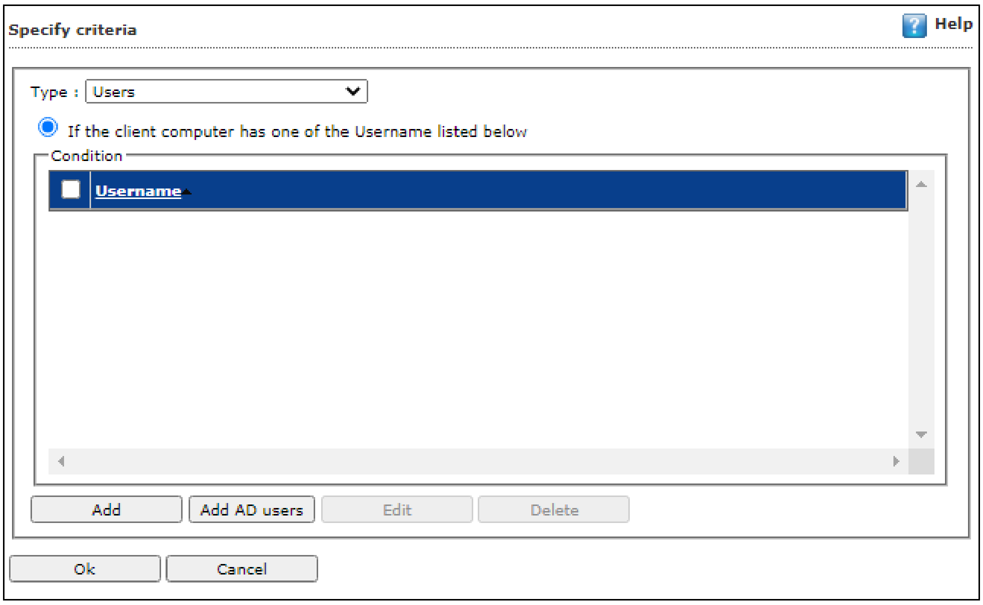
It display the client computer connect to the management server.


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

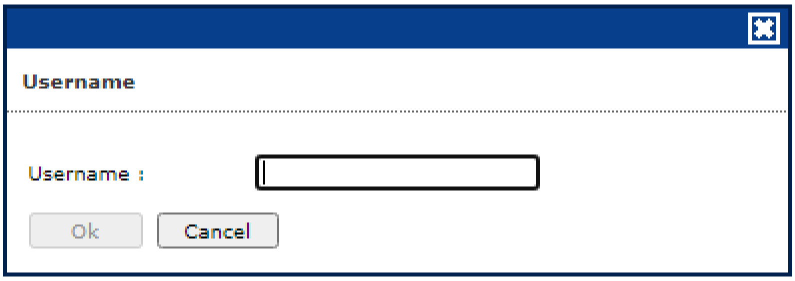
This option shows the list of username connected with client computer.


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 :

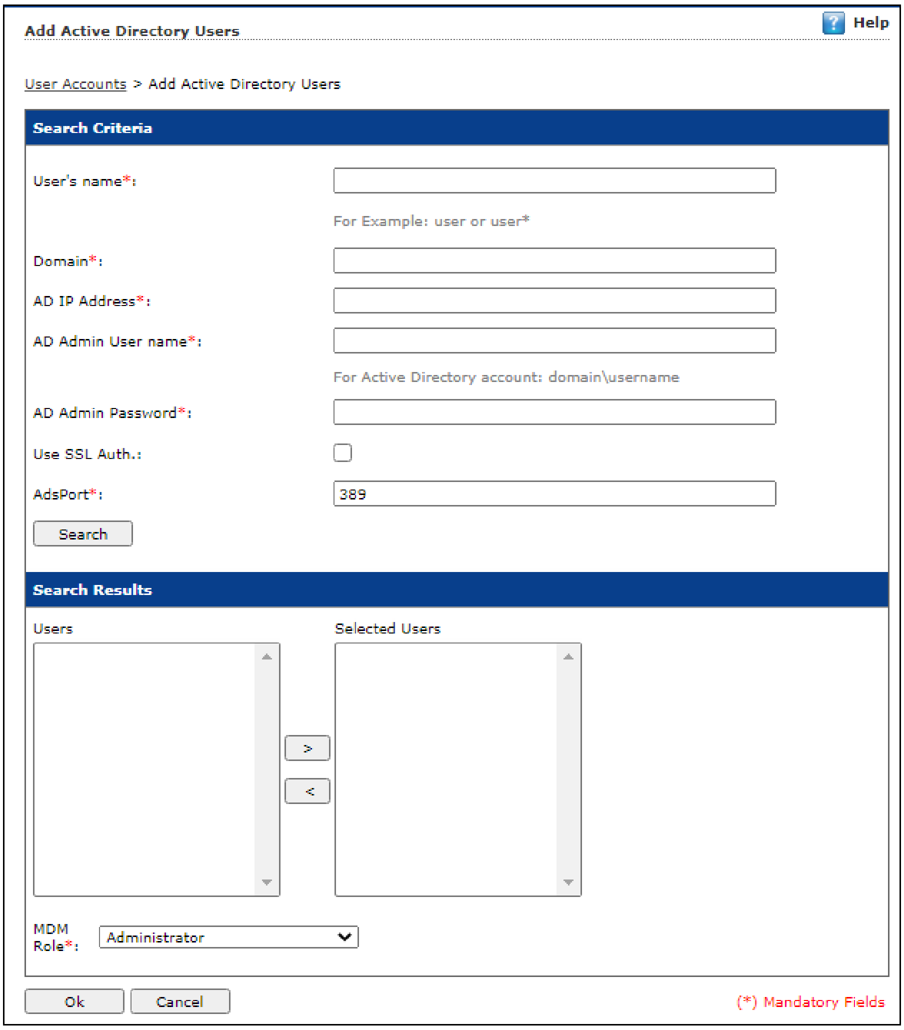
2. Enter a Username.

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 Users
? Help

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

Search Results

Users
Selected Users
>
<

MDM Role*: Administrator

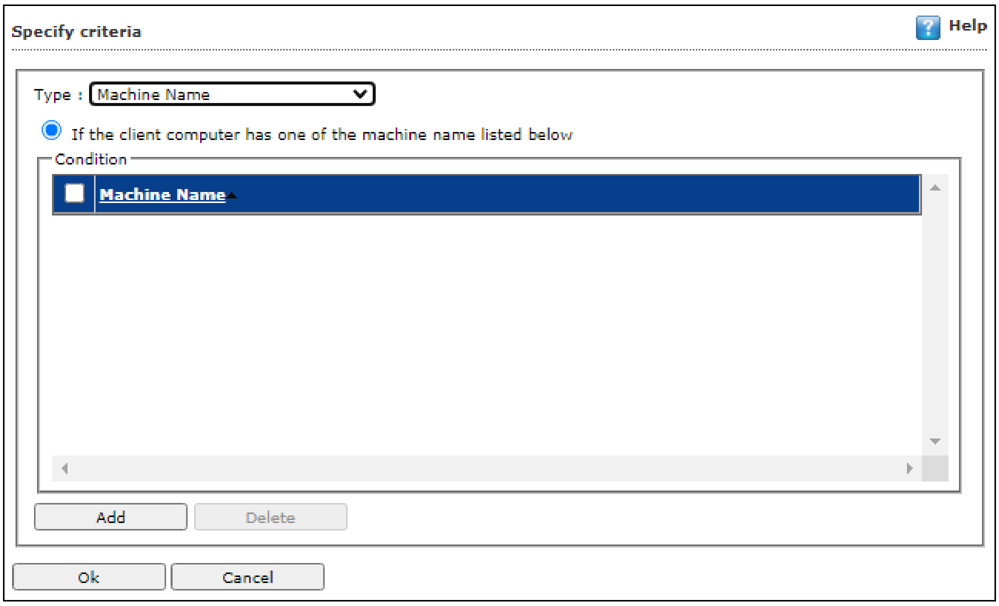
Ok Cancel
(*) Mandatory Fields

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 <.
5. Click **OK**.
   The Policy Criteria Template for Users will be saved.

Edit – Clicking **Edit** lets you edit user details of the policy template from the list.
Delete – Clicking **Delete** lets you delete user of the policy template from the list.

Machine Name

This option show list of machine name connected to the client computer.



Specify criteria

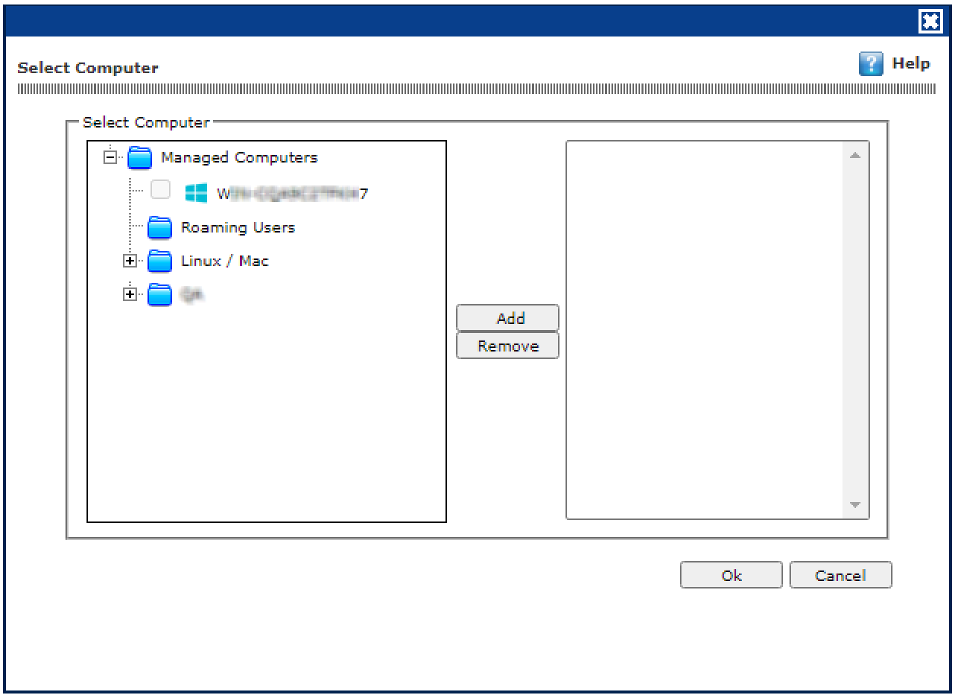
Type : Machine Name

● If the client computer has one of the machine name listed below

Condition

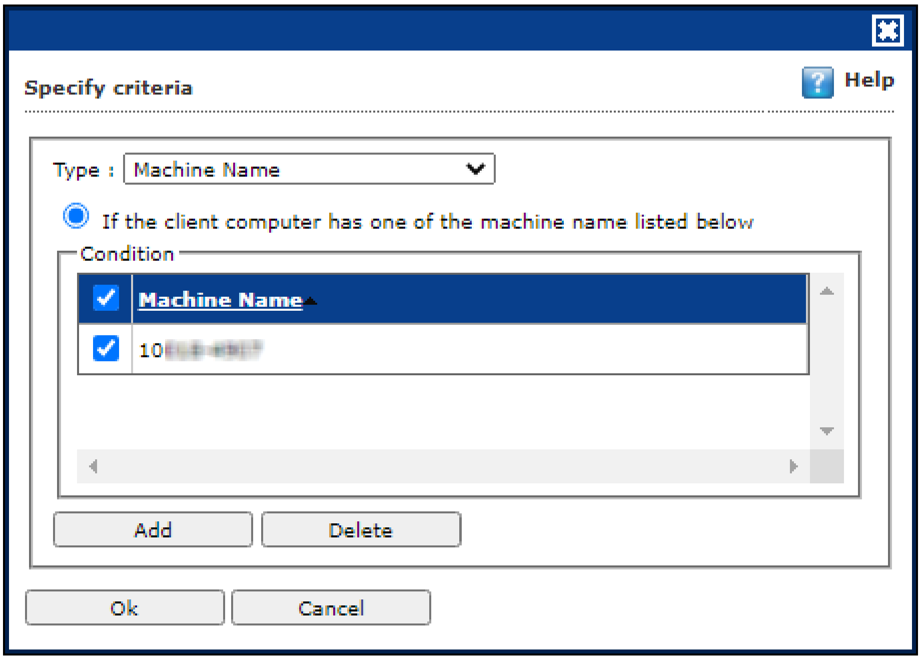
□	Machine Name

1. Click **Add**.
   Select Computer screen appears displaying all managed computers.



Select Computer

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.



Specify criteria

Help

Type : Machine Name

● If the client computer has one of the machine name listed below

Condition

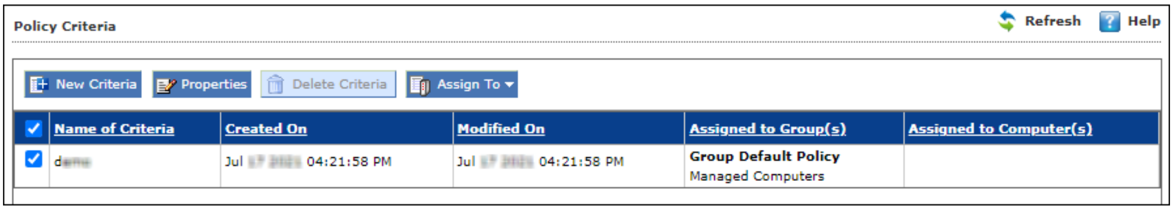
☑	Machine Name ▲
☑	10[redacted]

3. Select the Machine Name. This enable **Delete** button.
4. Click **Delete**.
   The machine will be deleted.

Viewing Properties of a Policy Criteria template

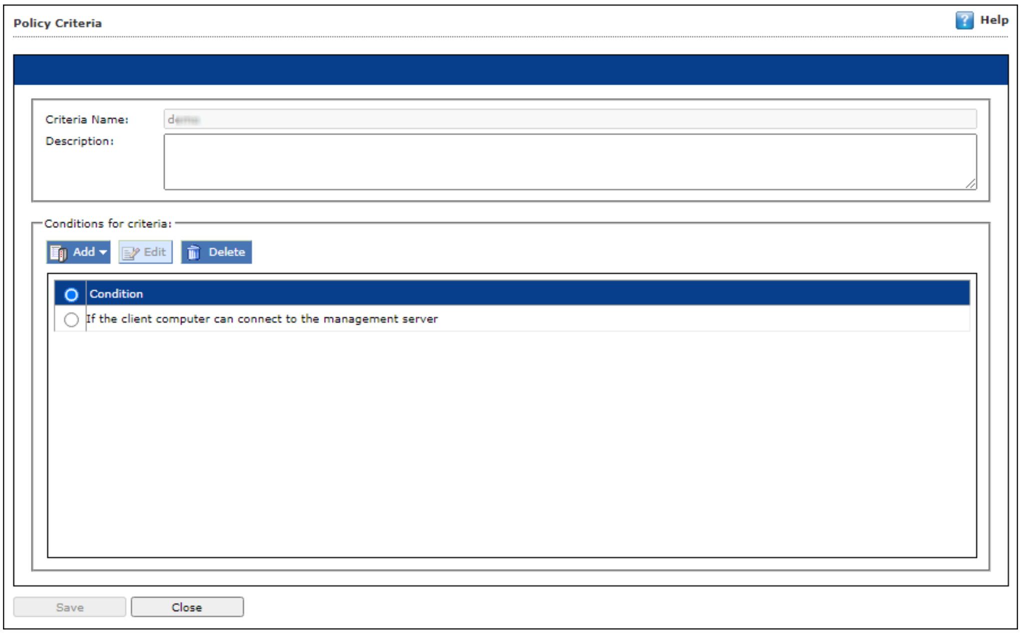
To view the properties of a Policy Criteria Template, follow the steps given below:

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:

○	Condition
○	If the client computer can connect to the management server

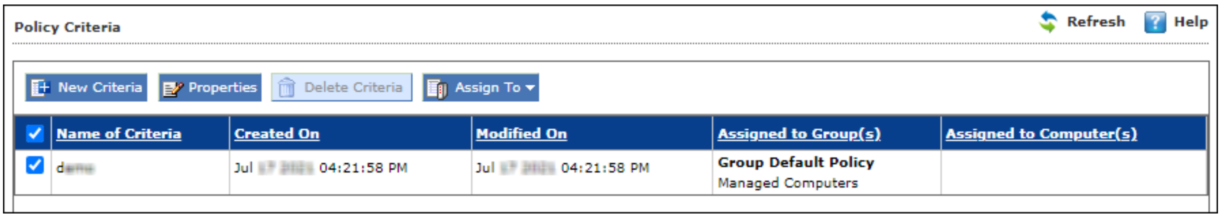
3. Make the necessary changes and click **Save**.
   The Policy Criteria template will be saved and updated.

Deleting a Policy Criteria template

To delete assigned policy criteria template, follow the steps given below:

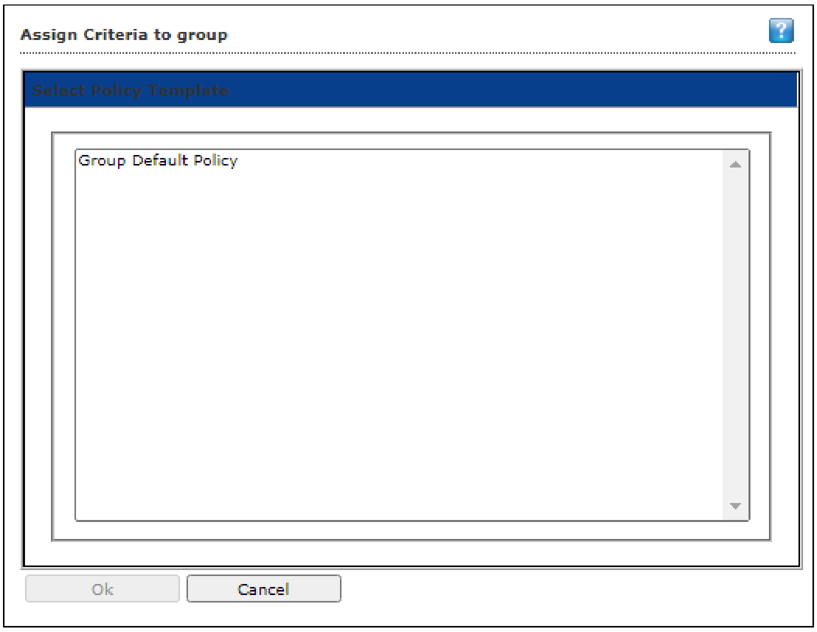
The Policy Criteria window displays to which group or computer the template is assigned in Assigned to Group(s) or Assigned to Computer(s) column.
For explanation, we are following the procedure as per the screenshot below

1. Select a policy criteria template.
2. Click **Assign To** > **Groups**.

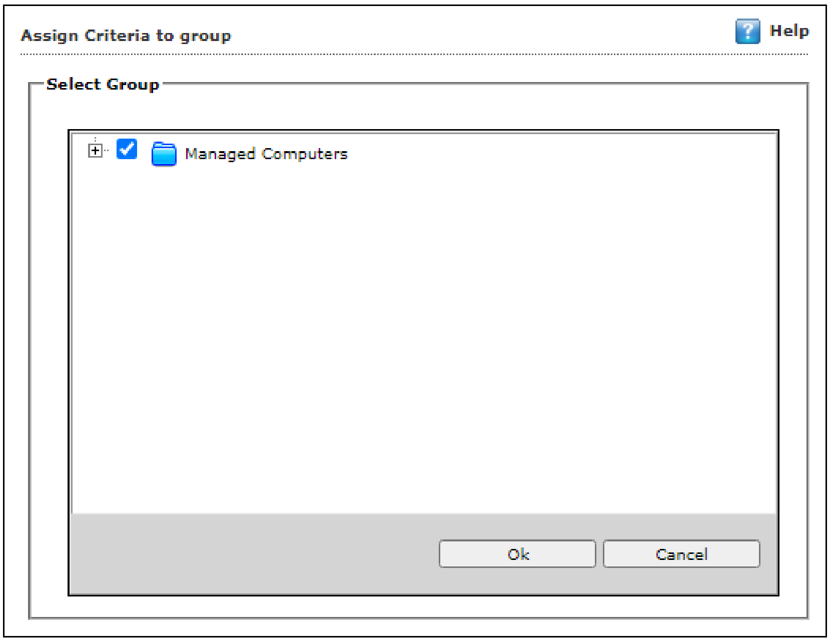


☑	Name of Criteria	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
☑	[redacted]	Jul [redacted] 04:21:58 PM	Jul [redacted] 04:21:58 PM	Group Default Policy Managed Computers	

Assign Criteria to Group window appears.

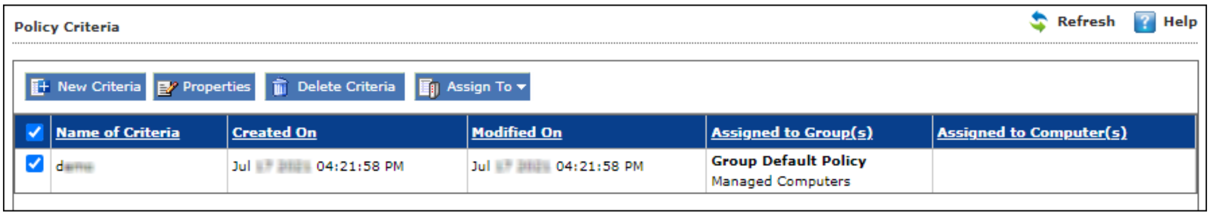


3. Click **Group Policy Template** > **OK**.
   Assign Criteria to group window displays Managed Computers folder tree.



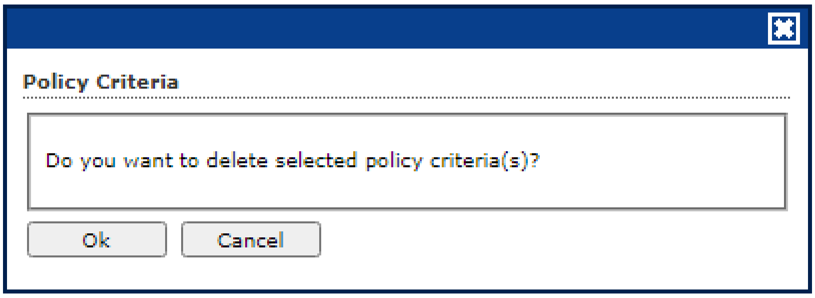
4. Uncheck the selected group.
5. Click **OK**.

The Policy Criteria Template will no longer be assigned to any group. This enables **Delete Criteria** button.



☑	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.



Do you want to delete selected policy criteria(s)?

8. Click **Ok**.
   The Policy Criteria Template will be deleted.

Unmanaged Computers

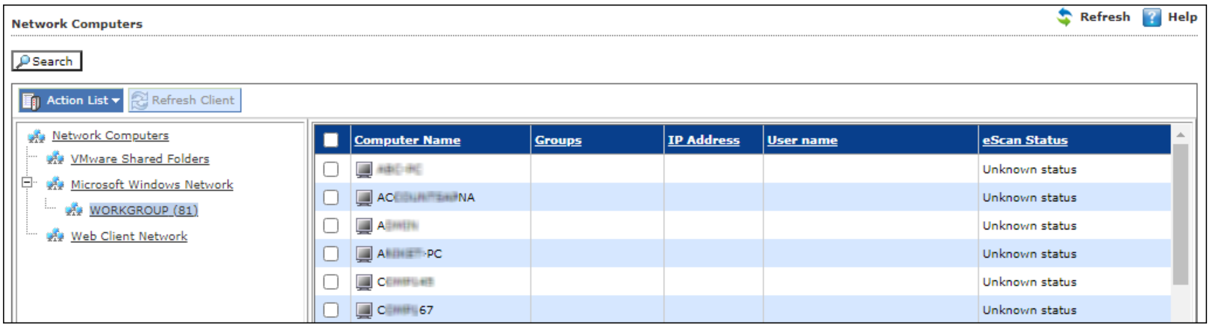
To install eScan Client, define policies and tasks on the basis of group, it is necessary to move computers to the created groups. You can move the computers from Unmanaged Computers to desired groups created in the Managed Computers using the following submodules:

- **Network Computers**
- **IP Range**
- **Active Directory**
- **New Computers Found**

Network Computers

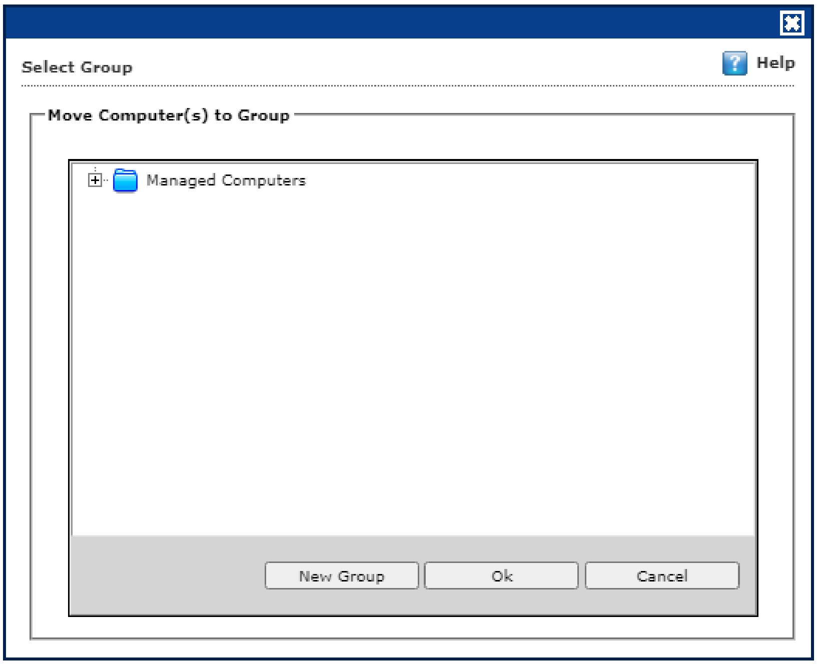
This submodule displays a list of available networks. You can move the computers from the list of computers present in the Network Computers using the following steps –

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.

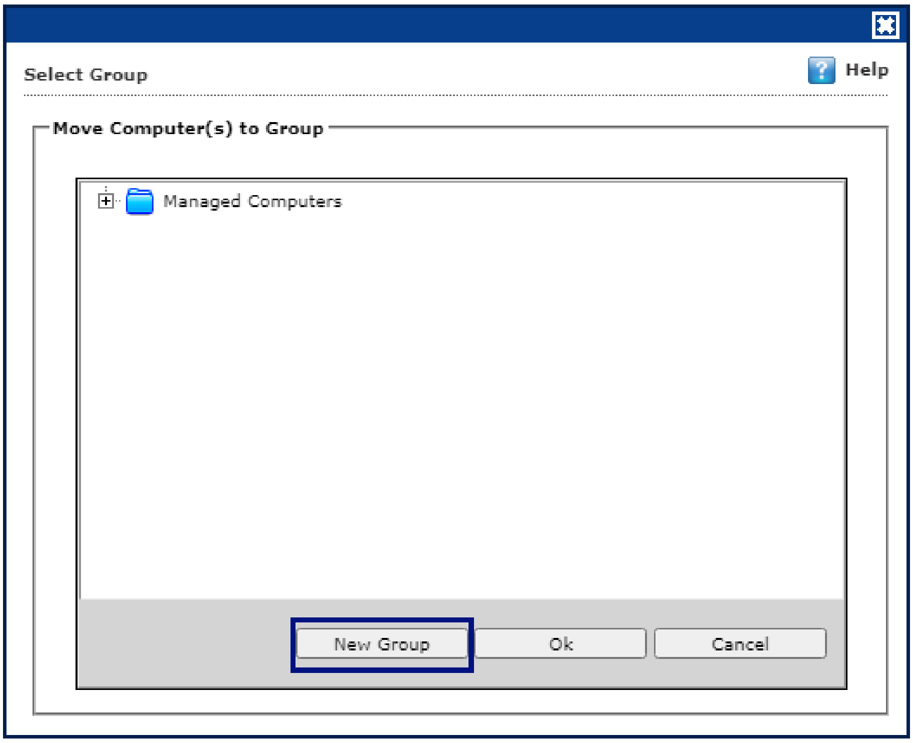


7. Select the group where you wish to move the selected computer(s) and click **OK**. The selected computer(s) will be moved to the group.

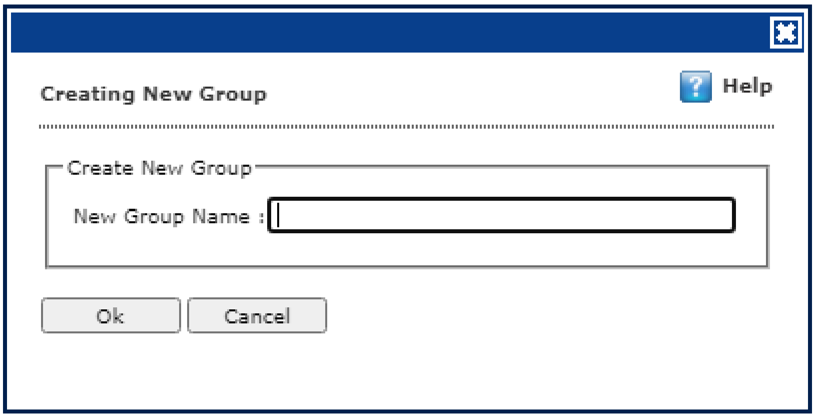
Creating a New Group from the Select Group window

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.



Creating New Group

Create New Group

New Group Name :

2. Enter a name for the group.
3. Click **OK**.

   A new group will be created.

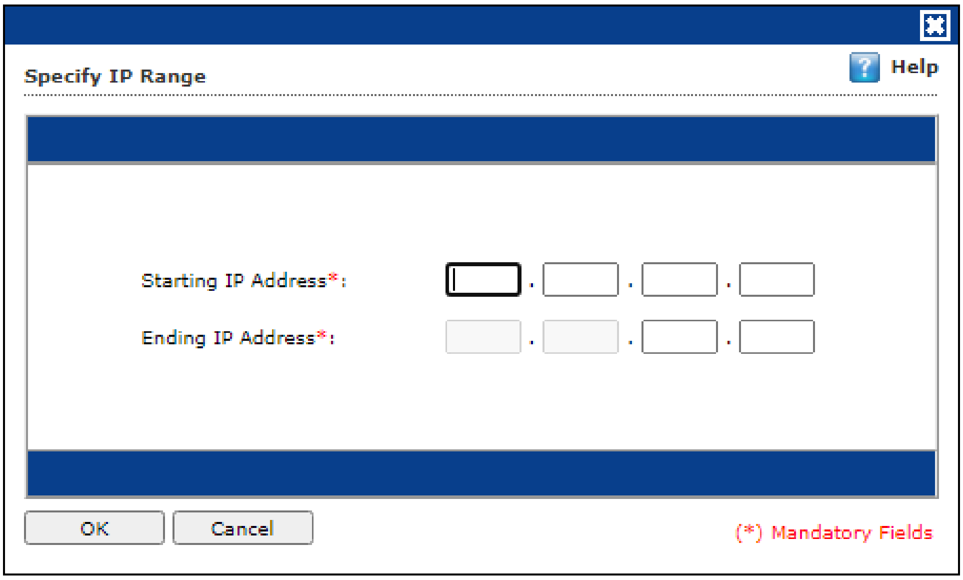
IP Range

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.



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:

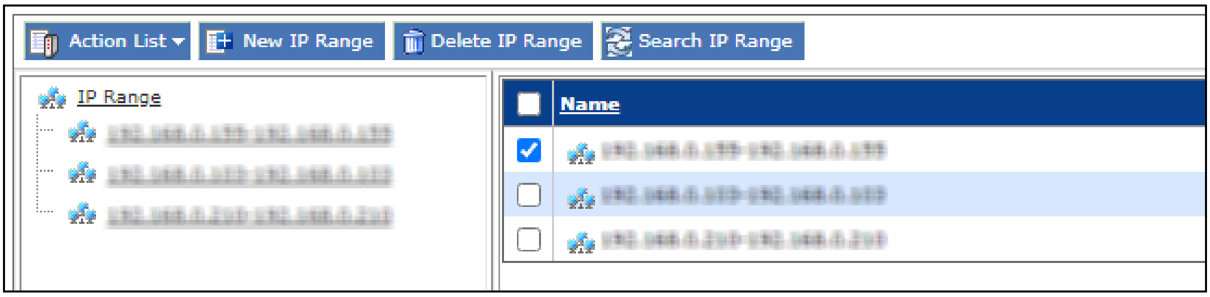
1. Select an IP range.
2. Select the checkbox next to Computer Name column.
3. Click **Action List** > **Move to Group**.
   Select Group window appears.

4. Select the destination group.
5. Click **OK.**
   The IP range will be moved to the specified group.

Deleting an IP Range

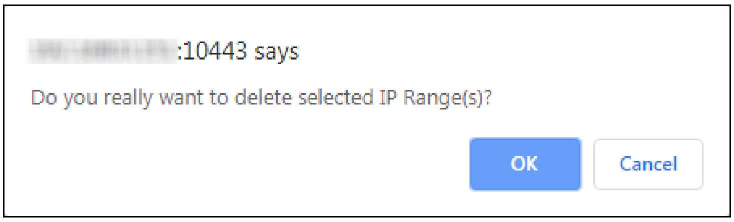
To delete an IP range, follow the steps given below:

1. Select an IP Range.
2. Click **Delete IP Range**.



□	Name
☑	[redacted]
□	[redacted]
□	[redacted]

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.

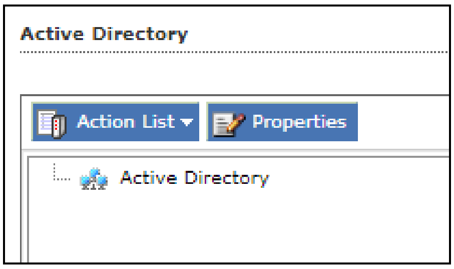
Active Directory

The Active Directory submodule lets you add computers from an Active Directory.

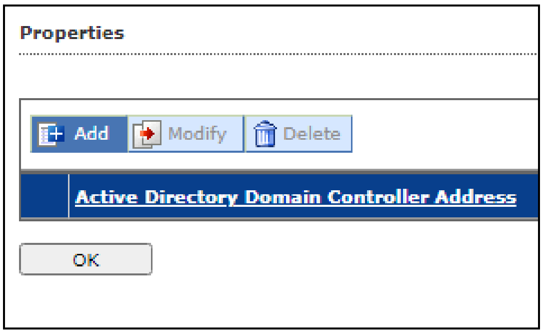
Adding an Active Directory

To add an Active Directory, follow the steps given below:

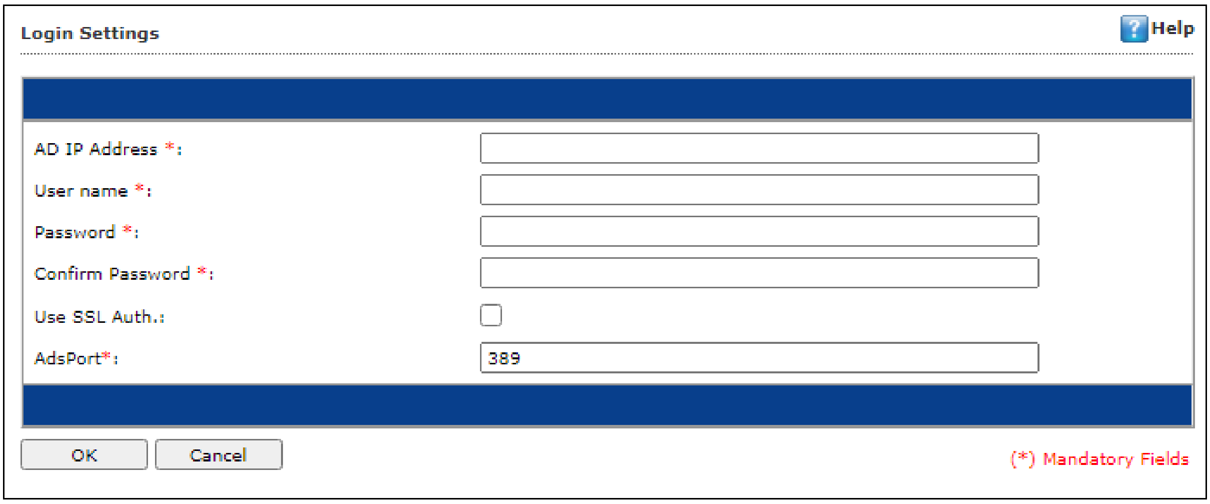
1. Click **Unmanaged Computers** > **Active Directory**.
2. Click **Properties**.



Properties window appears.



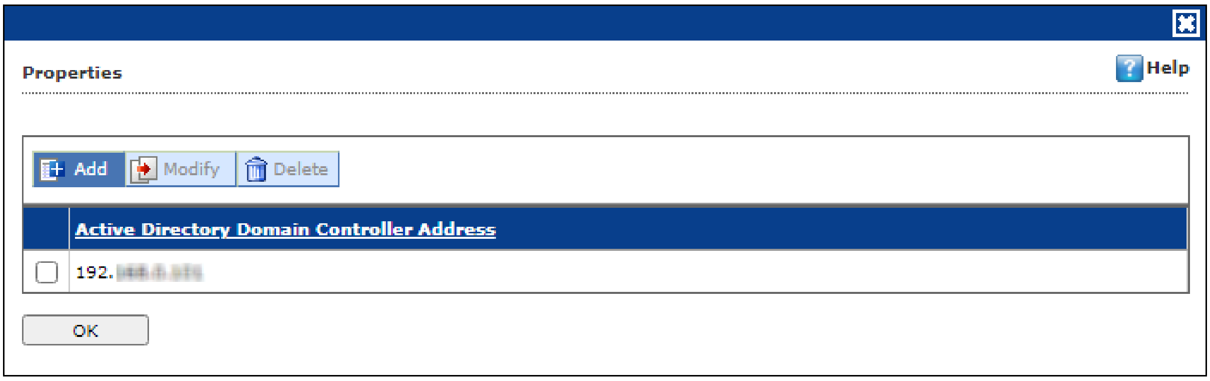
3. Click **Add**.
   Login Settings window appears.



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

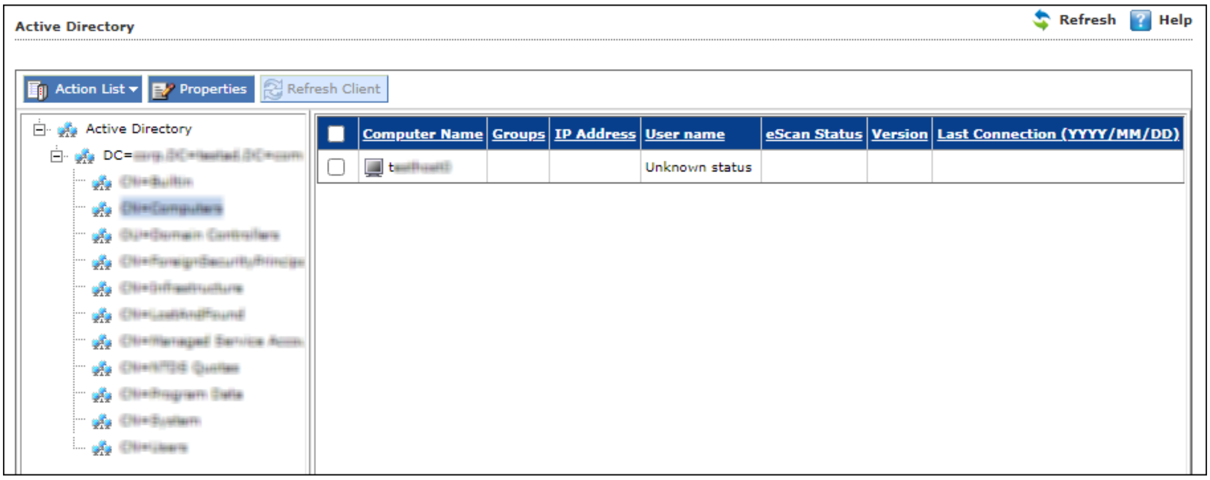
Help

Add | Modify | Delete

	Active Directory Domain Controller Address
□	192.[redacted]

OK

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

Refresh Help

Action List ▾ | Properties | Refresh Client

Active Directory
DC=[redacted]
[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

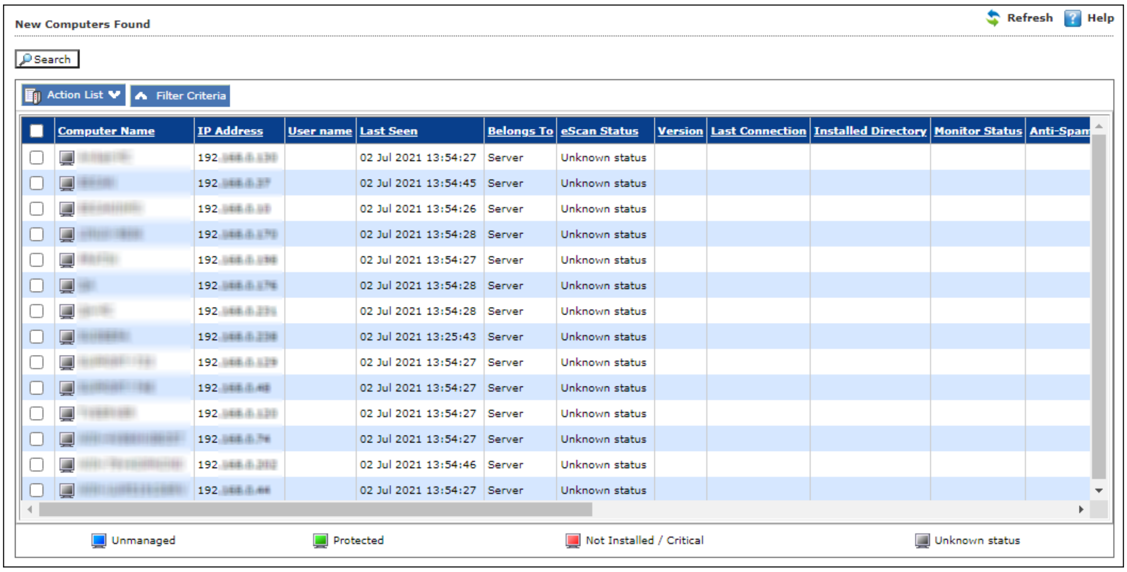
To move computers from an Active Directory, follow the steps given below:

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 it tasks, Set host configuration, Manage Policies, Deploy/Upgrade Client or deploy a Hotfix on all or any of the Managed Computer individually or in group.

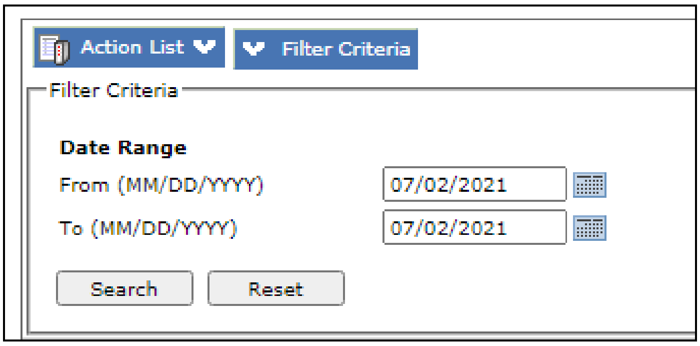


□	Computer Name	IP Address	User name	Last Seen	Belongs To	eScan Status	Version	Last Connection	Installed Directory	Monitor Status	Anti-Spam
□	[redacted]	192.[redacted]		02 Jul 2021 13:54:27	Server	Unknown status					
□	[redacted]	192.[redacted]		02 Jul 2021 13:54:45	Server	Unknown status					
□	[redacted]	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.



Filter Criteria

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

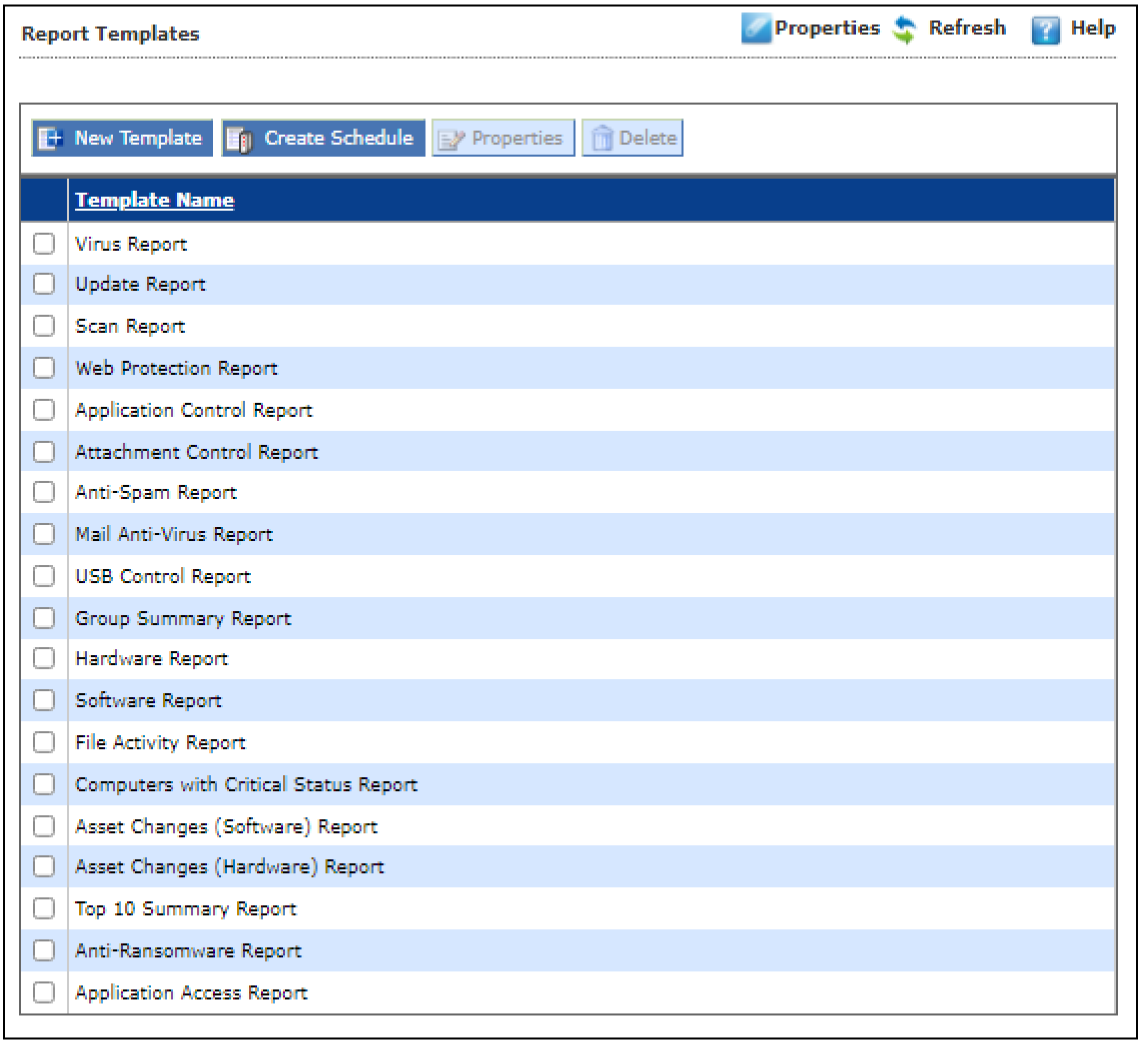
This drop-down provides following options:

- **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.

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.

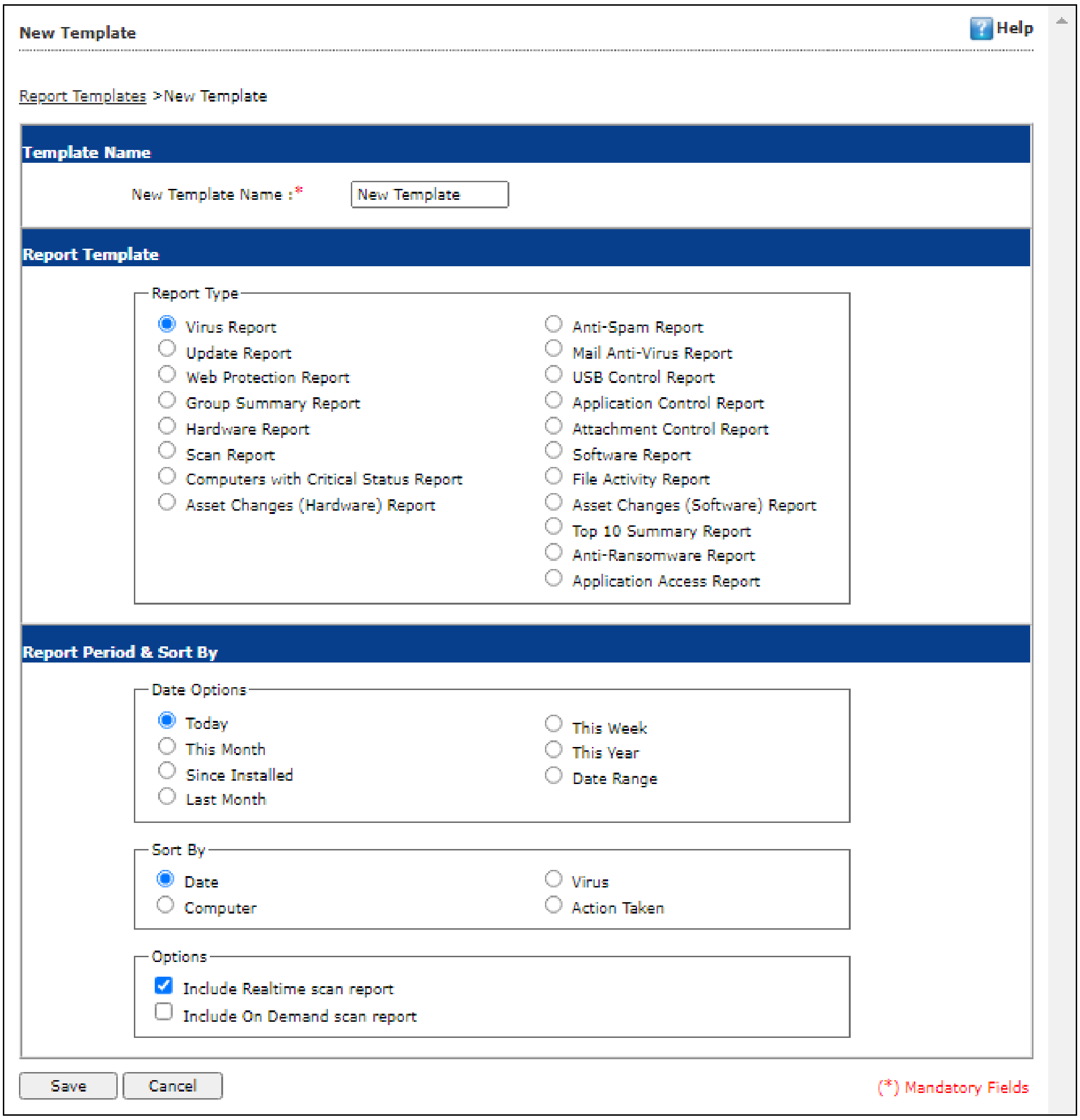


	Template Name
□	Virus Report
□	Update Report
□	Scan Report
□	Web Protection Report
□	Application Control Report
□	Attachment Control Report
□	Anti-Spam Report
□	Mail Anti-Virus Report
□	USB Control Report
□	Group Summary Report
□	Hardware Report
□	Software Report
□	File Activity Report
□	Computers with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

Creating a Report Template

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

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



New Template

Report Templates >New Template

Template Name

New Template Name :* 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
- ○ 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

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

- ☑ Include Realtime scan report
- □ Include On Demand scan report

(*) 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.

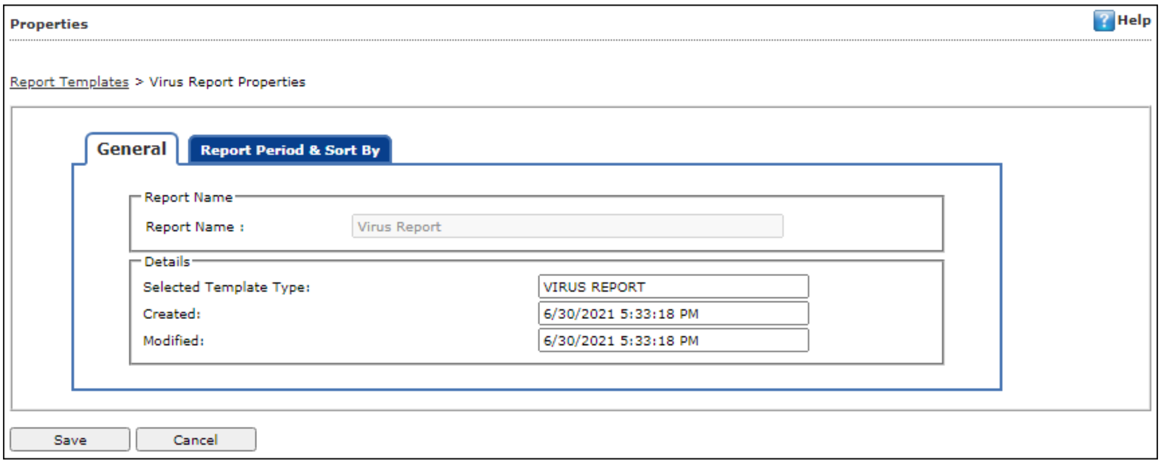
Creating Schedule for a Report Template

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.



Properties

Report Templates > Virus Report Properties

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.

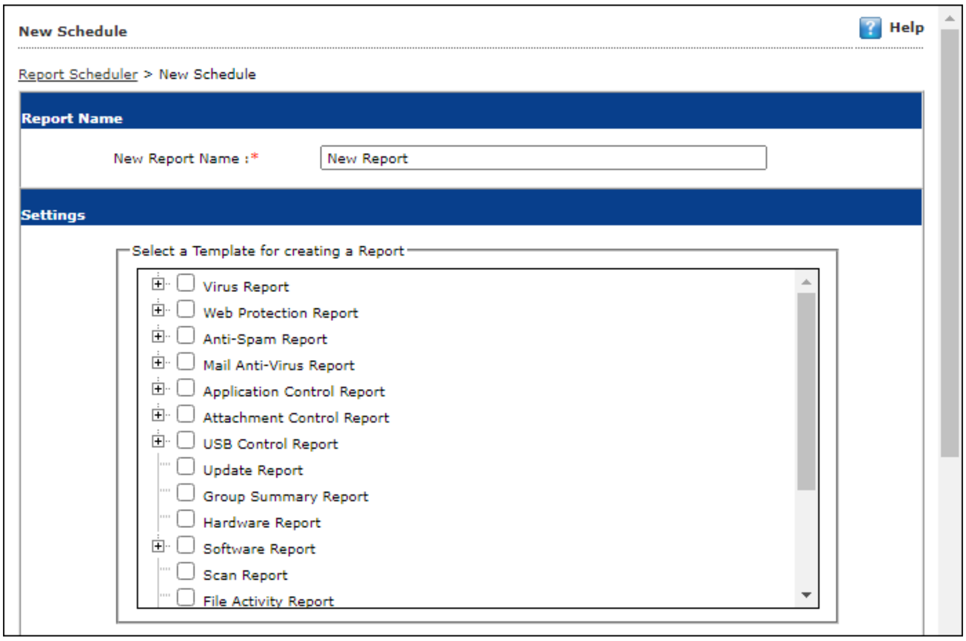
Report Scheduler

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

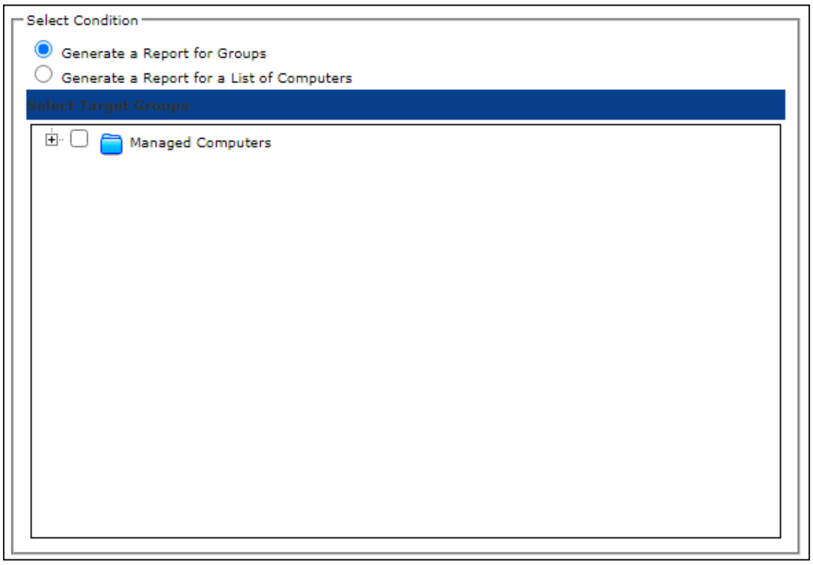
New Report Name :* New Report

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
- ☐ Software Report
- ☐ Scan Report
- ☐ File Activity Report

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



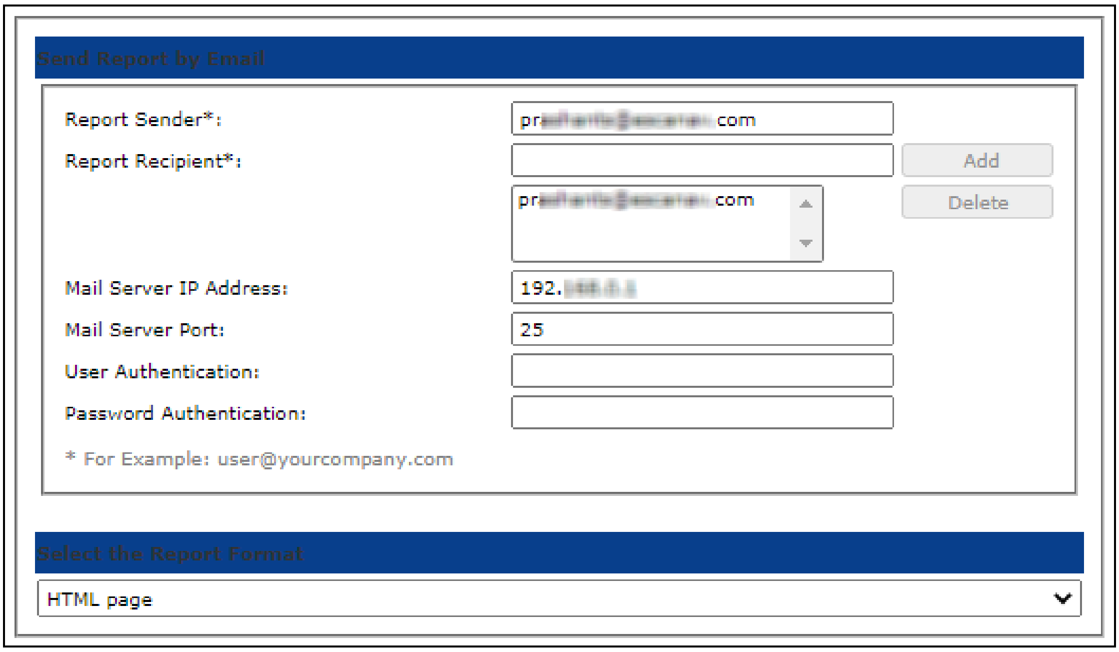
Select Condition

● 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:

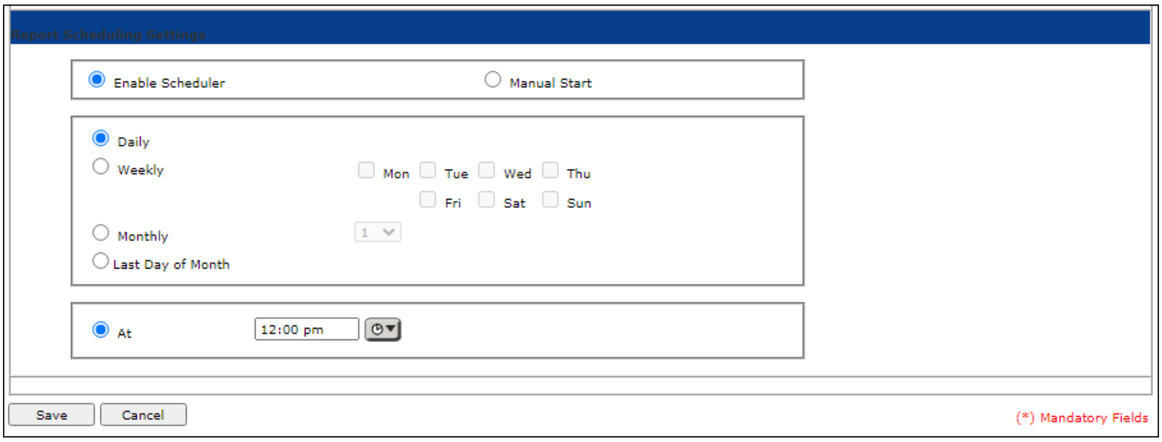
Password Authentication:

* 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

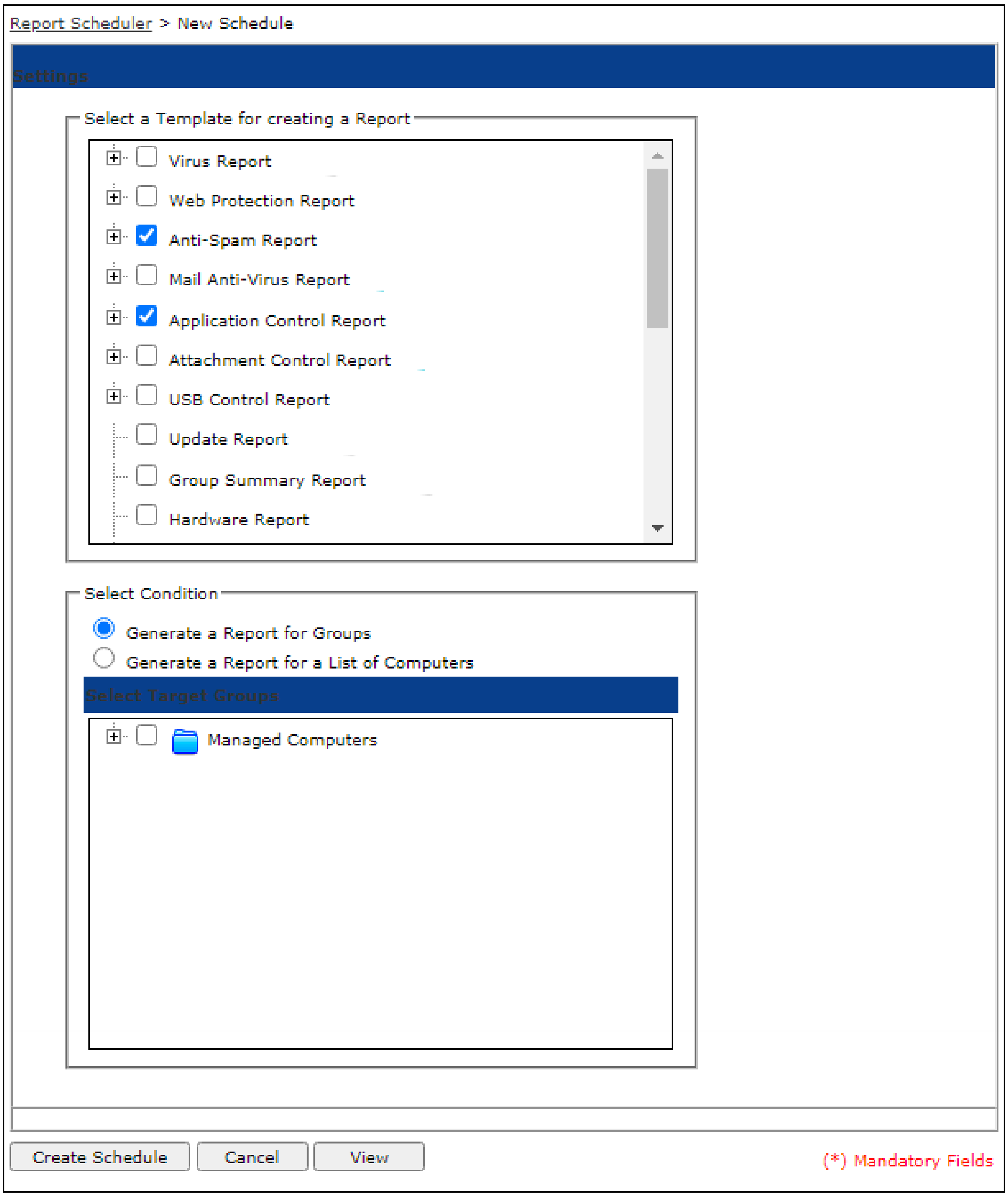
(*) Mandatory Fields

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

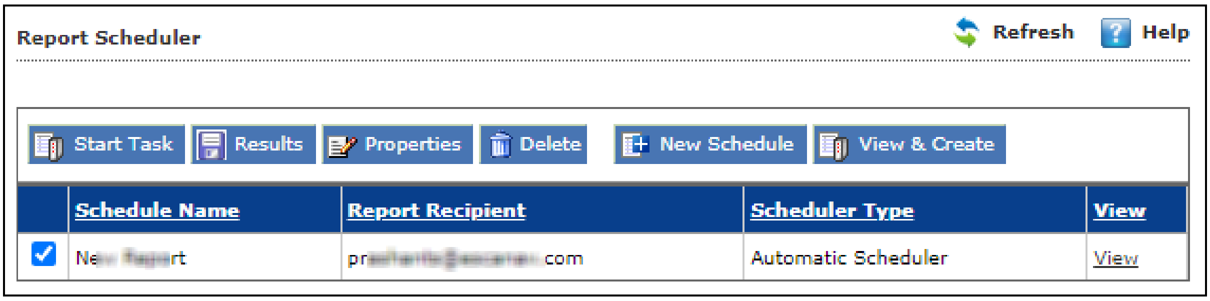
- □ Managed Computers

2. Select the **Template** options, the **Condition** and the **Target Groups**.
3. Click **View**.
   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

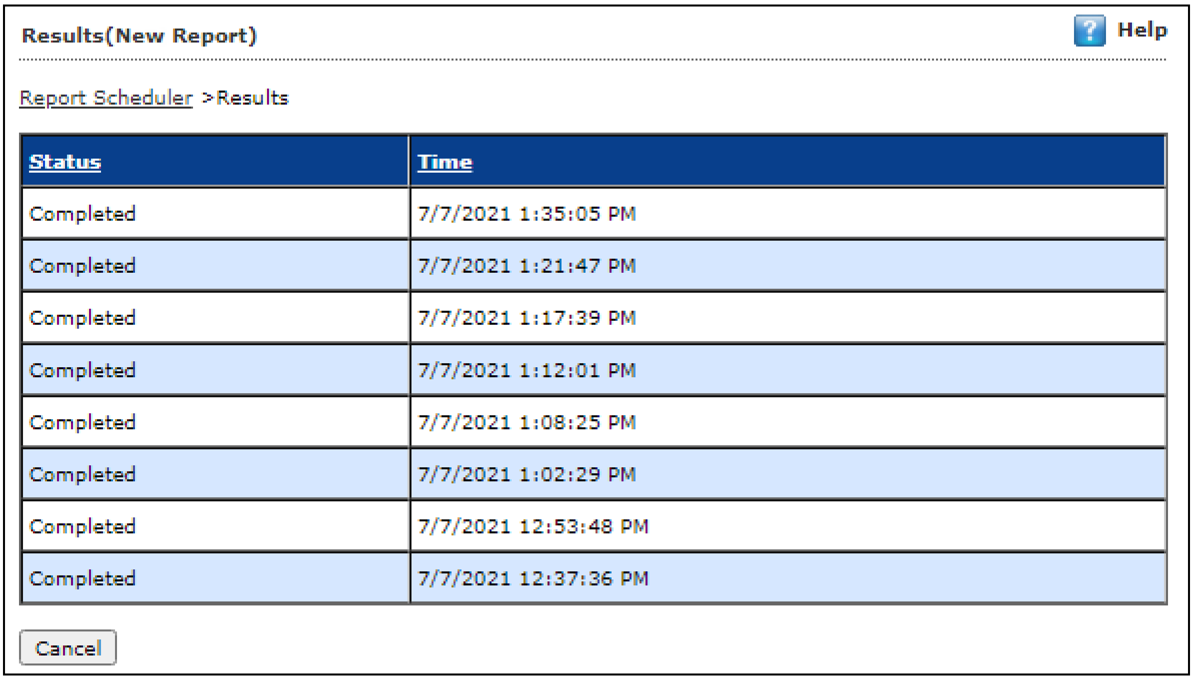
	Schedule Name	Report Recipient	Scheduler Type	View
☑	Ne[redacted]rt	pr[redacted]com	Automatic Scheduler	View

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(New Report)

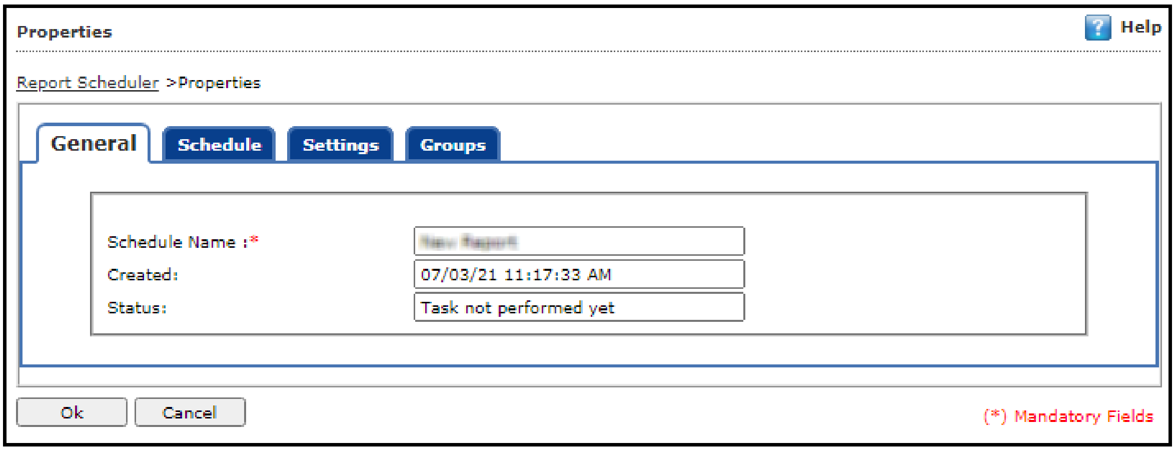
Report Scheduler >Results

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

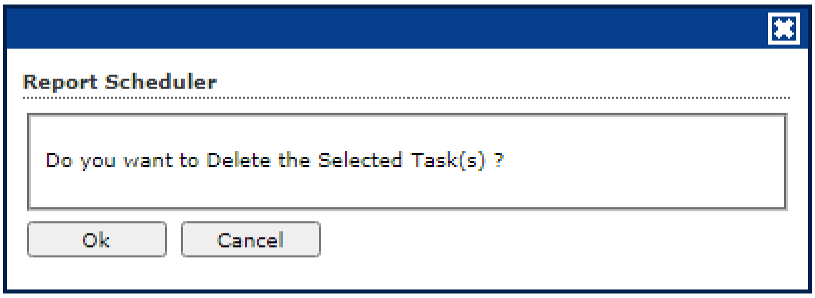
(*) Mandatory Fields

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

Deleting a Schedule

To delete a report schedule,

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

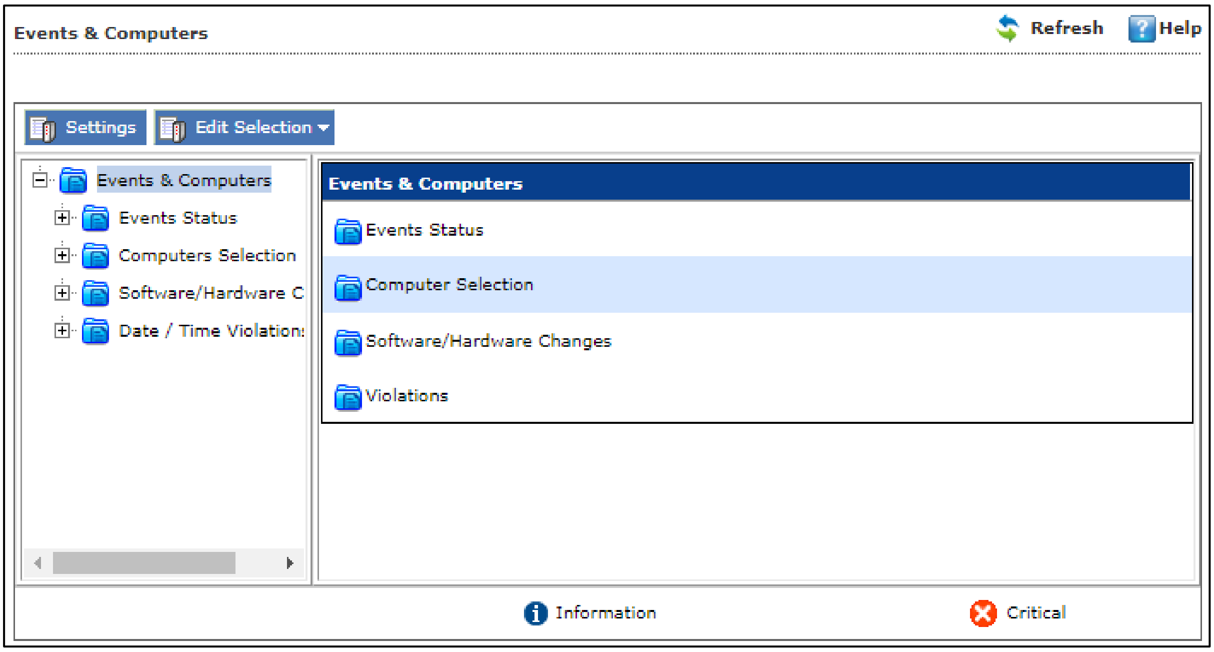


Do you want to Delete the Selected Task(s) ?

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; this module lets you sort the computer with specific properties.



Events Status

The Event Status subfolder is divided into following sections:

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

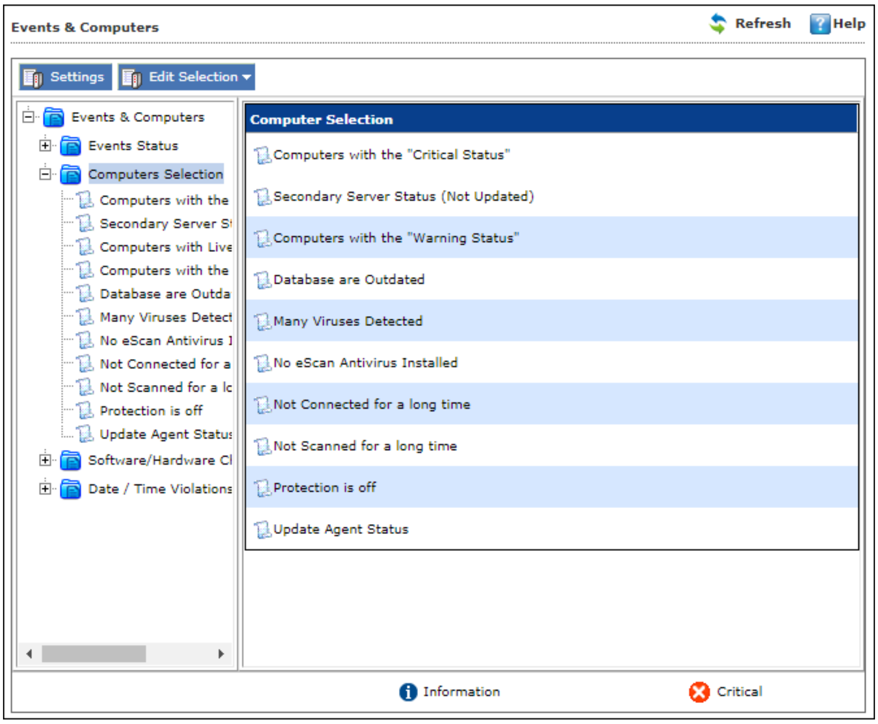
Recent
The Recent section displays both Information and Critical events.

Critical ☒
The Critical section displays Critical events and immediate attention.
For example, Virus detection, Monitor disabled.
The Critical events can be filtered on the basis of date range and the report can be exported in .xls or .html format.

Information ⓘ
The Information section displays basic information events.
For example, Virus database update, Status.

Computer Selection

The Computer Selection subfolder displays computers that fall under different categories. It lets you select the computer and take the preferred action. You can also set the criteria for each section and sort the computer accordingly.



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 the critical status**
- **Secondary Server Status (Not Updated)**
- **Computers with Live Status**
- **Computer with warning status**
- **Database is outdated**
- **Many Viruses Detected**
- **No eScan Installed**
- **Not connected for a long time**
- **Not scanned for a long time**
- **Protection is off**
- **Update Agent Status**

Computers with the critical status

This section displays computers marked with Critical status.

Secondary Server Status (Not Updated)

A secondary server receives downloads from the primary server and further distributes to the client computers. If the secondary server is not updated, it will be mentioned in the log.

Computers with Live status

This section displays whether the computers present in the network are online or offline.

To get the details of the specific computers' status, select **Computers with Live Status** option. This will display the computers with default online status along with other details such as IP Address, Group, Description, and more. To display all the endpoints in the network, you can use filter options that filters based on **Status Type**.

After selecting the computer from the list, you can choose **System Action List** drop-down option from the top panel. This option allows you to perform specific set of actions on the selected endpoints.

❗ **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.

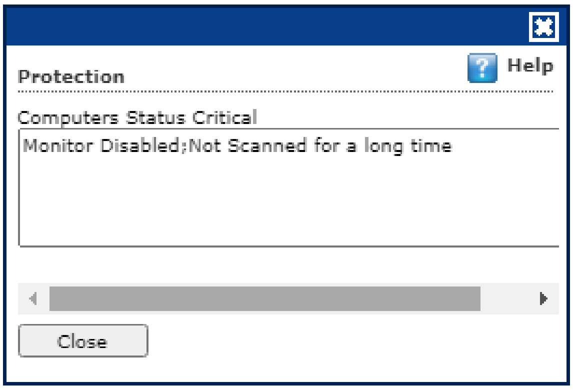
Update Agent Status
This section displays the status of computers assigned as Update Agent.

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.

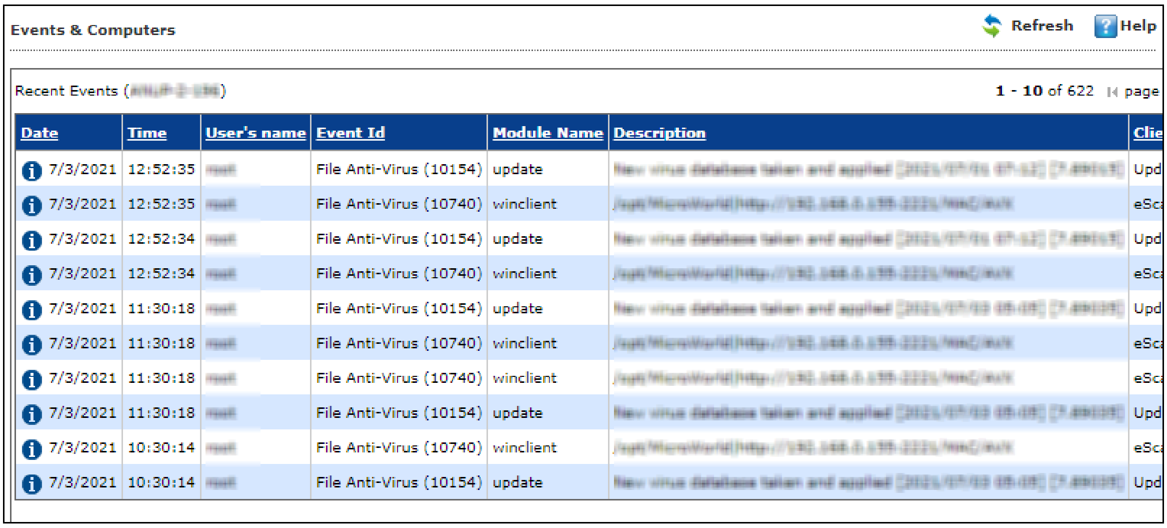


Protection

Computers Status Critical

Monitor Disabled;Not Scanned for a long time

- **Events**: This option displays the events that were performed in the particular computer.



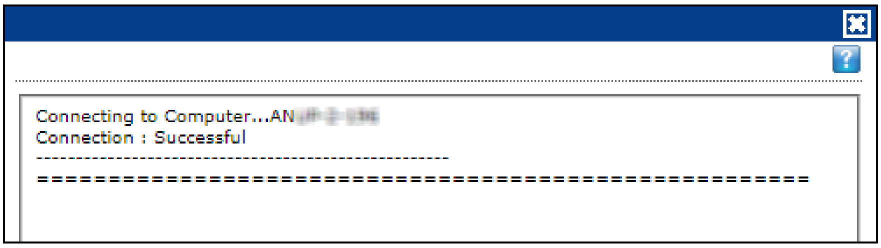
Events & Computers

Recent Events ([redacted])

1 - 10 of 622 page

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]	eSc
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]	eSc
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]	eSc
7/3/2021	11:30:18	[redacted]	File Anti-Virus (10740)	winclient	[redacted]	eSc
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]	eSc
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
---------------------------------------------------
================================================================
```

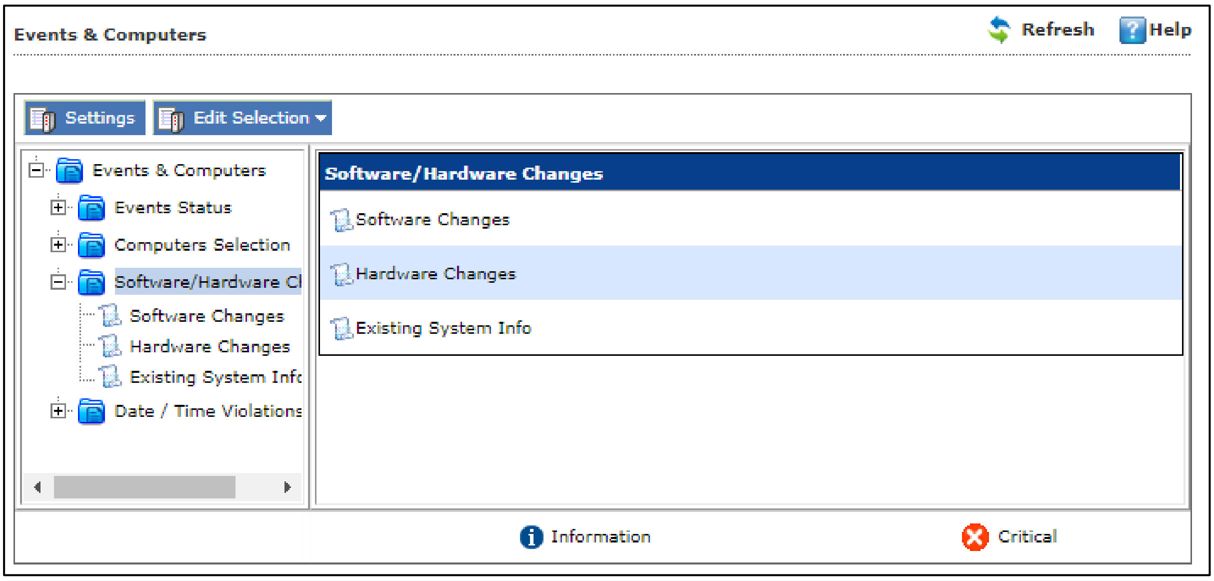
- **Remove from Group**: To learn about this option, click here.
- **Connect to Client (RMM)**: To learn about this option, click here.

- **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.

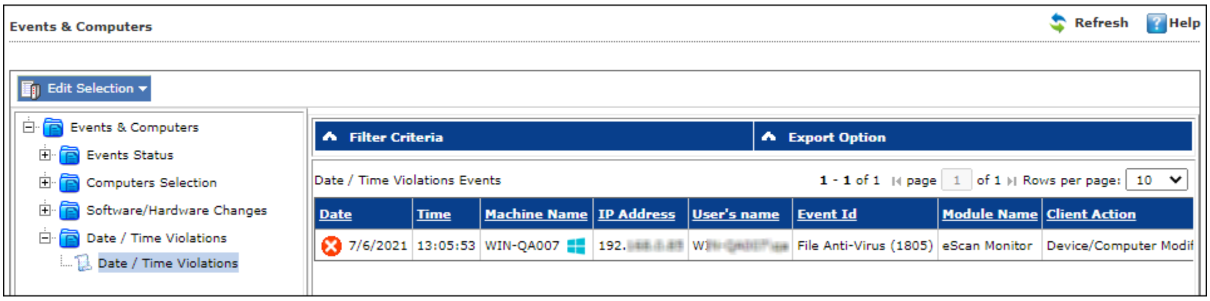
Existing System Info

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

Edit Selection

- Events & Computers
  - Events Status
  - Computers Selection
  - Software/Hardware Changes
  - Date / Time Violations
    - Date / Time Violations

Date / Time Violations Events — 1 - 1 of 1, page 1 of 1, Rows per page: 10

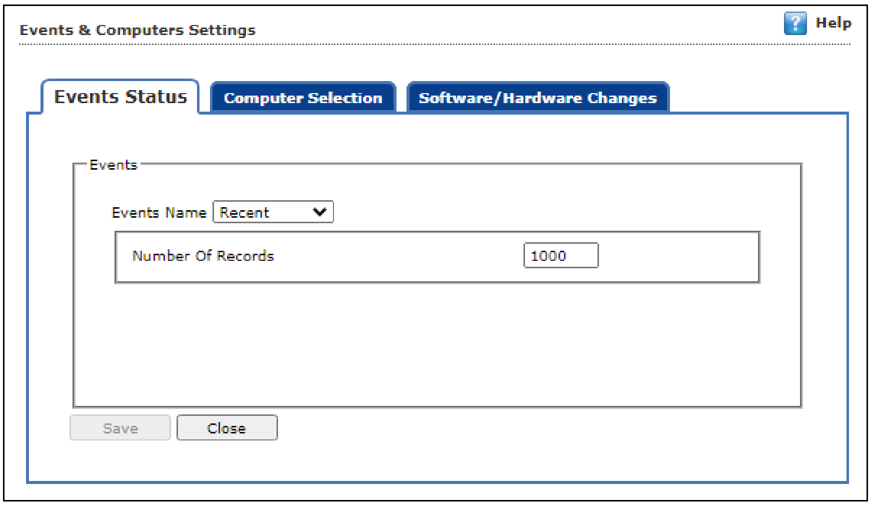
Date	Time	Machine Name	IP Address	User's name	Event Id	Module Name	Client Action
7/6/2021	13:05:53	WIN-QA007	192.[redacted]	W[redacted]	File Anti-Virus (1805)	eScan Monitor	Device/Computer Modif

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 Status | Computer Selection | Software/Hardware Changes

Events

Events Name: Recent

Number Of Records: 1000

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

- **Recent:** It displays both critical and information events that occurred recently on managed client computers.
- **Information:** It displays all informative types of events, such as virus database update, status, and so on.

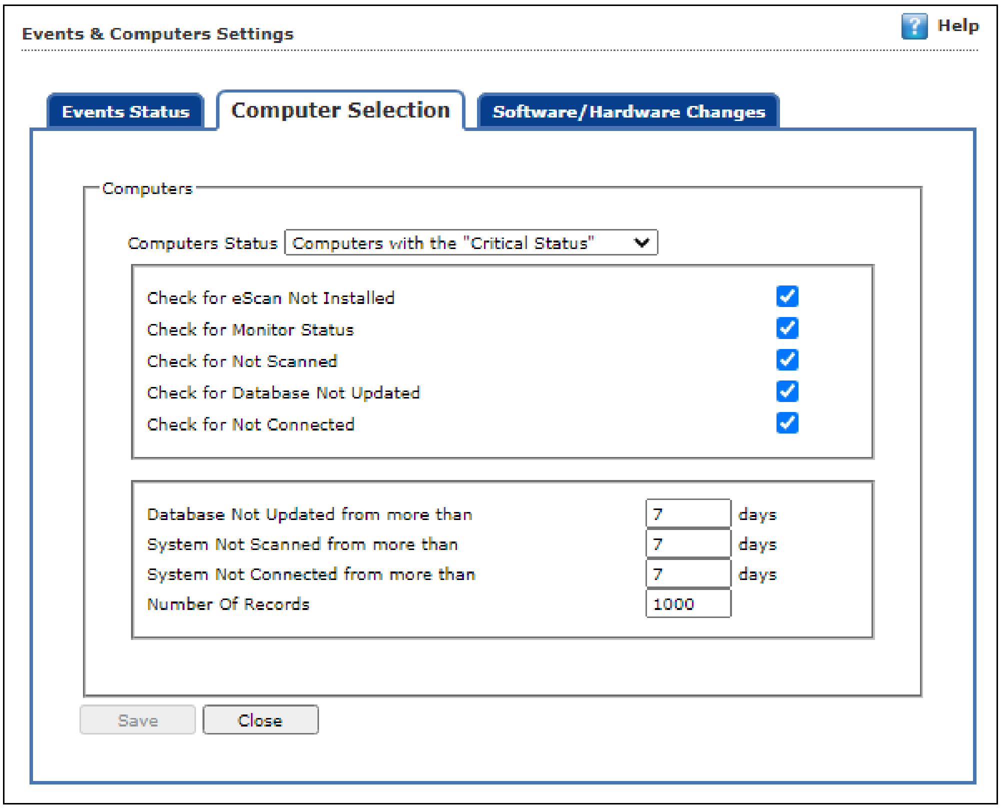
Steps to define event status settings:

Perform the following steps to save the event status settings:

1. Select the appropriate **Events Name**.
2. Enter the number of events that you want to view in a list, in the **Number of Records** field.

3. Click **Save**.
   The settings get saved.

Computer Selection



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 do the following activities:

Critical Status: It displays a list of computers that are critical in status, as per the criteria's selected in computer settings. Specify the following field details.

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

- **System Not Connected for more than**: Enter the number of days from when the client system has not been connected to eScan server.
- **Number Of Records**: Enter the number of client systems that you want to view in the list.

Warning Status: It displays the list of systems which are warning in status, as per the criteria's selected in computer settings. Specify the following field details:

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

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

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

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

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

No eScan Antivirus Installed: It displays the list of systems on which eScan has not been installed. Specify the following field detail:

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

Not connected for a long time: It displays the list of systems which have not been connected to the server from a long time. Specify the following field detail:

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

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

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

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

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

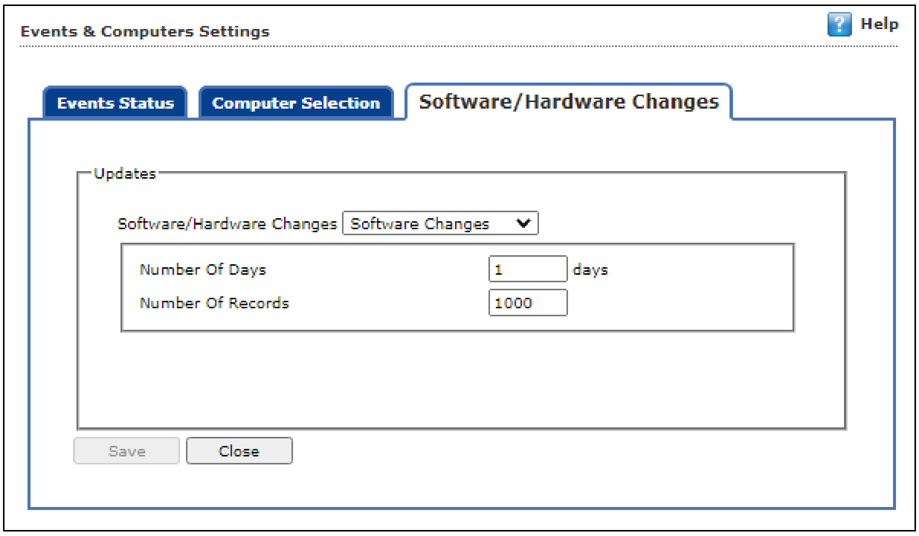
Steps to define computer settings

To save the computer settings, follow the steps given below:

1. Click **Computers Selection** tab.
2. Select a type of status for which you want to set criteria, from the **Computer status** drop-down.
3. Select the appropriate checkboxes, and then enter field details in the available fields. For more information, refer [Types and criteria of computer status] section.
4. Click **Save**.
   The settings will be saved.

Software/ Hardware Changes Setting

You can set these settings, if you want to get updates on any changes made in the software, hardware, and to existing system.



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.

Existing system info: It displays the list of existing systems on which software/hardware changes made for any module, as per the protection criteria's selected in computer settings. Specify the following field details.

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

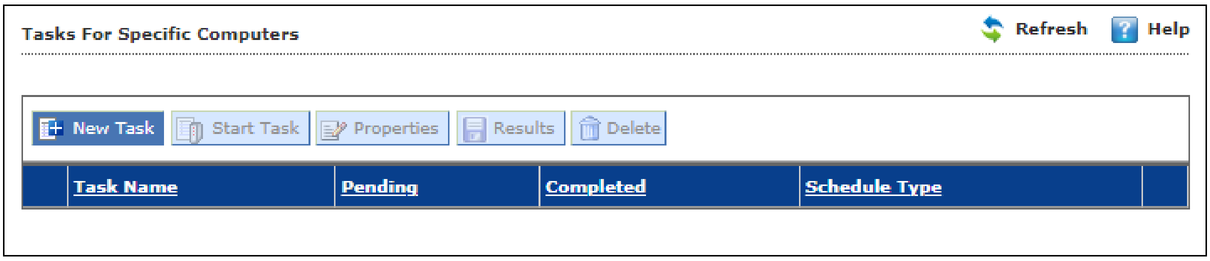
Performing an action for computer

To perform an action for a computer, follow the steps given below:

1. Select a computer.
2. Click **Edit Selection** drop-down. To learn more click here.
3. Click the preferred action.

Tasks for Specific Computers

The Tasks for Specific Computers module lets you create a new task for computer(s) according to your preferences.



Tasks For Specific Computers

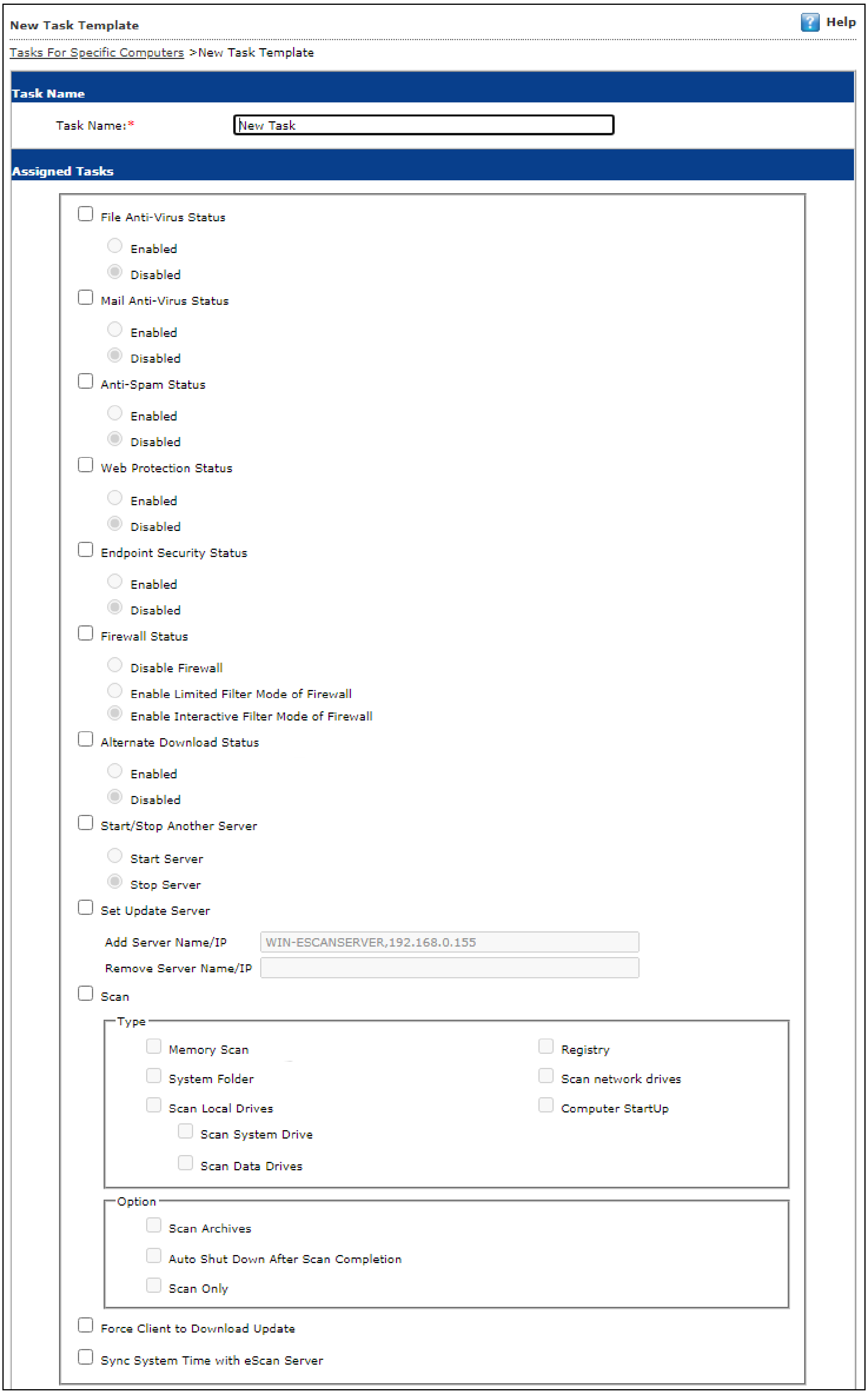
Task Name	Pending	Completed	Schedule Type

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

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

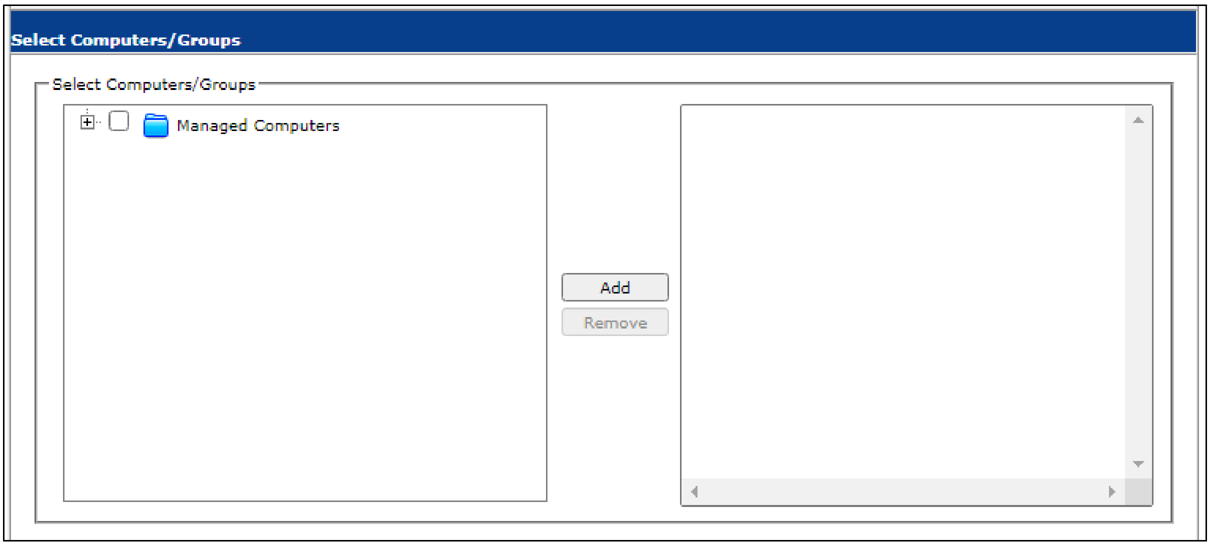
Type
- □ Memory Scan
- □ System Folder
- □ Scan Local Drives
  - □ Scan System Drive
  - □ Scan Data Drives
- □ Registry
- □ Scan network drives
- □ Computer StartUp

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

□ Force Client to Download Update

□ Sync System Time with eScan Server

3. Enter a name for task.
4. In the **Assigned Tasks** section, select the modules and scans 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**.

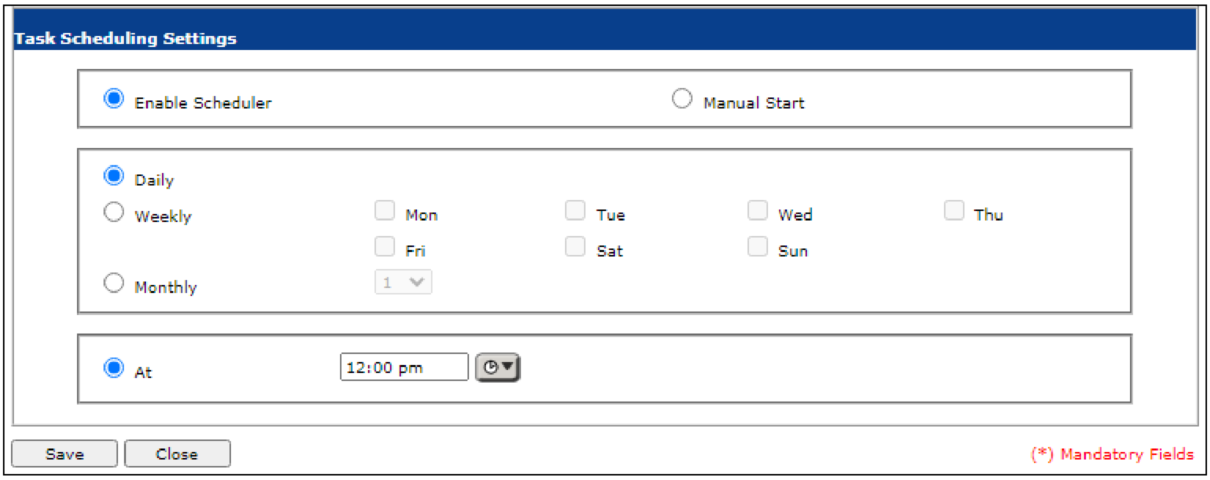


Select Computers/Groups

Select Computers/Groups

⊞ □ Managed Computers

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

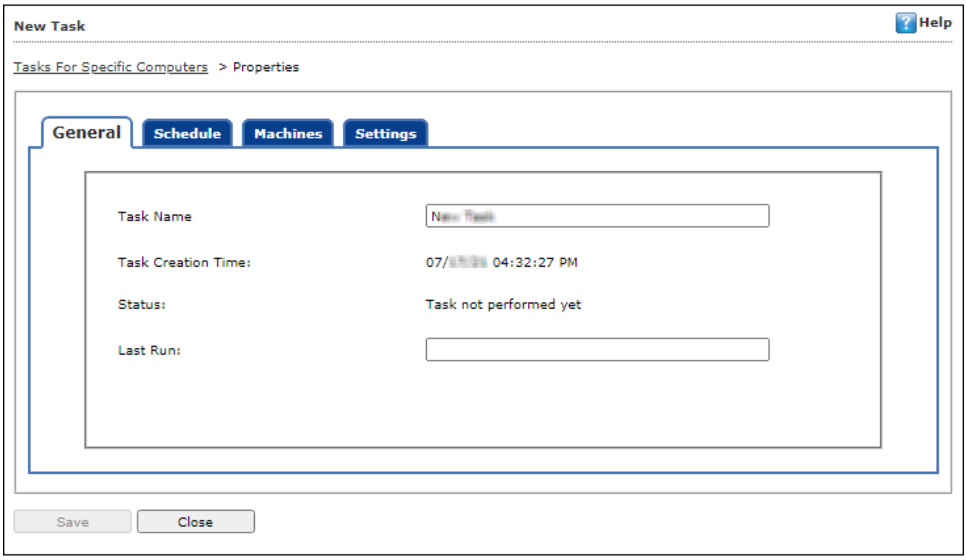
● At 12:00 pm

(*) Mandatory Fields

7. Click **Save**.
   The task will be saved and run for specific computers according to your preferences.

Viewing Properties of a task

To view Properties of a task, select the task and click **Properties**.



Task Name: New [redacted]

Task Creation Time: 07/[redacted] 04:32:27 PM

Status: Task not performed yet

Last Run:

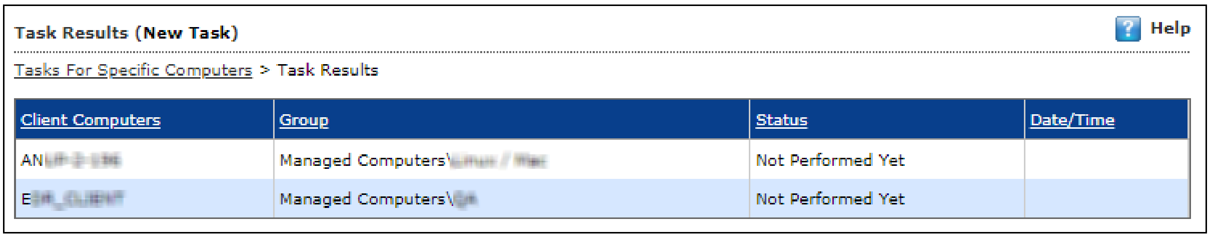
This section will have following tabs to configure:

- **General**: This tab will display details of the task created and provides details about the task name, task creation time, status, and last run.
- **Schedule**: This tab allows to change the scheduler setting for the particular task.
- **Machines**: This tab allows to add or remove the endpoints added to the particular task.
- **Settings**: This tab allows to modify or select the modules 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**.



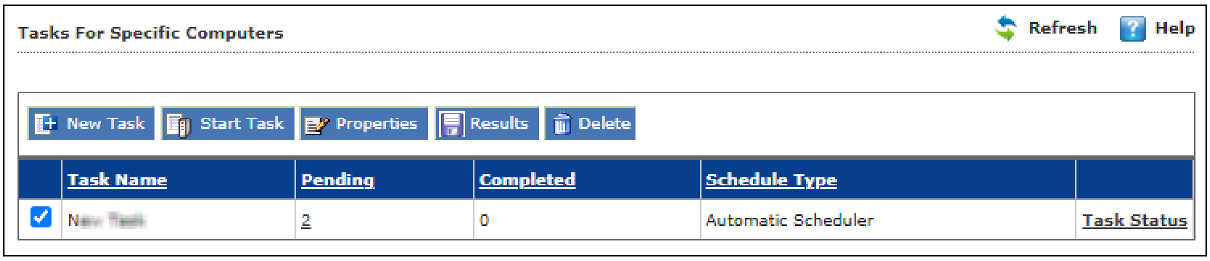
Client Computers	Group	Status	Date/Time
AN[redacted]	Managed Computers\[redacted]	Not Performed Yet	
E[redacted]	Managed Computers\[redacted]	Not Performed Yet	

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:

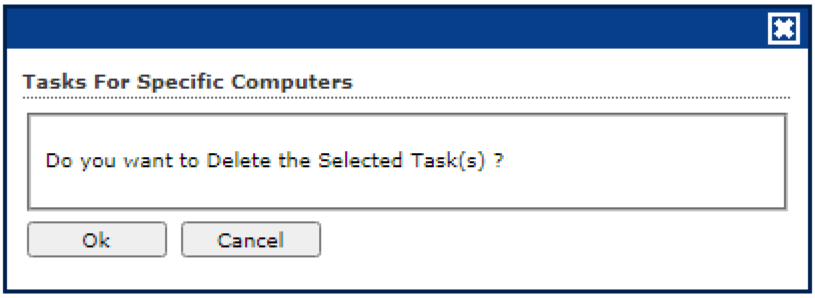
1. In the Tasks for Specific Computers screen, select the task you want to delete.



Tasks For Specific Computers

	Task Name	Pending	Completed	Schedule Type	
☑	[redacted]	2	0	Automatic Scheduler	Task Status

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



Tasks For Specific Computers

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

3. Click **OK**.
   The task will be deleted.

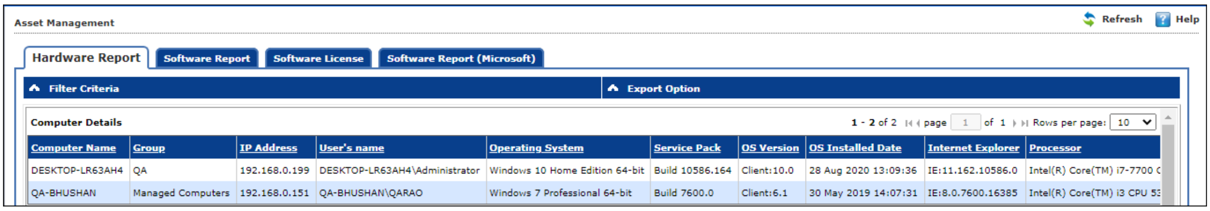
Asset Management

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 - 2 of 2 page 1 of 1 Rows per page: 10

Computer Name	Group	IP Address	User's name	Operating System	Service Pack	OS Version	OS Installed Date	Internet Explorer	Processor
DESKTOP-LR63AH4	QA	192.168.0.199	DESKTOP-LR63AH4\Administrator	Windows 10 Home Edition 64-bit	Build 10586.164	Client:10.0	28 Aug 2020 13:09:36	IE:11.162.10586.0	Intel(R) Core(TM) i7-7700 C
QA-BHUSHAN	Managed Computers	192.168.0.151	QA-BHUSHAN\QARAO	Windows 7 Professional 64-bit	Build 7600.0	Client:6.1	30 May 2019 14:07:31	IE:8.0.7600.16385	Intel(R) Core(TM) i3 CPU 53

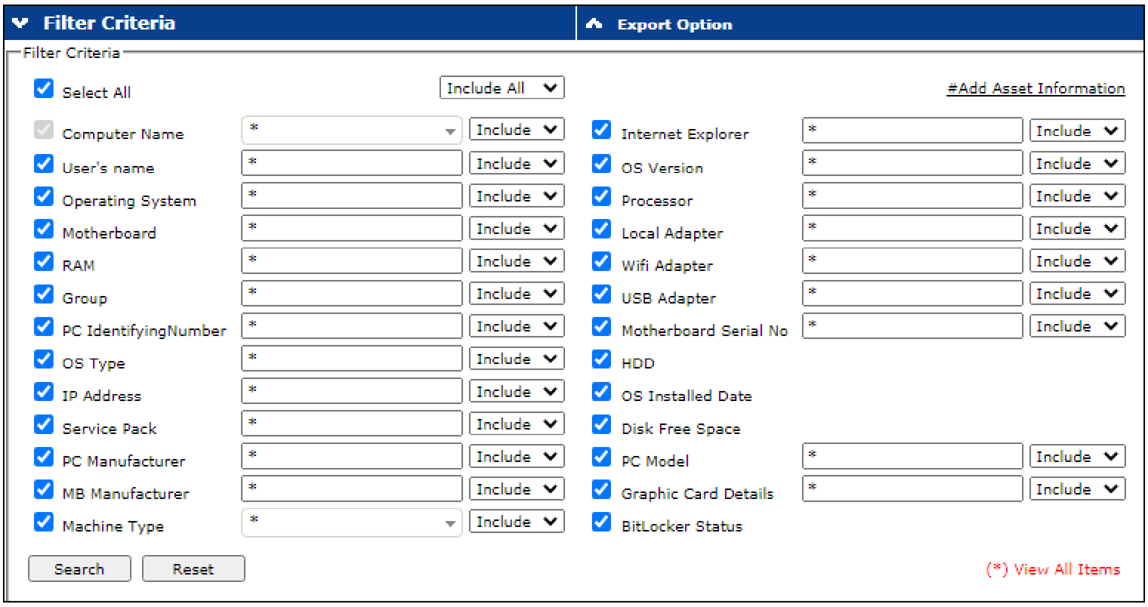
The tab displays following details of managed computers:

- Computer Name
- Group
- IP Address
- User name
- Operating System
- Service Pack
- OS Version
- OS Installed Date
- Internet Explorer
- Processor
- Motherboard
- RAM
- HDD
- PC Identifying Number
- Motherboard Serial No
- Network Speed
- Disk Free Space
- PC Manufacturer
- PC Model
- MB Manufacturer
- Graphic Card Details
- Machine Type
- BitLocker Status
- Software

To view the list of Software along with the installation dates, click **View** in **Software** column.

Filtering Hardware Report

To filter the Hardware Report as per your requirements, click **Filter Criteria** field.
Filter Criteria field expands.



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.

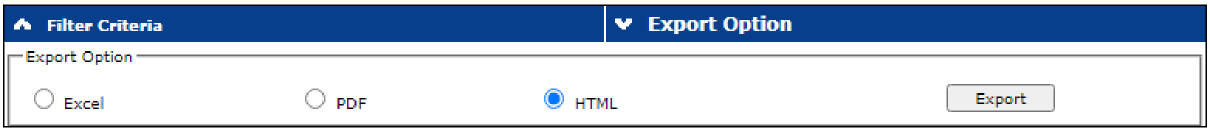
Include/Exclude
Selecting **Include/Exclude** for a parameter lets you include or exclude it from the report.

After making the necessary selections, click **Search.**
The Hardware Report will be filtered according to your preferences.

Reset all filter criteria in all field, click **Reset**.

Exporting Hardware Report

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

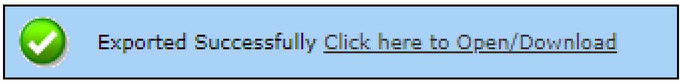


Filter Criteria | Export Option

Export Option

○ Excel ○ PDF ● HTML — Export

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

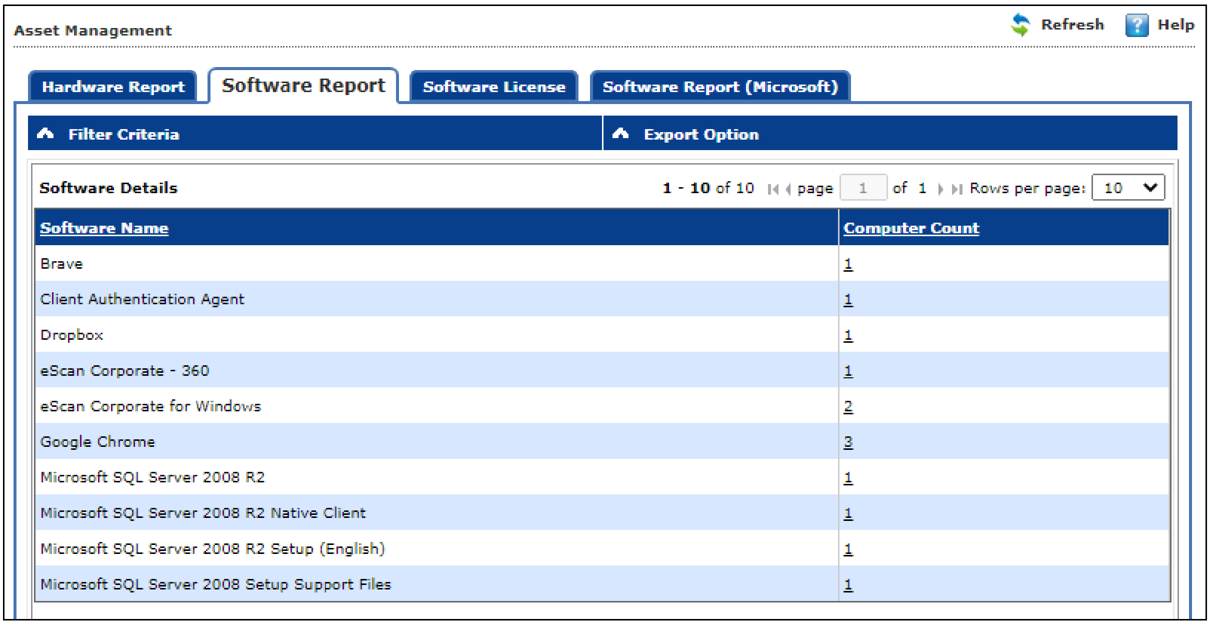


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Software Report

The Software Report tab displays list of Software along with the number of computers on which they are installed.



Software Name	Computer Count
Brave	1
Client Authentication Agent	1
Dropbox	1
eScan Corporate - 360	1
eScan Corporate for Windows	2
Google Chrome	3
Microsoft SQL Server 2008 R2	1
Microsoft SQL Server 2008 R2 Native Client	1
Microsoft SQL Server 2008 R2 Setup (English)	1
Microsoft SQL Server 2008 Setup Support Files	1

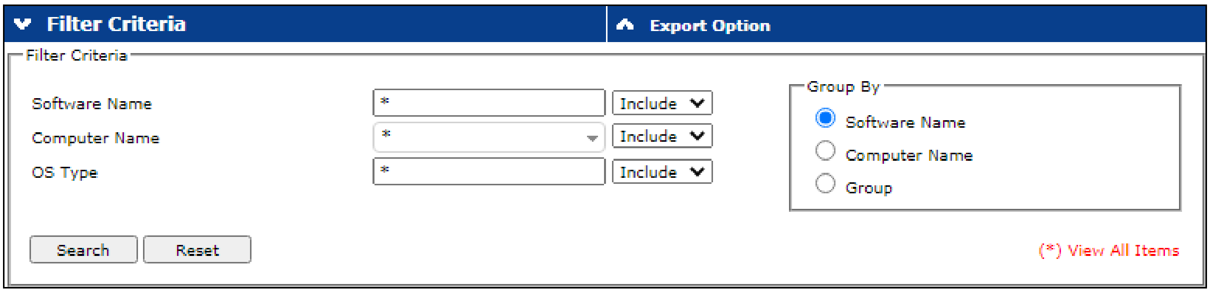
To view the computers on which the specific software is installed, click the numerical in Computer Count Column.

Computer list window appears displaying following details:

- Computer Name
- Group
- IP Address
- Operating System
- Software Version
- Installed Date

Filtering Software Report

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



Software Name: * 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

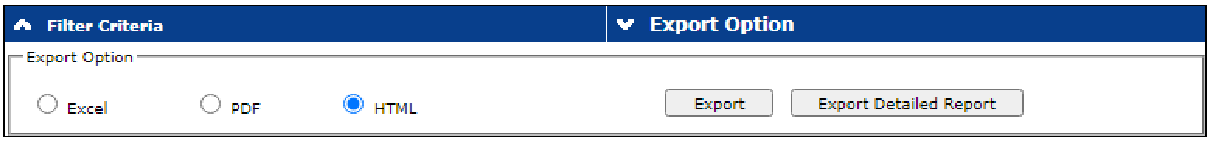
The results can be grouped by Software name, Computer name or Group.
If Group option is selected, the report can be filtered for a specific group.

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

Reset all filter criteria in all field, click **Reset**.

Exporting Software Report

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



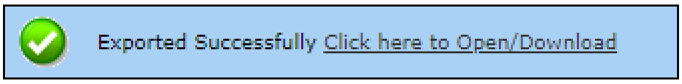
Export Option

○ 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.

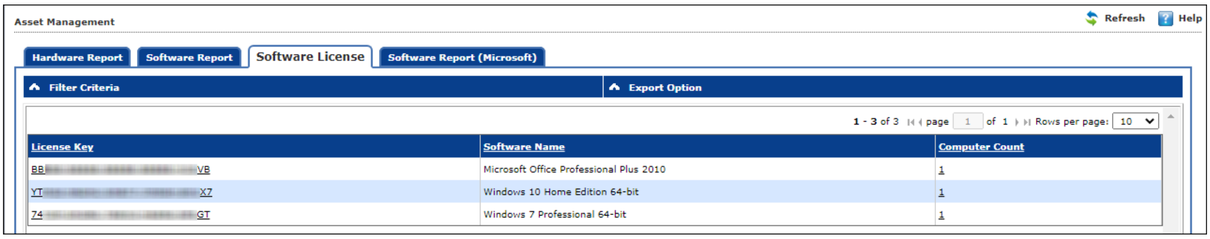


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Software License

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

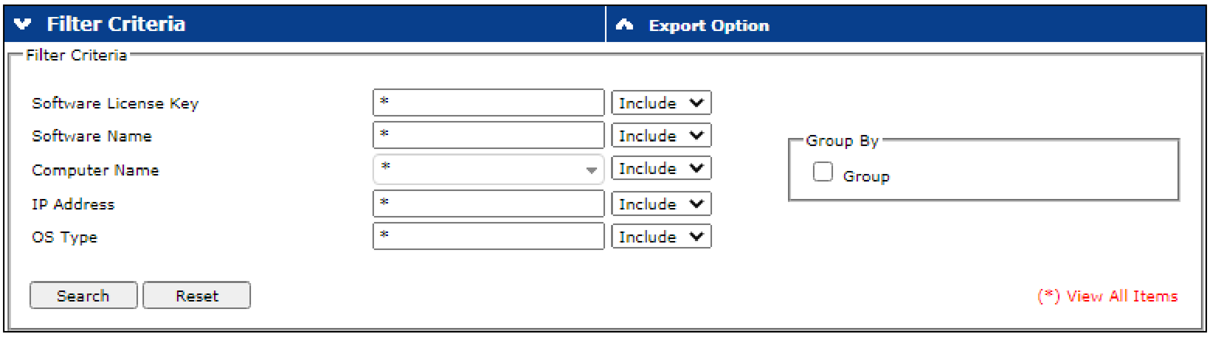


License Key	Software Name	Computer Count
BB[redacted]VB	Microsoft Office Professional Plus 2010	1
YT[redacted]X7	Windows 10 Home Edition 64-bit	1
74[redacted]GT	Windows 7 Professional 64-bit	1

The log displays License Key, Software Name and Computer Count.
To see more details of the computer's license key installed, click the numerical value in License Key or Computer Count column.

Filtering Software License Report

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



Software License Key	*	Include
Software Name	*	Include
Computer Name	*	Include
IP Address	*	Include
OS Type	*	Include

Software License Key
Entering the license key displays suggestions. Select the appropriate key.

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

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

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

OS Type
Enter the OS type.

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

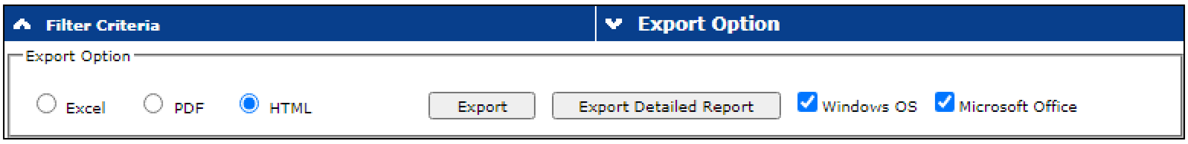
Group By
If Group option is selected, the report can be filtered for a specific group.

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

Reset all filter criteria in all the fields, click **Reset.**

Exporting Software License Report

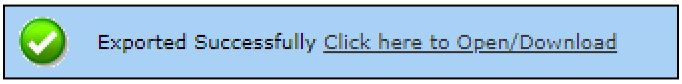
To export the Software License Report, click **Export Option**.
Export Option field expands.



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.

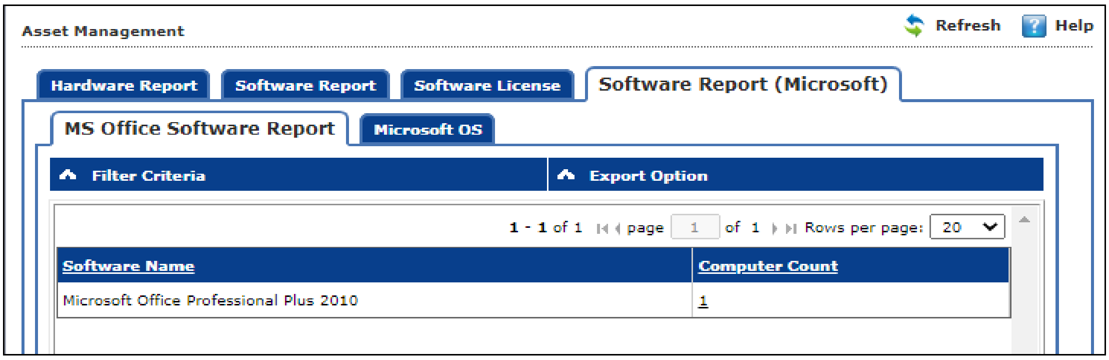


Exported Successfully Click here to Open/Download

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.



Software Name	Computer Count
Microsoft Office Professional Plus 2010	1

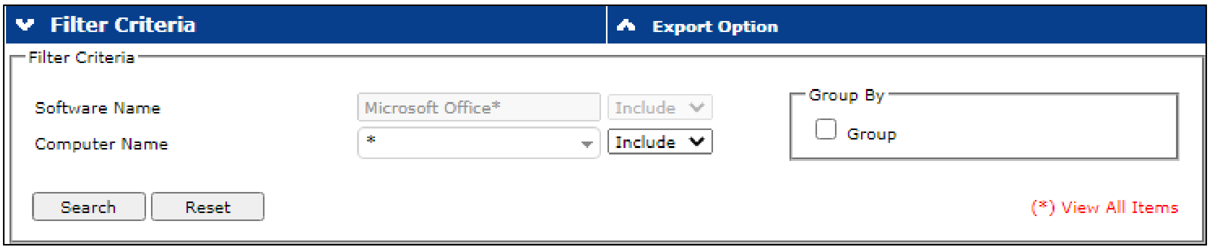
The tab consists following subtabs:

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.



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

Computer Name

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

Group By

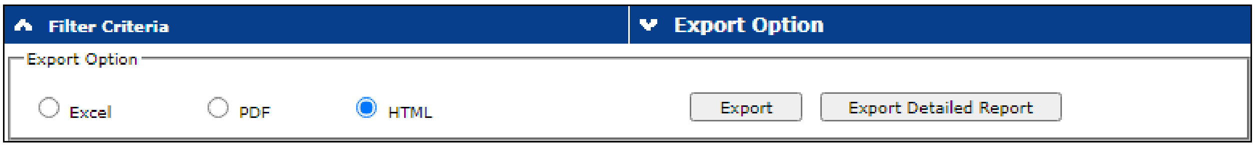
If this option is selected, the report can be filtered for a specific group.

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

Reset all filter criteria in all the fields, click **Reset.**

Exporting Software Report (Microsoft)

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



Filter Criteria | Export Option

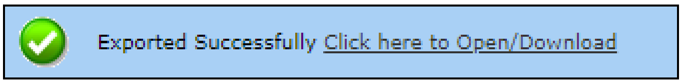
Export Option

○ Excel ○ PDF ● HTML

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.
A success message appears.

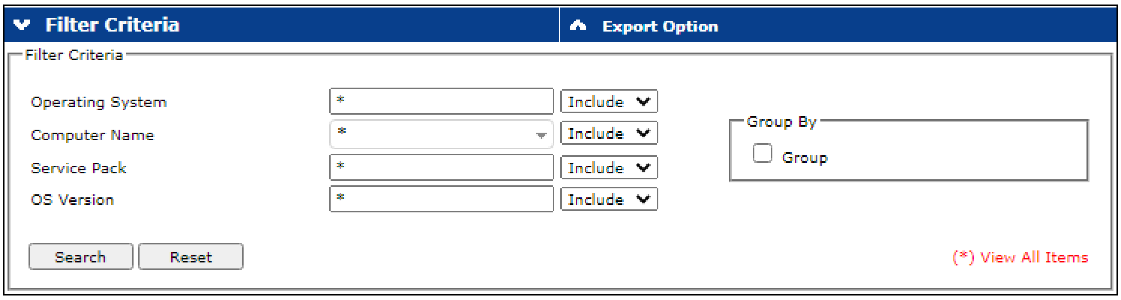


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Filtering Microsoft OS Report

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



Filter Criteria | Export Option

Filter Criteria

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

Group By

□ Group

Operating System
Entering the operating system name displays list of suggestions. Select the appropriate OS.

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

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

OS Version
Entering the OS version displays list of suggestions. Select the appropriate OS version.

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

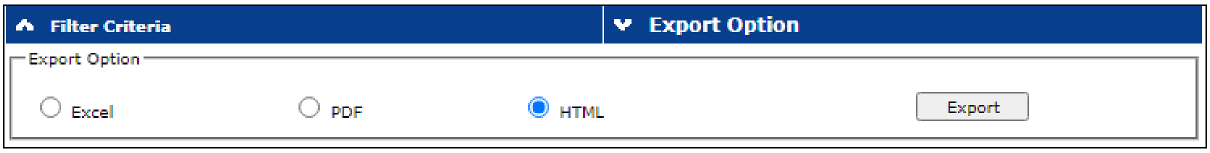
Group By
If **Group** option is selected, the report can be filtered for a specific group.

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

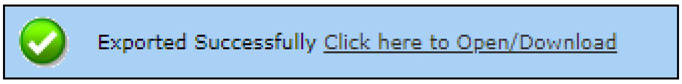
Reset all filter criteria in all the fields, click **Reset.**

Exporting Microsoft OS Report

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



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



Exported Successfully Click here to Open/Download

Click the link to open/download the file.

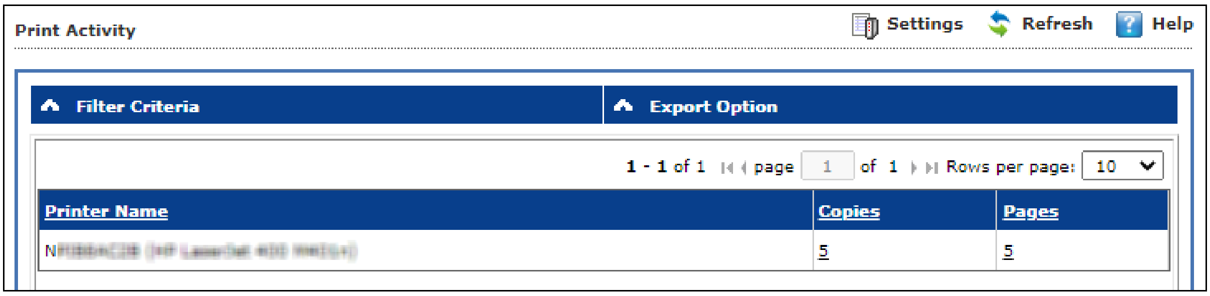
User Activity

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

- **Print Activity**
- **Session Activity**
- **File Activity**
- **Application Access Report**

Print Activity

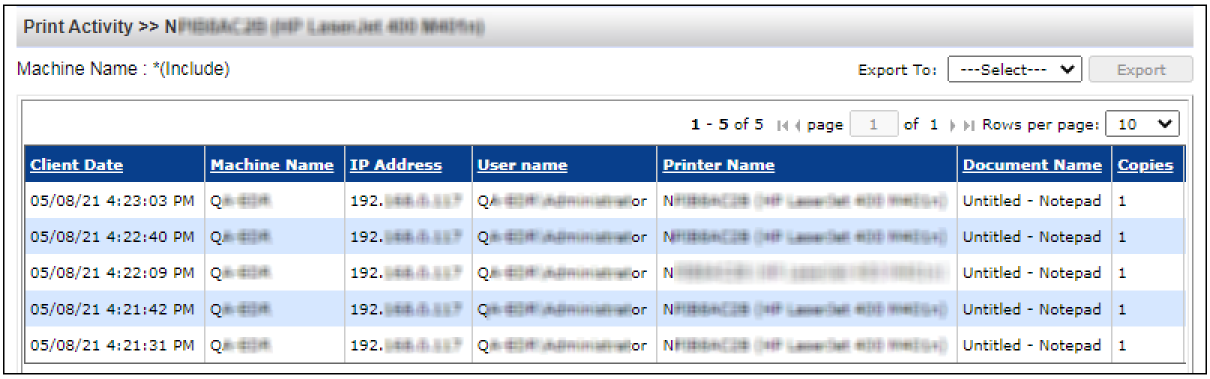
The Print Activity submodule monitors and logs print commands sent by all computers. It also lets you filter the logs on the basis of Computer name, Printer and Username. Furthermore, the module lets you export a detailed print activity report in XLS, PDF, and HTML formats. The log report generated consist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



Printer Name	Copies	Pages
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 details.



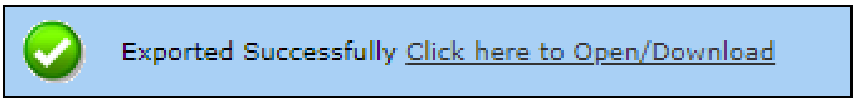
Machine Name : *(Include)

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.

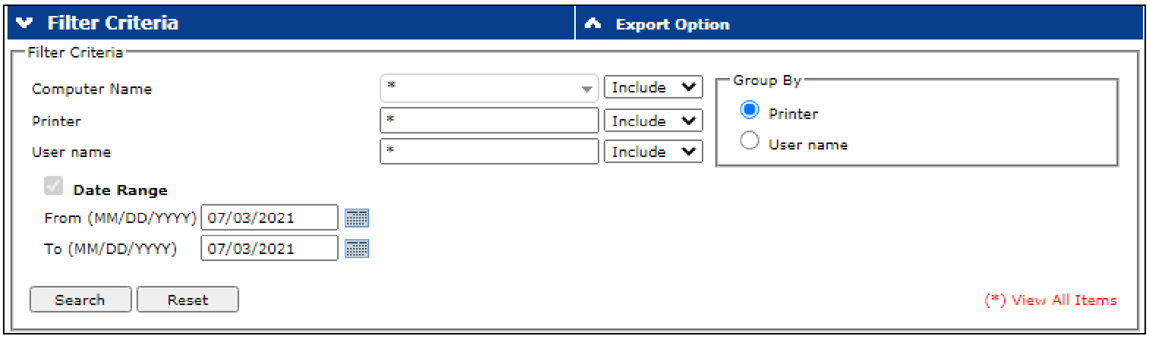


Exported Successfully Click here to Open/Download

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.

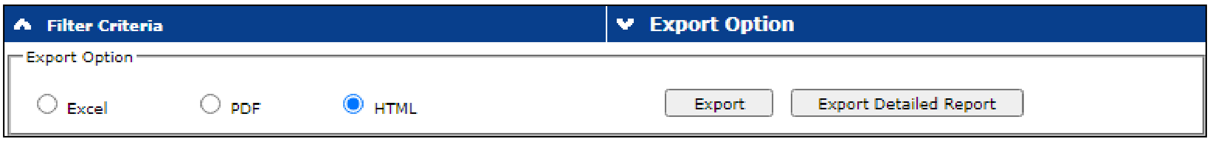
After filling all fields, click **Search**.
The Print activity log will be filtered and generated according to your preferences.

Reset all filter criteria fields, click **Reset.**

Group By
To view results by specific printer, select **Printer**, Date Range and then click **Search**.
To view results by specific user name, select **User name**, Date Range and then click **Search**.

Exporting Print Activity Report

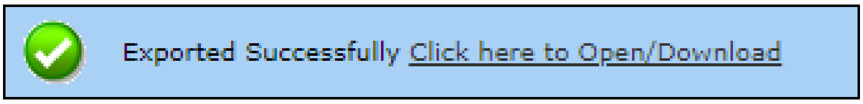
To export the generated log, click **Export Option**.
Export Option field expands.



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

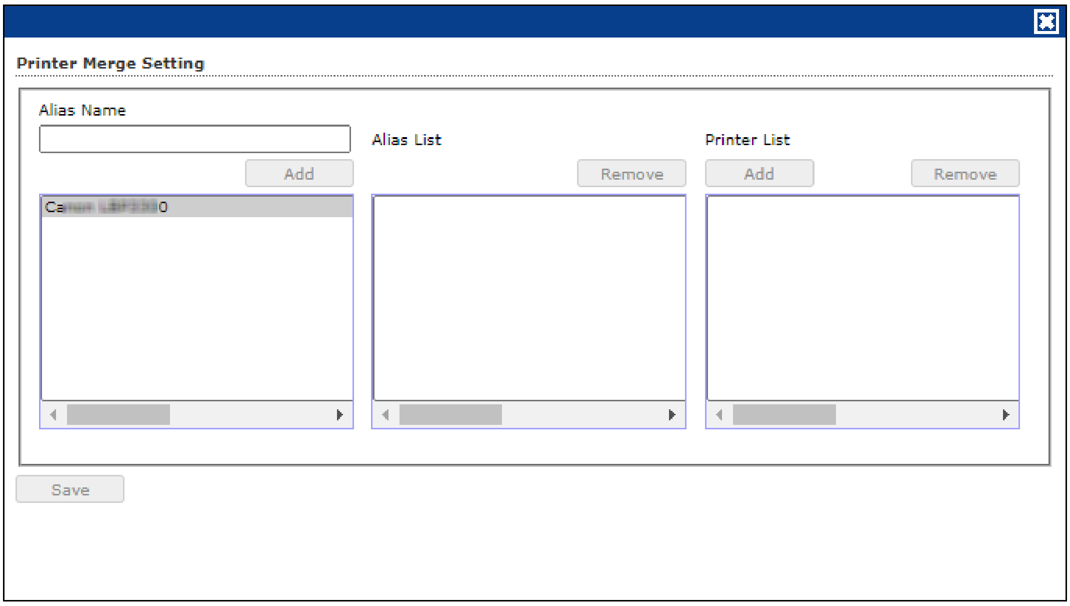
Click the link to open/download the file.

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.



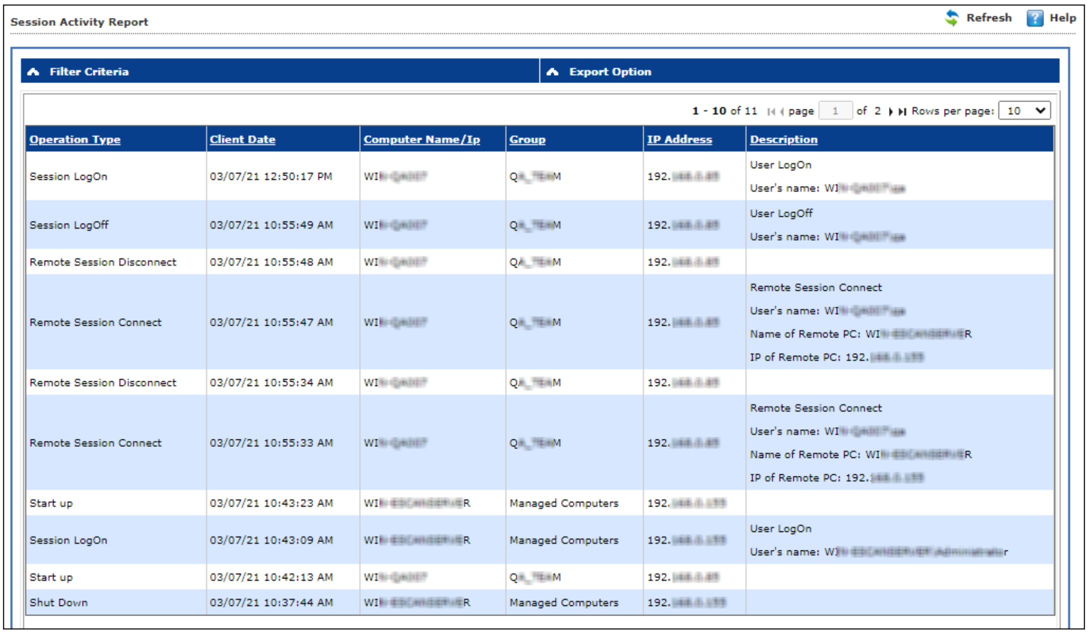
2. Enter name in Alias Name field.
3. Select printer(s) for the alias.
4. Click **Add**.
   The printer(s) will be added to the alias.
5. Click **Remove.**
   The printer(s) will be removed from the alias/printer list.
6. Click **Save**.
   The Print Activity Settings will be saved.

Session Activity Report

This 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

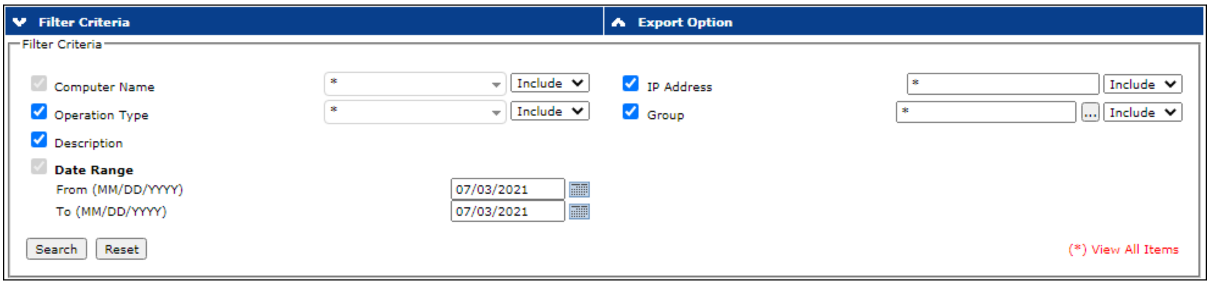
In the navigation panel, click **User Activity** > **Session Activity Report**.
The log displays list of session activities and type of operation performed. Options for Filtering or Exporting the log in desired formats are also present on the same interface.



Operation Type	Client Date	Computer Name/Ip	Group	IP Address	Description
Session LogOn	03/07/21 12:50:17 PM	WI[redacted]	Q[redacted]M	192.[redacted]	User LogOn User's name: WI[redacted]
Session LogOff	03/07/21 10:55:49 AM	WI[redacted]	Q[redacted]M	192.[redacted]	User LogOff User's name: WI[redacted]
Remote Session Disconnect	03/07/21 10:55:48 AM	WI[redacted]	Q[redacted]M	192.[redacted]	
Remote Session Connect	03/07/21 10:55:47 AM	WI[redacted]	Q[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]	Q[redacted]M	192.[redacted]	
Remote Session Connect	03/07/21 10:55:33 AM	WI[redacted]	Q[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: W[redacted]r
Start up	03/07/21 10:42:13 AM	WI[redacted]	Q[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	☑ IP Address	*	Include
☑ Operation Type	*	Include	☑ Group	*	Include
☑ Description					
☑ **Date Range**					
From (MM/DD/YYYY)	07/03/2021				
To (MM/DD/YYYY)	07/03/2021				

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.

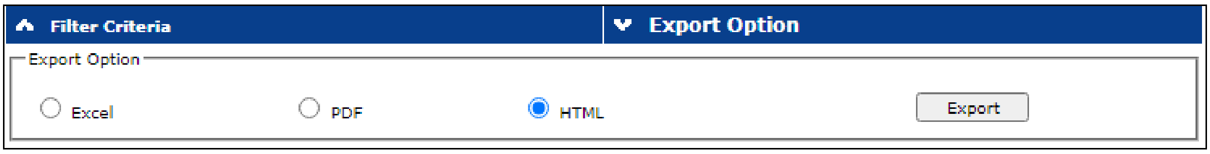
Group
Enter the group's name or click ... and select a group.

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**.
Reset all filter criteria fields, click **Reset.**

Exporting Session Activity Report

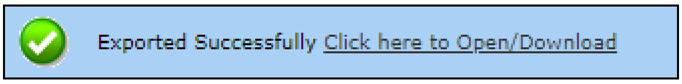
To export the generated log, click **Export Option**.
Export Option field expands.



Export Option

○ Excel ○ PDF ● HTML

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



Exported Successfully Click here to Open/Download

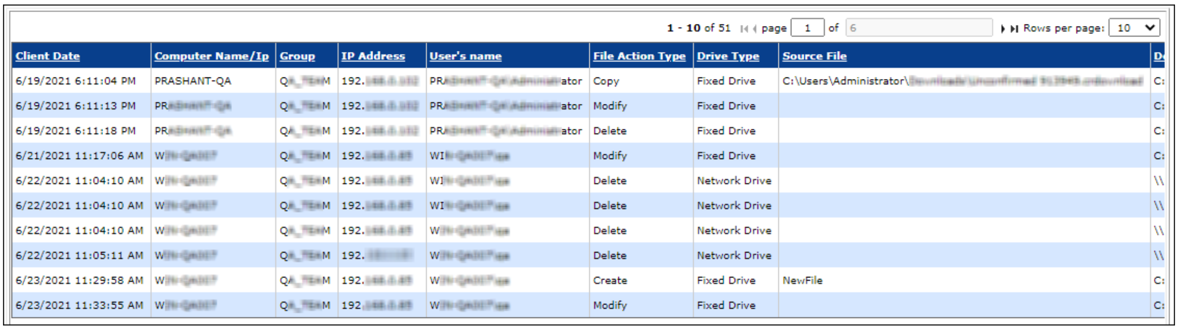
Click the link to open/download the file.

File Activity Report

The File Activity module displays a report of the files created, copied, modified, and deleted on managed computers. File Activity report will be generated when Record files copied is enabled in endpoint security. Additionally in case of a misuse of any official files can be tracked down to the user through the details captured in the report. Select and filter the report based on any of the details captured.

Viewing File Activity Log

In the navigation panel, click **User Activity** > **File Activity Report**.
The log displays list of files and the type of operation performed on them. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

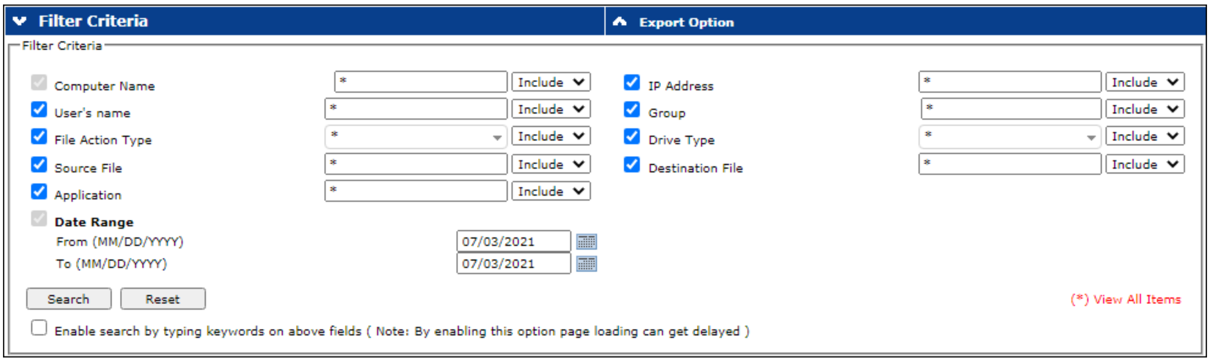


1 - 10 of 51 page 1 of 6 Rows per page: 10

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.



☑ 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

☐ 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.

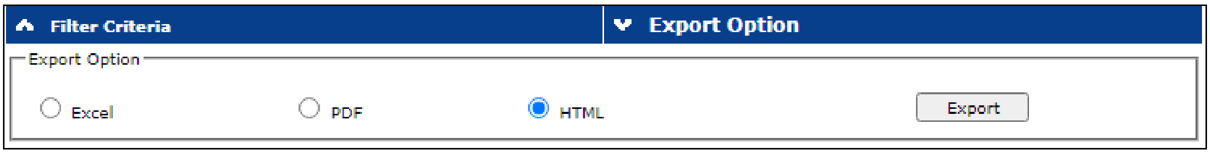
After filling all fields, click **Search**.
Reset all filter criteria fields, click **Reset.**

This checkbox **Enable search by typing keywords on above fields** allows you to search by typing keywords.

NOTE	Select **“Enable search by typing keywords on above fields”** option page loading can get delayed.

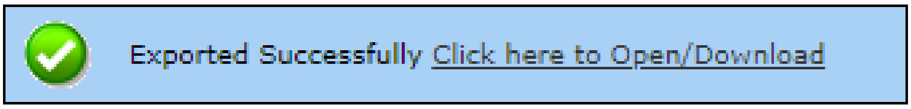
Exporting File activity Report

To export the generated 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

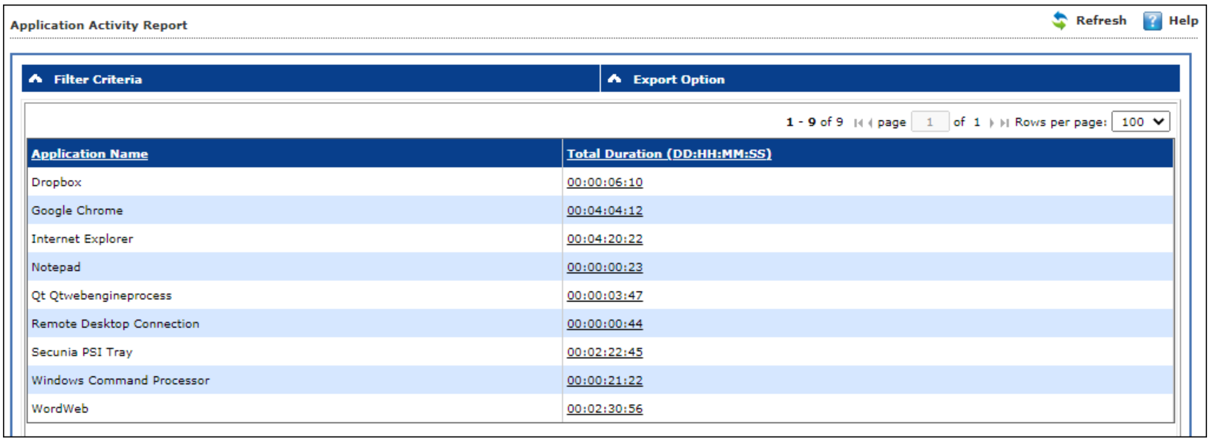
Click the link to open/download the file.

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

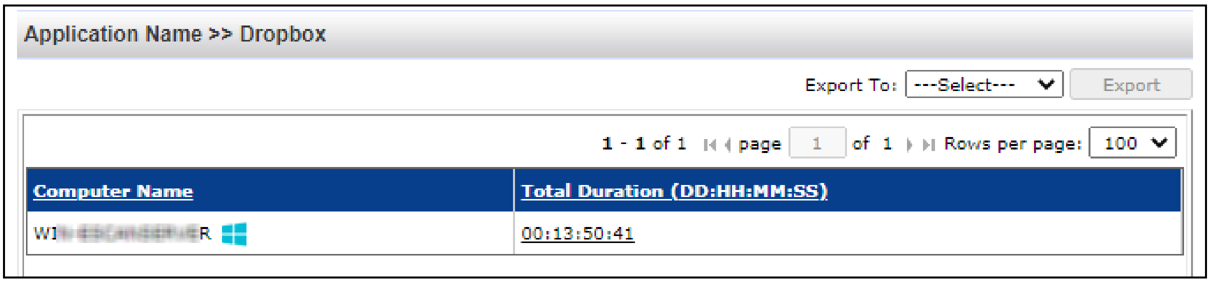
In the navigation panel, click **User Activity** > **Application Access Report**.
The log displays list of files and the type of operation performed on them. Options for Filtering or Exporting the log in desired formats are also present on the same interface.



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

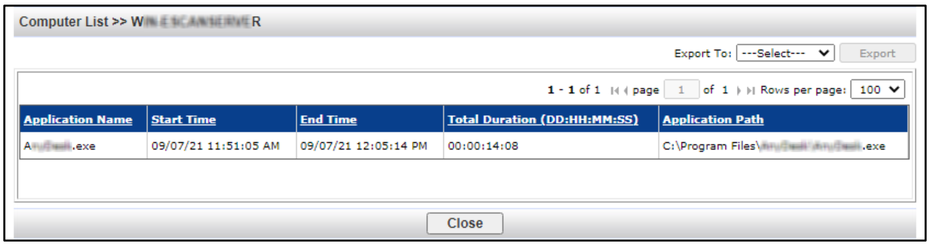
By clicking on the duration present under **Total Duration (DD:HH:MM:SS)** column, you will get the details of the computer name accessed the app and duration.



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.



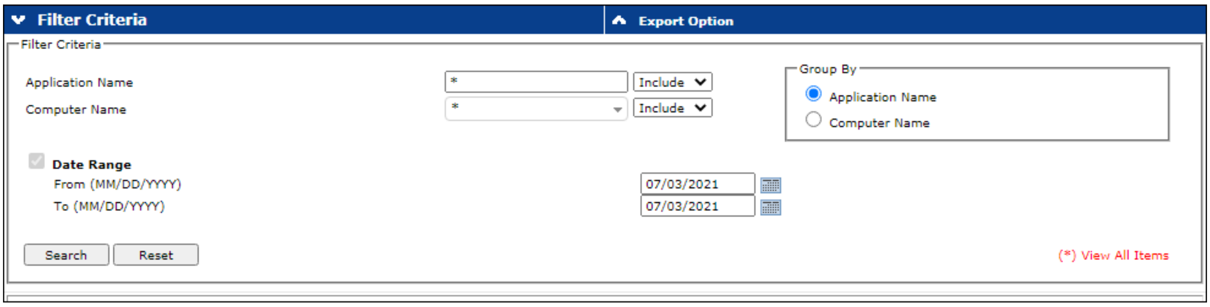
Computer List >> W[redacted]R

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 various format such as PDF, CSV, and HTML.

Filtering Application Access Report

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



Filter Criteria | Export Option

Filter Criteria

Application Name: * Include

Computer Name: * Include

Group By: ● Application Name ○ Computer Name

☑ Date Range
From (MM/DD/YYYY): 07/03/2021
To (MM/DD/YYYY): 07/03/2021

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).

Group By
The results can be grouped by Application name or Computer name.

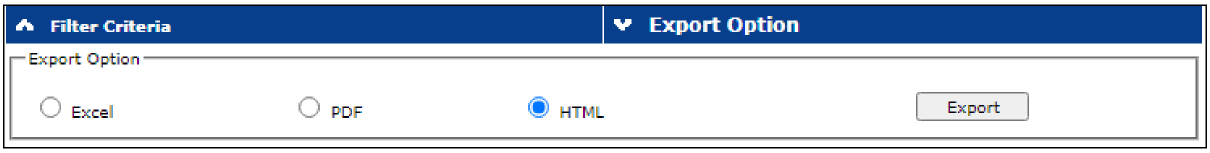
Date Range
To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the calendar icon and select **From** and **To** dates.

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

Reset all filter criteria fields, click **Reset.**

Exporting Application Access Report

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

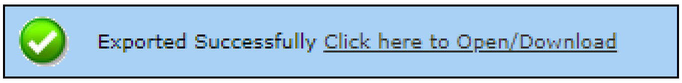


Filter Criteria | Export Option

Export Option

○ Excel ○ PDF ● HTML

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

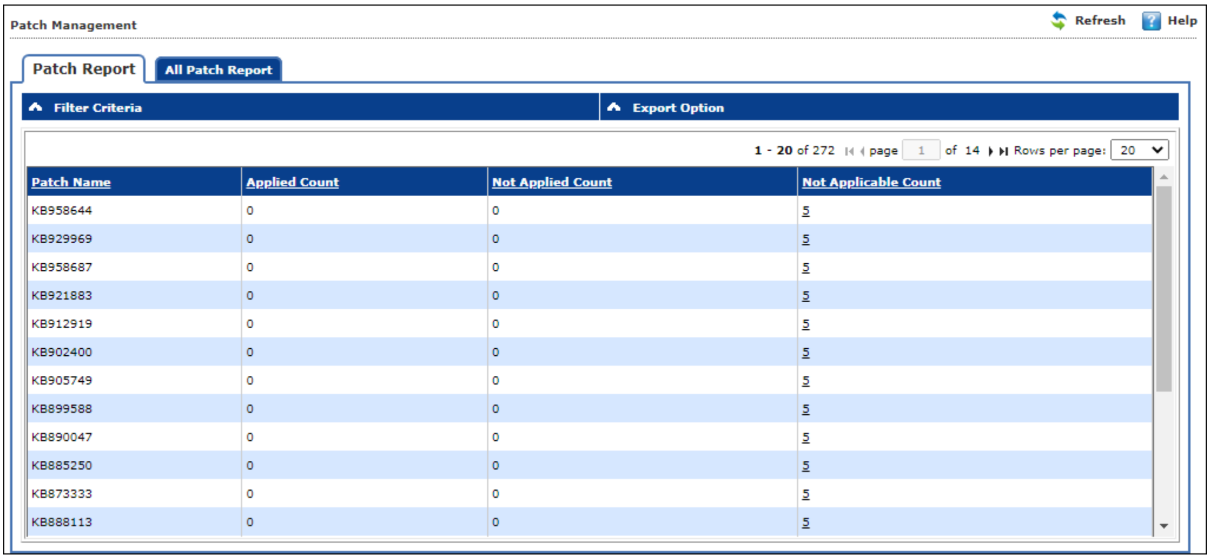


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Patch Report

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

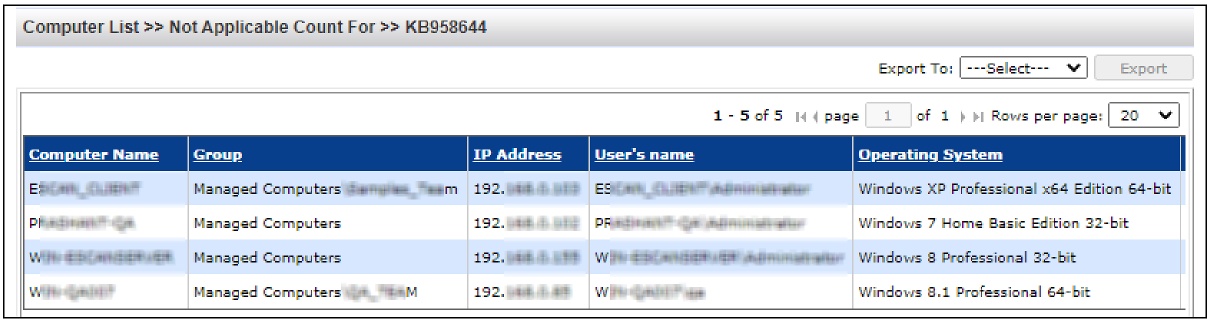


1 - 20 of 272 page 1 of 14 Rows per page: 20

Patch Name	Applied Count	Not Applied Count	Not Applicable Count
KB958644	0	0	5
KB929969	0	0	5
KB958687	0	0	5
KB921883	0	0	5
KB912919	0	0	5
KB902400	0	0	5
KB905749	0	0	5
KB899588	0	0	5
KB890047	0	0	5
KB885250	0	0	5
KB873333	0	0	5
KB888113	0	0	5

Patch Report

The Patch report tab displays the Patch Name, Applied Count, Not Applied Count and Not Applicable Count. Clicking the numerical displays the patch name, details about the computer, the group it belongs to, IP address and User's name.


Computer List >> Not Applicable Count For >> KB958644

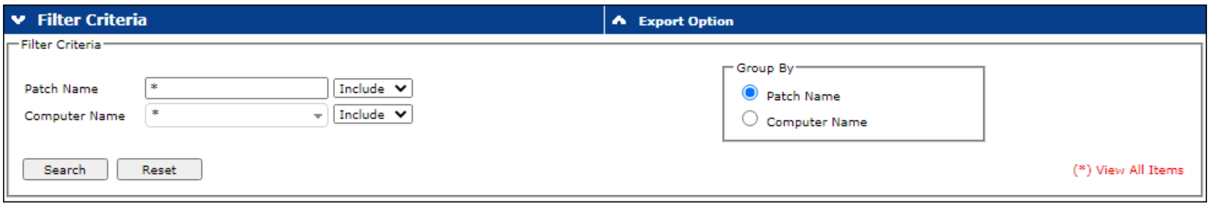
Export To: ---Select--- Export

1 - 5 of 5 page 1 of 1 Rows per page: 20

Computer Name	Group	IP Address	User's name	Operating System
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.



Patch Name * Include
Computer Name * Include

Group By
● Patch Name
○ Computer Name

(*) View All Items

Enter the **Patch Name** and **Computer Name** to be included in the filtered report.

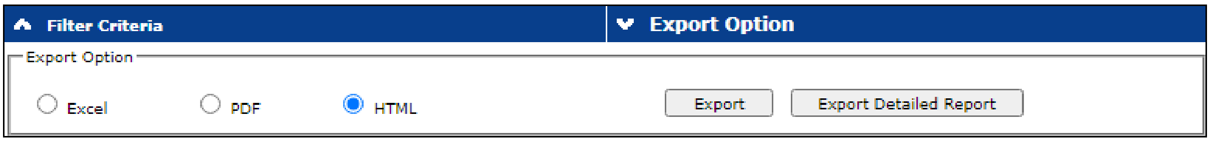
Include/Exclude
Selecting **Include/Exclude** for a parameter lets you include or exclude it from the report.

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

Clicking **Reset** button reset all the filter criteria.

Exporting Windows Patch Report

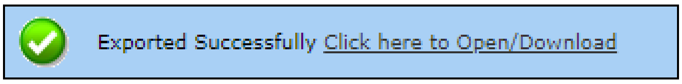
To export the Windows Patch Report, click **Export Option**.
Export Option field expands.



Select the preferred option and then click **Export**.

OR

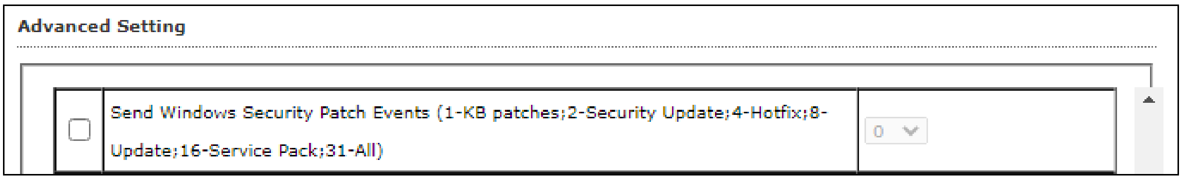
To export a detailed report, select the preferred option and then click **Export Detailed Report**.
A success message appears.



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 Settings**



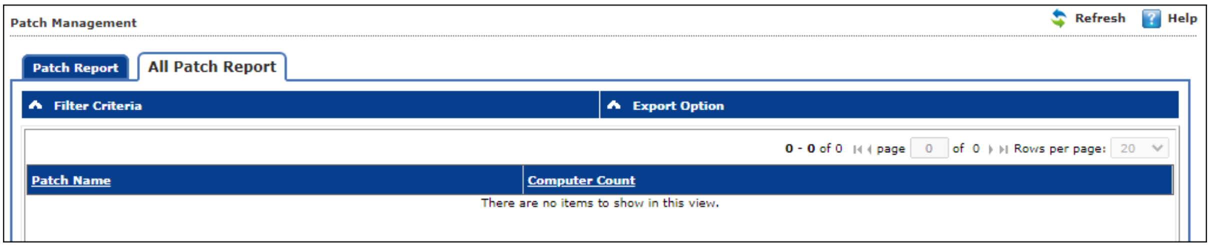
Advanced Setting

□ Send Windows Security Patch Events (1-KB patches;2-Security Update;4-Hotfix;8-Update;16-Service Pack;31-All) 0

All Patch Report

The All Patch Report tab displays all Microsoft patches based on following specific events.

- **1-KB patches**
- **2-Security Update**
- **4-Hotfix**
- **8-Update**
- **16-Service Pack**
- **31-All**


Patch Management

Refresh Help

Patch Report | All Patch Report

Filter Criteria | Export Option

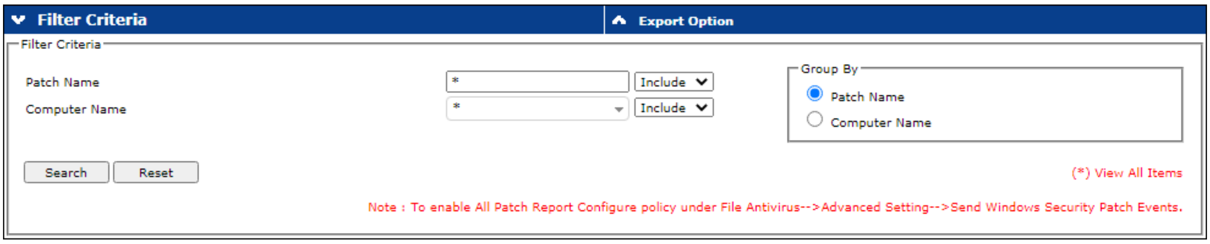
0 - 0 of 0 | page 0 of 0 | Rows per page: 20

Patch Name	Computer Count

There are no items to show in this view.

Filtering All Patch Report

To filter the All Patch Report as per your requirements, click **Filter Criteria** field.
Filter Criteria field expands.


Filter Criteria | Export Option

Filter Criteria

Patch Name: * Include

Computer Name: * Include

Group By: ● Patch Name ○ Computer Name

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 Windows All Patch Report Configure policy by going to **File Antivirus--> Advanced Setting-->Send Windows Security Patch Events**.

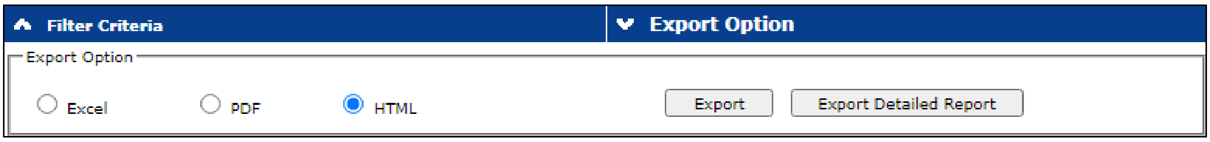
Include/Exclude
Selecting **Include/Exclude** for a parameter lets you include or exclude it from the report.

After making the necessary selections, click **Search.**
The Patch Report will be filtered according to your preferences.

Reset all filter criteria fields, click **Reset.**

Exporting All Patch Report

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


Filter Criteria | Export Option

Export Option

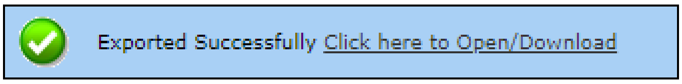
○ Excel ○ PDF ● HTML

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.

Notifications

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

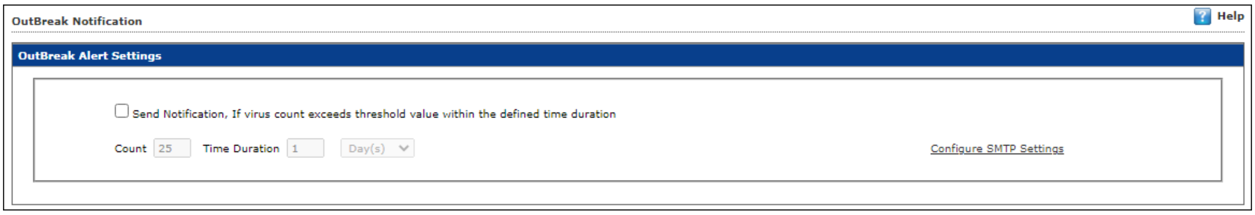
- **Outbreak Alert**
- **Event Alert**
- **Unlicensed Move Alert**
- **New Computer Alert**
- **Configure SIEM**
- **SMTP Settings**

Outbreak Alert

If the virus count exceeds the limits set by you, an outbreak email notification will be sent to the recipient.

To set an outbreak alert, follow the steps given below:

1. In the navigation panel, click **Notifications** > **Outbreak Alert**.
   Outbreak Notification screen appears.



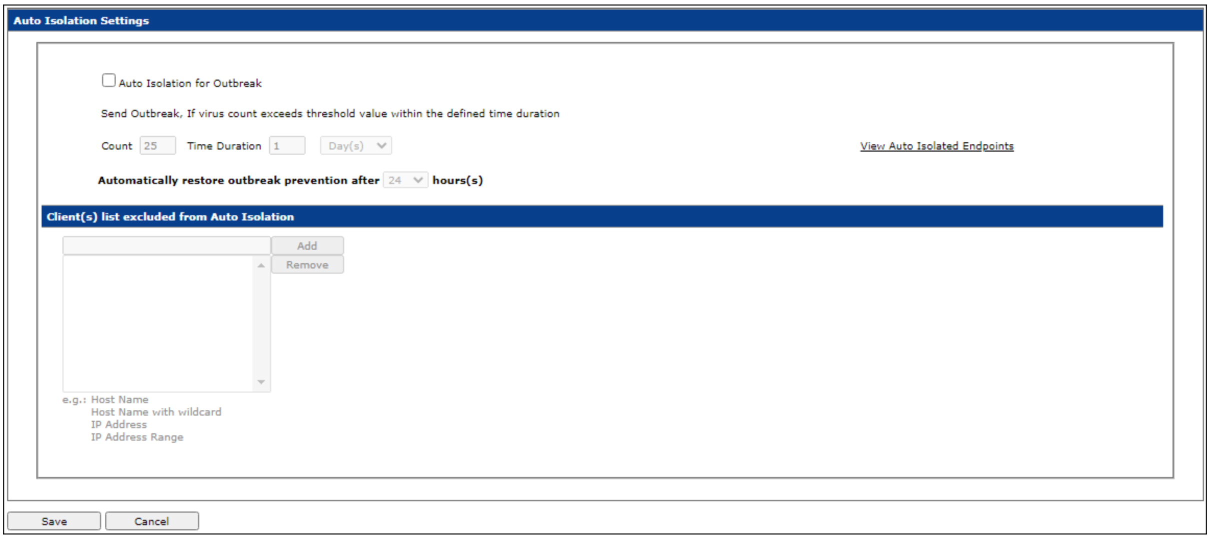
OutBreak Notification

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

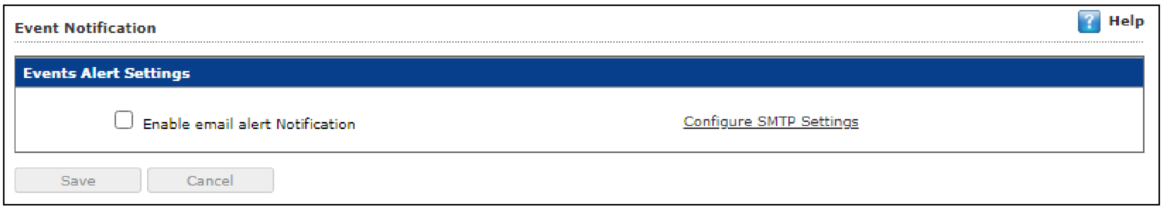
4. In **Auto Isolation Settings** section, select checkbox **Auto Isolation for Outbreak**.
5. Enter the preferred values in **Count** and **Time Limit** field.
6. Select the value in **Automatically restore outbreak prevention after hours(s)** field.

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.**
   The 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. 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.



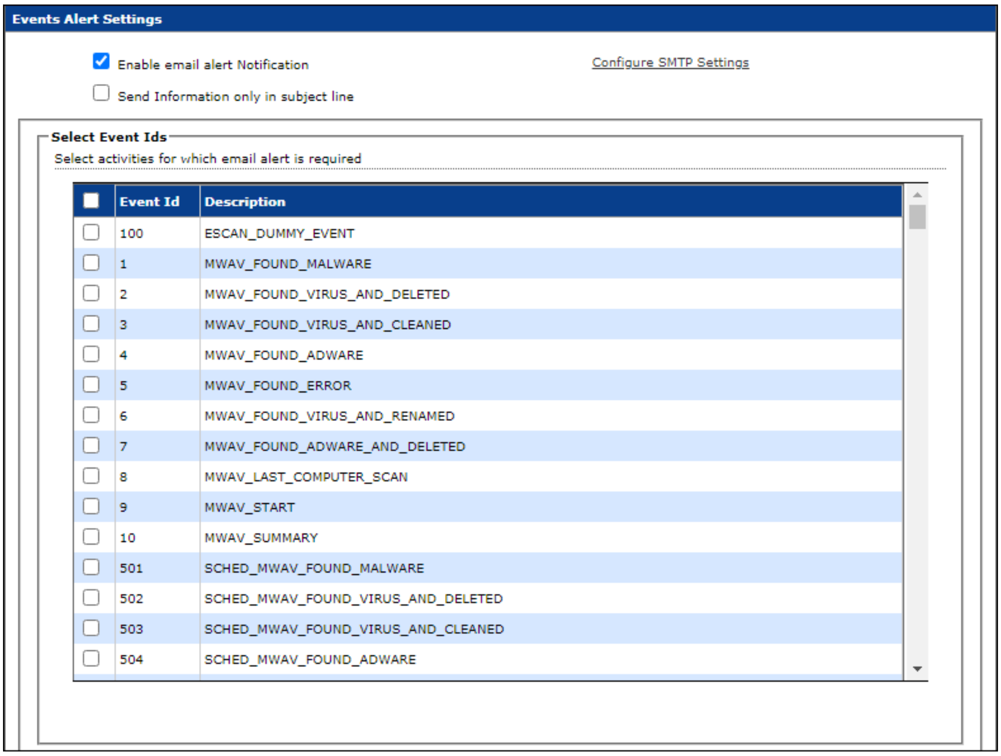
Event Notification

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 checkbox **Send Information in subject line**.
   This checkbox enable after selecting enable email alert notification.
4. Select the events from the list for which you prefer an alert.



Events Alert Settings

☑ Enable email alert Notification

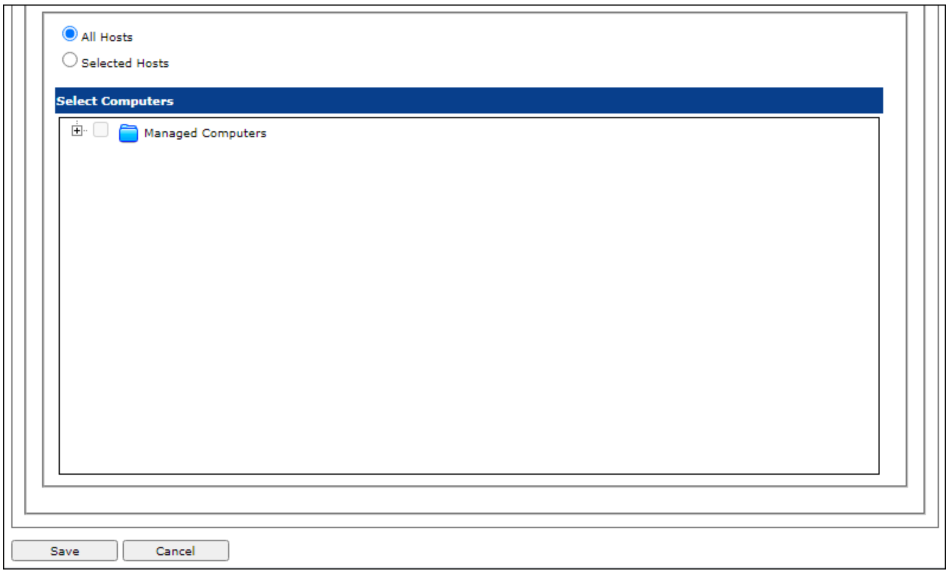
□ Send Information only in subject line

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

5. Select the required hosts or group.

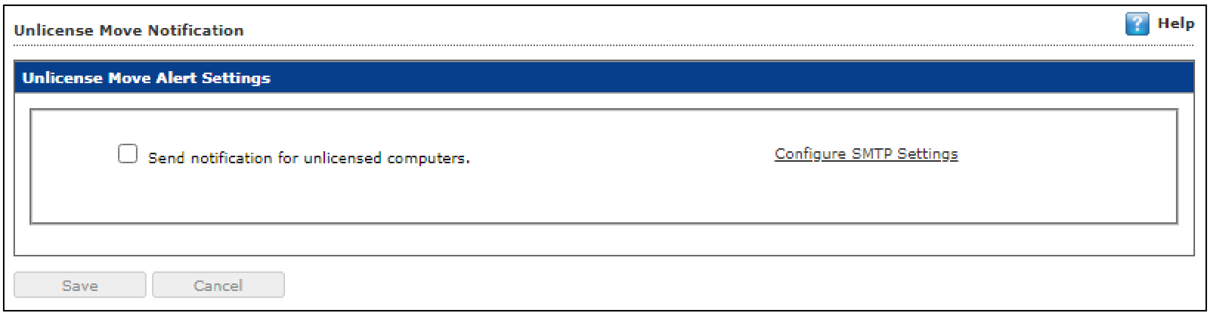


● All Hosts
○ Selected Hosts

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

Unlicensed Move Alert

This submodule lets you enable notification alert when a computer automatically moves to Unlicensed Computers category based on the setting done (under events and computers) for the computer which is not connected to the server for a long time.



Unlicense Move Notification

Unlicense Move Alert Settings

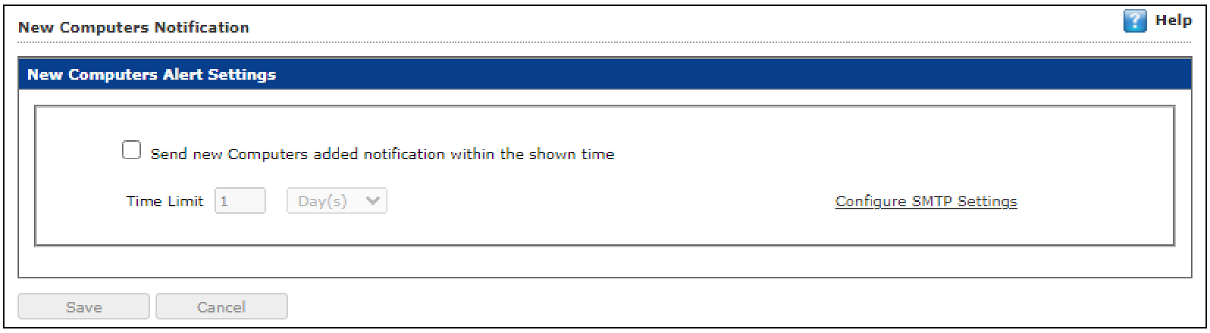
□ Send notification for unlicensed computers.

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

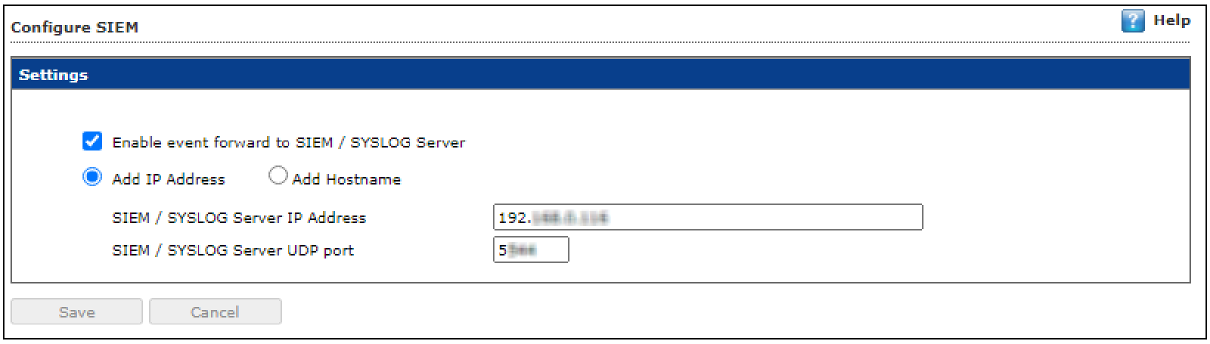
Time Limit 1 Day(s)

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]

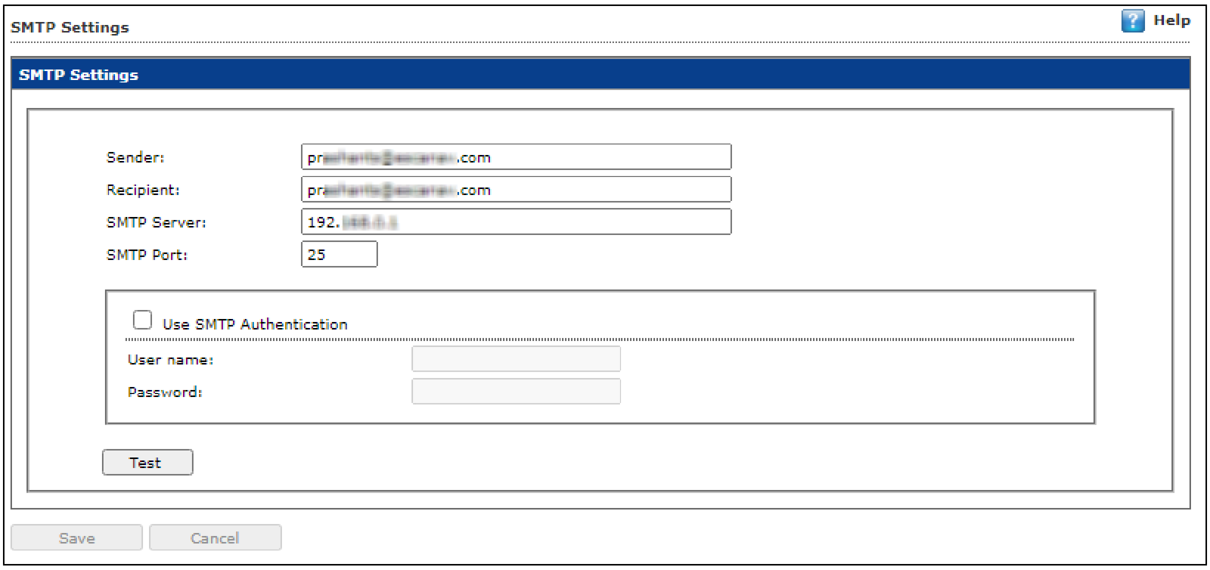
SIEM / SYSLOG Server UDP port: 5[redacted]

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.

SMTP Settings

This submodule lets you configure the SMTP settings for all the email notifications.



SMTP Settings

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

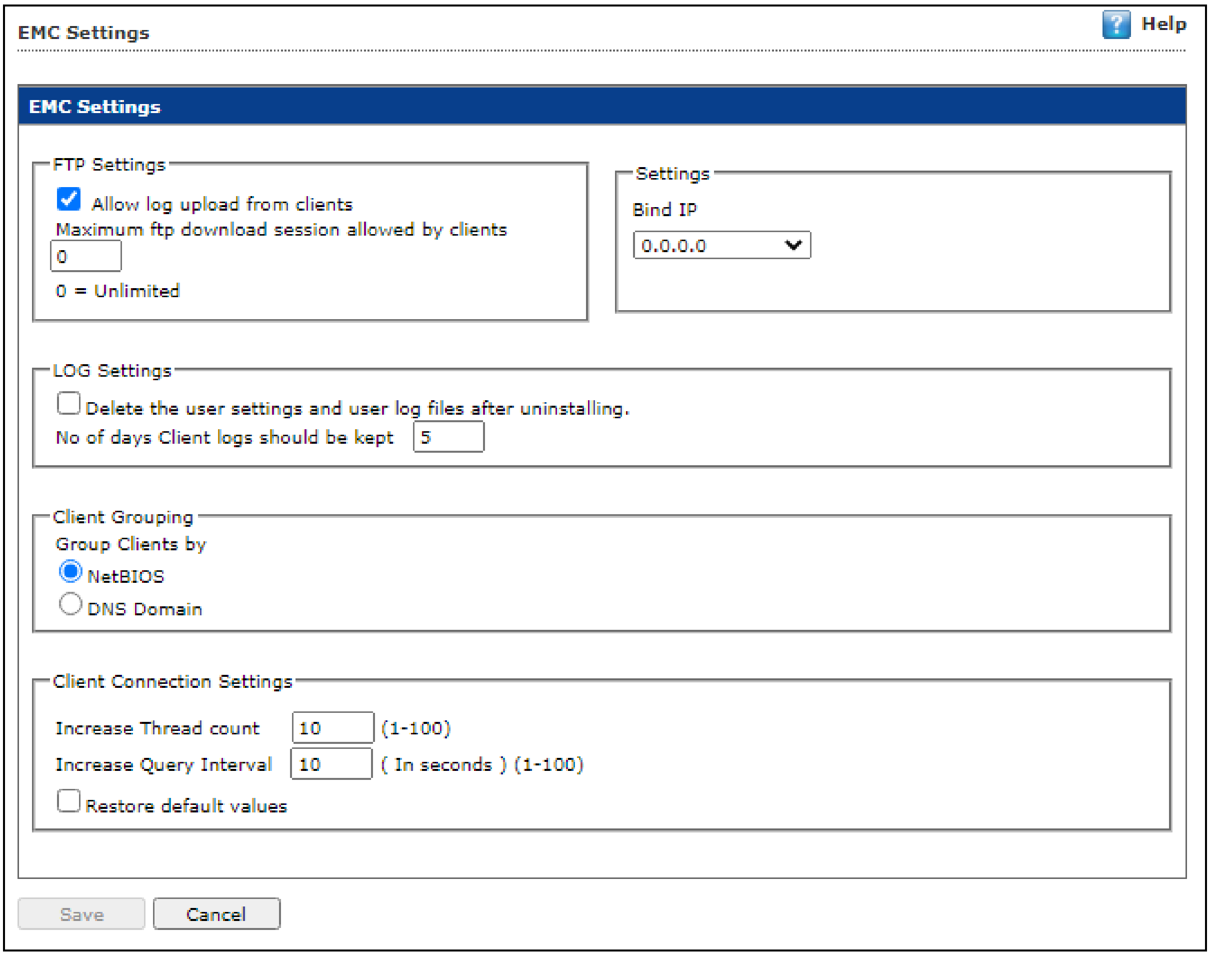
The Settings module lets you configure general settings. It contains following submodules.

- **EMC Settings**: This submodule lets you define settings for FTP sessions, Log Settings, Client Grouping and Client connection settings.
- **Web Console Settings**: This submodule lets you define settings for web console timeout, Dashboard Settings, Login Page settings, SQL Server Connection settings, SQL Database compression settings.
- **Update Settings**: This submodule lets you define settings for General Configuration, Update Notifications, and Scheduling.
- **Auto-Grouping**: This submodule lets you define settings for Grouping of computers after installation of eScan client is carried out.
- **Two-Factor Authentication**: This submodule lets you to add extra layer of protection to your endpoints.

EMC Settings

The EMC (eScan Management Console) Settings lets you configure the eScan Management Console. You can configure the FTP settings, Bind to IP Settings, Log Settings, Client Grouping and Client Connection Settings.

You can bind announcement of FTP server to particular IP by selecting the IP address in the list. However, you can choose to leave it as 0.0.0.0, which mean it will announce on all available interface/IP.



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: 5

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

FTP Settings

This setting lets you approve the log upload from client computers. It also lets you set the maximum FTP download sessions allowed for client computers. (Note: 0 means unlimited)

Bind IP Settings

This setting lets you bind an IP address. Click the drop-down and select the preferred IP address for binding. The default IP address is 0.0.0.0.

Log Settings

This setting provides you with the option to delete the User settings and Log files after uninstallation of eScan from the computer. To enable the above setting, select the checkbox. After selecting the checkbox, you can store client logs for the preferred number of days.

Client Grouping

This setting lets you manually manage domains and computers grouped under them after performing fresh installations.

Select **NetBIOS**, if you want to group clients only by hostname.

Select **DNS Domain**, if you want to group clients by hostname containing the domain name.

Client Connection Settings

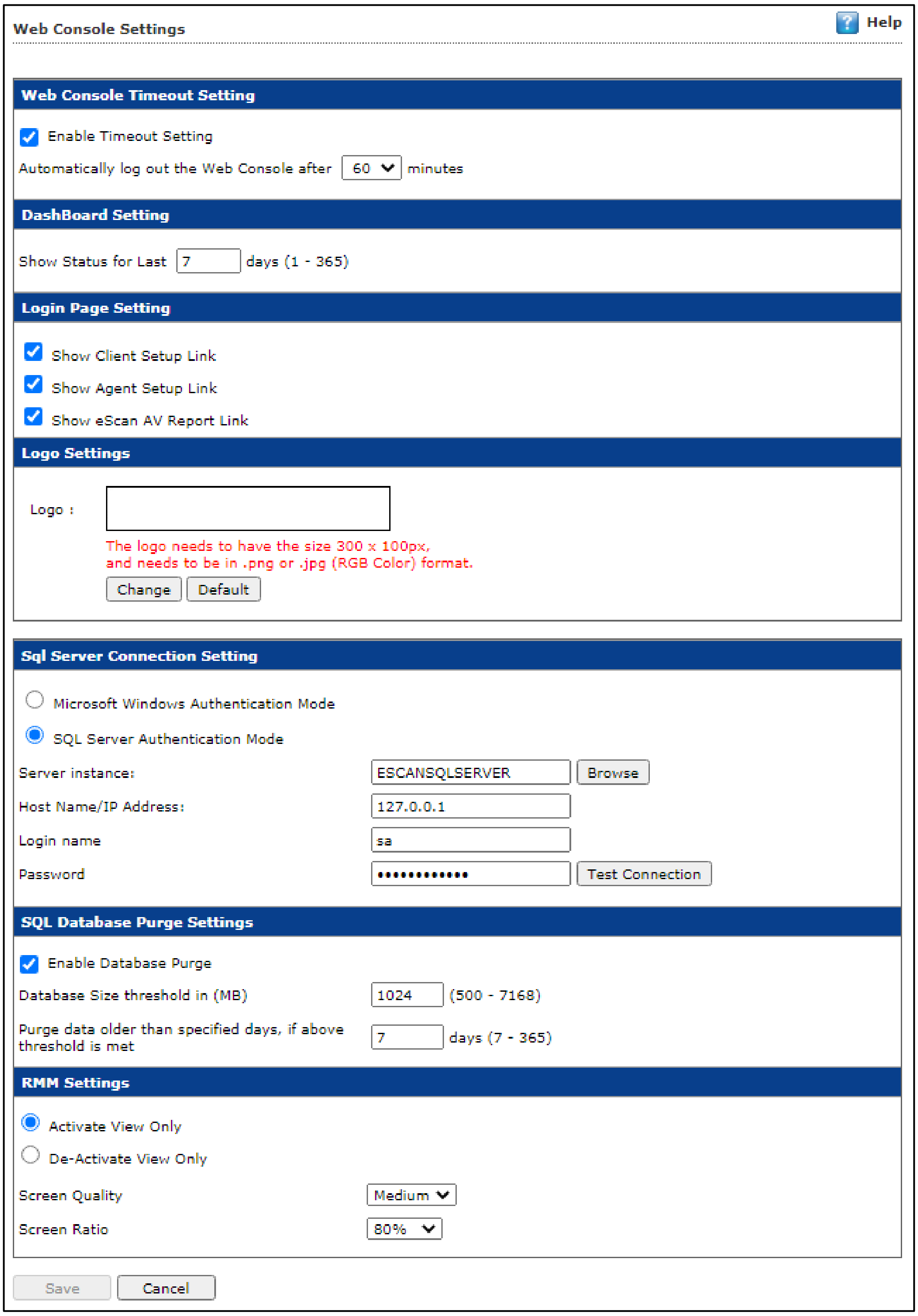
This setting lets you modify **Thread Count** and **Query Interval** (In Seconds). To reset the values, select **Restore default values** checkbox.

After performing the necessary changes, click **Save**.

The EMC Settings will be updated.

Web Console Settings

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



Web Console Settings

Web Console Timeout Setting

☑ Enable Timeout Setting

Automatically log out the Web Console after 60 minutes

DashBoard Setting

Show Status for Last 7 days (1 - 365)

Login Page Setting

☑ Show Client Setup Link

☑ Show Agent 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: ESCANSQLSERVER

Host Name/IP Address: 127.0.0.1

Login name sa

Password ••••••••••••

SQL Database Purge Settings

☑ Enable Database Purge

Database Size threshold in (MB) 1024 (500 - 7168)

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%

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.

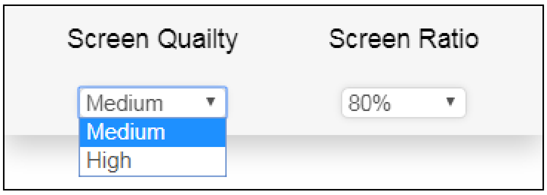
De-Activate View Only

To perform activity on an endpoint after taking remote connection, click **De-Activate View Only**.

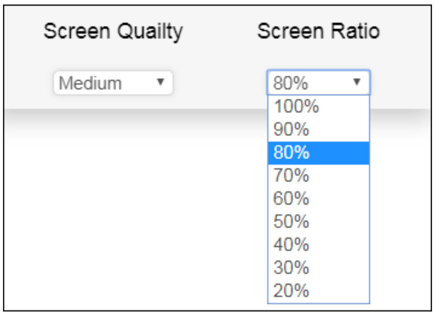
Screen Quality Settings

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.

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

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

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

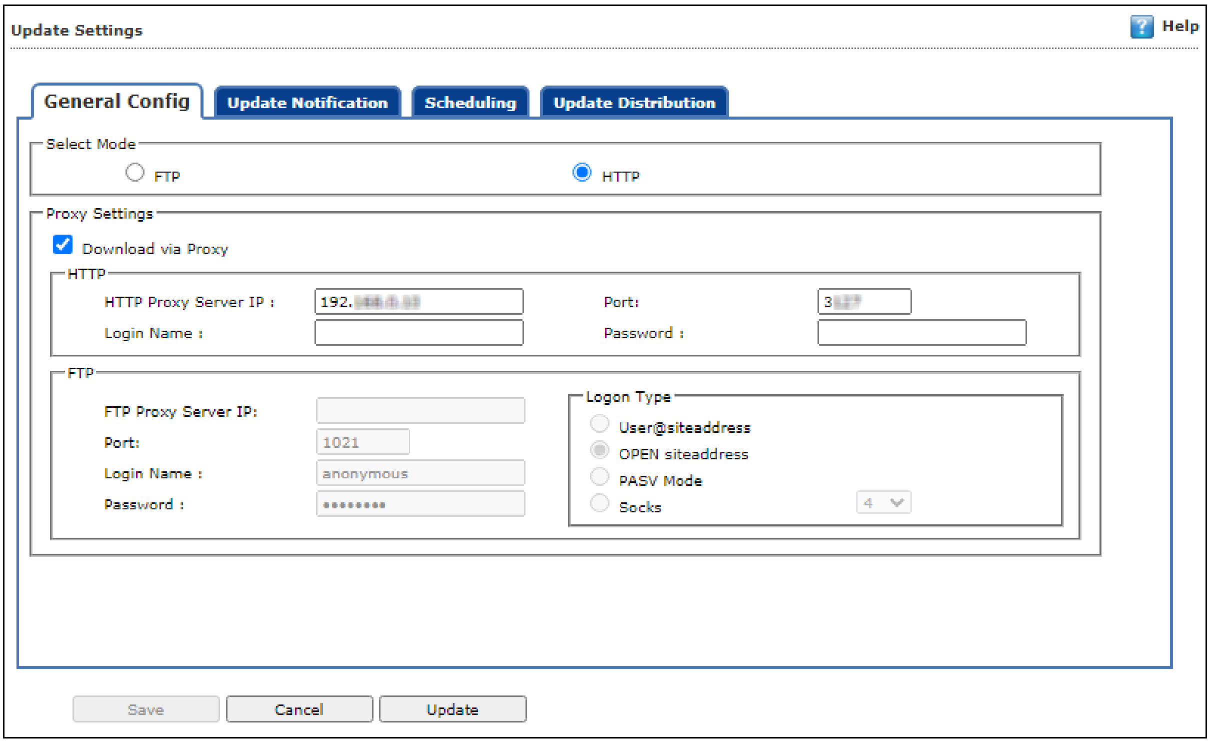
Update Settings

The Update Settings submodule keeps your virus definitions up-to-date and protects your computer from emerging species of viruses and other malicious programs. This submodule lets you configure update settings, update notifications and schedule updates according to your need.

You can configure eScan to download updates automatically either from eScan update servers or from the local network by using FTP or HTTP. You can configure following settings.

General Config

The **General Config** tab lets you configure update settings. The settings let you select the mode of update and configure proxy settings.



Select Mode

○ FTP ● HTTP

Proxy Settings

☑ Download via Proxy

HTTP

HTTP Proxy Server IP : 192.[redacted] Port: 3[redacted]

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
- HTTP

Proxy Settings

Proxy Settings lets you configure proxy for downloading updates.
To enable Proxy Settings, select **Download via Proxy** checkbox. You will be able to configure proxy settings depending on the mode of selection.

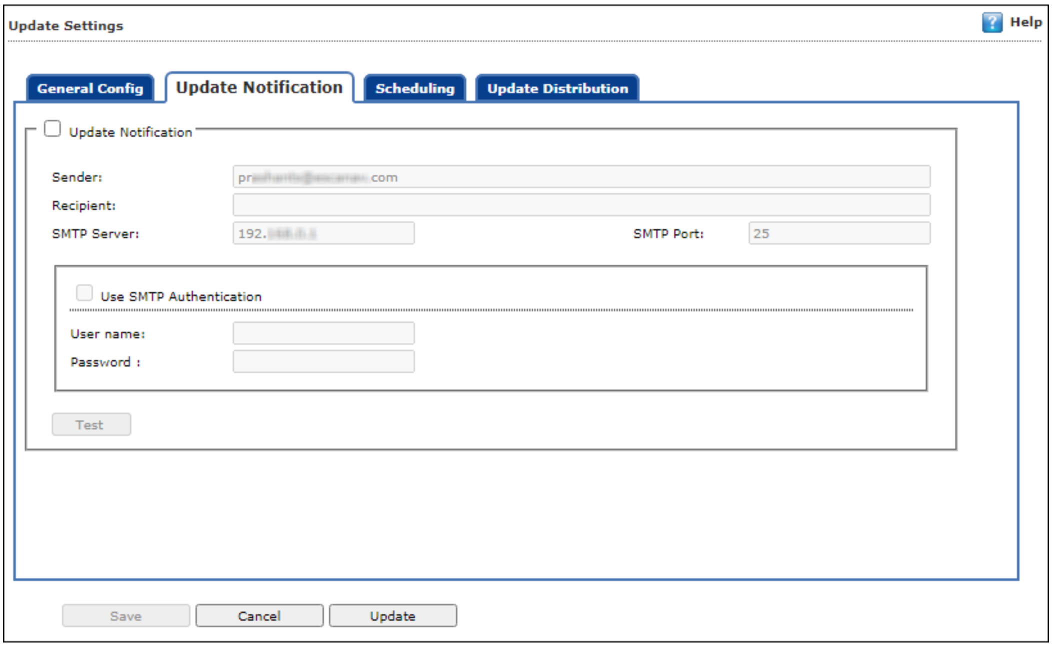
If you are using HTTP proxy servers, enter the HTTP proxy server IP address, port number and HTTP proxy server's authentication credentials.

If you are using FTP proxy servers, along with HTTP settings mentioned above you will have to enter FTP proxy server IP address, Port number, FTP proxy server's authentication credentials and Logon enter.

After filling the necessary data, click **Save > Update**.
The General Config tab will be saved and updated.

Update Notification

The Update Notification tab lets you configure email address and SMTP settings for email notifications about database update.



Update Settings

□ 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.

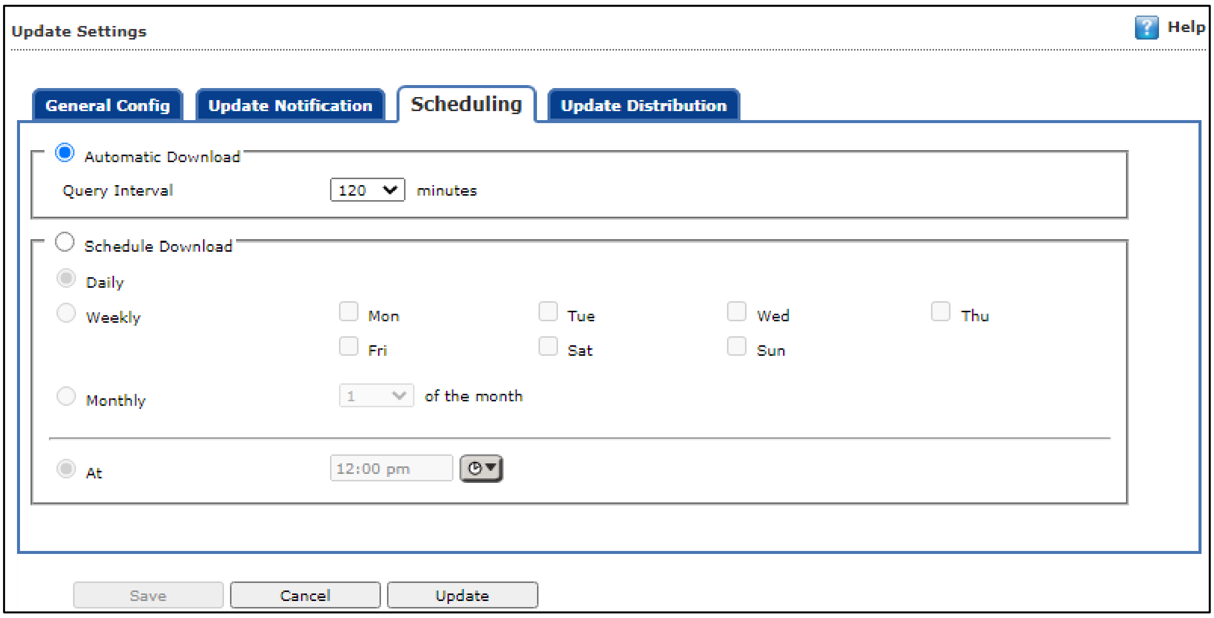
SMTP Server and Port
Enter the SMTP server's IP address and Port number in the respective fields.

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

● 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.

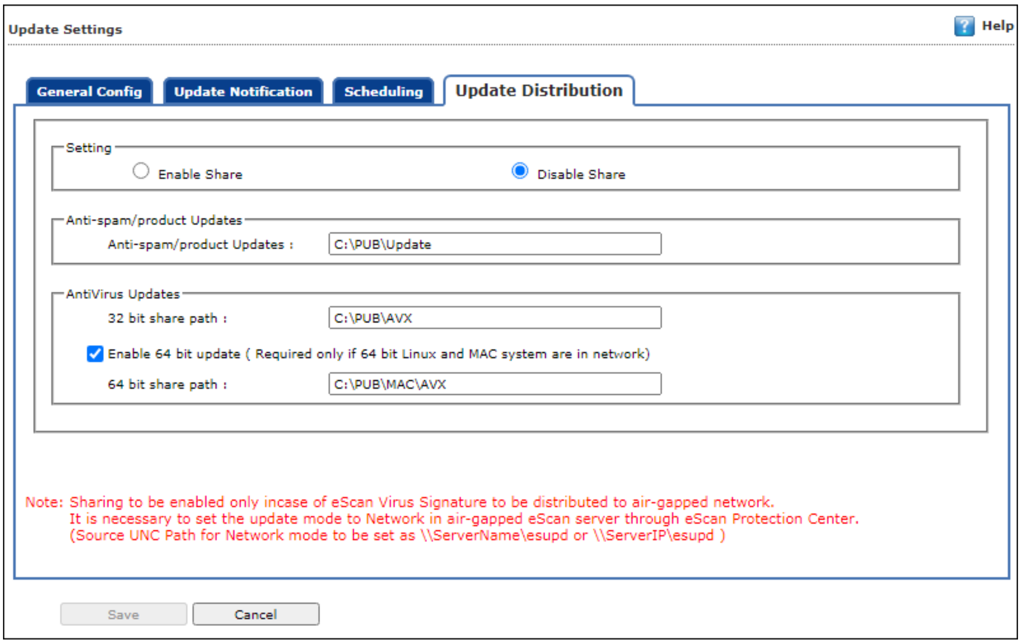
Schedule Download

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

Setting
○ Enable Share ● Disable Share

Anti-spam/product Updates
Anti-spam/product Updates : C:\PUB\Update

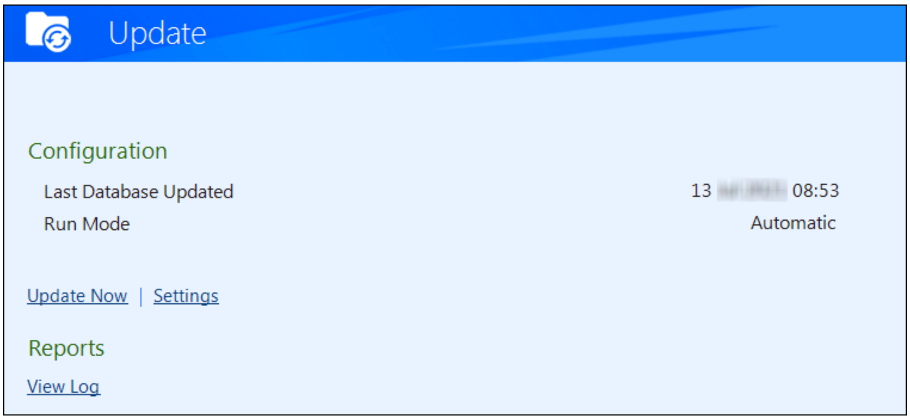
AntiVirus Updates
32 bit share path : C:\PUB\AVX
☑ Enable 64 bit update (Required only if 64 bit Linux and MAC system are in network)
64 bit share path : C:\PUB\MAC\AVX

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.

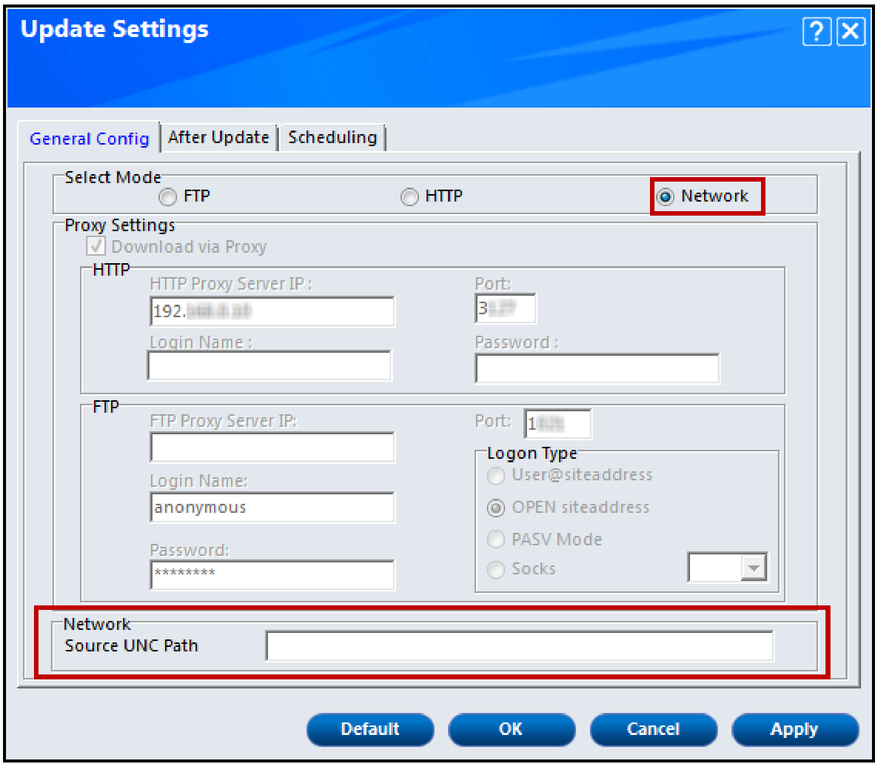


Update

Configuration

Last Database Updated	13 [illegible] 08:53
Run Mode	Automatic

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

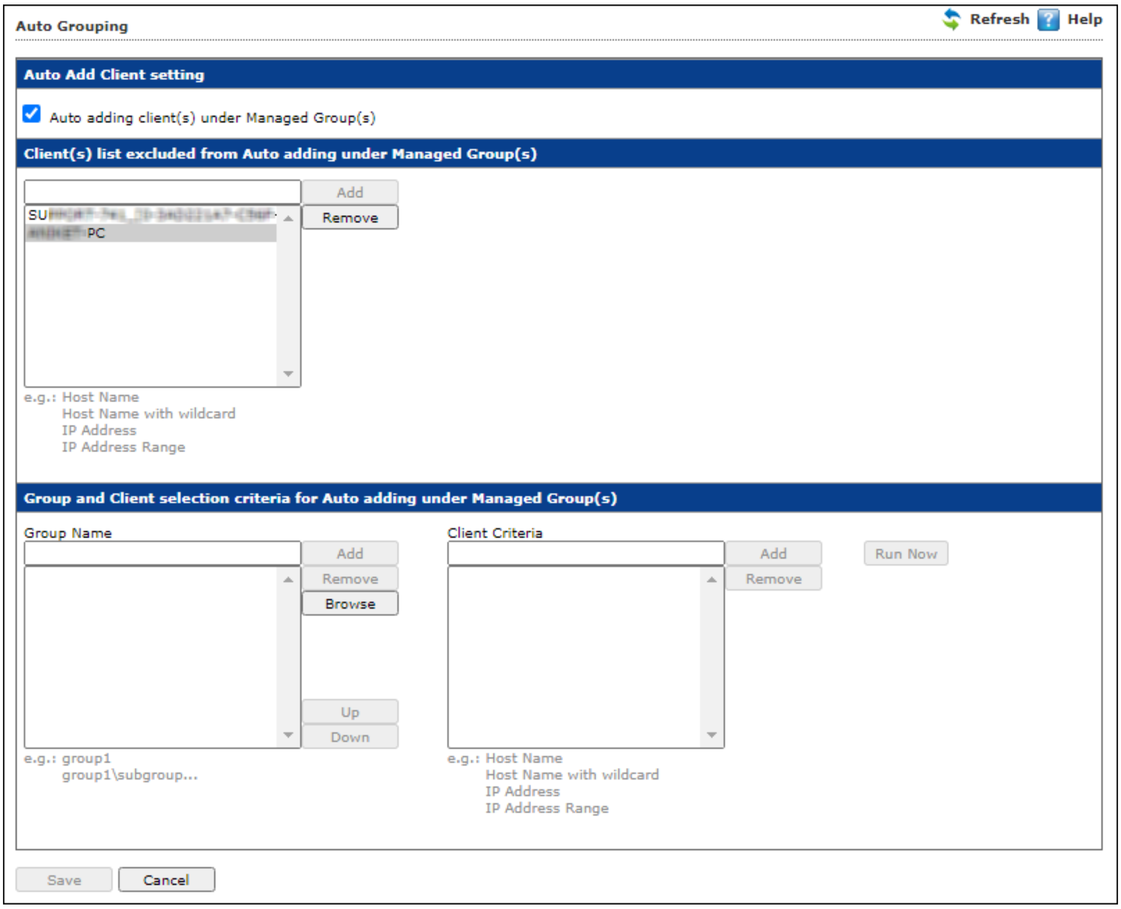
Network
Source UNC Path

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

Refresh Help

Auto Add Client setting

☑ Auto adding client(s) under Managed Group(s)

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

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

To remove the clients from the excluded list,

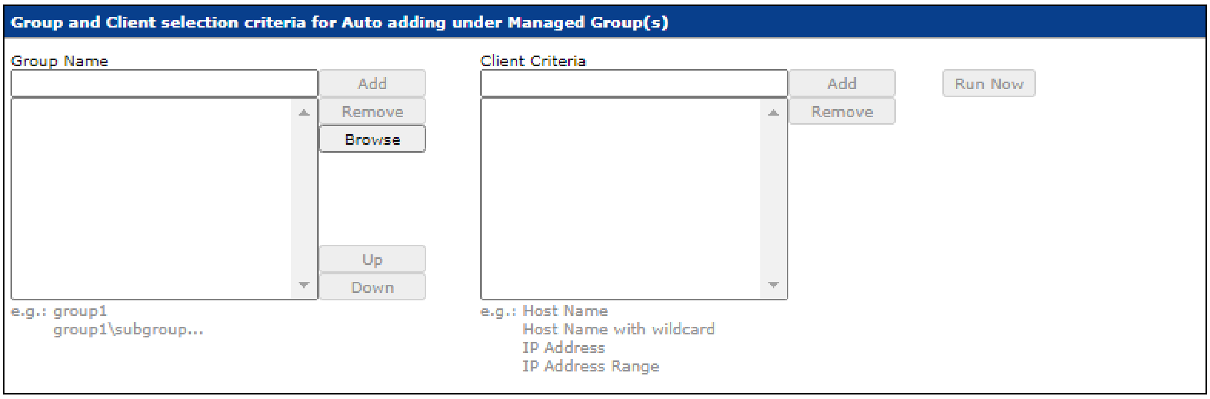
1. Select the computer you want to remove.
2. Click **Remove**.
   The client computer will be removed from the list.

Group and Client selection criteria for Auto adding under Managed Group(s)

This 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:



Group and Client selection criteria for Auto adding under Managed Group(s)

1. Under the Group Name, enter the group's name and click **Add**.

   OR

   Click **Browse** and select the group from the existing list.

NOTE	To browse through the list of groups, click **Up** or **Down**.

2. Select the group for which you want to define the criteria.

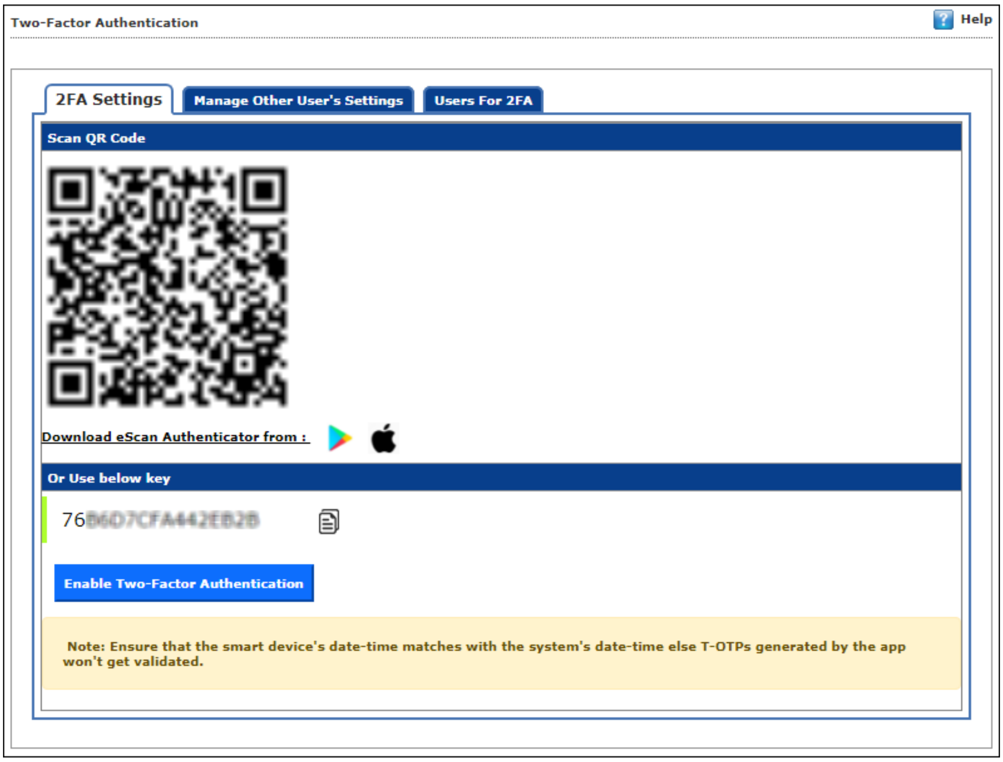
3. Under the Client Criteria, enter either Hostname, Hostname with wildcard, IP address or IP address range and click **Add.** The clients displayed in the list will be added under the selected group.
4. Click **Save**.
   The client will be saved under that group.
5. To apply the settings for the newly added client, click **Run Now**.

Two-Factor Authentication (2FA)

The system login password is Single-Factor Authentication which is considered unsecure as it may put your organization's data at high risk of compromise. The Two-Factor Authentication, also more commonly known as 2FA, adds an extra layer of protection to your eScan web console login.

The 2FA feature mandates you to enter a Time-based One-Time Password (TOTP) after entering eScan credentials. So, even if somebody knows your eScan credentials, the 2FA feature secures data against unauthorized logins. Only administrator can enable/disable the 2FA feature. It can also be enabled for added users as well.

To use 2FA login feature, you need to install the **Authenticator** app from Play Store for Android devices or from App Store for iOS devices. The Authenticator app needs camera access for scanning a QR code, so ensure you get an appropriate approval to use device camera in your organization. If a COD or BYOD policy restricts you from using device camera in your organization, enter the **Account Key** in the Authenticator app.



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]

Enable 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.

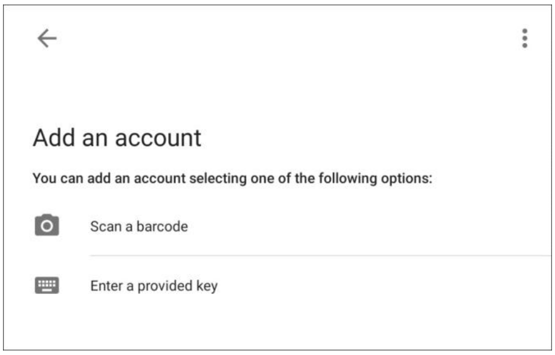
NOTE	Ensure that the smart device's date and time matches with the system's date and time, else TOTPs generated by app won't get validated.

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,

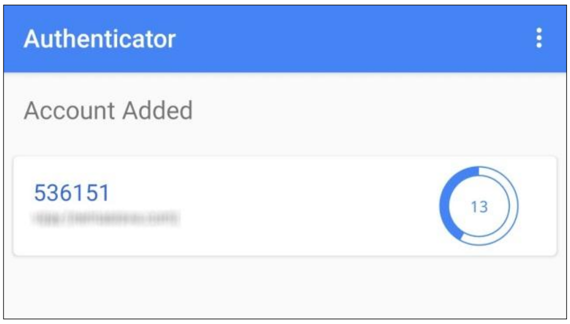
1. Go to **Settings** > **Two-Factor Authentication**.
2. Open the Authenticator app.
   After basic configuration following screen appears on smart device.



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.

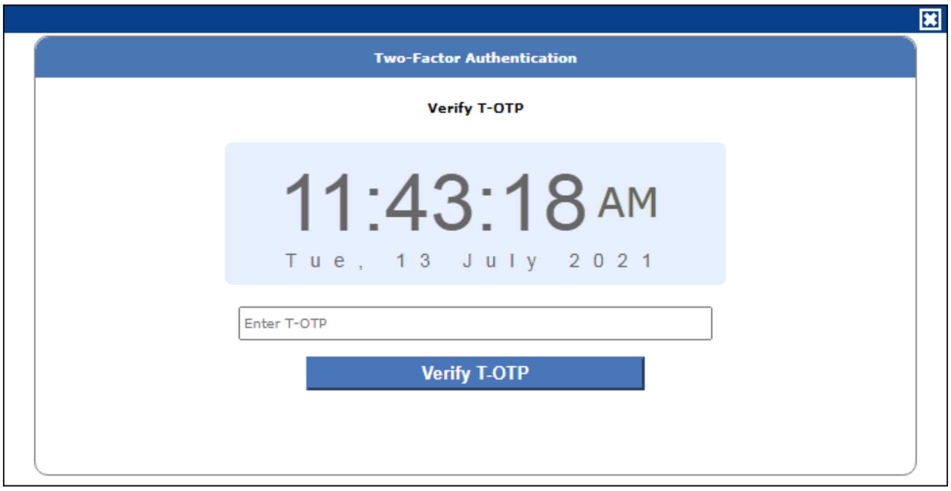


Authenticator

Account Added

536151

4. Click **Enable Two-Factor Authentication**.
   Verify TOTP window appears.



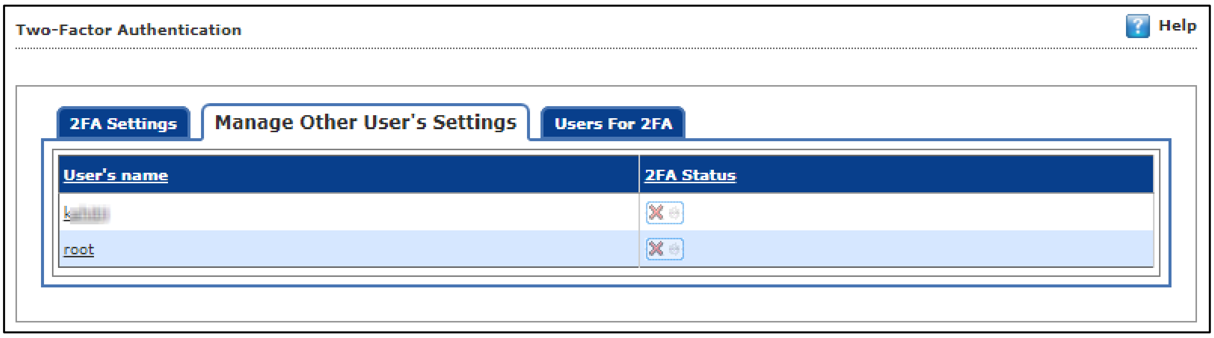
Two-Factor Authentication

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.
   ✗ - 2FA Disabled
   ✓ - 2FA Enabled



Two-Factor Authentication

User's name	2FA Status
[redacted]	✗
root	✗

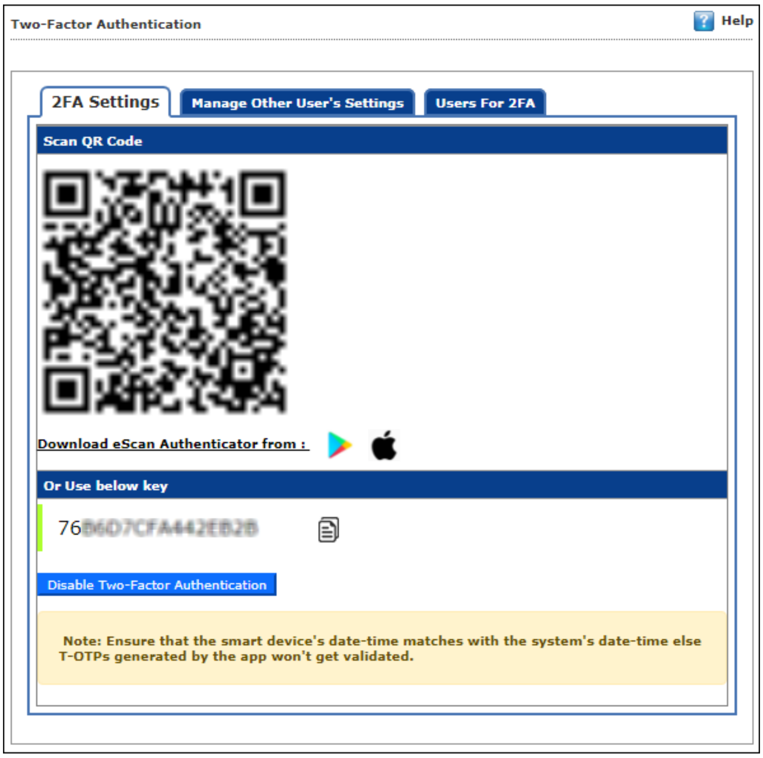
7. To enable 2FA login for an added user, click the button to check icon.

The 2FA login for added users gets enabled. After enabling the 2FA login for users, whenever they log in to eScan web console Verify TOTP window appears.

Disabling 2FA login

To disable 2FA login,

1. Go to **Settings** > **Two Factor Authentication**.
2. Click **Disable Two-Factor Authentication**.



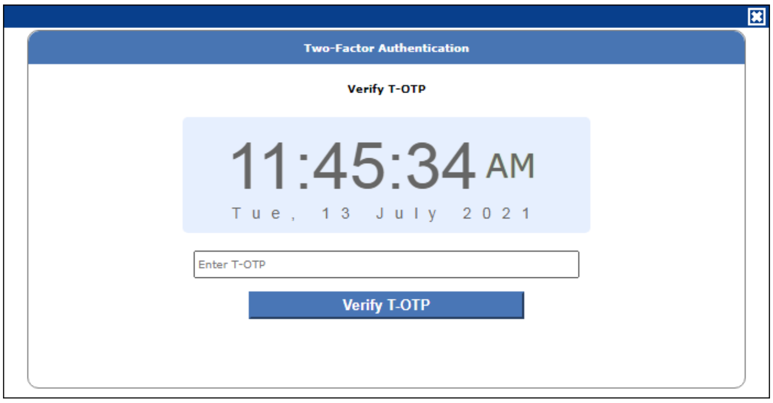
Two-Factor Authentication

Help
2FA Settings
Manage Other User's Settings
Users For 2FA
Scan QR Code
Download eScan Authenticator from :
Or Use below key
Disable 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.

Verify TOTP window appears.

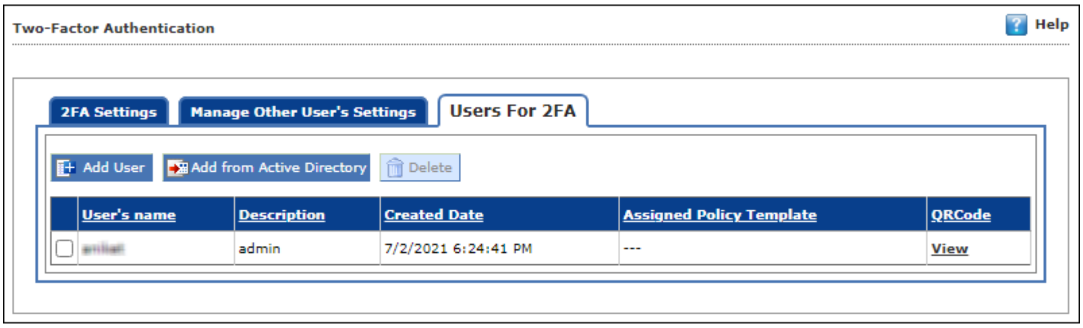


3. Enter the **TOTP** and then click **Verify TOTP**.
   The 2FA feature gets disabled.

NOTE	After disabling the 2FA feature and enabling it again, the 2FA login status will be reinstated for added users.

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.

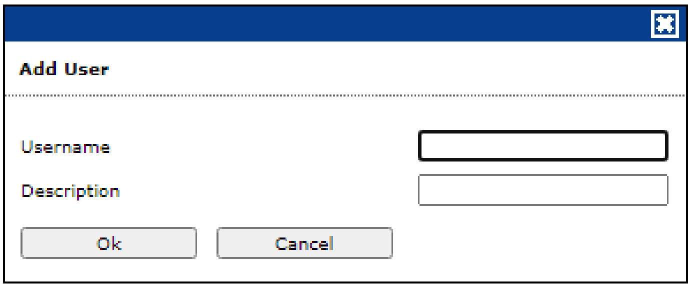

Two-Factor Authentication
Help
2FA Settings
Manage Other User's Settings
Users For 2FA
Add User
Add from Active Directory
Delete

	User's name	Description	Created Date	Assigned Policy Template	QRCode
□	[redacted]	admin	7/2/2021 6:24:41 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.

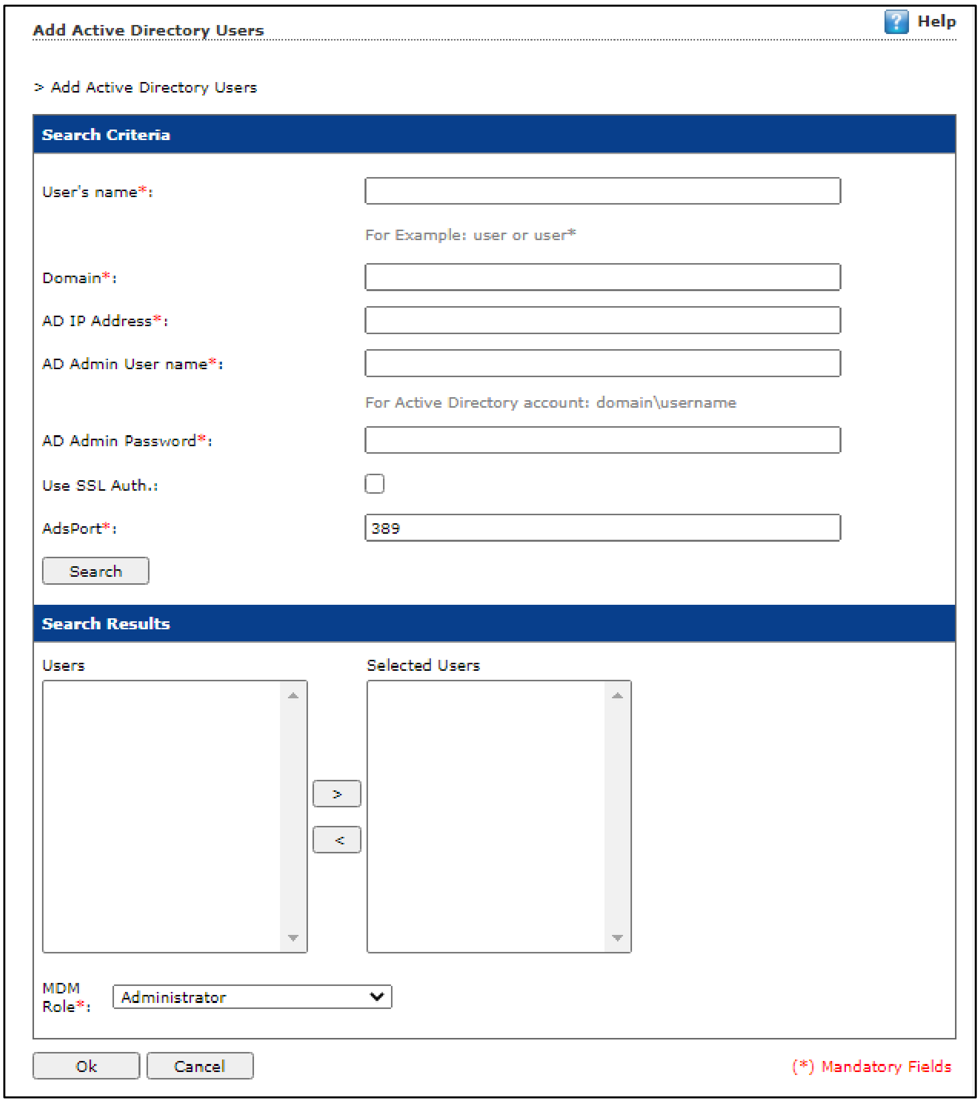


3. Enter the **Username** and **Description**.
4. Click **OK**.
   The user will be added for 2FA.

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.



Add Active Directory Users

> 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

MDM Role*: Administrator

(*) Mandatory Fields

3. Enter the required information.
4. Click **Ok**.
   The Active Directory Users will be added.

Administration

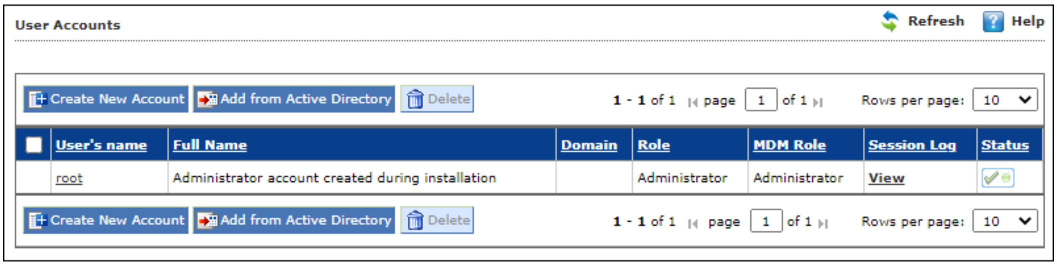
The Administration module lets you create User Accounts and allocate them Admin rights for using eScan Management Console. In a large organization, installing eScan client on all computers may consume lot of time and efforts. With this option, you can allocate rights to the other employees and allow 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.

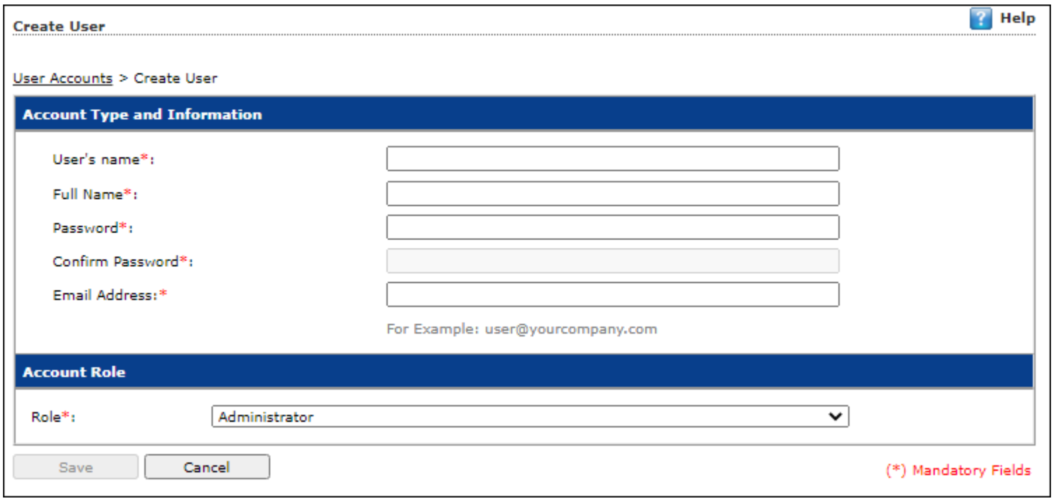


□	User's name	Full Name	Domain	Role	MDM Role	Session Log	Status
	root	Administrator account created during installation		Administrator	Administrator	View	✓

Create New Account

To create a User Account,

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

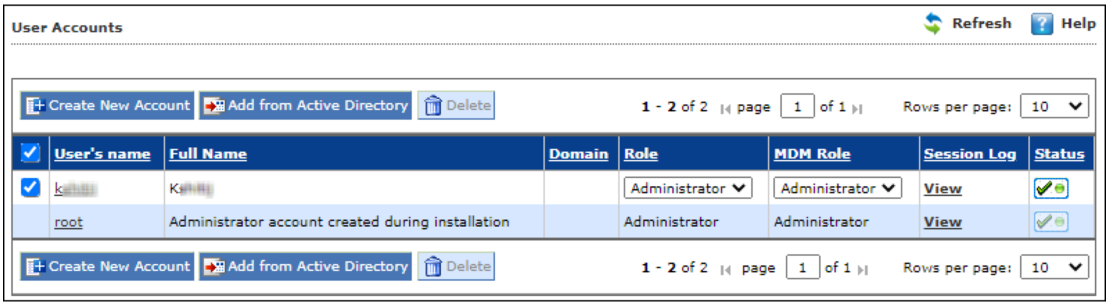


2. From **Account Role** field, click drop-down and assign the role to the account.
3. After filling all the details, click **Save**.
   The user will be added to the User Accounts list.

Delete a User Account

To delete a user account,

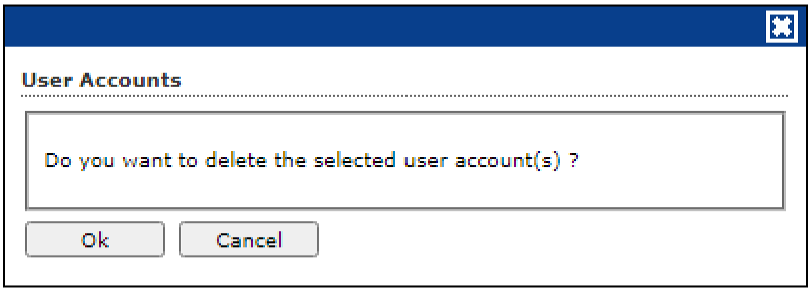
1. In the User Accounts screen, select the user you want to delete.



User Accounts

☑	User'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.



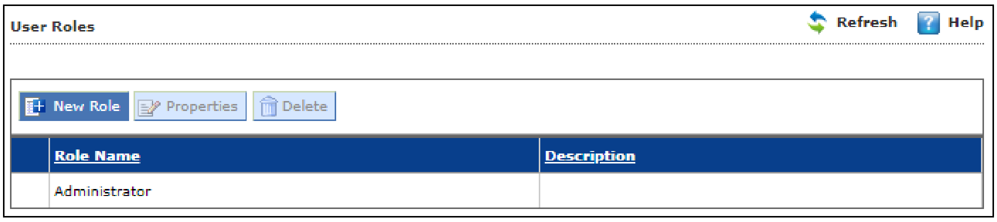
User Accounts

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

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

User Roles

The User Roles submodule lets you create a role and assign it to the User Accounts with variable permissions and rights as defined in the role being assigned to them. It can be an Administrator role with set of permissions and rights Group Admin Role or a Read only Role.



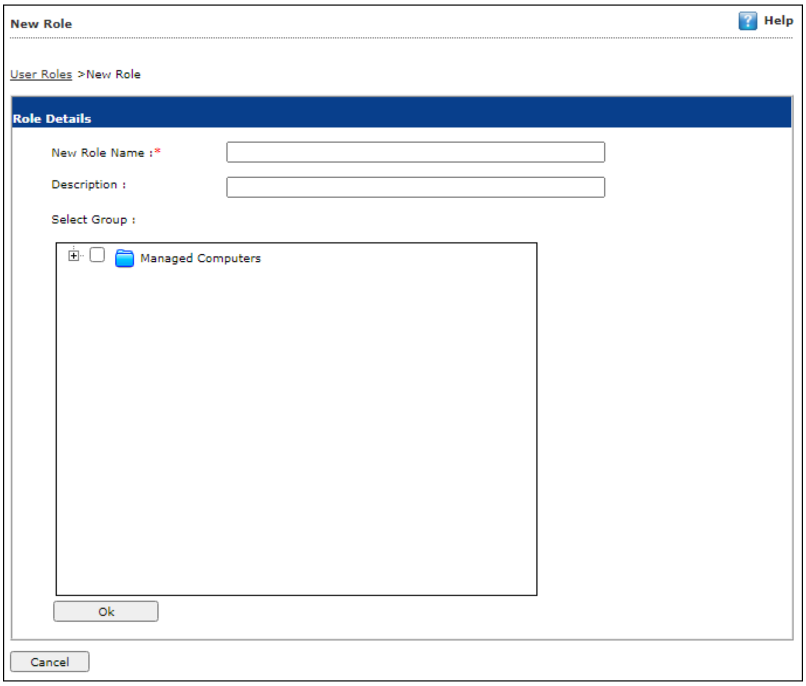
Role Name	Description
Administrator	

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

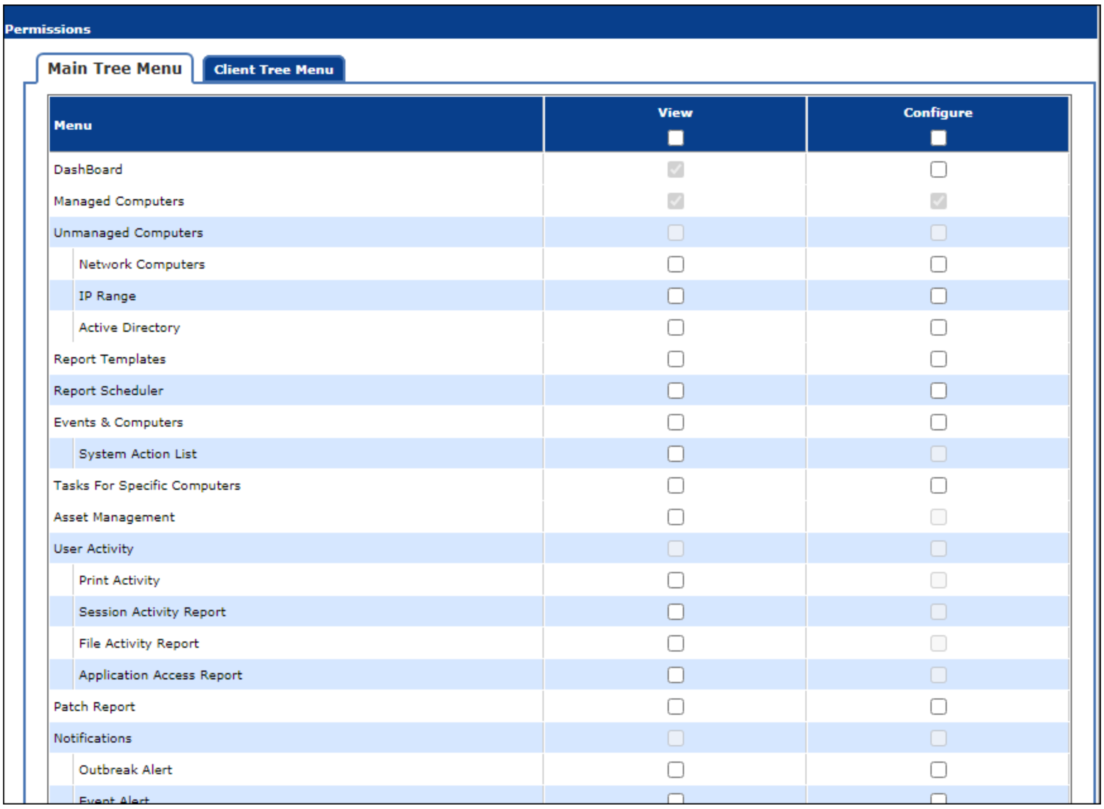
To add a user role,

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



2. Enter name and description for the role.
3. Click **Managed Computers** and select the specific group to assign the role.
   The added role will be able to manage and monitor only the selected group's activities.
4. Click **OK.**

Permissions section appears displaying Main Tree Menu and Client Tree Menu tabs. The Main Tree Menu consists of Navigation Panel Access permissions while the Client Tree Menu consists of selected groups on which permissions the user is allowed to take further.



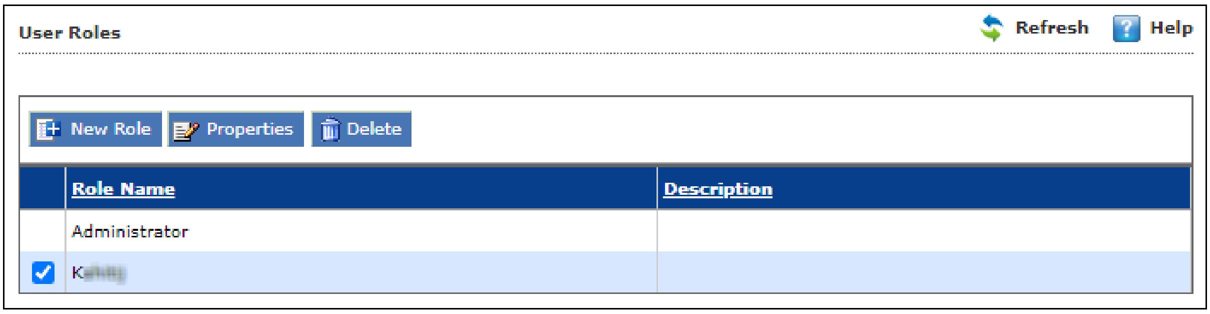
Menu	View □	Configure □
DashBoard	☑	□
Managed Computers	☑	☑
Unmanaged Computers	□	□
Network Computers	□	□
IP Range	□	□
Active Directory	□	□
Report Templates	□	□
Report Scheduler	□	□
Events & Computers	□	□
System Action List	□	□
Tasks For Specific Computers	□	□
Asset Management	□	□
User Activity	□	□
Print 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

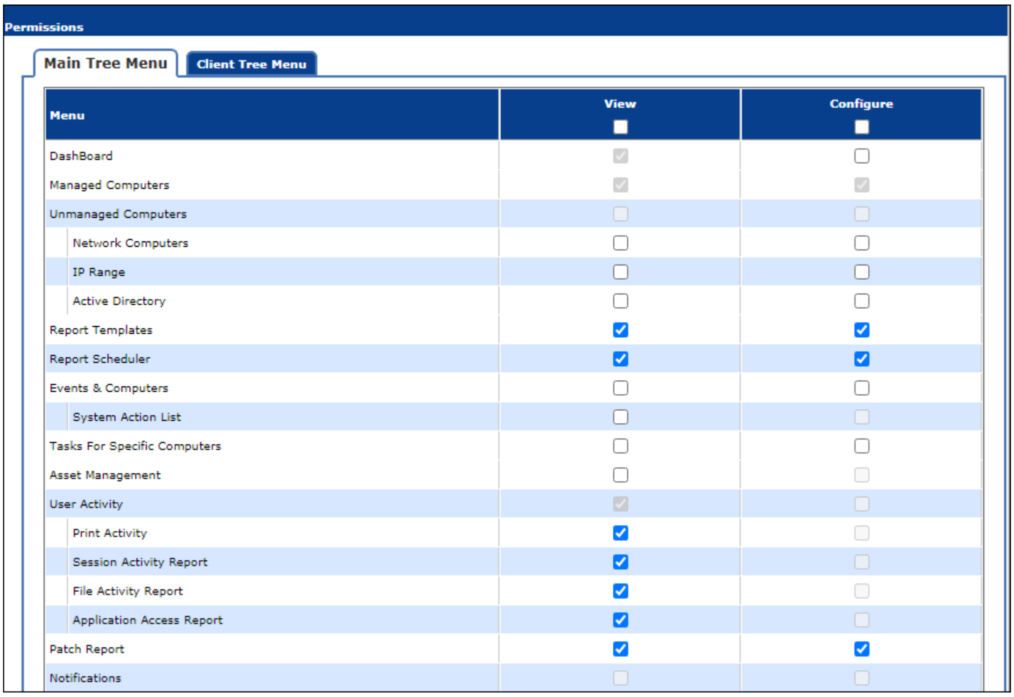
To view the properties of a role,

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



	Role Name	Description
	Administrator	
☑	[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**.



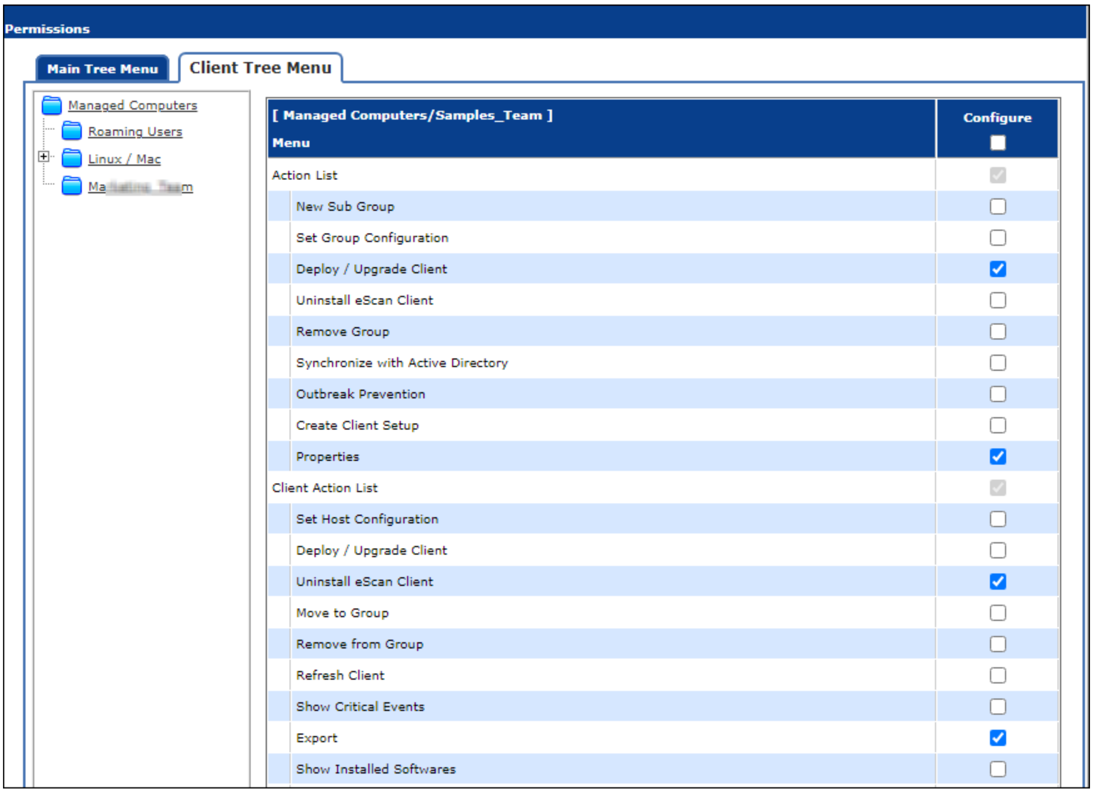
Permissions

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/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	☐

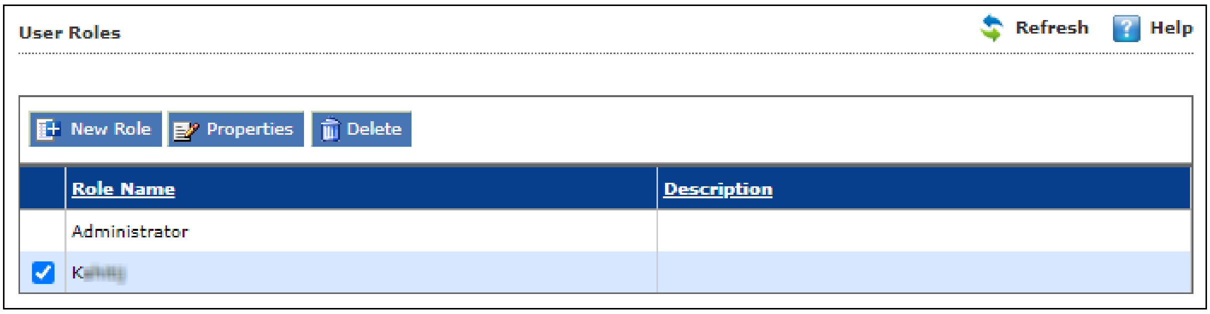
5. To let the role configure these actions, under the Configure column select the checkboxes of corresponding actions.

6. Click **Save**.
   The Role Properties will be updated accordingly.

Delete a User Role

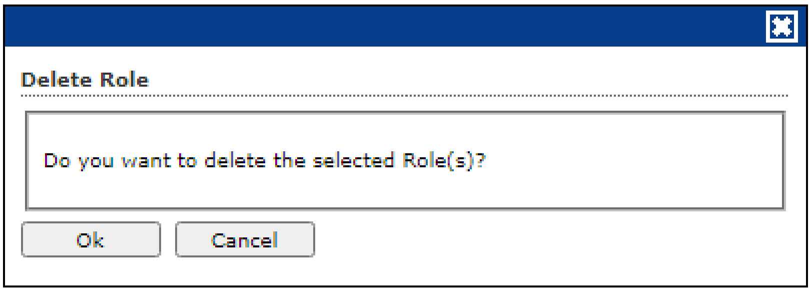
To delete a user role,

1. In the User Roles screen, select the user role you want to delete**.**



	Role Name	Description
	Administrator	
☑	K[redacted]	

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



Do you want to delete the selected Role(s)?

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

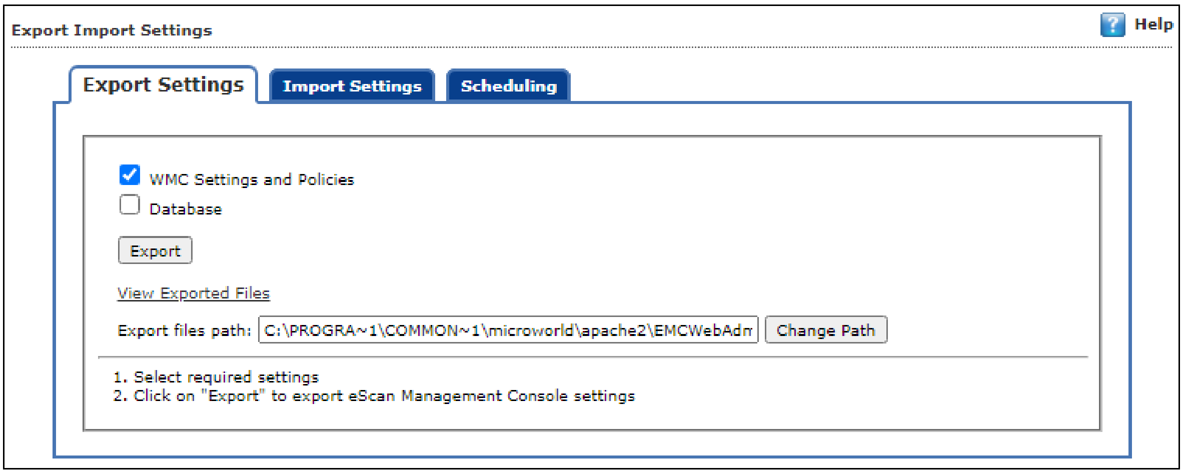
Export & Import

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.

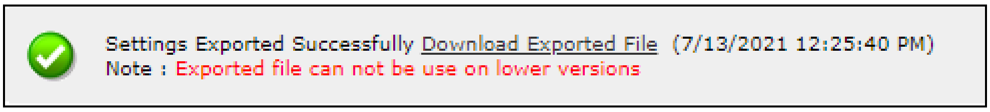


☑ WMC Settings and Policies
□ Database

Export files path: C:\PROGRA~1\COMMON~1\microworld\apache2\EMCWebAdm

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**. Enter the file path and click **Add**.
3. To view the exported files, click **View Exported Files**.
4. Click **Export**.
   The backup file will be exported to the destination path.
   A success message appears at the top displaying date, time, and a download link for the exported file.

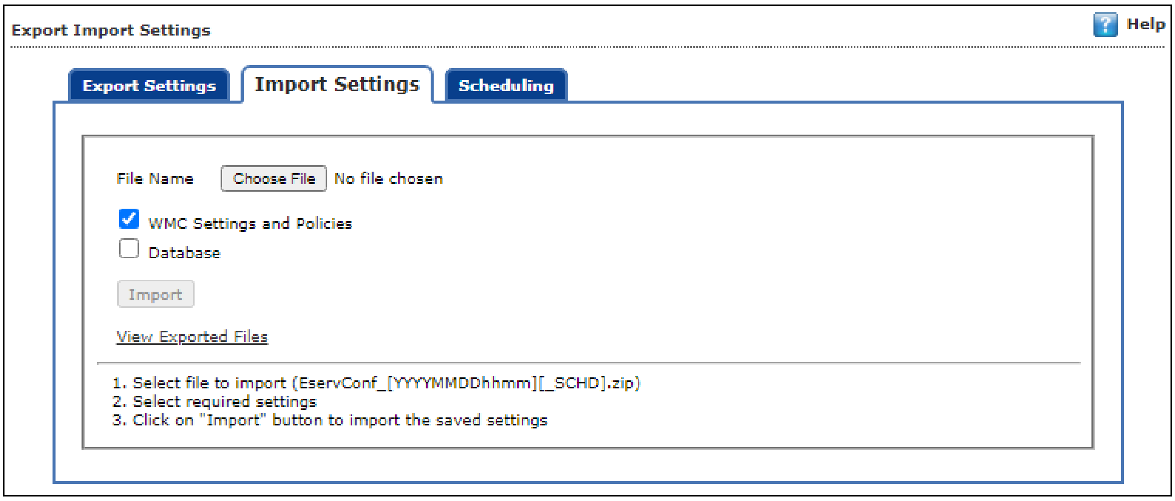


Settings Exported Successfully Download Exported File (7/13/2021 12:25:40 PM)
Note : Exported file can not be use on lower versions

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.



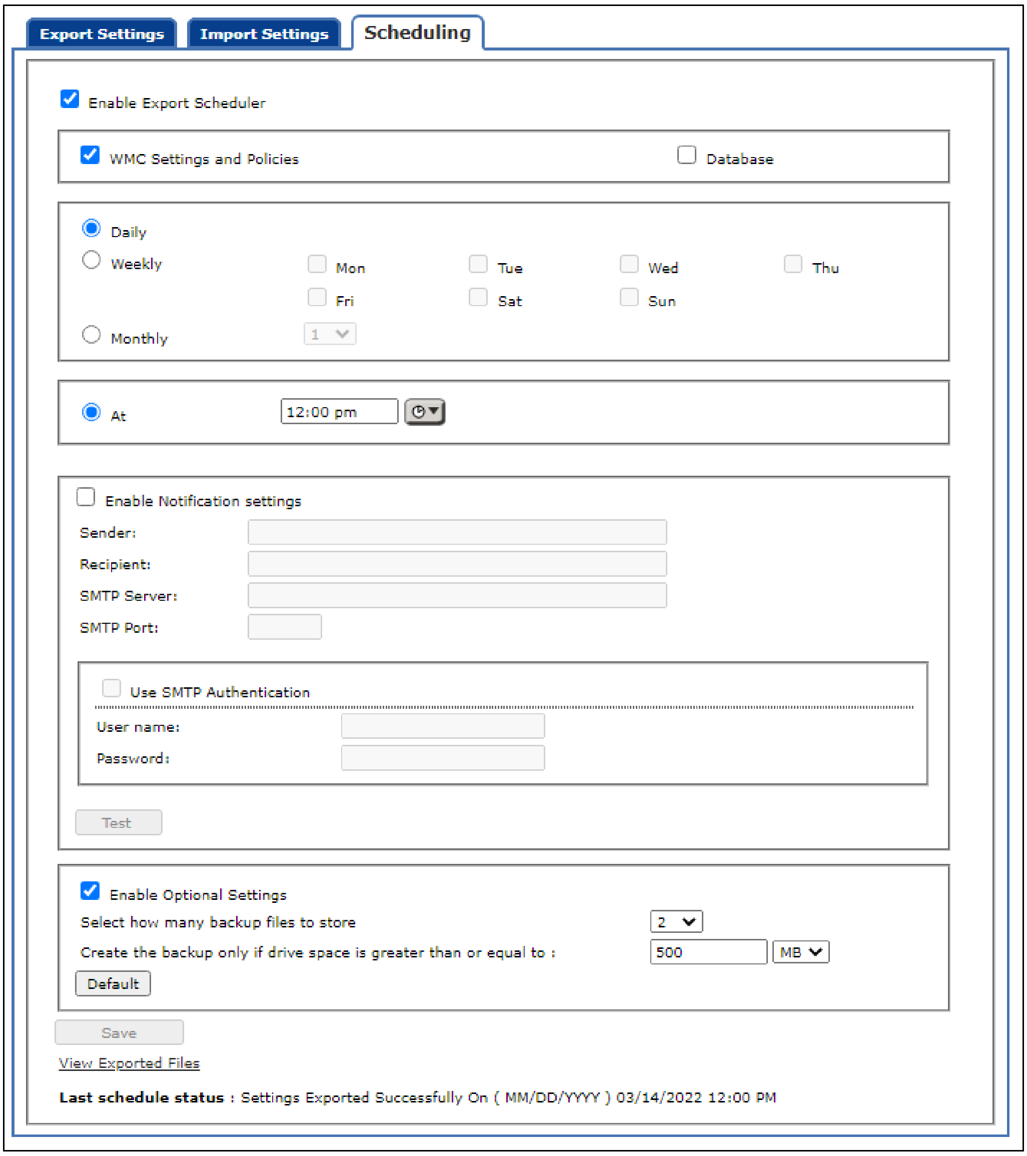
1. Select file to import (EservConf_[YYYYMMDDhhmm][_SCHD].zip)
2. Select required settings
3. Click on "Import" button to import the saved settings

2. Click **Choose File**.
   The Import Settings tab lets you import only Settings and Policies or Database.
3. To import **WMC Settings and Policies** and **Database**, select both the checkboxes.
4. To view the exported files, click **View Exported Files**.
5. Click **Import**.
   The backup file will be imported.
   A success message is displayed after complete import.

NOTE	After successfully taking a backup, eScan asks you to restart the server.

Scheduling

This tab lets you schedule auto-backing up of Settings, Policies, and Database.



☑ 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) 03/14/2022 12:00 PM

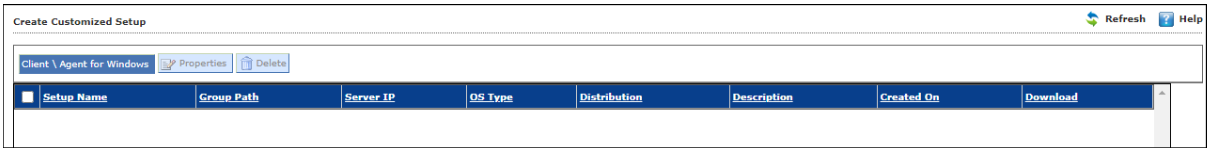
To create a Schedule for export, follow the steps given below:

1. Select **Enable Export Scheduler** checkbox.
2. Select the checkboxes whether to back up both **WMC Settings and Policies** and **Database**.
3. Schedule the backup for a **Daily**, **Weekly** (Select a day) or **Monthly** (Select a date) basis.
4. For the **At** field, click the drop-down and select a time for backing up data.
   If you want to receive email notifications about the procedure, select **Enable Notifications Settings** checkbox and fill in the necessary details.
5. If the SMTP server requires authentication, select the **Use SMTP Authentication** checkbox and enter the credentials.
6. To check if the SMTP settings are correct, click **Test**.
   A test email will be sent to recipient email ID.

7. To configure additional settings for backup file, select the **Enable Optional Settings**, and make the necessary changes.
8. To restore the changes made, click **Default**.
9. To view the exported files, click **View Exported Files**.
10. After performing all the necessary steps, click **Save**.
    The export schedule will be saved.

Customize Setup

This 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.



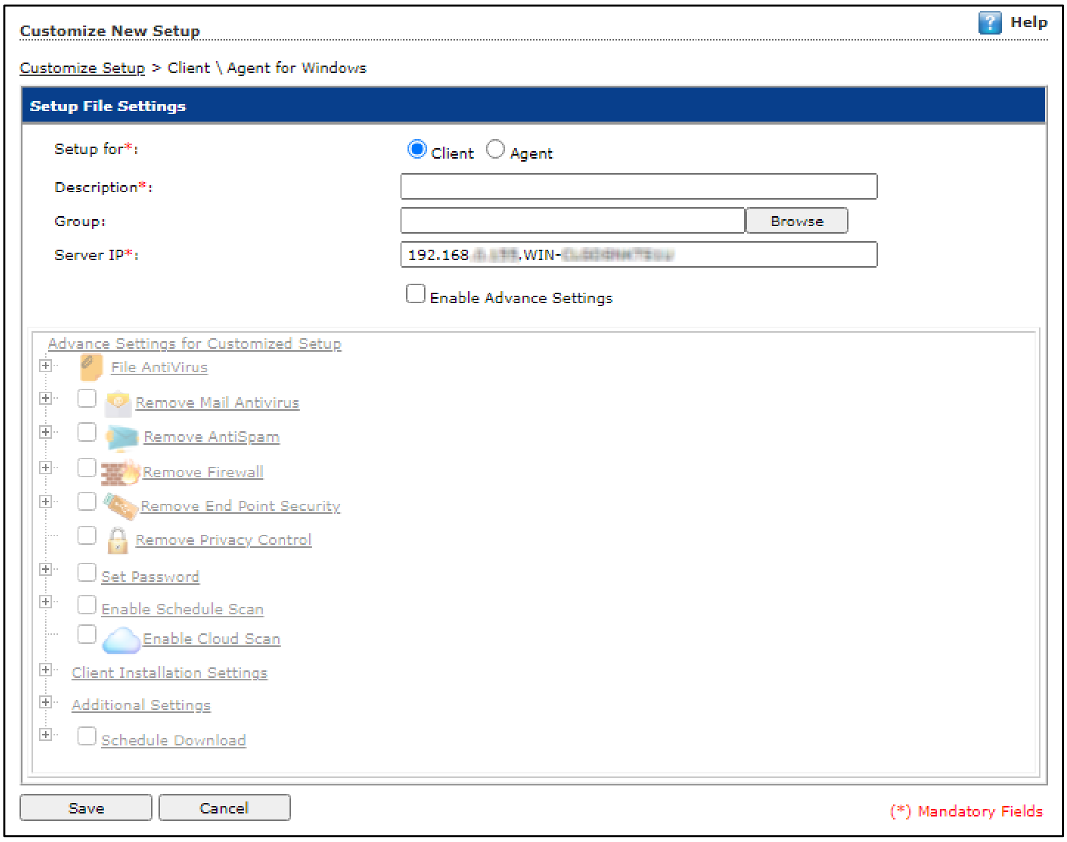
Create Customized Setup

☐	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.



Customize New Setup

Customize Setup > Client \ Agent for Windows

Setup File Settings

Setup for*: ● Client ○ Agent

Description*:

Group:

Server IP*: 192.168.[redacted].WIN-[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

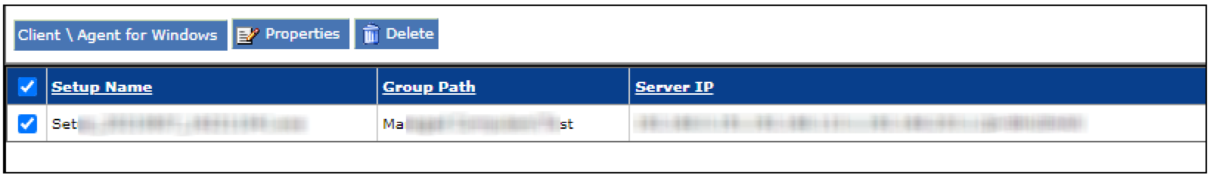
(*) Mandatory Fields

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. Select the setting checkboxes you want to provide.

7. Click **Save**.
   The customized setup for Windows will be created.

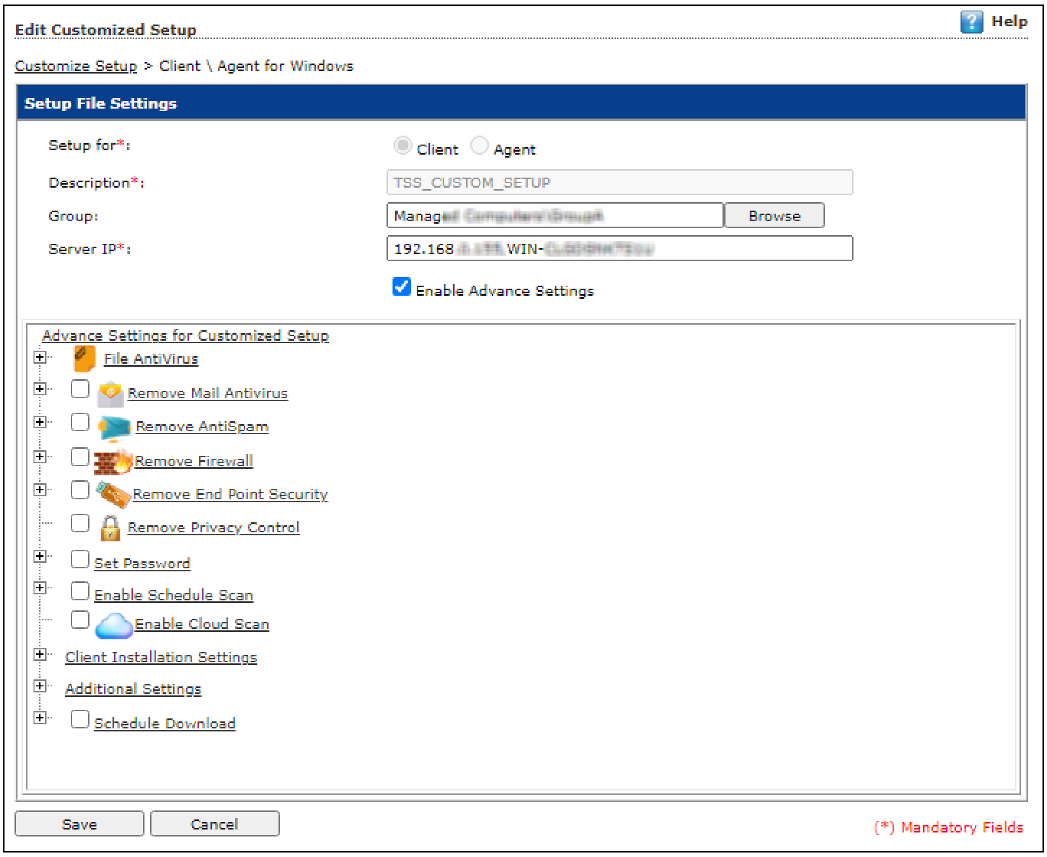
Editing Setup Properties

The properties can be edited only for customized Windows setup. To edit the customized Windows setup's properties, follow the steps given below:



☑	Setup Name	Group Path	Server IP
☑	Set[redacted]	Ma[redacted]st	[redacted]

1. In the Create Customized Setup screen, select the Windows setup you want to edit.
2. Click **Properties**.
   Edit Customized Setup screen appears.



Setup for*: ● Client ○ Agent

Description*: TSS_CUSTOM_SETUP

Group: Manage[redacted] Browse

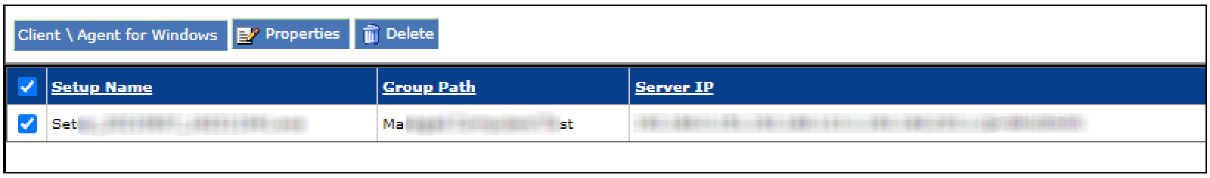
Server IP*: 192.168[redacted] WIN-[redacted]

☑ Enable Advance Settings

3. Make the necessary changes and then click **Save**.
   The setup will be updated.

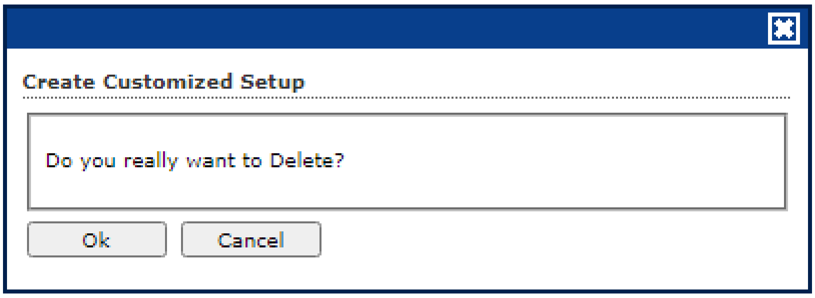
Deleting a Setup

To delete a setup, follow the steps given below:



☑	Setup Name	Group Path	Server IP
☑	Set[redacted]	Ma[redacted]st	[redacted]

1. In the Create Customized Setup screen, select the setup you want to delete.
2. Click **Delete**.



Create Customized Setup

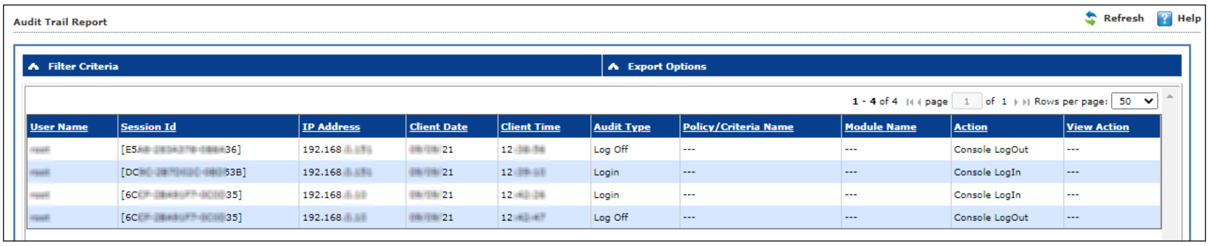
Do you really want to Delete?

4. Click **Ok**.

   The setup will be deleted.

Audit Trail

The Audit Trail submodule let you record the security relevant data, operation, event, Action, policy updates. Audit logs are used to track the date, time and activity of each user, including the policy/criteria that have been changed. A record of the changes that have been made to a database. You can get audit trail of user activity across all these systems.



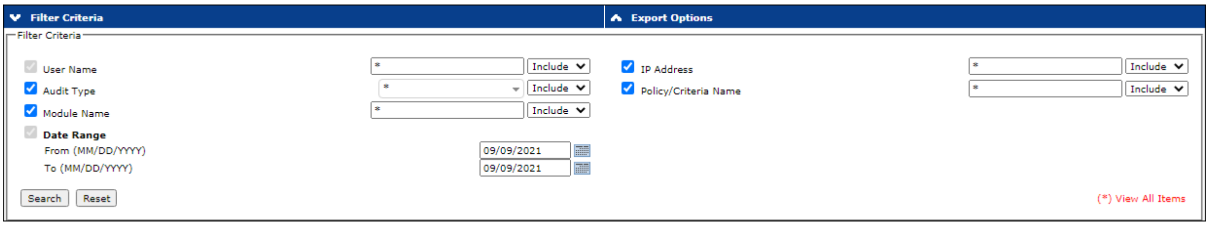
Audit Trail Report

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** field.
Filter Criteria field expands.



Filter Criteria

☑ User Name * Include
☑ Audit Type * Include
☑ Module Name * Include
☑ **Date Range**
From (MM/DD/YYYY) 09/09/2021
To (MM/DD/YYYY) 09/09/2021
☑ IP Address * Include
☑ Policy/Criteria Name * Include

(*) View All Items

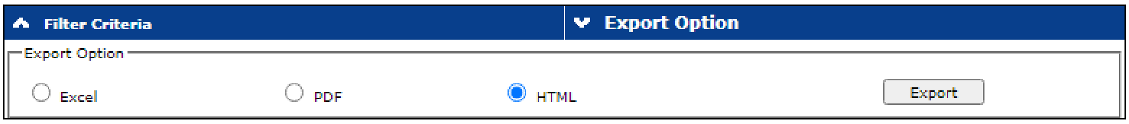
Select the parameters you want to be included in the filtered report.

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

After making the necessary selections, click **Search.**
The Audit Trail Report will be filtered according to your preferences.

Exporting Audit Trail

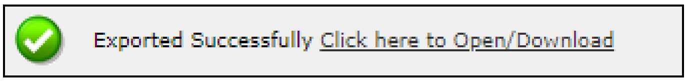
To export the Audit Trail Report, click **Export Option**.
Export Option field expands.



Export Option

○ Excel ○ PDF ● HTML

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

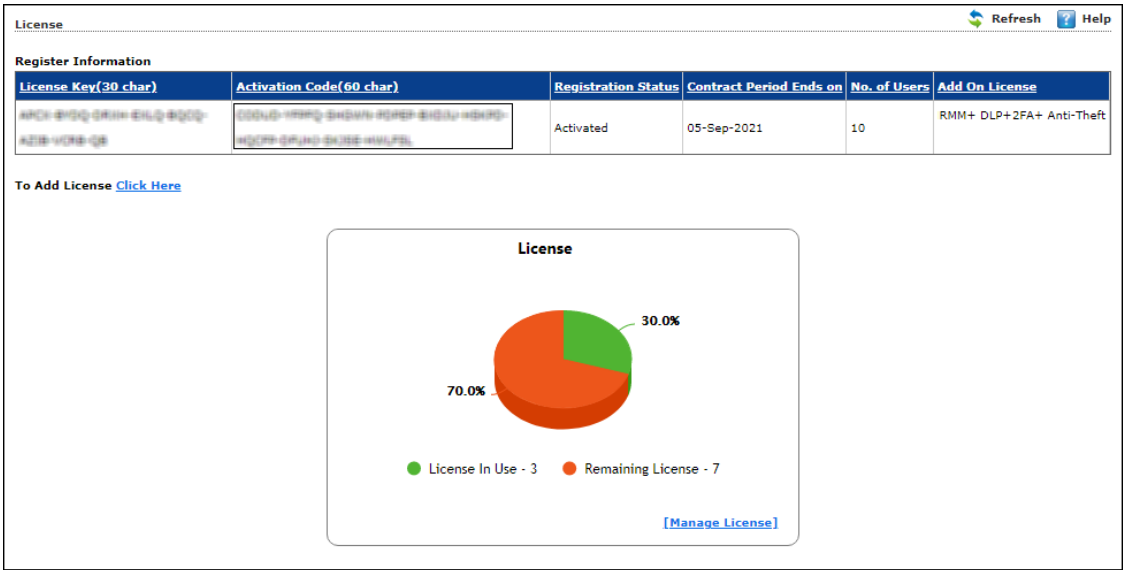


Exported Successfully Click here to Open/Download

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, and licenses remaining with their corresponding values. The module also lets you move the licensed computers to non-licensed computers and vice versa. Here you can also view the number of add-on license along with the name of it. For example, as you can see here there are 15 add-on licenses for eBackup feature. The add-on license is available for RMM, 2FA, and DLP features.



License

Register Information

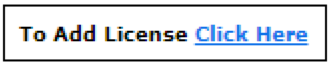
License Key(30 char)	Activation Code(60 char)	Registration Status	Contract Period Ends on	No. of Users	Add On License
[redacted]	[redacted]	Activated	05-Sep-2021	10	RMM+ DLP+2FA+ Anti-Theft

To Add License Click Here

Adding and Activating a License

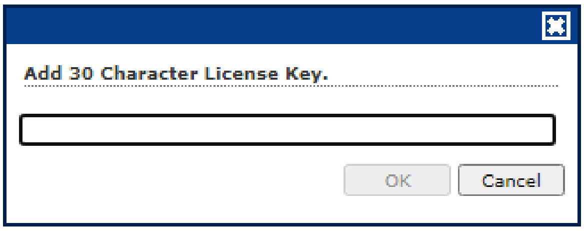
To add and activate a license,

1. In the License screen, click on **Click Here** link.



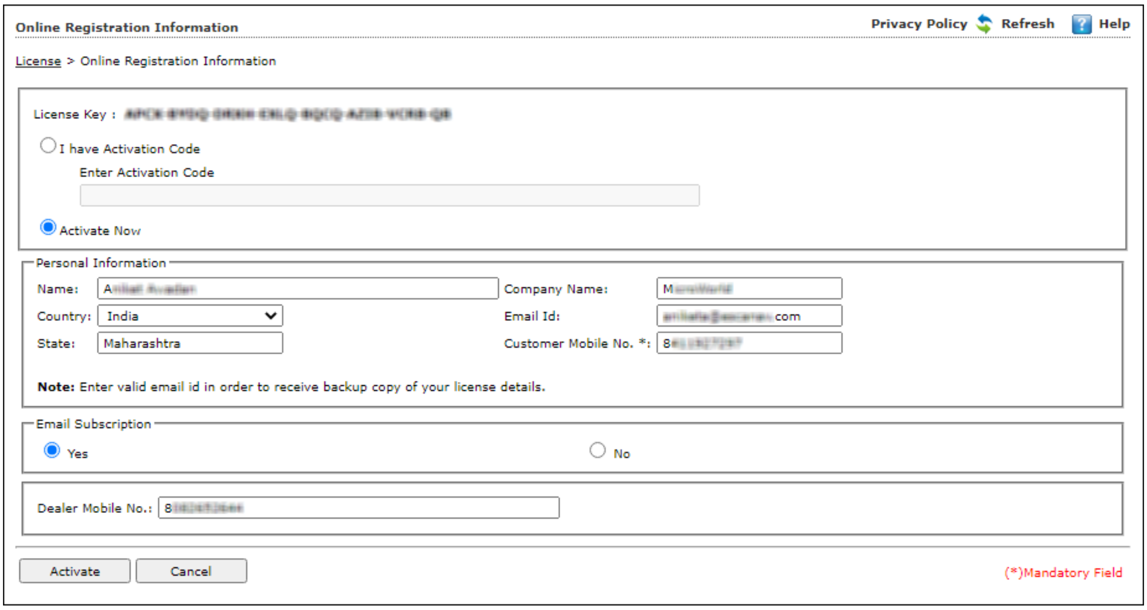
To Add License Click Here

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.
3. To activate the added license, click **Activate Now**.
4. Click **Activate now** link displayed in Activation Code column to activate the license key on eScan server system.
   Online Registration Information form appears.



Online Registration Information

Privacy Policy   Refresh   Help

License > Online Registration Information

License Key : [redacted]

○ I have Activation Code

Enter Activation Code

● Activate Now

Personal Information

Name:	[redacted]	Company Name:	M[redacted]
Country:	India	Email Id:	[redacted].com
State:	Maharashtra	Customer Mobile No. *:	8[redacted]

Note: Enter valid email id in order to receive backup copy of your license details.

Email Subscription

● Yes   ○ No

Dealer Mobile No.: 8[redacted]

Activate   Cancel

(*)Mandatory Field

5. Select a desired option for activation.
6. Enter details in **Personal Information** section.

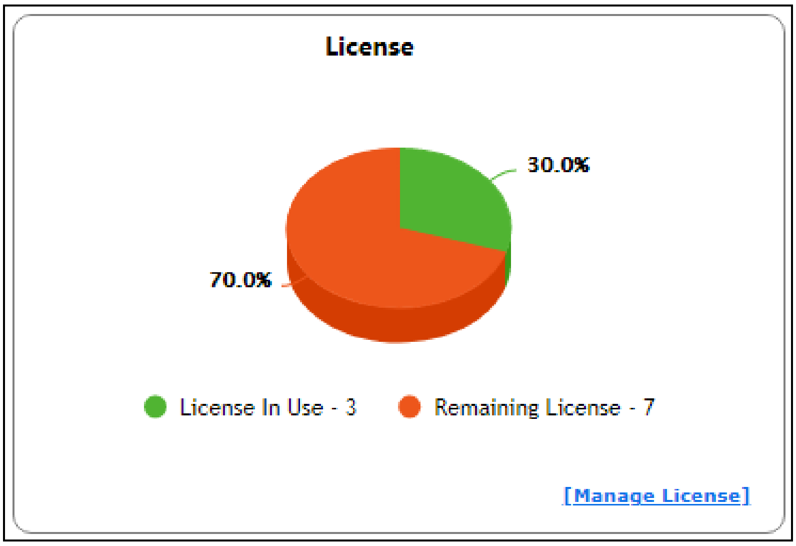
NOTE	Enter valid email id in order to receive backup copy of your license details.

7. Select a desired option for **Email Subscription**.
8. Enter the **Dealer Mobile Number**.
9. Click **Activate**. (Ensure that the Internet connection is Active.)

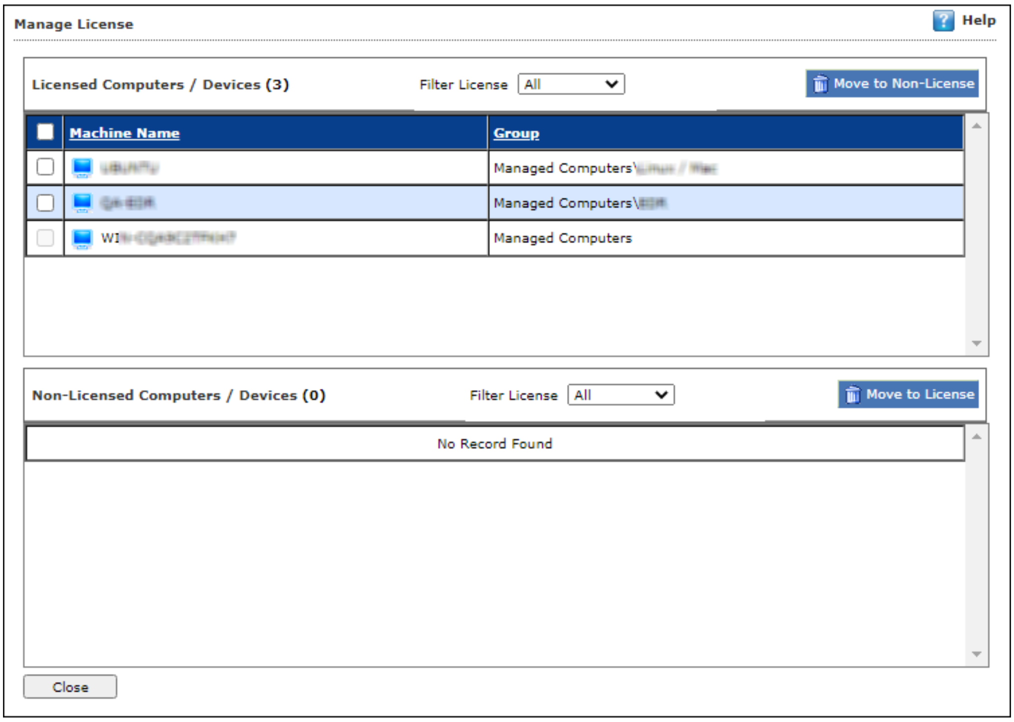
Moving Licensed Computers to Non-Licensed Computers

To move licensed computers to non-licensed computers,

1. In the License statistics box, click **Manage License**.



Manage License window appears.



Manage License

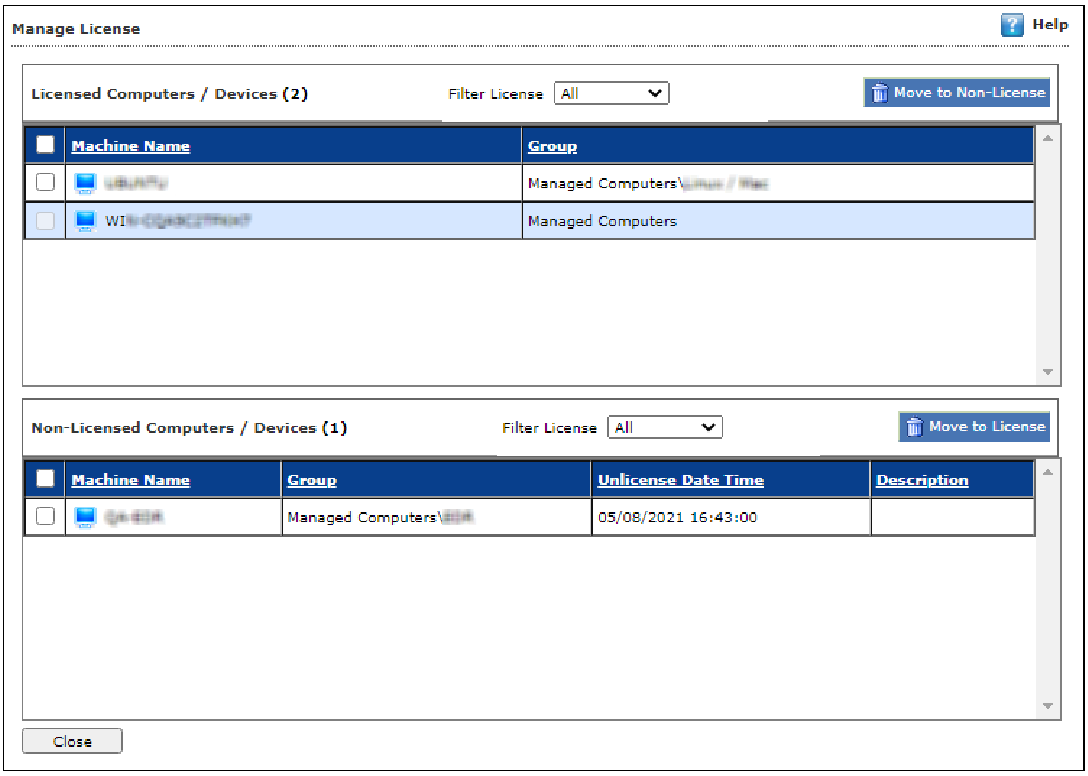
Licensed Computers / Devices (3) Filter License: All

□	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**.
   The selected computer(s) will be moved to Non-Licensed computers section.



Manage License

Licensed Computers / Devices (2) Filter License: All

□	Machine Name	Group
□	[redacted]	Managed Computers\[redacted]
□	WI[redacted]	Managed Computers

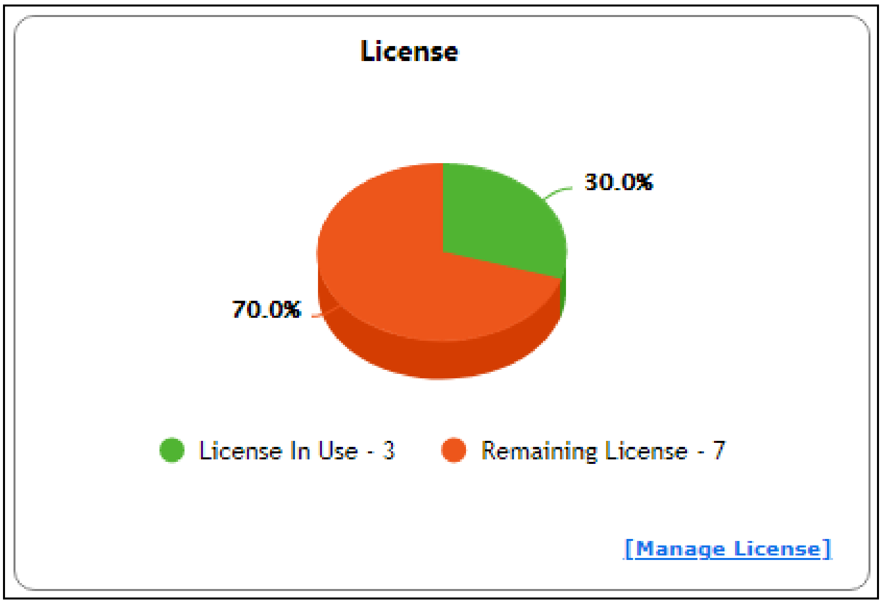
Non-Licensed Computers / Devices (1) Filter License: All

□	Machine Name	Group	Unlicense Date Time	Description
□	[redacted]	Managed Computers\[redacted]	05/08/2021 16:43:00	

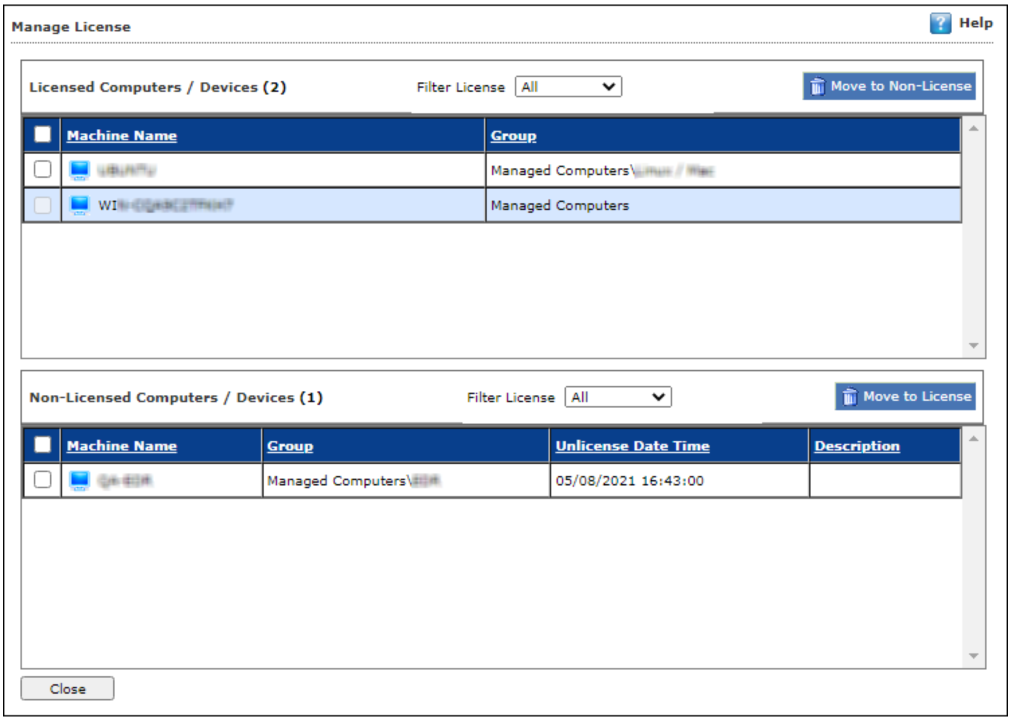
Moving Non-Licensed Computers to Licensed Computers

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

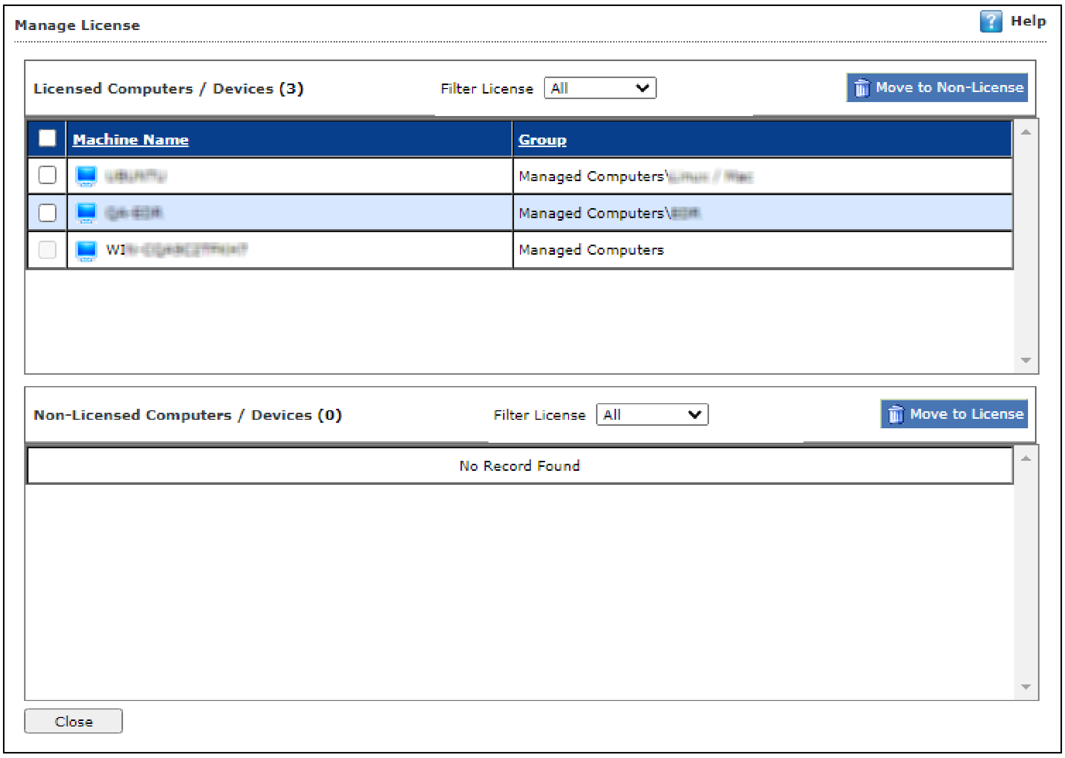
□	Machine Name	Group
□	[redacted]	Managed Computers\[redacted]
□	WI[redacted]	Managed Computers

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	

2. Under the **Non-Licensed Computers** section, select the computer(s) that you want to move to Licensed Computers section.

3. Click **Move to License**.
   The selected computer(s) will be moved to Licensed Computers section.



Manage License

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

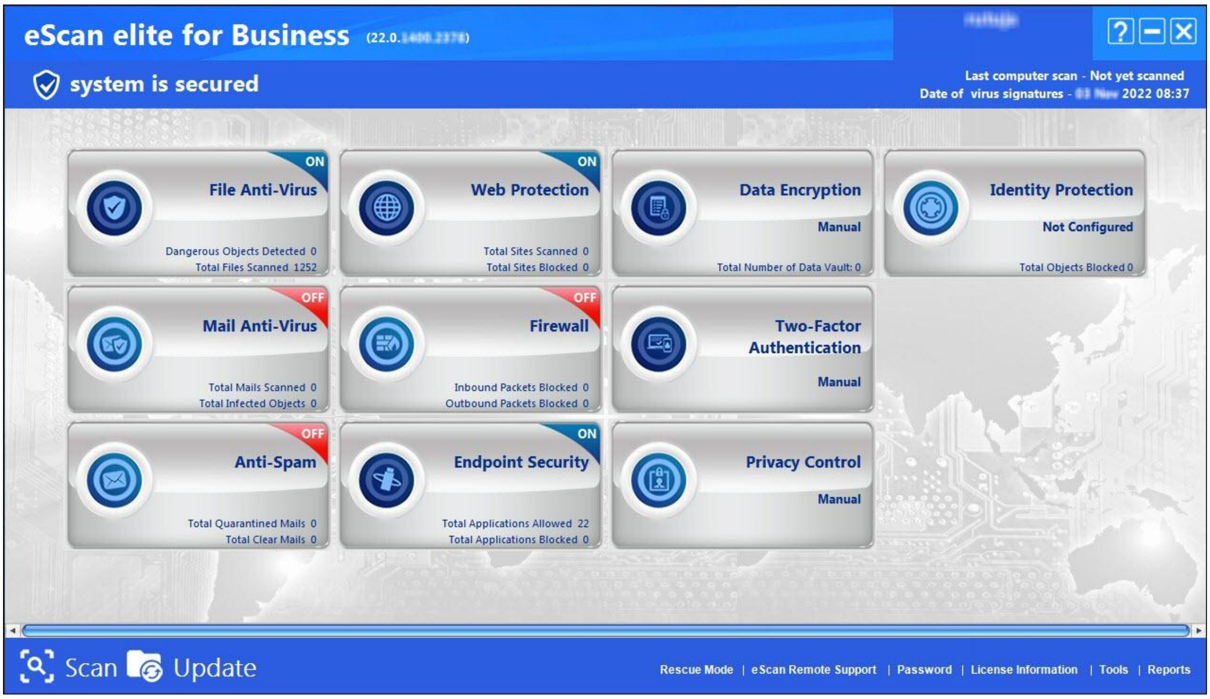
Getting Started

The following sections will be give you the detailed description and configuration procedure of all the eScan GUI and Modules presents in the eScan Elite for Business.

Graphical User Interface (GUI)

eScan 22 is not only equipped with the latest innovative technology but also has very simple yet trendy GUI. It is packed modules that gives brief details about the file scanned, quarantined, infected, and many more. It displays the date on which the computer was last scanned and virus signature updated.

eScan displays the real-time status of the computer (secured or not secured) along with additional options buttons and quick access links.



eScan elite for Business (22.0.[redacted]) [redacted]

system is secured

Last computer scan - Not yet scanned
Date of virus signatures - [redacted] 2022 08:37

File Anti-Virus ON
Dangerous Objects Detected 0
Total Files Scanned 1252

Web Protection ON
Total Sites Scanned 0
Total Sites Blocked 0

Data Encryption
Manual
Total Number of Data Vault: 0

Identity Protection
Not Configured
Total Objects Blocked 0

Mail Anti-Virus OFF
Total Mails Scanned 0
Total Infected Objects 0

Firewall OFF
Inbound Packets Blocked 0
Outbound Packets Blocked 0

Two-Factor Authentication
Manual

Anti-Spam OFF
Total Quarantined Mails 0
Total Clear Mails 0

Endpoint Security ON
Total Applications Allowed 22
Total Applications Blocked 0

Privacy Control
Manual

Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

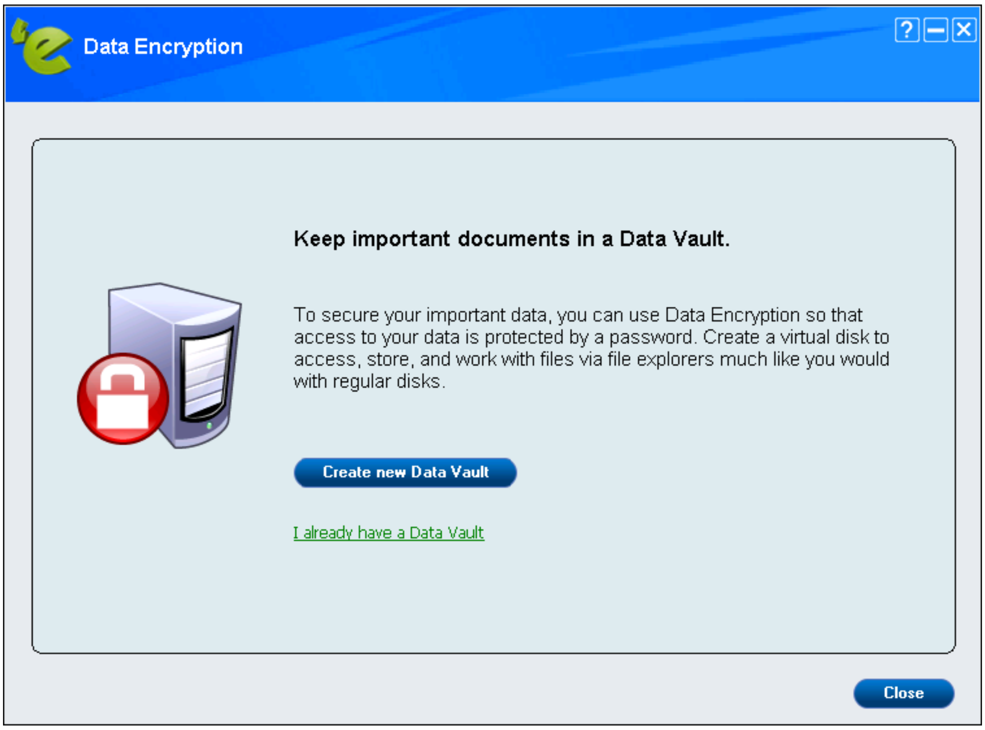
Data Encryption

The Data Encryption module lets you protect sensitive and confidential data from unauthorized access and data leak. With this module, the user can create a Vault that stores data in encrypted format.
The Vault is encrypted using 256-bit Advanced Encryption Standard (AES) and HMAC-SHA 256-bit key. A password is required to access the vault. After you access the vault, the data stored will be automatically decrypted. Vice versa, after you close the vault, the data stored will be automatically encrypted.

How to Create a Vault?

To create a vault, follow the steps given below:

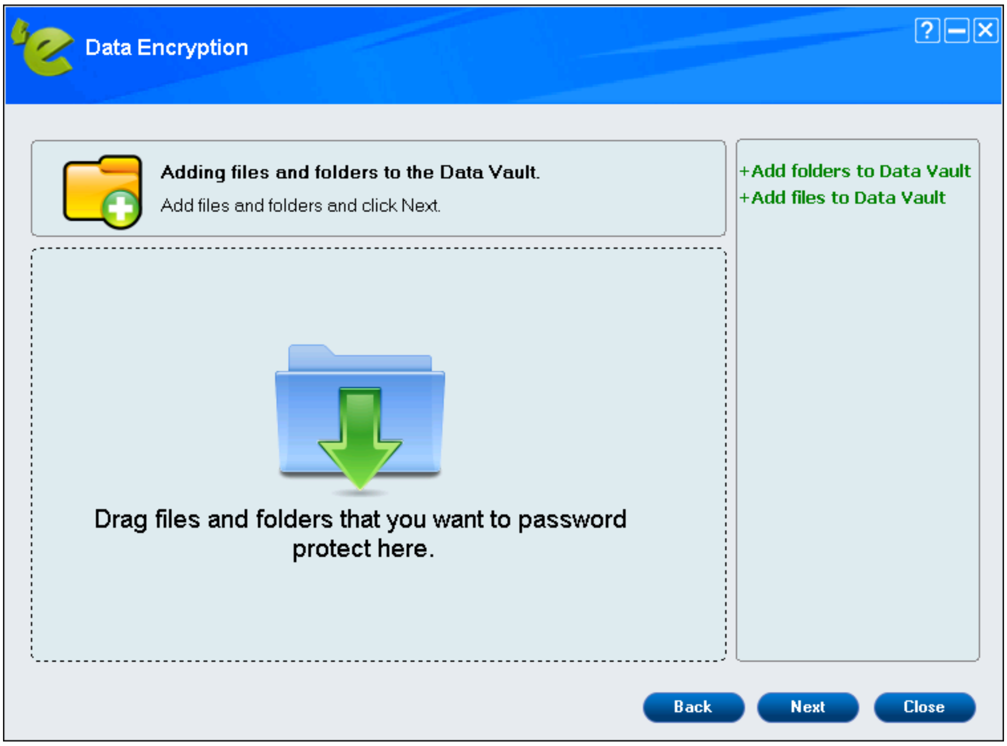
1. Launch eScan.
2. Click **Data Encryption**.
   Data Vault window appears.
3. Click **Create new Data Vault**.



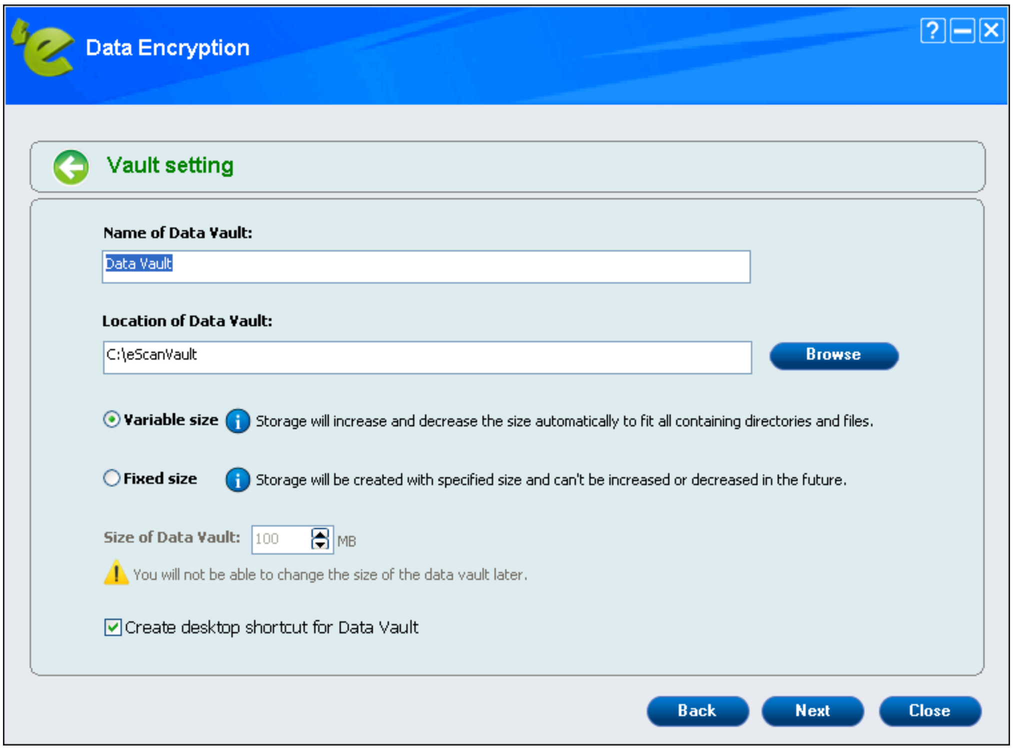
Keep important documents in a Data Vault.

To secure your important data, you can use Data Encryption so that access to your data is protected by a password. Create a virtual disk to access, store, and work with files via file explorers much like you would with regular disks.

4. To add files or folders in Data Vault, click **Add folders to Data Vault** or **Add files to Data Vault**. You can add files and folders by drag files and folders to vault.


Data Encryption
?
Adding files and folders to the Data Vault.
Add files and folders and click Next.
+Add folders to Data Vault
+Add files to Data Vault
Drag files and folders that you want to password protect here.
Back
Next
Close

5. After adding required files and folder, click **Next**.
6. Configure the Data Vault:
   - **Name of Data Vault**: Enter a name for the vault.
   - **Location of Data Vault**: To select a custom location for Data Vault, click **Browse**. The default path for vault is **c:\eScanVault**.
   - Select a size for Data Vault, **Variable size** or **Fixed size**. If selected **Fixed size** enter the size in below field or use the arrow buttons to specify size.
   - Optionally, select the checkbox **Create desktop shortcut for Data Vault**.



Name of Data Vault:
Data Vault

Location of Data Vault:
C:\eScanVault

● Variable size Storage will increase and decrease the size automatically to fit all containing directories and files.

○ Fixed size Storage will be created with specified size and can't be increased or decreased in the future.

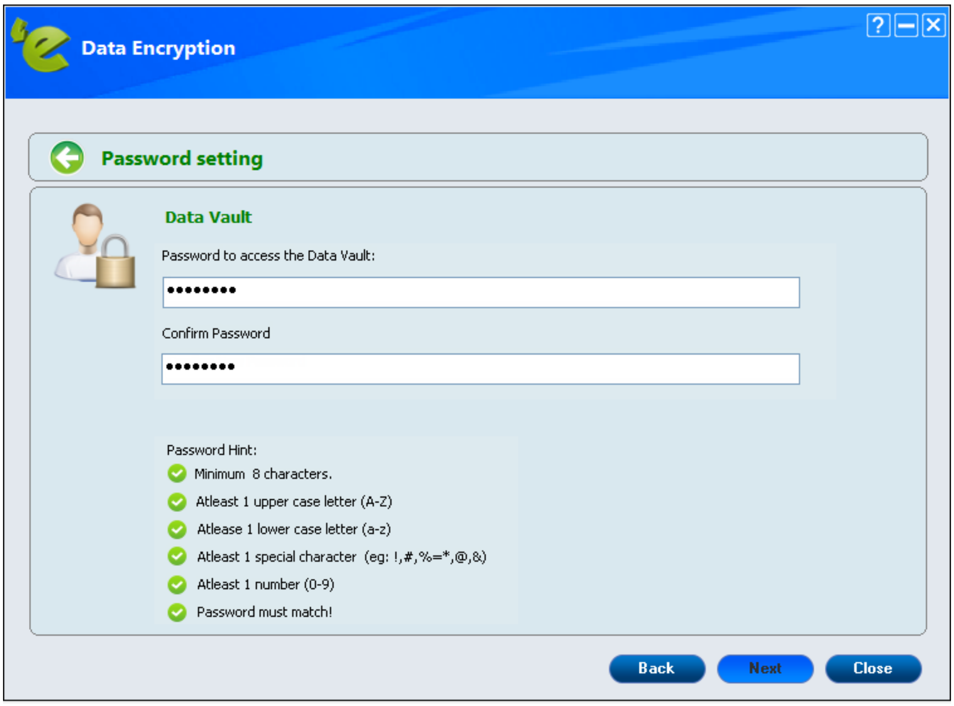
Size of Data Vault: 100 MB

You will not be able to change the size of the data vault later.

☑ Create desktop shortcut for Data Vault

7. After filling all the details, click **Next**.
8. Read the **Password Hint** and then enter the password.

NOTE	In case, if you forget your password, it can be recovered with the help of eScan Team.



Data Vault

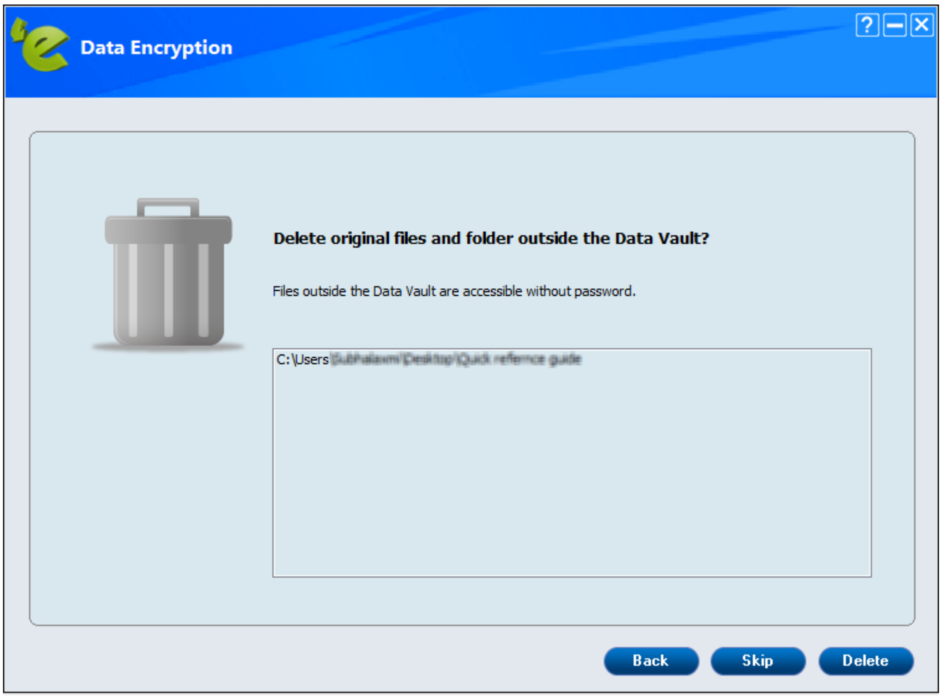
Password to access the Data Vault:
••••••••

Confirm Password
••••••••

Password Hint:
- ✓ Minimum 8 characters.
- ✓ Atleast 1 upper case letter (A-Z)
- ✓ Atlease 1 lower case letter (a-z)
- ✓ Atleast 1 special character (eg: !,#,%=*,@,&)
- ✓ Atleast 1 number (0-9)
- ✓ Password must match!

9. Click **Next**.

10. Data will be copied to the Data Vault. If you wish to delete the original files and folders outside the data vault by clicking **Delete** or else click **Skip**.

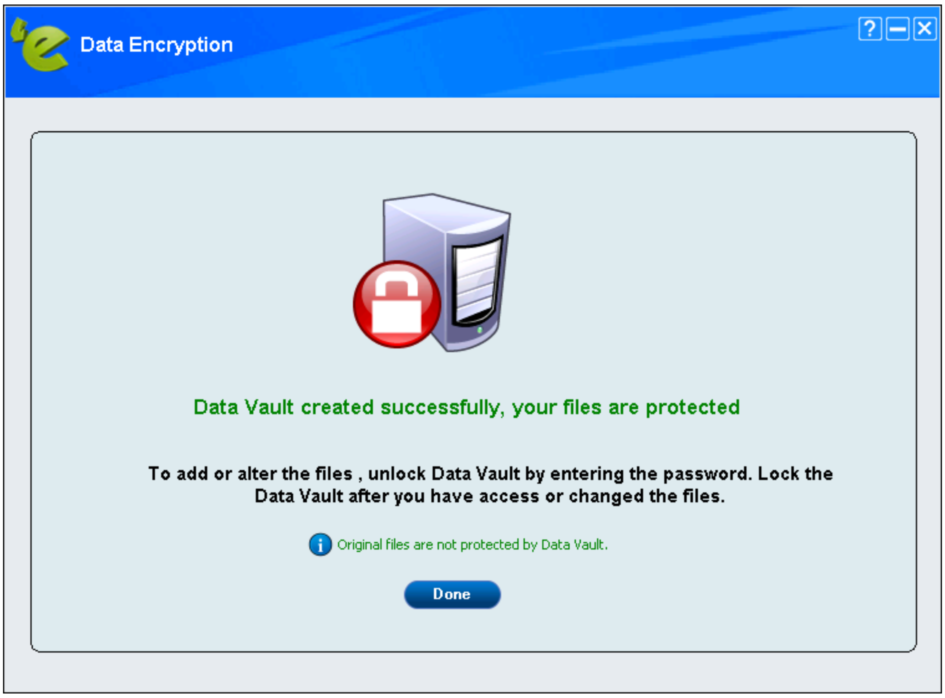


Delete original files and folder outside the Data Vault?

Files outside the Data Vault are accessible without password.

C:\Users[redacted]

11. Click **Finish**.
12. Data Encryption window appears, click **Done**.

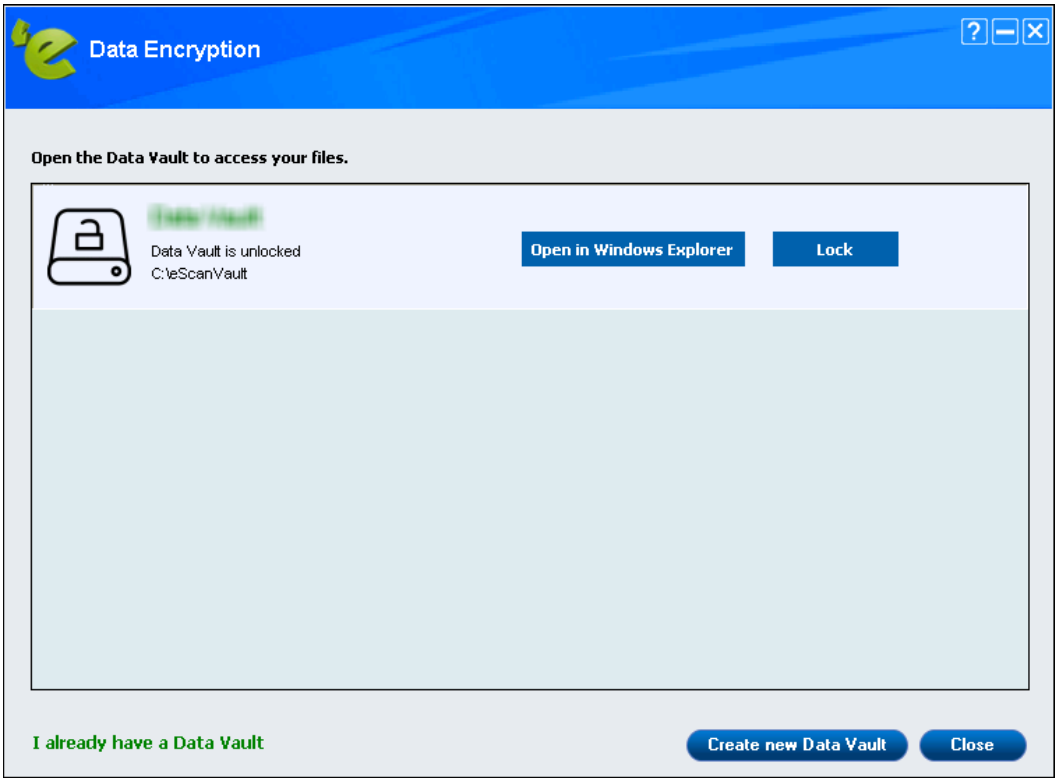


Data Vault created successfully, your files are protected

To add or alter the files , unlock Data Vault by entering the password. Lock the Data Vault after you have access or changed the files.

Original files are not protected by Data Vault.

13. The Data Vault will be created and get displayed on the data encryption list. To encrypt your data, click **Lock**.

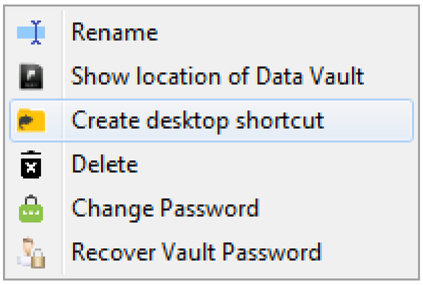


Open the Data Vault to access your files.

[redacted]
Data Vault is unlocked
C:\eScanVault

14. Click **Close**.
    The created Data Vault will be encrypted.

After the data vault is locked, you will get **More** button displayed the right-hand side of the screen. Through this option, you will get the following setting to configure the data vault:

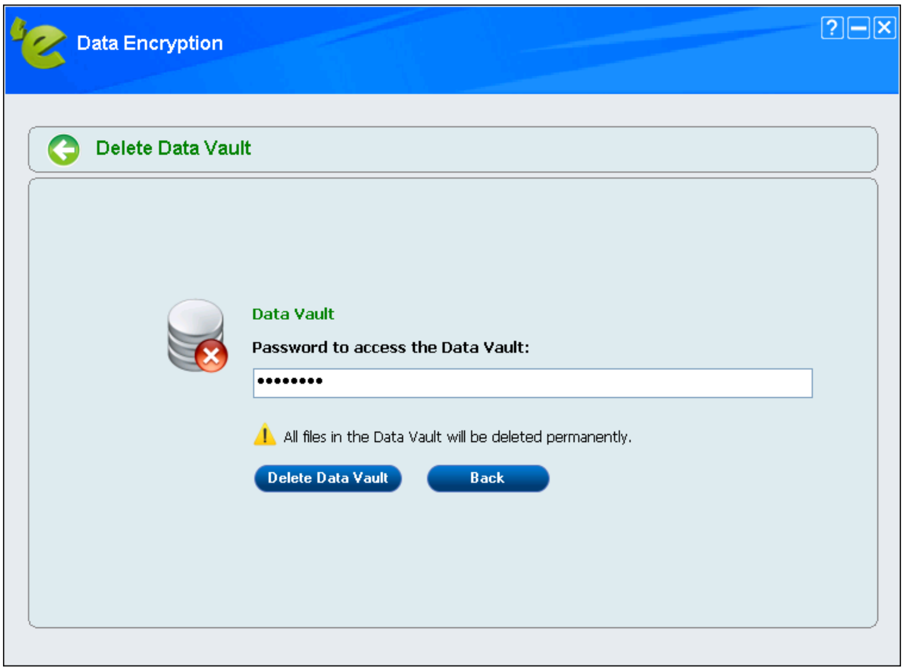


Rename
You can rename the existing data vault. After clicking on this option, Rename window appears, change the name and click **Save**.

Show location of Data Vault
This option will open the location where data vault is created.

Create desktop shortcut
This option will create shortcut for the created vault for accessing it easily.

Delete
You can delete the existing data vault. Click on this option, the screen will prompting for password.



Data Vault

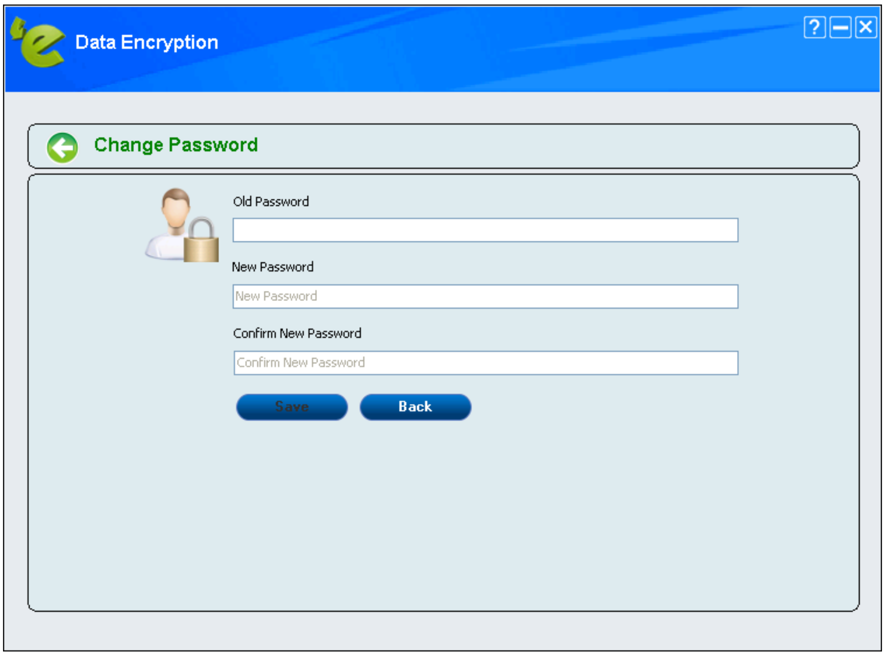
Password to access the Data Vault:

••••••••

⚠ All files in the Data Vault will be deleted permanently.

After entering the password, click **Delete Data Vault**.
This will delete the selected data vault.

Change Password
This option allows you to change the password set for the data vault. Click this option; you will be forwarded to the Data Encryption window.



Old Password

New Password

New Password

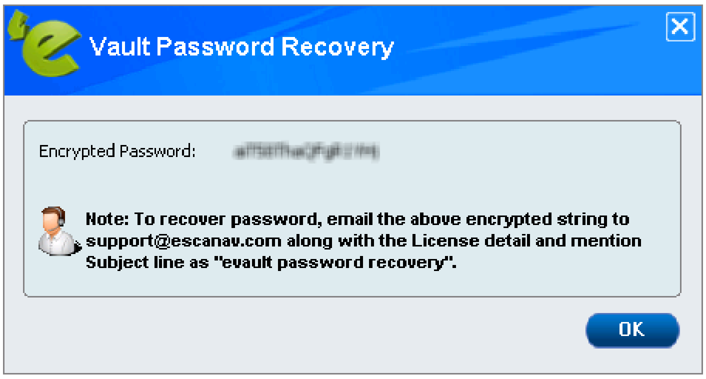
Confirm New Password

Confirm New Password

Enter the **Old Password**, **New Password**, and **Confirm New Password**.
Click **Save**.
This will change the password of the data vault.

Recover Password

This option is used to recover password, this will generate the password in an encrypted format.



Encrypted Password: [redacted]

Note: To recover password, email the above encrypted string to support@escanav.com along with the License detail and mention Subject line as "evault password recovery".

NOTE	If you selected **Create desktop shortcut for Data Vault** checkbox, it will create a shortcut of data vault to the desktop ().

Two-Factor Authentication

The system login password is Single-Factor Authentication which is considered unsecure as it may put your system's data at high risk of compromise. The Two-Factor Authentication, also more commonly known as 2FA, adds an extra layer of protection to your computer.

The 2FA feature mandates you to enter a Time-based One-Time Password (TOTP) after entering Windows login credentials. So, even if somebody knows your login credentials, the 2FA feature secures data against unauthorized logins.

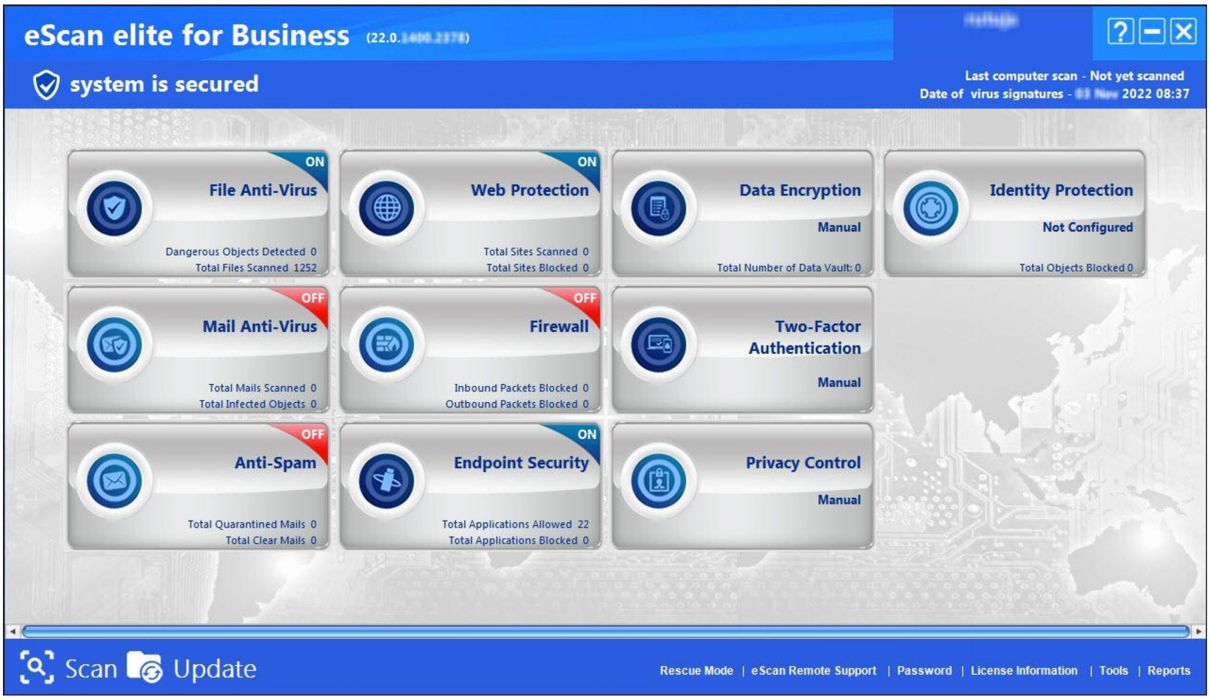
You can use various options to set password for the 2FA. You can set password or you can use the eScan administrator password in case the system is offline (without internet access). To use 2FA online authentication, you need to install the Authenticator app for Android devices from Play Store or for iOS devices from App Store on your smart device. The Authenticator app needs camera access for scanning a QR code in the Authenticator app.

NOTE	Ensure that the smart device's date and time matches with the system's date and time or else TOTPs generated by app won't get validated.

Enabling 2FA login

To enable 2FA login, follow the below steps:

1. Open eScan Protection Center,
   - From desktop, double-click the 🛡 icon.
   - From taskbar, right-click the 🛡 icon and click **Open eScan Protection Center**.



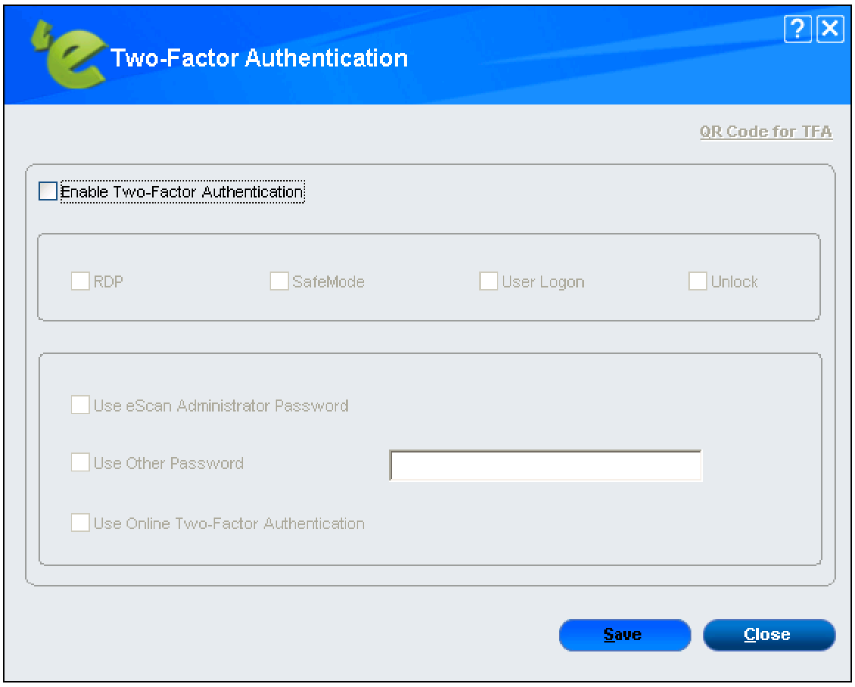
eScan elite for Business (22.0.[redacted])

[redacted]

system is secured

Last computer scan - Not yet scanned
Date of virus signatures - [redacted] 2022 08:37

2. Click **Two-Factor Authentication**.



Two-Factor Authentication

QR Code for TFA

□ Enable Two-Factor Authentication

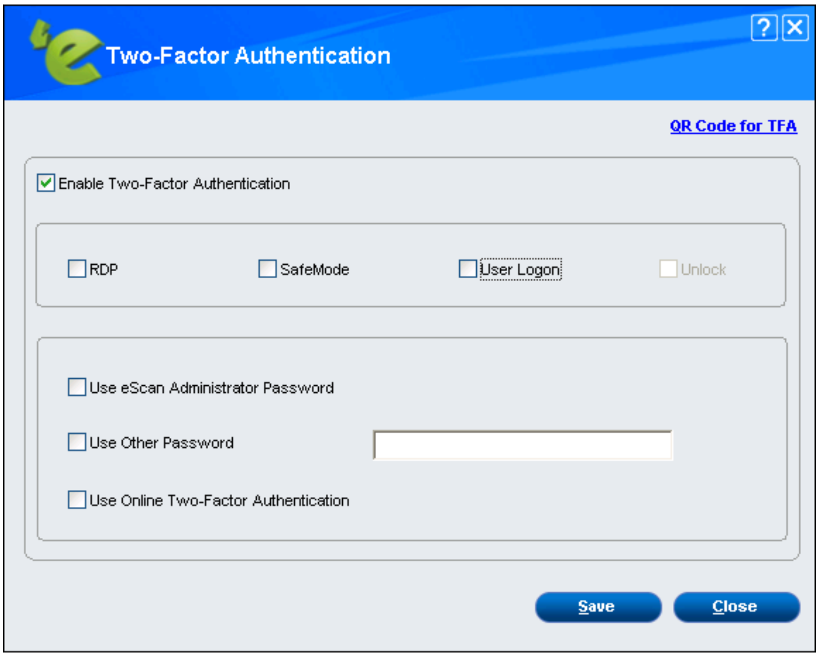
□ RDP □ SafeMode □ User Logon □ Unlock

□ Use eScan Administrator Password

□ Use Other Password

□ Use Online Two-Factor Authentication

3. Select **Enable Two-Factor Authentication**. This will enable the other configuration settings.



Two-Factor Authentication

QR Code for TFA

☑ Enable Two-Factor Authentication

□ RDP □ SafeMode □ User Logon □ Unlock

□ Use eScan Administrator Password

□ Use Other Password

□ Use Online Two-Factor Authentication

NOTE	**Unlock** option will be enabled only after selecting **User Logon** option.

4. You can configure it according to your requirement and click **Save**.
   The 2FA will work according to the configuration.

Login Scenarios

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

RDP

RDP stands for Remote Desktop Protocol. Whenever someone takes remote control of your system, the personnel will have to enter system login credentials and 2FA passcode to access the system.

Safe Mode

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

User Logon

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

Unlock

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

Password Types

You can use following password types to log in:

Use eScan Administrator Password

You can use the existing eScan Administrator password for 2FA login.

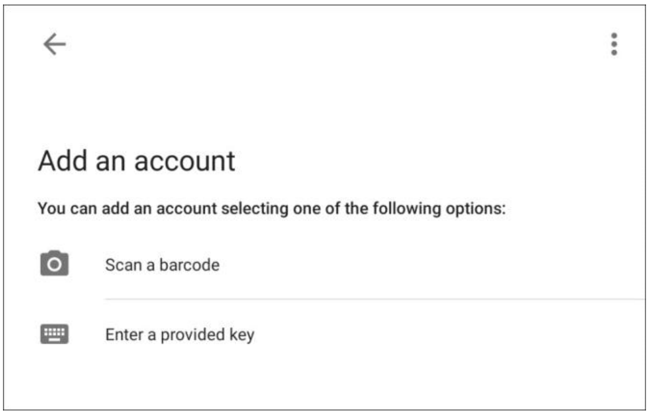
Use Other Password

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

Use Online Two-Factor Authentication

To use Online 2FA authentication, follow the steps given below:

1. Install the Authenticator app from Play Store for Android devices or App Store for iOS devices.
2. Open the Authenticator app and tap **Scan a barcode**.

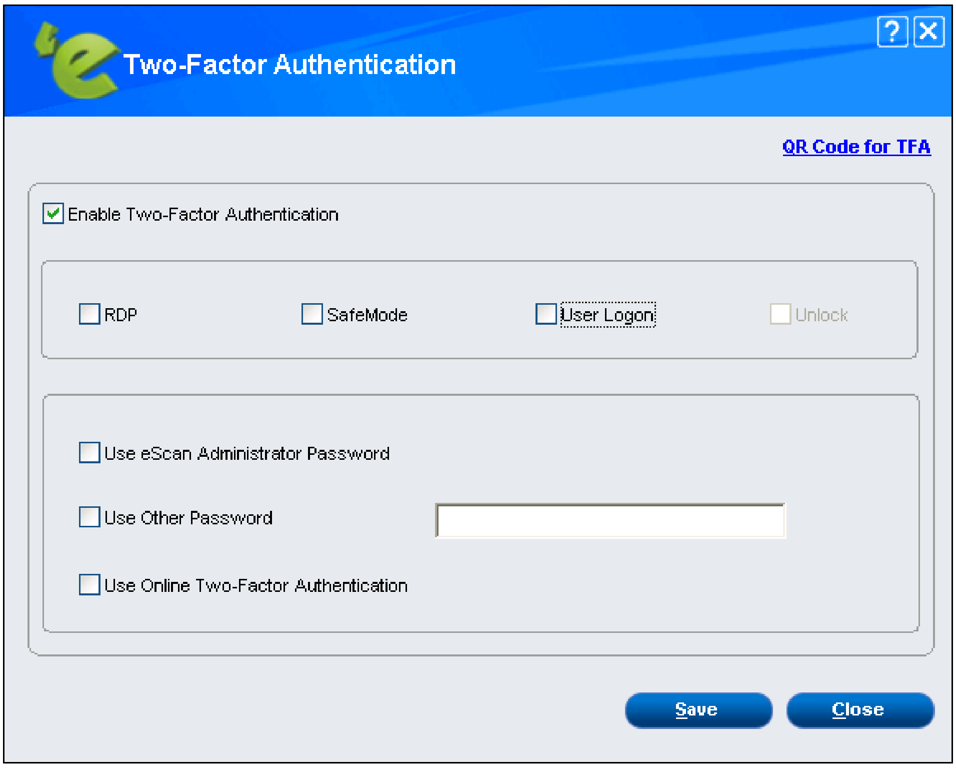


Add an account

You can add an account selecting one of the following options:

3. Now, open **eScan Protection Center** on your system and click **Two-Factor Authentication**.

4. Select **Enable Two-Factor Authentication.**



Two-Factor Authentication

QR Code for TFA

☑ Enable Two-Factor Authentication

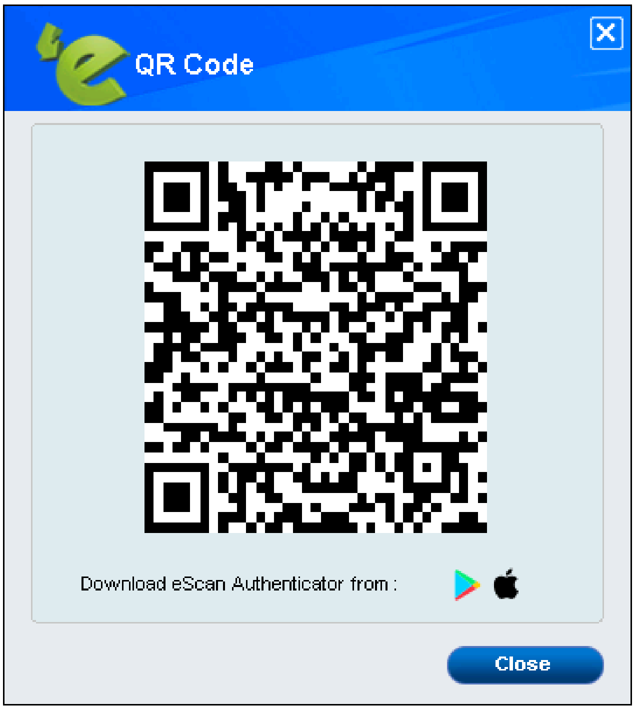
☐ RDP ☐ SafeMode ☐ User Logon ☐ Unlock

☐ Use eScan Administrator Password

☐ Use Other Password

☐ Use Online Two-Factor Authentication

5. Configure the login scenarios according to your need and select **Use Online Two-Factor Authentication.**
6. On the top right corner, click **QR code for TFA**.
   A QR code appears.

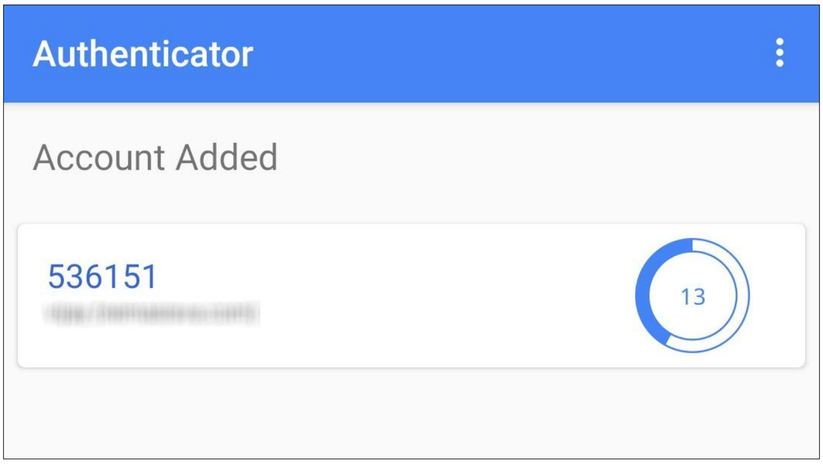


QR Code

Download eScan Authenticator from :

7. Scan the onscreen QR code via the Authenticator app.

A Time-based One-Time Password (TOTP) appears on smart device.



Authenticator

Account Added

536151

8. You can use this TOTP for login.
   This TOTP will get updated after every 30 seconds.

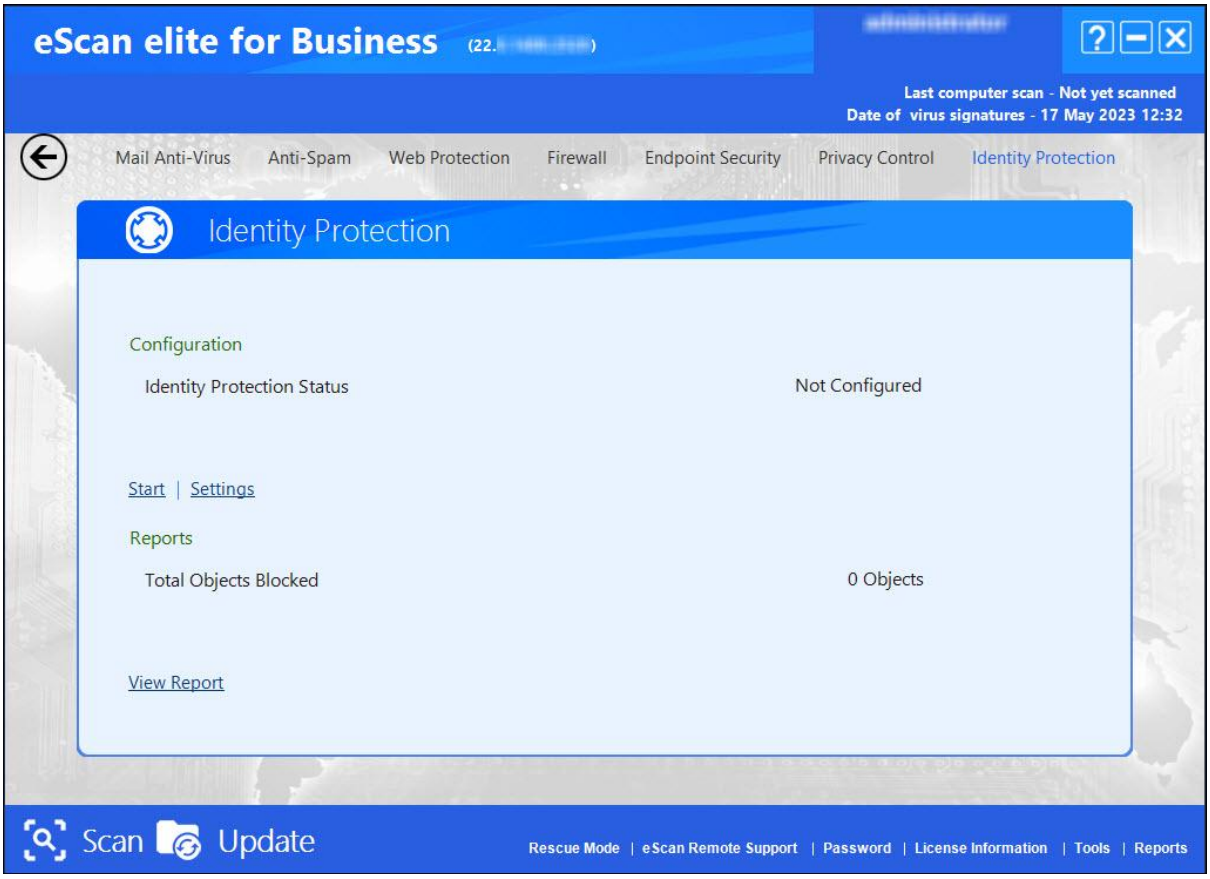
Disabling 2FA login

To disable the 2FA login, follow the below steps:

1. Open **eScan Protection Center** > **Two-Factor Authentication**.
2. Uncheck the **Enable Two-Factor Authentication** option.
3. Click **Save**.
   The 2FA feature gets disabled.

Identity protection

Identity protection is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss. The person whose identity has been assumed may suffer adverse consequences, especially if they are held responsible for the perpetrator's actions. Identity theft occurs when someone uses another's personally identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.



Last computer scan - Not yet scanned
Date of virus signatures - 17 May 2023 12:32

Identity Protection

Configuration

Identity Protection Status: Not Configured

Reports

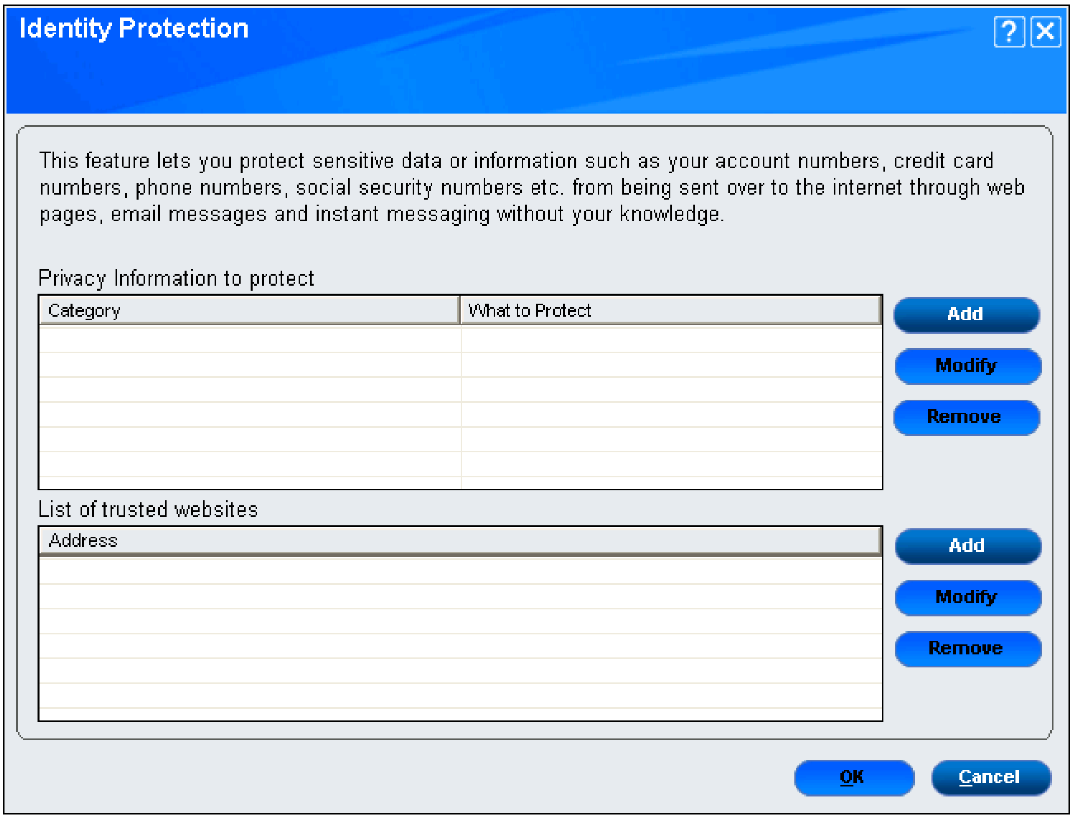
Total Objects Blocked: 0 Objects

This module provides you with options required to configure the module. You can configure the settings from the following sections.

Configuration

This section displays the following information:

- **Identity protection Status:** It displays whether Identity protection is configured or not.
- **Start/Stop**: Click on this option to enable or disable identity protection module.
- **Settings**: This option gives you Identity Protection popup window. Under this we have two sections.


Identity Protection

This feature lets you protect sensitive data or information such as your account numbers, credit card numbers, phone numbers, social security numbers etc. from being sent over to the internet through web pages, email messages and instant messaging without your knowledge.

Privacy Information to protect

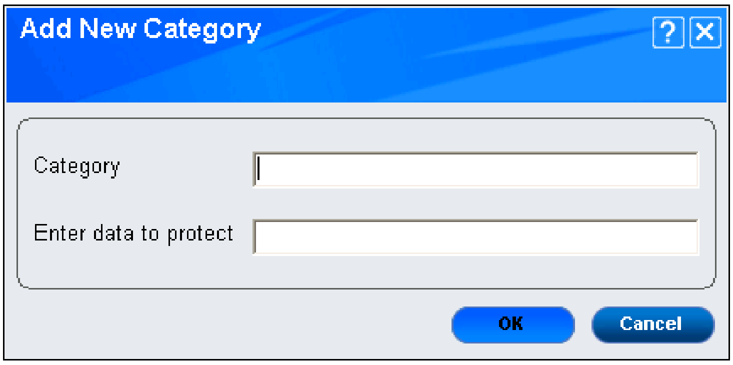
Category	What to Protect

List of trusted websites

Address

This section lets you protect sensitive data or information such as your account numbers, credit card numbers, phone numbers, and more from being sent over the internet through web pages, email messages, and instant messaging without your knowledge.

- **Privacy Information to protect:** From the **Privacy Information to protect** section click on **Add**. This Button helps you add domain category, and a textbox to add data that needs to be protected.

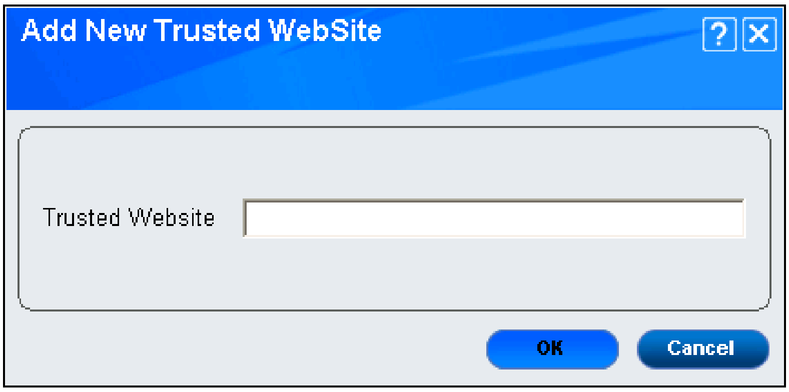

Add New Category

Category

Enter data to protect

Once domains are added in the list you can modify them by clicking on the **Modify** button.

- **List of trusted websites**: Under **List of trusted websites** click the **Add** button to add the name of trusted website address.



Once websites are added in the list you can modify them by clicking on the **Modify** button.

Reports

It displays following count along with the report:

Total Objects Blocked

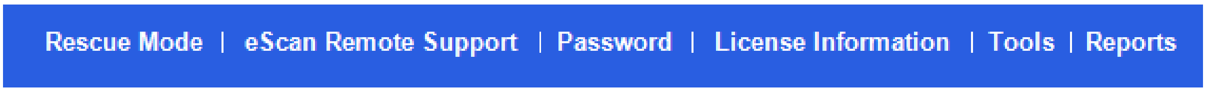
This option gives you the total number of objects blocked by the eScan Identity Protection module.

View Report

To view reports, click **View Report**.

Quick Access Links

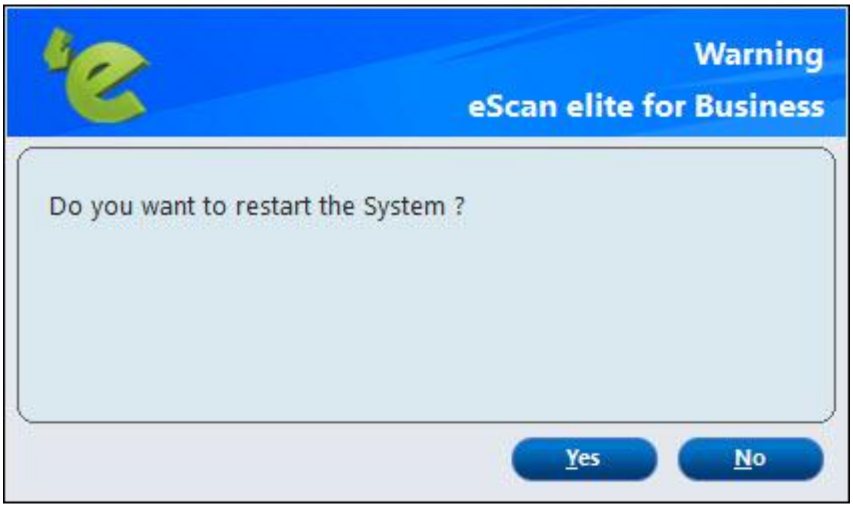
On lower-right corner of the screen, you can view the following quick access links:



Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Rescue Mode

Rescue Mode is an eScan feature that enables you to scan and disinfect all existing partitions on your hard drive inside and outside your operating system. Some sophisticated malware, like rootkits, need to be removed before Windows starts. Once eScan detects a threat that cannot be removed, it prompts you to reboot the computer in Rescue Mode for clean-up and restoration.



Warning
eScan elite for Business

Do you want to restart the System ?

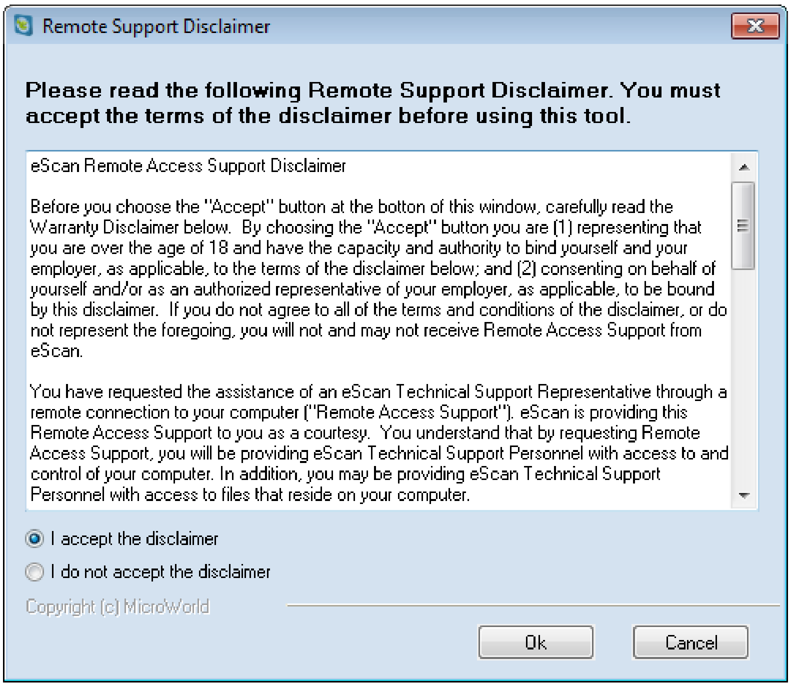
It allows you to boot into a secure environment during system startup without using any optical media. It uses Windows as well as Linux -based environment that not only helps you to scan and clean the system but also allows you to fix registry changes made by viruses and rootkits.

eScan Remote Support

eScan Remote Support is the option to get remote help from our Support Center; the Technical Support Executive will take control of your system for resolving the reported issue. It requires an active internet connection.

Steps for availing remote support:

1. Click on **eScan Remote Support** link at the bottom of the interface.
   Remote Support Disclaimer window will be opened.



Remote Support Disclaimer

Please read the following Remote Support Disclaimer. You must accept the terms of the disclaimer before using this tool.

eScan Remote Access Support Disclaimer

Before you choose the "Accept" button at the botton of this window, carefully read the Warranty Disclaimer below. By choosing the "Accept" button you are (1) representing that you are over the age of 18 and have the capacity and authority to bind yourself and your employer, as applicable, to the terms of the disclaimer below; and (2) consenting on behalf of yourself and/or as an authorized representative of your employer, as applicable, to be bound by this disclaimer. If you do not agree to all of the terms and conditions of the disclaimer, or do not represent the foregoing, you will not and may not receive Remote Access Support from eScan.

You have requested the assistance of an eScan Technical Support Representative through a remote connection to your computer ("Remote Access Support"). eScan is providing this Remote Access Support to you as a courtesy. You understand that by requesting Remote Access Support, you will be providing eScan Technical Support Personnel with access to and control of your computer. In addition, you may be providing eScan Technical Support Personnel with access to files that reside on your computer.

● I accept the disclaimer

○ I do not accept the disclaimer

Copyright (c) MicroWorld

2. Read and accept the disclaimer and click **Ok**.
   eScan Remote Support tool will open.
3. It will generate a user ID and password. Send this user id and password to the technical support executive.
   The executive will take remote support of your system.

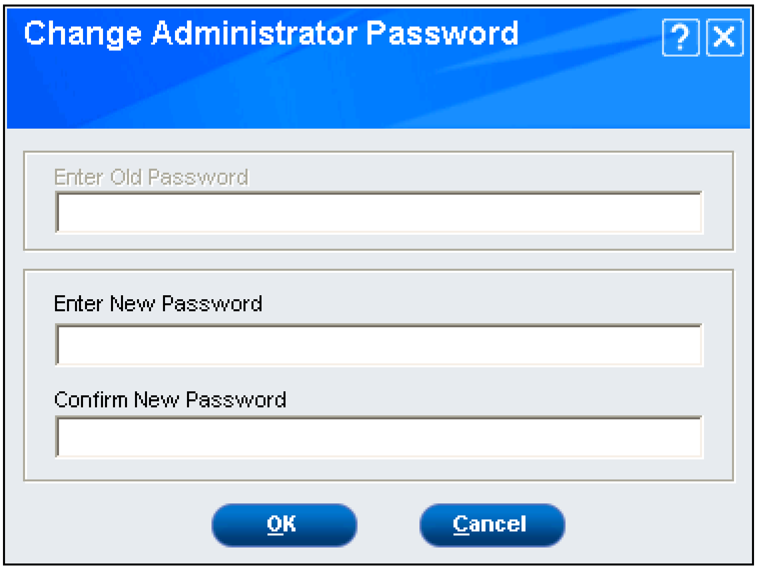
Password

Password will secure your system from making any unauthorized changes to the settings and configurations defined by you.

Using Password Protection for opening eScan

You can define a password for accessing eScan. Use the following steps for defining a password:

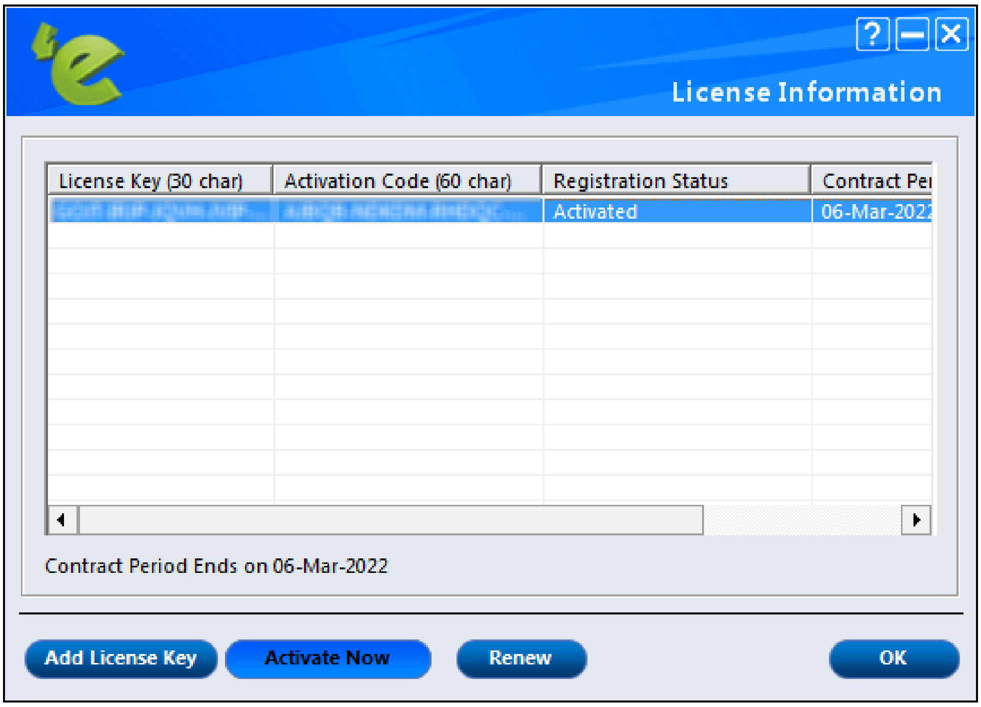
1. Open eScan Window.
2. Click **Password** link at the bottom of the interface.
3. Type a Password in the **Enter New Password** field. It is recommended to enter alphanumeric password.
4. Re-enter the Password in **Confirm New Password** field and click **OK**. You will have to enter this password to change any settings and also to open eScan.



NOTE	For removing the password, Click the password link and Enter old **Password**, leave **Enter New Password** and **Confirm New Password** fields as blank. Now click **OK**. The defined password will be removed and you will not be prompted to enter password to open eScan.

License Information

Click License Information link present in Quick access links at the bottom of eScan Protection Center. You will be forwarded to License information window, it displays following important information.

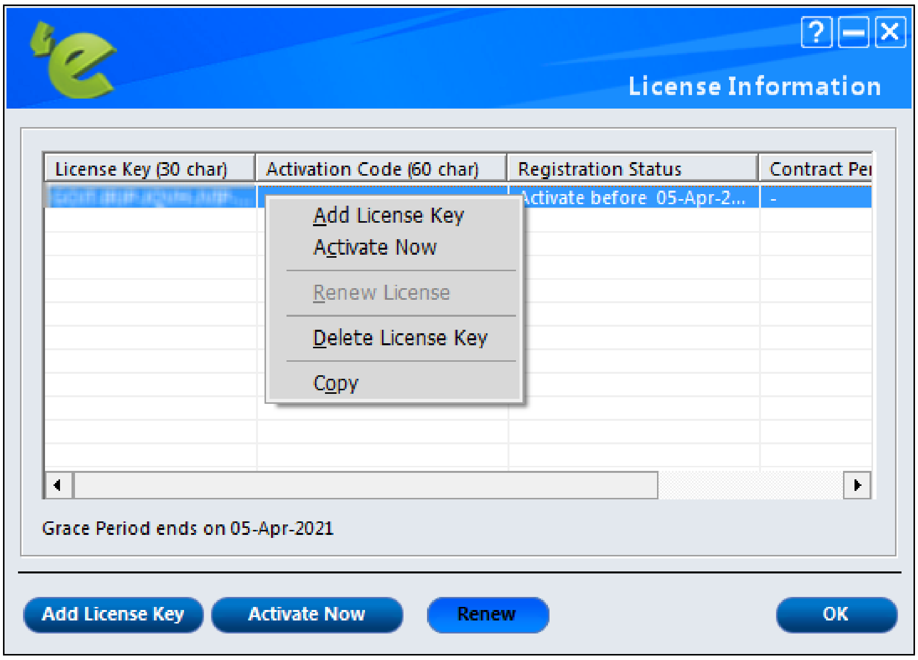


License Key (30 char)	Activation Code (60 char)	Registration Status	Contract Pe
[redacted]	[redacted]	Activated	06-Mar-2022

Contract Period Ends on 06-Mar-2022

- **License Key**: Displays the License Key of the product.
- **Activation Code**: Displays the Activation Code of the product.
- **Registration Status**: Displays the registration status of the product namely, Active, Trail, or Expired.
- **Contract Period Ends on**: Displays the expiry date of the product activation.
- **Version**: Displays the version number of the antivirus software.

Additionally, it also allows you to perform following actions on right click.



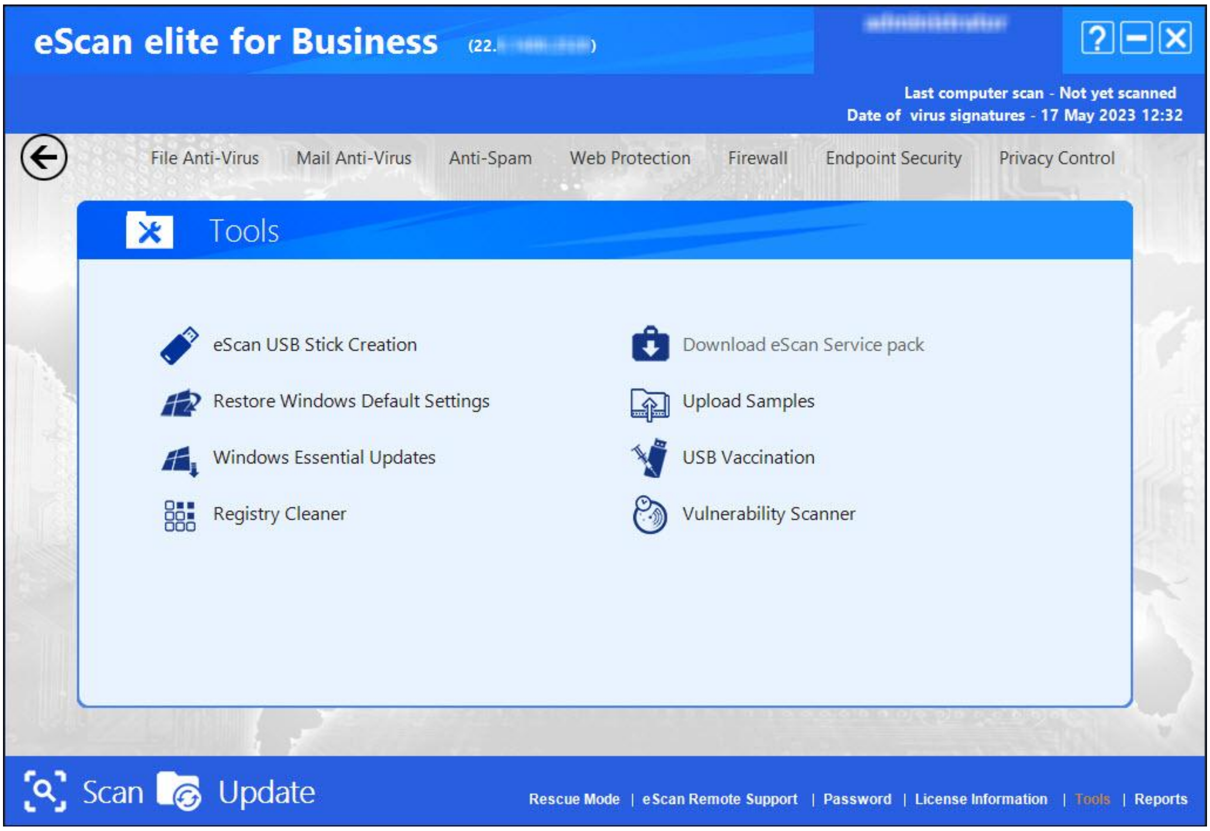
License Key (30 char)	Activation Code (60 char)	Registration Status	Contract Pe
[redacted]		Activate before 05-Apr-2...	-

Grace Period ends on 05-Apr-2021

- **Add License Key**: Click on this button to add license key.
- **Activate Now**: Click on this button to activate the license key.
- **Renew License**: Click on this button to renew the license key.
- **Delete License Key**: Click on this button to delete the added license key.
- **Copy**: This option will copy license key.

Tools

The Tools link provides you with the options for easy and quick access to various tools for eScan and each tool will have its own functions.

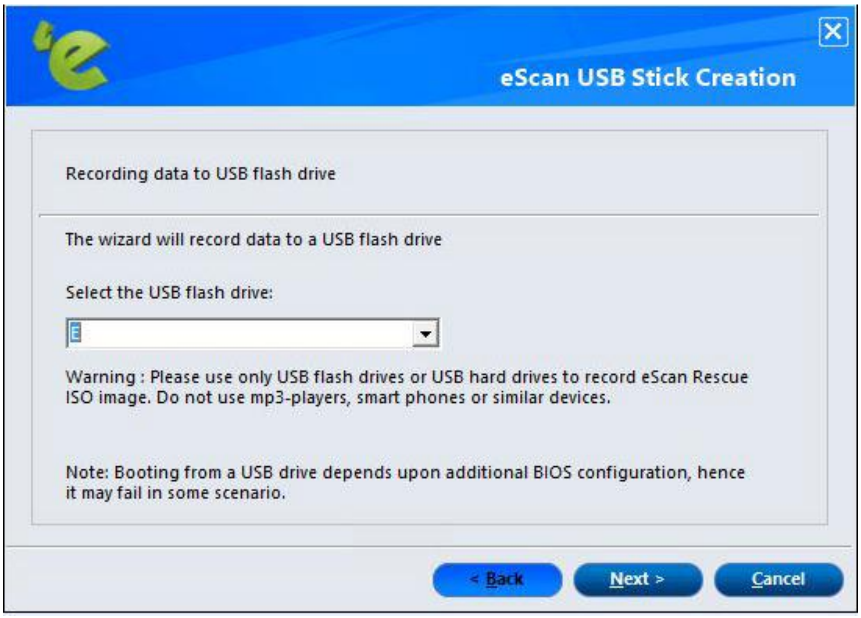

eScan elite for Business (22.[redacted])
[redacted]
?
File Anti-Virus
Mail Anti-Virus
Anti-Spam
Web Protection
Firewall
Endpoint Security
Privacy Control
Tools
eScan USB Stick Creation
Restore Windows Default Settings
Windows Essential Updates
Registry Cleaner
Download eScan Service pack
Upload Samples
USB Vaccination
Vulnerability Scanner
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Last computer scan - Not yet scanned
Date of virus signatures - 17 May 2023 12:32

It gives you access to the various eScan Elite for Business tools and it performs the following actions.

eScan USB Stick Creation

You will have to burn the image on to a USB device before using it to repair/clean infected or damaged systems. You can connect your USB to the device and select the device from the drop-down menu.



Recording data to USB flash drive

The wizard will record data to a USB flash drive

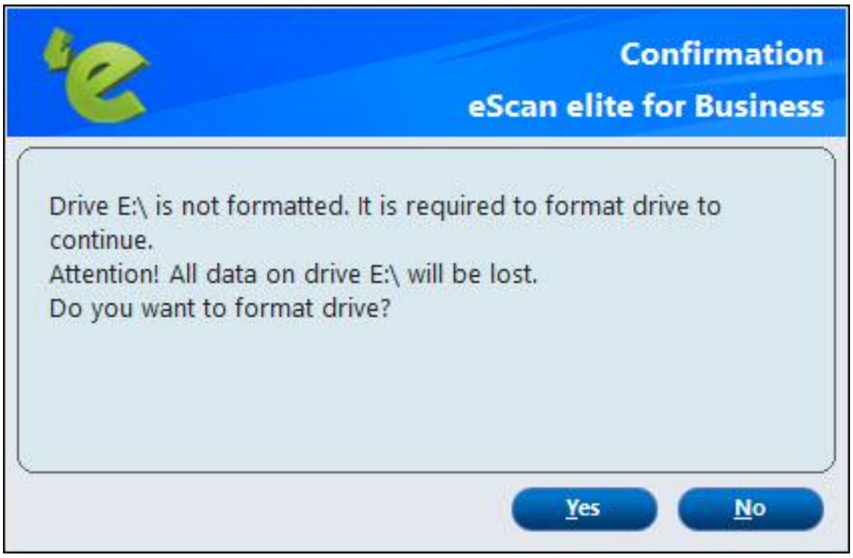
Select the USB flash drive:

E

Warning : Please use only USB flash drives or USB hard drives to record eScan Rescue ISO image. Do not use mp3-players, smart phones or similar devices.

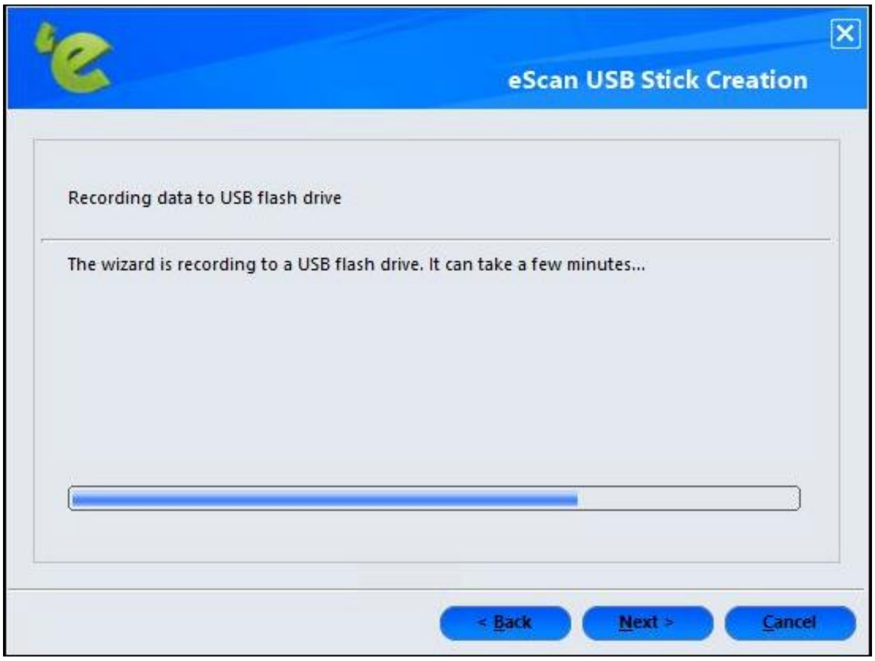
Note: Booting from a USB drive depends upon additional BIOS configuration, hence it may fail in some scenario.

After selecting the device, click **Next>**.
It will prompt you to format the USB drive.



Drive E:\ is not formatted. It is required to format drive to continue.
Attention! All data on drive E:\ will be lost.
Do you want to format drive?

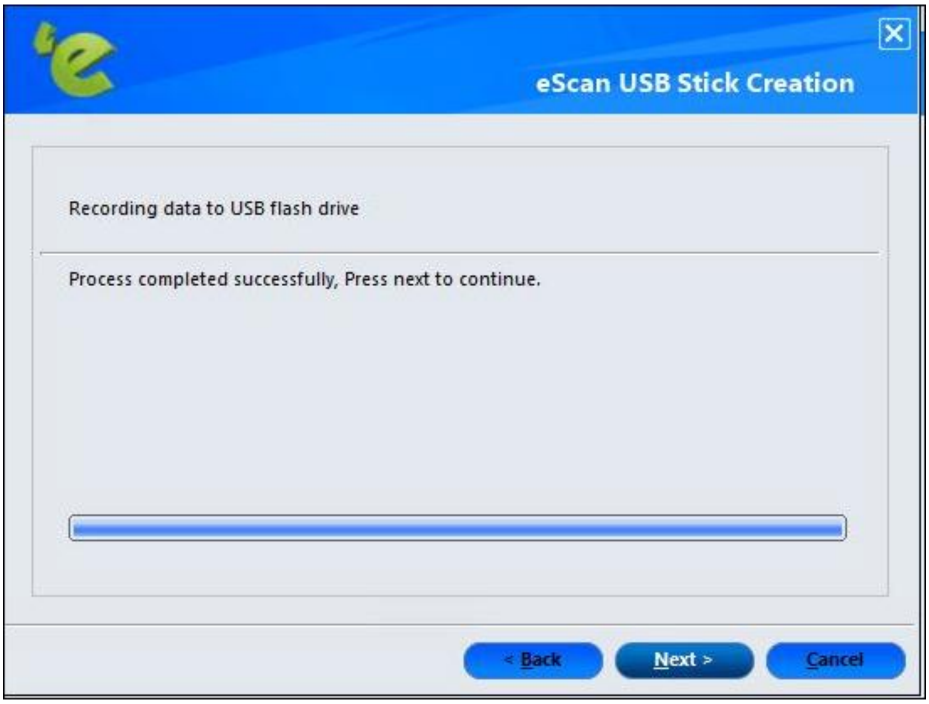
Click **Yes**.
The process of recording the data in the USB will be initialized and you will get the following screen:


eScan USB Stick Creation

Recording data to USB flash drive

The wizard is recording to a USB flash drive. It can take a few minutes...

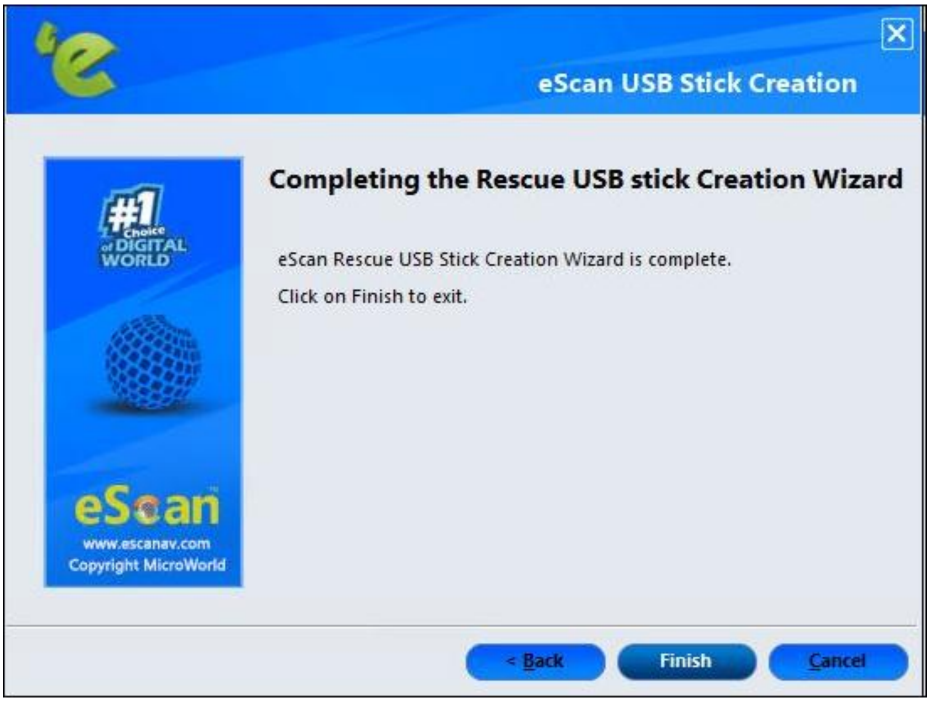
Once the recording process is completed, you will get the following screen. Click **Next>**.


eScan USB Stick Creation

Recording data to USB flash drive

Process completed successfully, Press next to continue.

Completing the Rescue USB stick Creation Wizard appears.
Click **Finish**.



Completing the Rescue USB stick Creation Wizard

eScan Rescue USB Stick Creation Wizard is complete.

Click on Finish to exit.

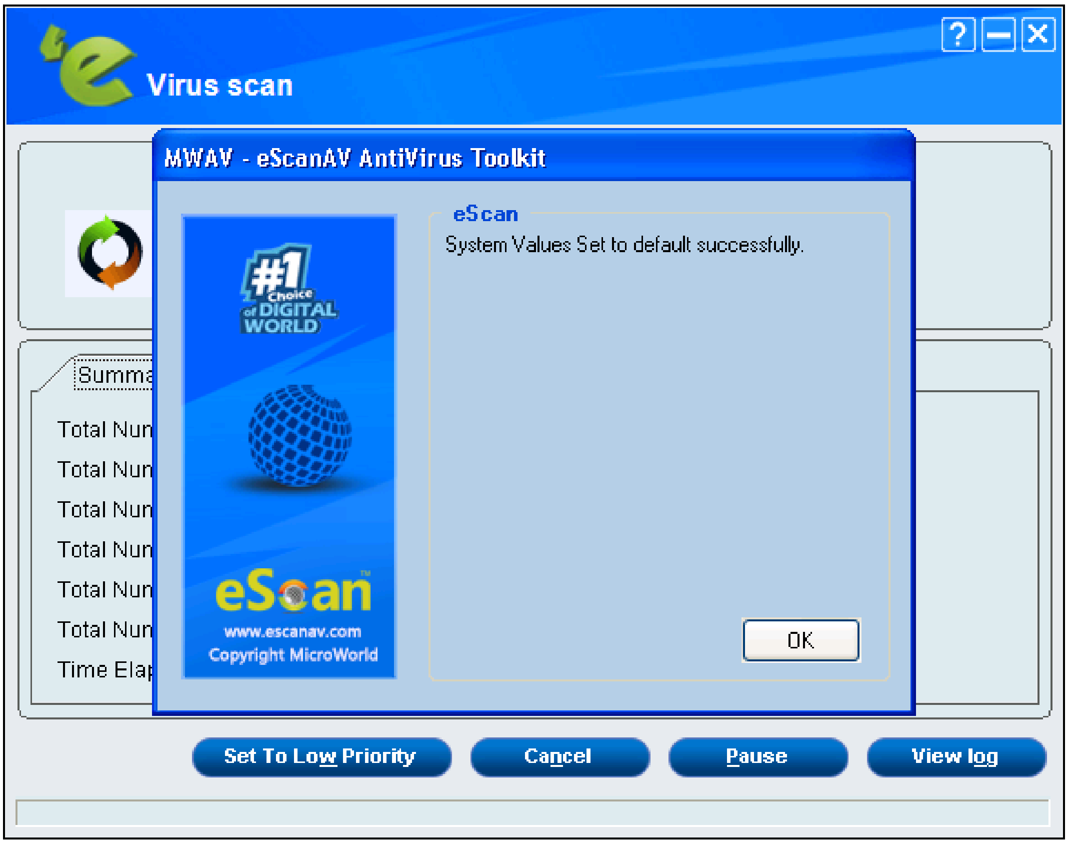
The Rescue USB stick will be created successfully.

Download eScan service pack

You can download the latest eScan service pack directly from here. This will include all the latest updates.

Restore Windows Default Settings

You can restore the Windows® operating system settings, such as desktop and background settings, to eliminate all the modifications made by a virus attack by using this button. eScan automatically scans your computer for viruses when you click this button and sets the system variables to their default values.



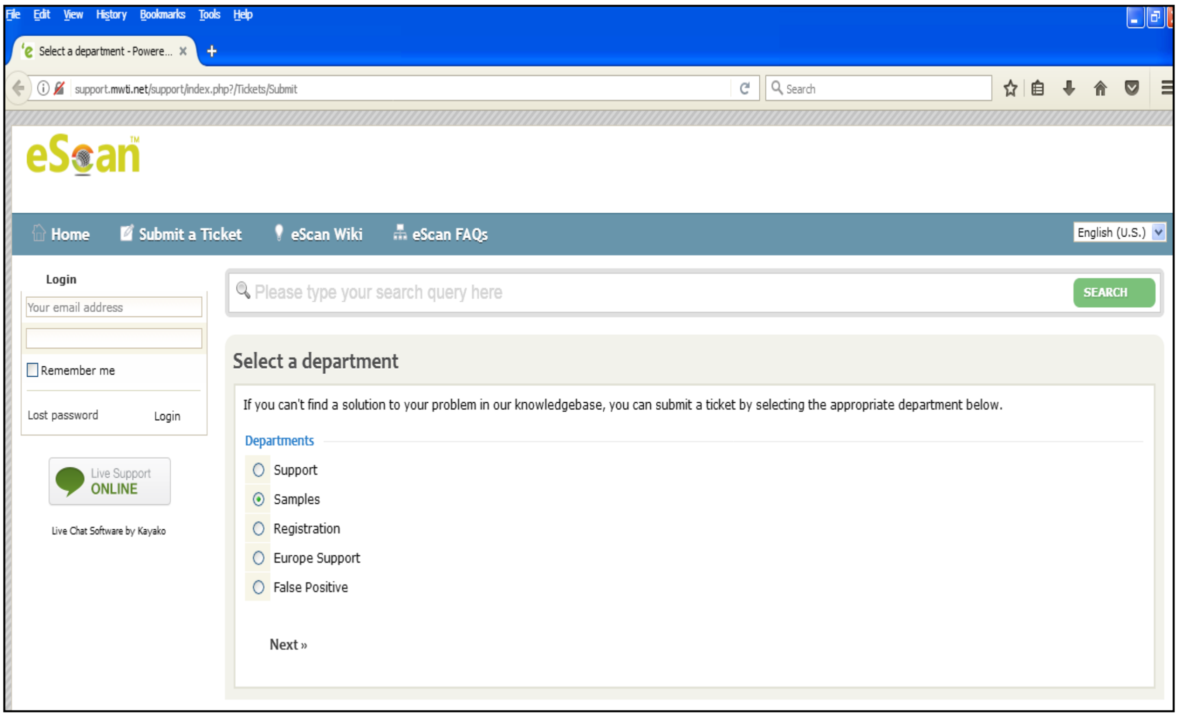
MWAV - eScanAV AntiVirus Toolkit

eScan

System Values Set to default successfully.

Upload Samples

This functionality will allow you upload the suspicious files that will be checked by eScan's R&D team. You can click on this link, it will be redirect to our website, where you can upload the sample and post your queries.



File Edit View History Bookmarks Tools Help
Select a department - Powere...
support.mwti.net/support/index.php?/Tickets/Submit
Search
eScan
Home
Submit a Ticket
eScan Wiki
eScan FAQs
English (U.S.)
Login
Your email address
Remember me
Lost password
Login
Live Support ONLINE
Live Chat Software by Kayako
Please type your search query here
SEARCH

Select a department

If you can't find a solution to your problem in our knowledgebase, you can submit a ticket by selecting the appropriate department below.

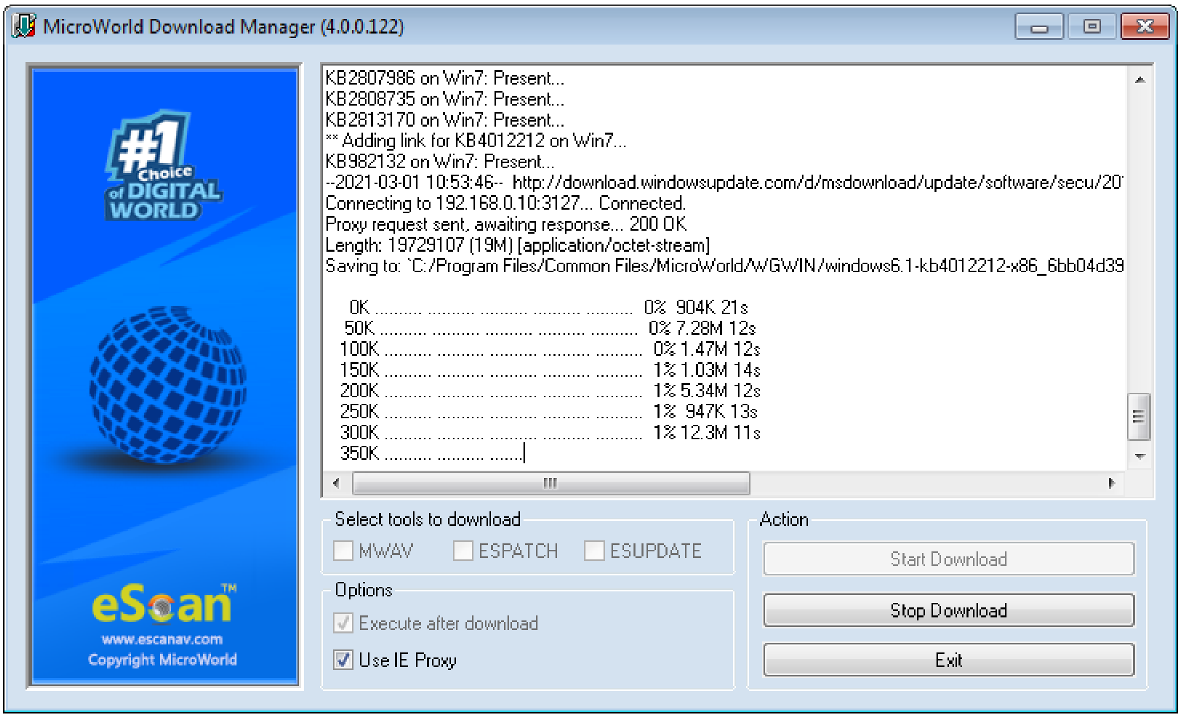
Departments

- ○ Support
- ● Samples
- ○ Registration
- ○ Europe Support
- ○ False Positive

Next »

Windows Essential Updates

It will update your system with the latest windows patch updates. eScan maintains a list of critical Windows Update patches on every computer that are available for free, whenever the user clicks on **Download Latest Hotfix (Microsoft Windows OS)** option, it checks the computer for missing patches on the OS by matching the installed patches with the released patch list in the database. The missing critical Windows update patches are then downloaded and installed on the computer where eScan is running. The database list is categorized on the basis of the operating system.



MicroWorld Download Manager (4.0.0.122)

```
KB2807986 on Win7: Present...
KB2808735 on Win7: Present...
KB2813170 on Win7: Present...
** Adding link for KB4012212 on Win7...
KB982132 on Win7: Present...
--2021-03-01 10:53:46--  http://download.windowsupdate.com/d/msdownload/update/software/secu/20
Connecting to 192.168.0.10:3127... Connected.
Proxy request sent, awaiting response... 200 OK
Length: 19729107 (19M) [application/octet-stream]
Saving to: `C:/Program Files/Common Files/MicroWorld/WGWIN/windows6.1-kb4012212-x86_6bb04d39

   0K .......... .......... .......... .......... ..........  0%  904K 21s
  50K .......... .......... .......... .......... ..........  0% 7.28M 12s
 100K .......... .......... .......... .......... ..........  0% 1.47M 12s
 150K .......... .......... .......... .......... ..........  1% 1.03M 14s
 200K .......... .......... .......... .......... ..........  1% 5.34M 12s
 250K .......... .......... .......... .......... ..........  1%  947K 13s
 300K .......... .......... .......... .......... ..........  1% 12.3M 11s
 350K .......... .......... .......
```

Select tools to download: □ MWAV □ ESPATCH □ ESUPDATE

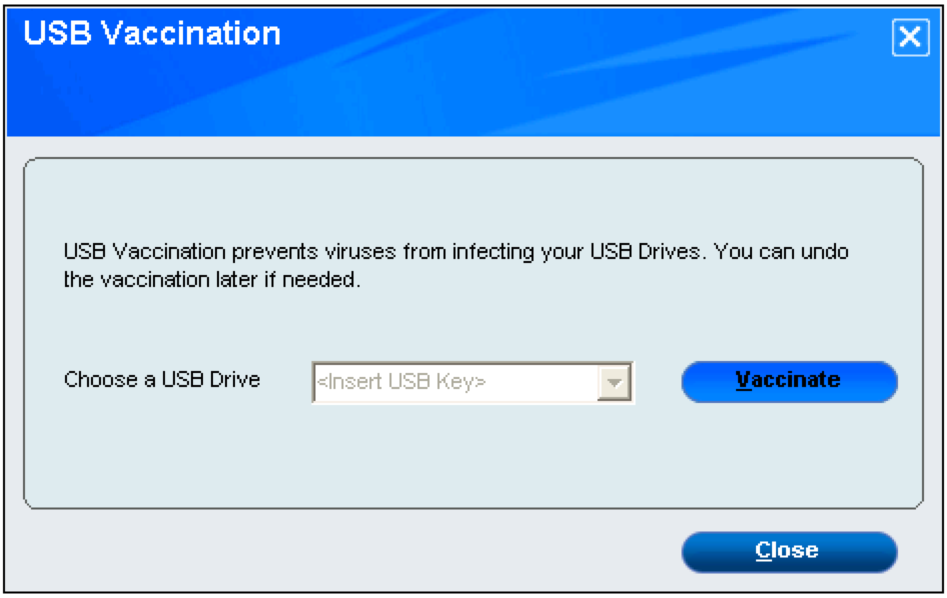
Options: ☑ Execute after download ☑ Use IE Proxy

USB Vaccination

The USB devices are used for various purposes, but while using them you may not be aware that the system to which you are connecting is virus infected. When connected to such machines the USB devices also tend to get infected. So, to prevent such cases, eScan has introduced a feature wherein you can vaccinate USB device, whenever needed. Once vaccinated it stays protected even if you connect the flash drive to an infected system, it doesn't become a carrier to infection.

By default, the **Choose a USB Drive** drop-down list and **Vaccinate** button appears dimmed. It is available only when you connect any USB device to your system.

To vaccinate, select an appropriate USB drive, which you want to vaccinate from the **Choose a USB Drive** drop-down list, and click the **Vaccinate** button.



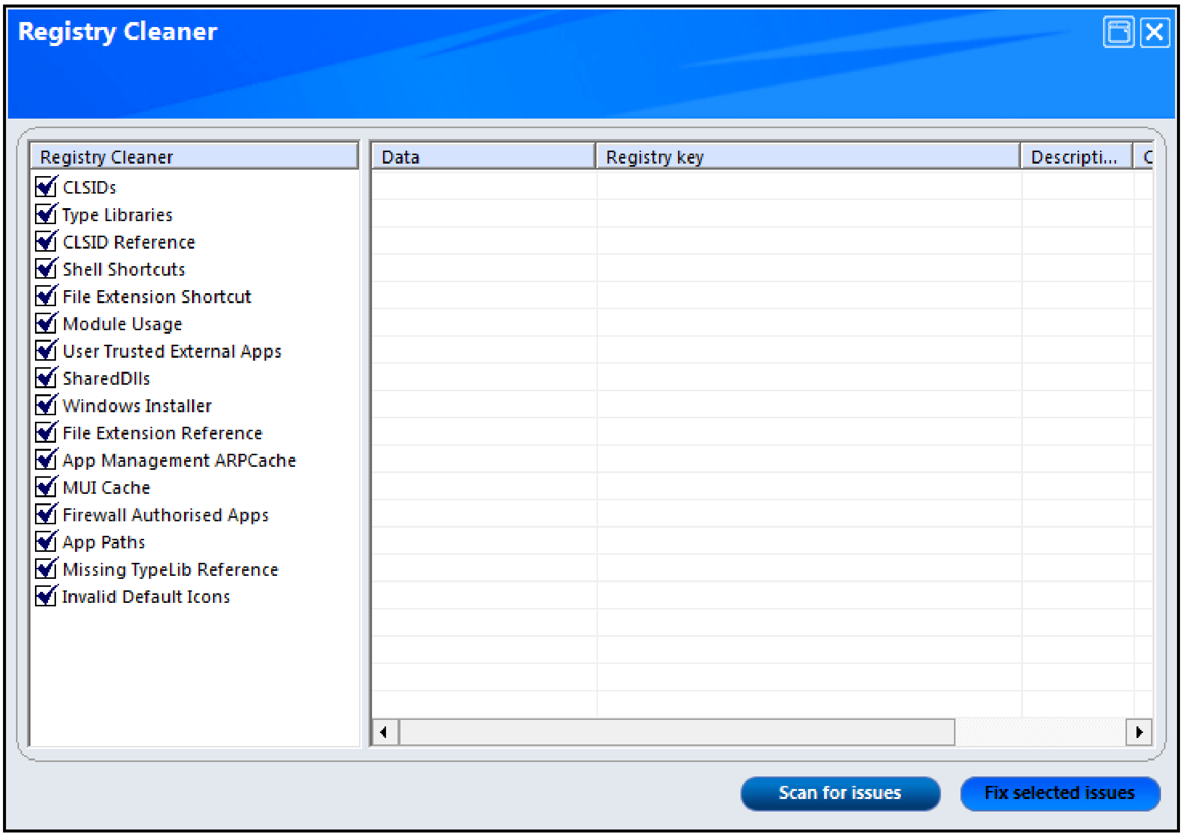
USB Vaccination

USB Vaccination prevents viruses from infecting your USB Drives. You can undo the vaccination later if needed.

Choose a USB Drive <Insert USB Key>

Registry Cleaner

eScan will scan for issues in the selected registry entries, all issues found will be displayed in the Panel on the right. You can select / unselect the issues found by eScan and fix selected issues button to fix the issues. eScan will fix the selected issues instantly.

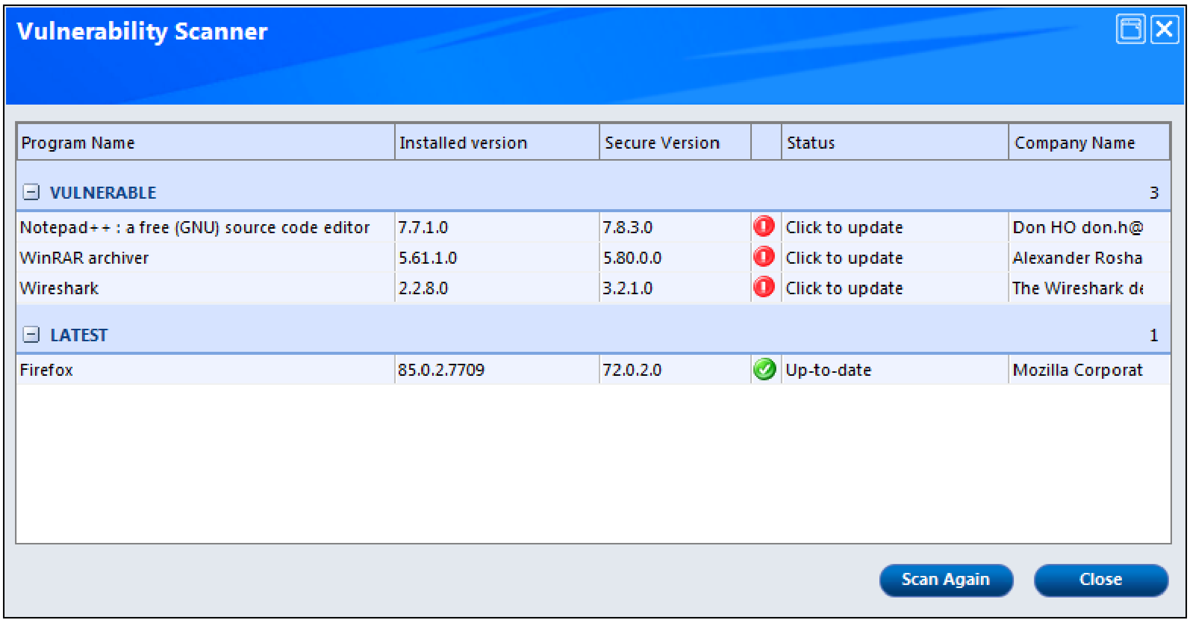


Registry Cleaner

- ☑ CLSIDs
- ☑ Type Libraries
- ☑ CLSID Reference
- ☑ Shell Shortcuts
- ☑ File Extension Shortcut
- ☑ Module Usage
- ☑ User Trusted External Apps
- ☑ SharedDlls
- ☑ Windows Installer
- ☑ File Extension Reference
- ☑ App Management ARPCache
- ☑ MUI Cache
- ☑ Firewall Authorised Apps
- ☑ App Paths
- ☑ Missing TypeLib Reference
- ☑ Invalid Default Icons

Vulnerability Scanner

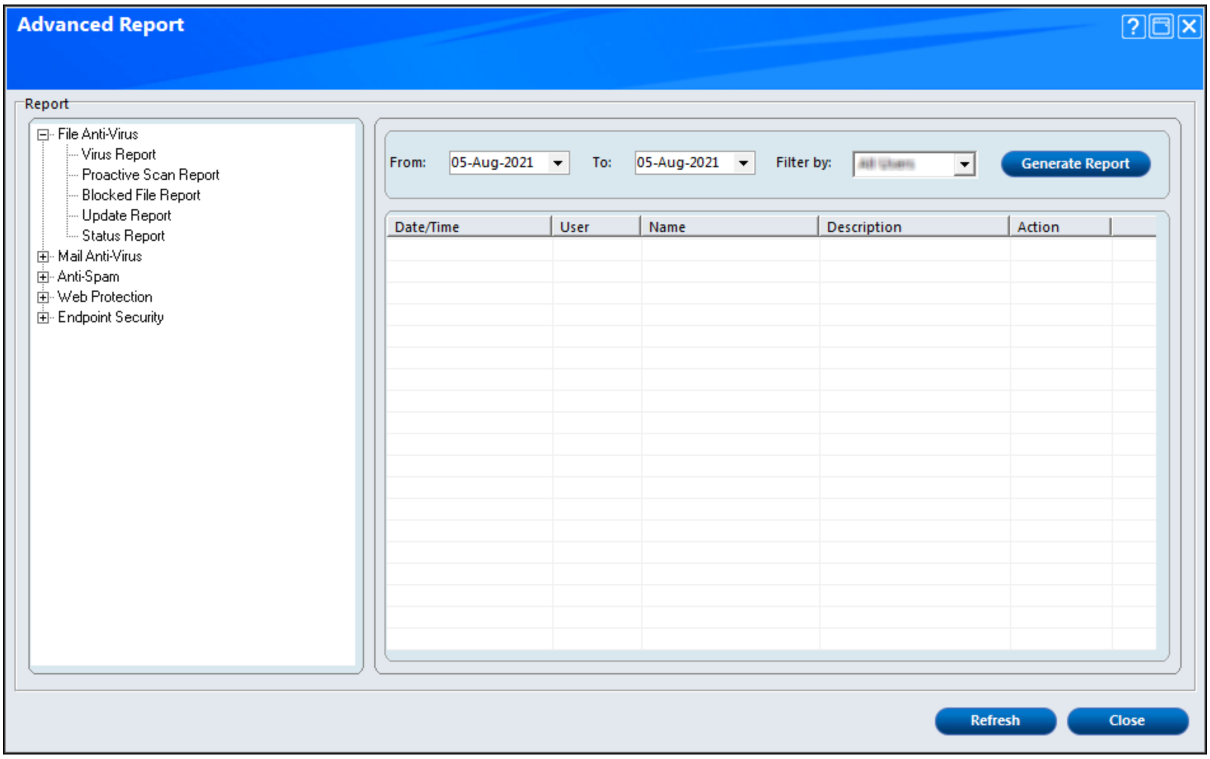
This option will check the vulnerability of the software installed on your computer for any kind of weakness that can be used by the attacker to gain access to the information stored on your computer without your permission. Using the options present in Vulnerability Scanner module of eScan, you can easily update the listed software's with the more secured version of the same.



Program Name	Installed version	Secure Version		Status	Company Name
⊟ VULNERABLE					3
Notepad++ : a free (GNU) source code editor	7.7.1.0	7.8.3.0	!	Click to update	Don HO don.h@
WinRAR archiver	5.61.1.0	5.80.0.0	!	Click to update	Alexander Rosha
Wireshark	2.2.8.0	3.2.1.0	!	Click to update	The Wireshark de
⊟ LATEST					1
Firefox	85.0.2.7709	72.0.2.0	✓	Up-to-date	Mozilla Corporat

Reports

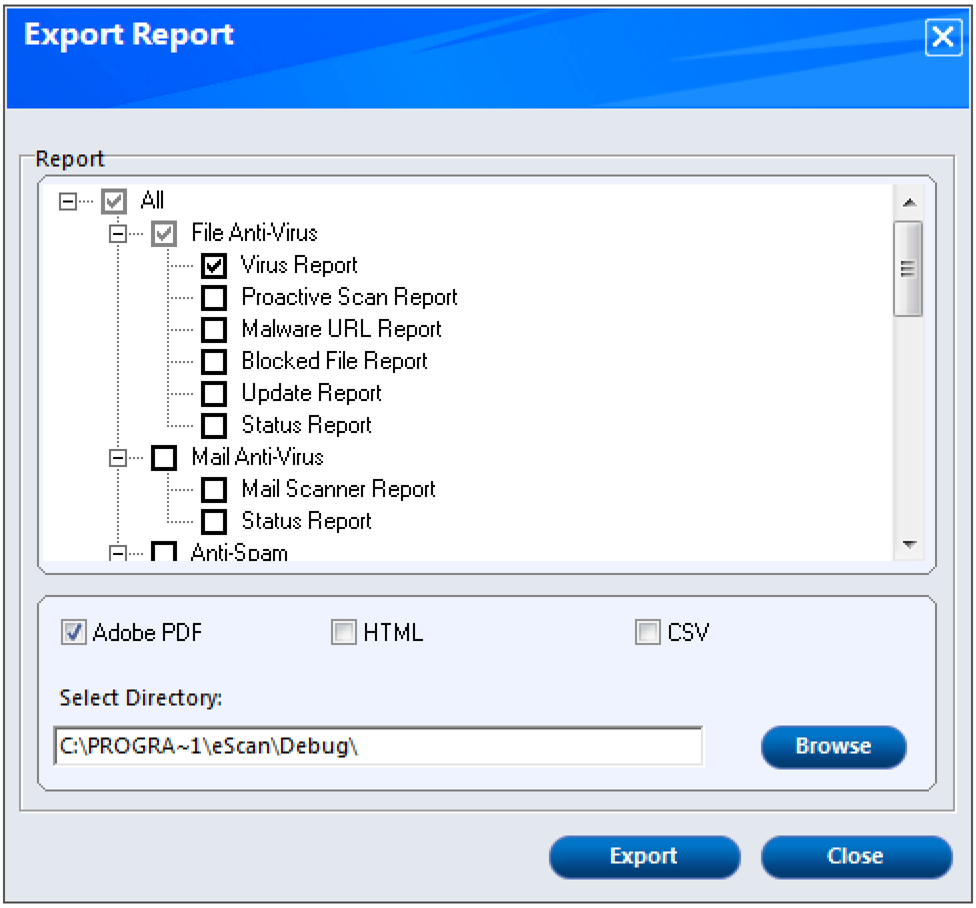
eScan generate reports for File Anti-Virus, Mail Anti-Virus, Anti-Spam, Web Protection, Firewall, Endpoint Security, Identity Protection, and eScan Cloud modules. Click **Reports** link present in Quick access links at the bottom of eScan Protection Center. You will be forwarded to Advance Report window; it displays the report for all the modules of eScan Elite for Business.



From: 05-Aug-2021 To: 05-Aug-2021

- eScan generates reports of all its modules; you can View/Generate a report of any module through Reports link present in every module.
- eScan maintains a log of all the recent activities; it includes the date and timestamp, the user details, description and the action taken.

- It will also allow you to export the particular report as per your requirement or all the existing reports in PDF/ HTML/CSV format; it will also allow you to choose the path to save these reports on to your computer.



Export Report

Report

- ☑ All
  - ☑ File Anti-Virus
    - ☑ Virus Report
    - □ Proactive Scan Report
    - □ Malware URL Report
    - □ Blocked File Report
    - □ Update Report
    - □ Status Report
  - □ Mail Anti-Virus
    - □ Mail Scanner Report
    - □ Status Report
  - □ Anti-Spam

☑ Adobe PDF □ HTML □ CSV

Select Directory: C:\PROGRA~1\eScan\Debug\

Procedure to export the report files

1. Select the particular files that you want to export or select the checkbox next to **All** option to select all the report.
2. Select the particular format of the file that you want to export; you can select from PDF/HTML/CSV file formats.
3. Click **Browse** and select the path where the file has to be saved.
4. Click **Export** to export the report files, or click **Close** to exit the window.

Contact Us

We offer 24/7 free online technical support to our customers through email and live chat. We also provide free telephonic support to customers during our business hours.

Before you contact technical support team, ensure that your system meets all the requirements and you have Administrator access to it. Also, ensure that a qualified person is available at the system in case it becomes necessary to replicate the error/situation.

Ensure that you have the following information when you contact technical support:

- Endpoint hardware specifications
- Product version in use and patch level
- Network topology and NIC information
- Gateway, IP address and router details
- List of hardware, software and network changes if any carried out
- Step-by-step description of error/situation
- Step-by-step description of troubleshooting if any attempted
- Screenshots, error messages and log/debug files

In case you want the Technical Support team to take a remote connection:

- IP address and login credentials of the system

Forums

Join the **Forum** to discuss eScan related problems with experts.

Chat Support

The eScan Technical Support team is available round the clock to assist you with your queries via **Live Chat**.

Email Support

If you have any queries, suggestions and comments regarding our products or this User Guide, write to us at **support@escanav.com**