

eScan Corporate 360

User Guide

Product Version: 14.0.1400.xxxx

Document Version: 14.0.1400.xxxx

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

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

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

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

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

Document Number:	5BUG/02.07.2021/14.1
Current Software Version:	14.0.1400.xxxx
Technical Support:	support@escanav.com
Sales:	sales@escanav.com
Forums:	http://forums.escanav.com
eScan Wiki:	http://wiki.escanav.com/wiki/index.php/
Live Chat:	http://www.escanav.com/english/livechat.asp
Printed by:	MicroWorld Software Services Private Limited
Date:	July, 2021

Content

Introduction	14
Pre-requisites for eScan Server	14
System Requirements.....	15
Installing eScan Corporate 360 Server	16
Installation.....	17
Components of eScan Server	25
Web Console Login.....	26
Main Interface.....	29
Navigation Panel.....	31
Dashboard.....	34
Deployment Status.....	34
eScan Status	35
License.....	35
eScan version	36
Protection Status	37
Update Status.....	37
Scan Status	38
File Anti-Virus.....	39
Proactive	39
Mail Anti-Virus	40
Anti-Spam.....	40
Web Anti-Phishing	41
Mail Anti-Phishing	41
Web Protection	42
Firewall	42
Endpoint Security.....	43
Privacy	44
Anti – Ransomware.....	44
Protection Statistics.....	45
File Anti-Virus.....	46
Mail Anti-Virus	48
Anti-Spam.....	48
Web Protection	49
Endpoint Security-USB	49
Endpoint Security-Application	50
Summary Top 10	51
Asset Changes.....	52
Live Status.....	52

Configure the Dashboard Display.....	53
Managed Computers	54
Search.....	55
Update Agent	55
Adding an Update Agent.....	56
Delete an Update Agent.....	57
Action List	58
Creating a Group.....	58
Removing a Group.....	59
Set Group Configuration.....	59
Managing Installations.....	60
Deploy/Upgrade Client.....	62
Refresh Client.....	64
Moving computer from one group to other	65
Viewing installed software (on Client computer)	65
Removing computers from a group.....	65
Installing eScan on Linux and MAC Computers	65
Manual installation of eScan Client on network computers	70
Installing eScan Client Using Agent.....	70
Installing other Software (Third Party Software).....	71
Uninstall eScan Client (Windows, Mac, and Linux)	73
Synchronize with Active Directory.....	74
Outbreak Prevention.....	75
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.....	82
Client Action List	84
Set Host Configuration.....	85
Deploy/Upgrade Client.....	86
Uninstall eScan Client.....	87
Move to Group	88
Remove from Group	88
Connect to Client (RMM).....	88
Add to RMM License.....	88
Manage Add-On License.....	89
Assign Policy Template	90
Show Critical Events	90

Export	91
Show Installed Softwares	92
Force Download	93
On Demand Scanning	94
Send Message	95
Outbreak Prevention.....	96
Delete All Quarantine Files.....	98
Create OTP.....	98
Pause Protection.....	101
Resume Protection	102
Properties of Selected Computer	103
Policy Template.....	104
Managing Policies	104
Creating Policy Template for a group/specific computer	106
Configuring eScan Policies for Windows Computers	107
Configuring eScan Policies for Linux and Mac Computers.....	182
Assigning Policy Template to a group.....	197
Assigning Policy Template to Computer(s)	199
Copy a Policy Template.....	200
Parent Policy.....	201
Data Encryption	203
Policy Criteria Templates.....	209
Adding a Policy Criteria Template	209
Viewing Properties of a Policy Criteria template.....	214
Copying a Policy Template	214
Deleting a Policy Criteria template.....	215
Unmanaged Computers.....	217
Network Computers.....	217
Creating a New Group from the Select Group window	218
IP Range	219
Adding New IP Range	219
Moving an IP Range to a Group.....	220
Deleting an IP Range	220
Active Directory.....	221
Adding an Active Directory.....	221
Moving Computers from an Active Directory.....	222
New Computers Found.....	223
Filter Criteria.....	223
Action List.....	224
Report Templates.....	225



Creating a Report Template.....	226
Creating Schedule for a Report Template	226
Viewing Properties of a Report Template	227
Deleting a Report Template	227
Report Scheduler	228
Creating a Schedule	228
Viewing Reports on Demand	230
Managing Existing Schedules	231
Generating Task Report of a Schedule	231
Viewing Results of a Schedule	231
Viewing Properties of a Schedule	232
Deleting a Schedule.....	232
Events and Computers	233
Events Status.....	233
Computer Selection.....	234
Software/Hardware Changes.....	235
Violations	236
Settings.....	236
Event Status Setting.....	237
Computer Selection.....	238
Software/ Hardware Changes Setting	241
Performing an action for computer.....	241
Tasks for Specific Computers	242
Creating a task for specific computers.....	242
Viewing Properties of a task	244
Viewing Results of a task	244
Deleting a task for specific computers.....	245
Asset Management	246
Hardware Report.....	246
Filtering Hardware Report.....	247
Exporting Hardware Report	248
Software Report.....	248
Filtering Software Report.....	249
Exporting Software Report.....	249
Software License.....	250
Filtering Software License Report	250
Exporting Software License Report.....	251
Software Report (Microsoft).....	252
Filtering Software Report (Microsoft).....	252
Exporting Software Report (Microsoft).....	253

Filtering Microsoft OS Report.....	253
Exporting Microsoft OS Report.....	254
User Activity.....	255
Print Activity	255
Viewing Print Activity Log.....	255
Exporting Print Activity Log	256
Filtering Print Activity Log	256
Exporting Print Activity Report.....	257
Print Activity Settings	258
Session Activity Report	259
Viewing Session Activity Log.....	259
Filtering Session Activity Log	259
Exporting Session Activity Report.....	260
File Activity Report.....	261
Viewing File Activity Log	261
Filtering File Activity Log	261
Exporting File activity Report	262
Application Access Report.....	263
Viewing Application Access Report	263
Filtering Application Access Report.....	264
Exporting Application Access Report.....	264
Patch Report.....	265
Patch report.....	265
Filtering Patch Report.....	265
Exporting Patch Report.....	266
All Patch Report	266
Filtering All Patch Report	267
Exporting All Patch Report.....	267
Notifications	268
Outbreak Alert	268
Event Alert	269
Unlicensed Move Alert.....	270
New Computer Alert	270
Configure SIEM.....	271
SMTP Settings.....	271
Settings	273
EMC Settings.....	274
Web Console Settings	275
Update Settings	278
General Config	278

Update Notification	279
Scheduling	280
Update Distribution.....	281
Auto-Grouping	283
Excluding clients from auto adding under Managed Group(s).....	284
Removing clients from the excluded list	284
Defining a group and client selection criteria for auto adding under managed computer(s)	285
Two-Factor Authentication (2FA).....	286
Enabling 2FA login	287
Disabling 2FA login	288
Administration	290
User Accounts	290
Create New Account.....	290
Delete a User Account.....	291
User Roles.....	292
New Role	292
View Role Properties	293
Delete a User Role	295
Export & Import.....	297
Export Settings	297
Import Settings.....	298
Scheduling	299
Customize Setup.....	301
Creating a customized setup for Windows	301
Creating a customized setup for Linux.....	302
Editing Setup Properties (only Windows).....	303
Deleting a Setup.....	304
License	305
Adding and Activating a License.....	305
Moving Licensed Computers to Non-Licensed Computers	306
Moving Non-Licensed Computers to Licensed Computers	307
eScan Mobility Management	308
Getting Started.....	309
Dashboard.....	310
Deployment Status.....	311
Enrollment Status	312
eScan Status	312
eScan Version (Android - MDM App).....	313
eScan Version (Android - Container App).....	313

eScan Version (iOS - MDM App).....	314
Android Version	314
iOS Version	315
Device Sync Status (Successful)	315
Device Compliance	316
Kiosk Status	316
Protection Status	317
Update Status.....	318
Scan Status	318
Anti-Virus.....	319
Web Control.....	320
Application Control.....	320
Call and SMS Filter	321
Firewall Status	321
Protection Statistics.....	322
Anti-Virus.....	322
Web Control.....	323
Application Control.....	323
Call Statistics.....	324
SMS Statistics.....	324
Settings.....	325
Managed Mobile Devices	326
Action List	326
Creating a New Group.....	328
Adding a New Device.....	329
Adding Multiple Devices	330
Removing a group.....	331
Changing Server IP address	332
Synchronizing with Active Directory	333
Client Action List	336
Moving Devices from one group to the other group	336
Checking a Device's Properties	338
Removing a device from group	339
Resending Enrollment Email	339
Changing a User's Name/Email ID.....	340
Disenrolling a device	340
Select/Add Columns.....	341
Policy	342
Steps for Defining Policies for the Group.....	342
Creating New Template	343

Android Template.....	344
Anti-Virus Policy	345
Call & SMS Filter Policy.....	347
Web and Application Control.....	356
App Specific Network Blocking.....	361
Anti-Theft Policy	362
Additional Settings Policy	364
Password Policy	365
Device Oriented Policy.....	365
Required Applications Policy	366
Importing an application	367
Deleting an application from "Required Applications Policy"	369
Wi-Fi Settings Policy.....	370
Enable Wi-Fi Restrictions (For devices with Android version below 6.0)	370
Adding a Wi-Fi SSID.....	370
Deleting a Wi-Fi network SSID.....	372
Scheduled Backup (Contacts & SMS).....	373
Creating a schedule	373
Modifying a schedule	375
Deleting a schedule	376
Content Library Policy.....	377
Import a file	377
Kiosk Mode Policy.....	379
Location Fencing.....	382
iOS Template.....	383
Device Passcode Policy	384
Restrictions Policy.....	386
WebClip Policy.....	391
Adding a WebClip.....	391
Deleting a WebClip	392
Email Policy.....	393
Wi-Fi Settings Policy.....	397
Content Library Policy.....	399
Importing a file	399
Deleting a file.....	400
Required Applications Policy	401
Importing an application	401
Deleting an application	402
Group Tasks	403
Creating a New Group Task	403

Installation and Enrollment of Android Device for MDM Group.....	406
Adding a device to the console.....	406
Installation and Enrollment of Android Device for COD and BYOD Group.....	415
Adding a device to the console.....	415
Enrolling the added device.....	416
Differences between COD and BYOD group	423
Installing eScan Container app.....	424
Installation and Enrollment of iOS Device	431
Adding a device to the console.....	431
Enrolling the added device.....	432
Manage Backup	445
Taking a backup from devices to the server.....	445
Anti-Theft.....	448
Wipe Data.....	449
Block Device.....	450
Unblock Device 	451
Scream.....	451
Send Message	452
Locate Device	453
Remove work Profile 	453
Asset Management	454
Asset Management – Hardware Information.....	454
Viewing Hardware information	454
Asset Management – Application Information	456
Filtering the Application information.....	456
Asset Management – Export Options for the Generated Reports.....	457
Exporting a Report	457
Report Templates.....	458
Creating a Report Template.....	458
Editing a Report Template.....	459
Deleting a Report Template	460
Viewing a Report.....	460
Report Scheduler.....	461
Adding a Scheduler	461
Running a schedule.....	465
Editing a Schedule	466
Deleting a Schedule.....	466
Viewing the report.....	467
Viewing results of a report.....	467
Events and Devices	468

Viewing Events	468
Settings	473
Certificate Management	473
Importing an SSL certificate	474
Email Notification Settings	475
Data Purge	475
Connection Sequence	476
App Store	477
Adding an Android application with In-House Apps (Android) option	477
Adding an Android application with Play Store Apps (Android) option	479
Adding an iOS application	480
Deleting an application from the App Store	481
Content Library	482
Adding a file	482
Editing a file description	483
Deleting a file	483
Call Logs	485
Data Usage	486
History	487
Location History	487
Battery Status/Signal Strength	488
Geo Fence History	488
App Usage History	489
Fencing Location(s)	490
Creating a Fencing Location	490
Editing a Fencing Location	491
Deleting a Fencing Location	492
View On Map	492
Administration	493
User Accounts	493
Creating a User Account	494
Adding a User from Active Directory	495
Deleting a User Account	496
User Roles	497
Adding a User Role	498
Role Properties	500
Deleting a User Role	500
Contact Us	501
Forums	501
Chat Support	501

Email Support.....	501
--------------------	-----

Introduction

eScan Corporate 360 is a comprehensive Anti-Virus and Information Security Solution that allows you to manage risk and protect your critical infrastructure efficiently. In addition, a Secure Web Interface is included in the latest eScan Management Console (EMC) module, which enables dynamic security management of servers, endpoints and mobile devices on the corporate network. It is an excellent combination of advanced and futuristic technologies that ensures protection to Windows as well as Macintosh, Linux, and Android-based devices and endpoints in the corporate network. eScan Corporate 360 also includes Mobile Device Management module which is specifically designed with an aim to facilitate administrator to remotely monitor, secure, and manage all Android-based devices in the network.

The web-based EMC that lets you do following activities:

- Monitor the Security Status of all computers connected across the network.
- Create and Manage policies for computers on your network.
- Create and View customized reports of the Security Status of the computers.
- Manage Notifications.
- View statistics for different modules in graphical format.

Pre-requisites for eScan Server

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

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

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

System Requirements

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

eScan Management Console can be accessed by using following browsers:

- Internet Explorer 7 / 8 / 9 / 10
- Firefox 14 and above
- Google Chrome latest version

Installing eScan Corporate 360 Server

- **Installing eScan Corporate 360 Server from CD/DVD**

Installing eScan Corporate 360 from the CD/DVD is very simple, insert the CD/DVD in the ROM and wait few seconds for the Autorun to run the installation wizard. In case the installation wizard does not run automatically, locate and double-click the **MDMcwn4k3ek** on CD-ROM. This will run the installation wizard based setup of eScan Corporate 360. To complete the installation, follow the instructions on screen.

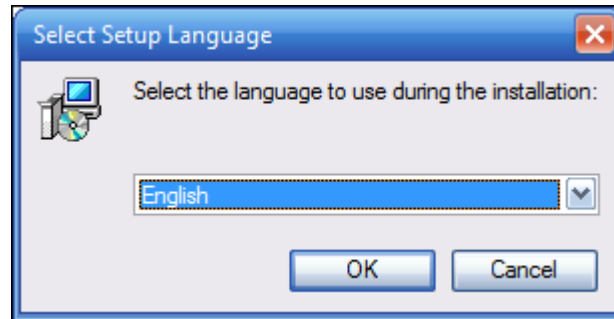
- **Downloading and installing eScan Corporate 360 Server from internet**

To download the setup file click [here](#). To install eScan Server from the downloaded file, double click the MDMcwnxxxx.exe and follow the instructions on screen to complete the installation process.

Installation

To install the eScan Corporate 360, follow the steps given below:

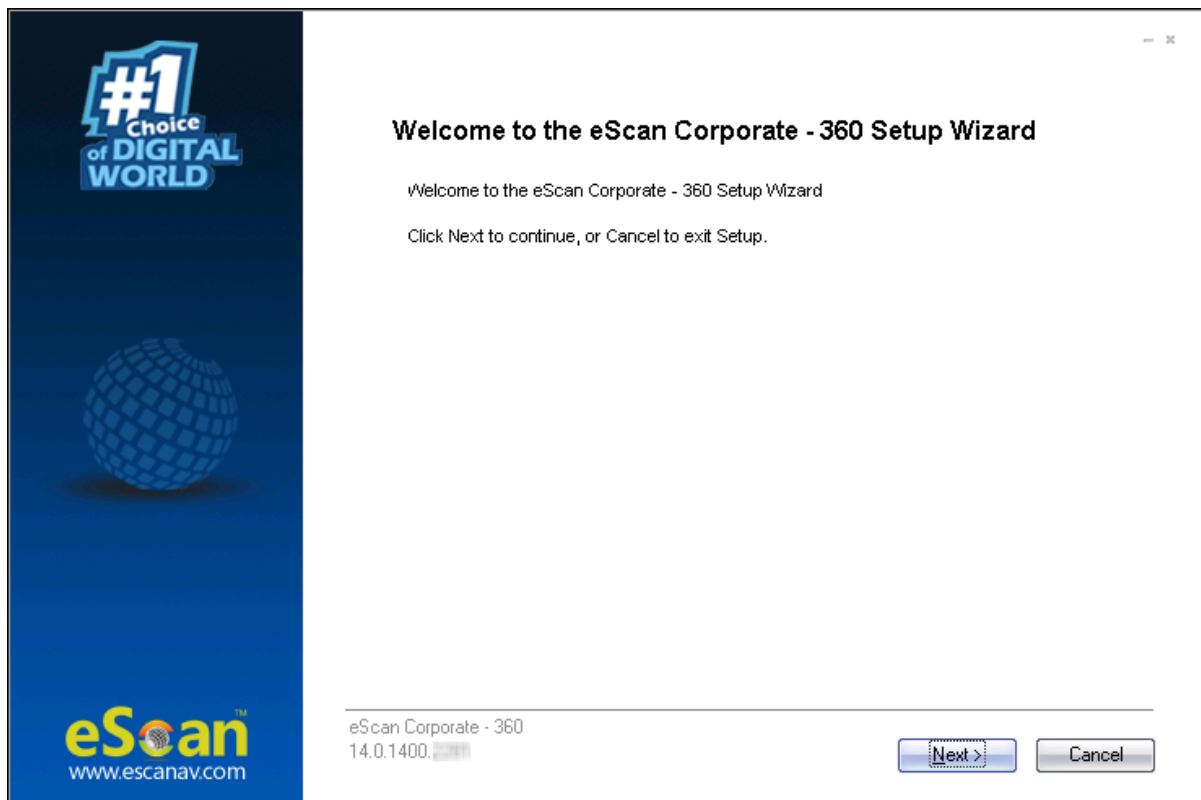
1. The installation wizard displays following window:



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

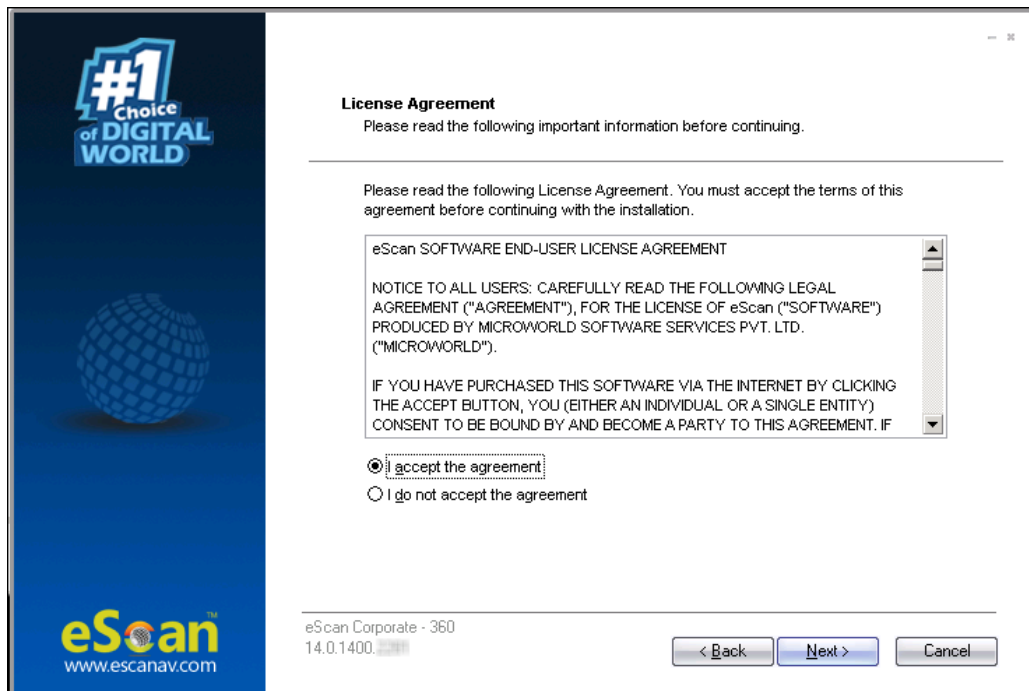
Note	The Default Language displayed in the drop-down menu is dependent on the Operating System's language installed on the computer.
-------------	---

The installation wizard welcomes you.

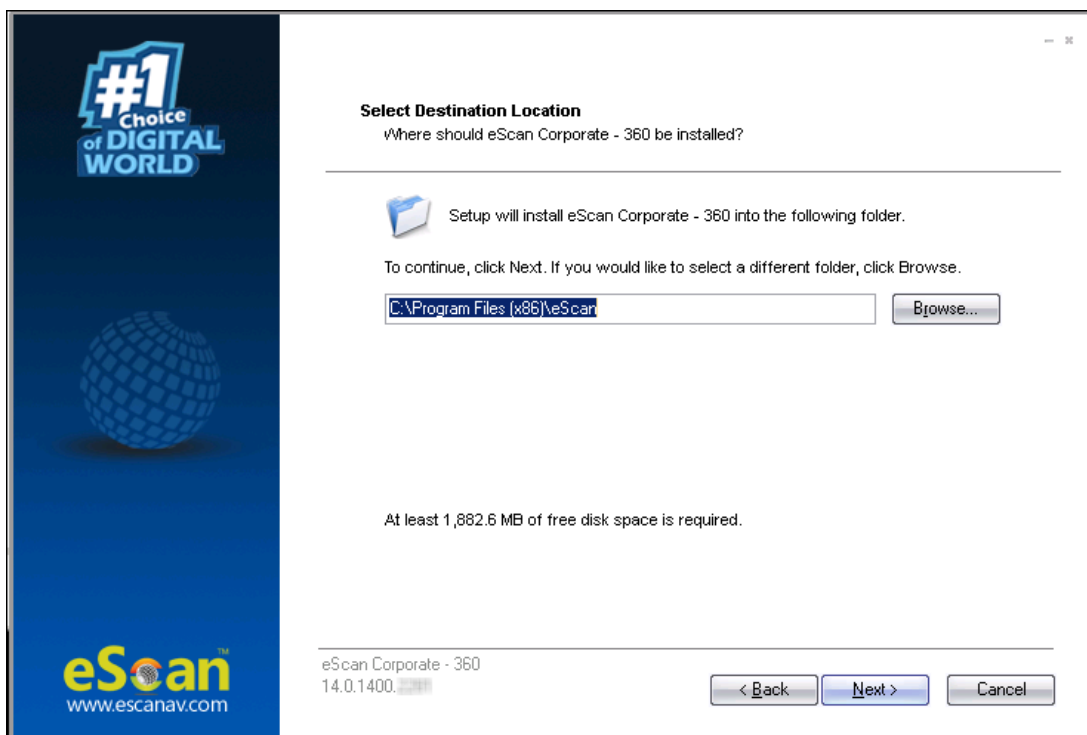


4. To proceed, click **Next**.

License Agreement screen appears.



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

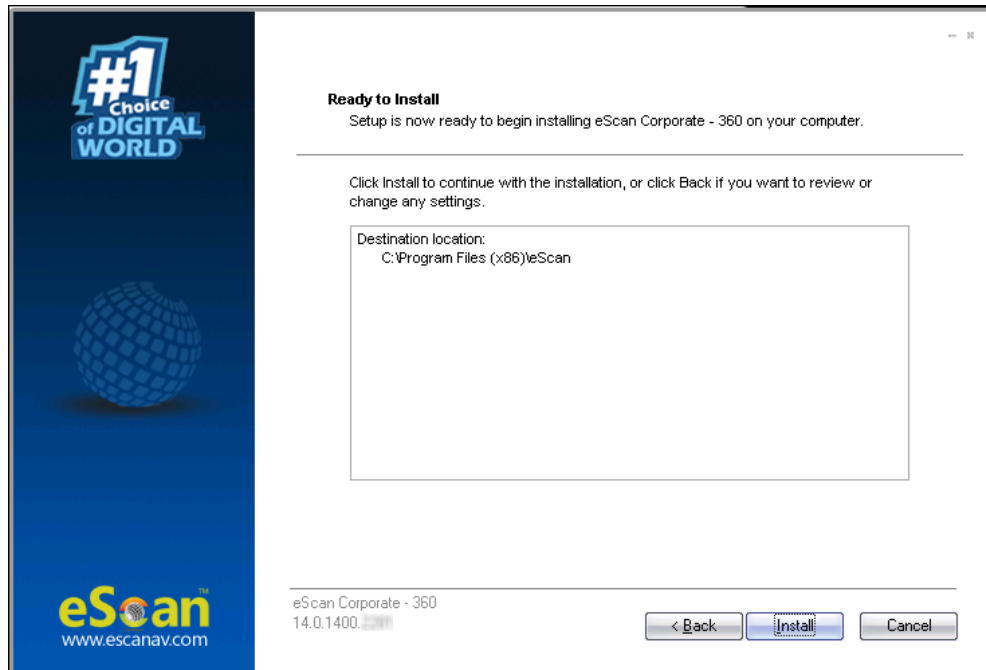


6. If you want to select a different installation location, click **Browse** and select the destination folder for installation.
Click **Next** to proceed with the installation.

NOTE

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

Ready to install screen appears displaying destination location.



7. To proceed, click **Install**.

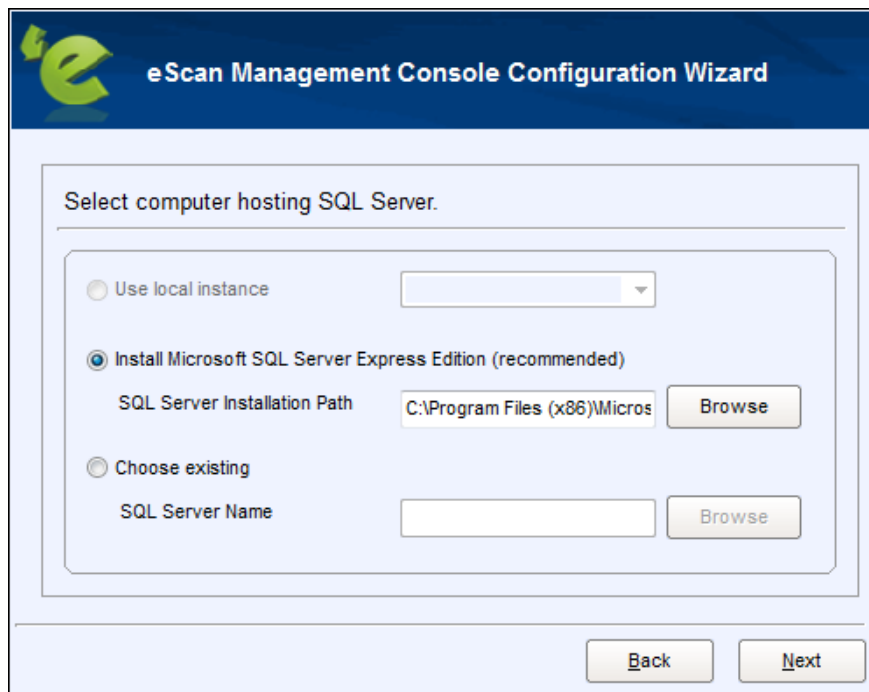
The installation wizard initiates installation and displays the process.



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



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



The window displays following options:

- **Use local instance**
If you already have SQL instances running locally, click the drop-down and select a desired local instance.
- **Install Microsoft SQL Server Express Edition (recommended)**
If the computer selected for eScan server installation doesn't have SQL server installed, it is recommended that you select this option. Click Browse and select an installation path for SQL server installation.

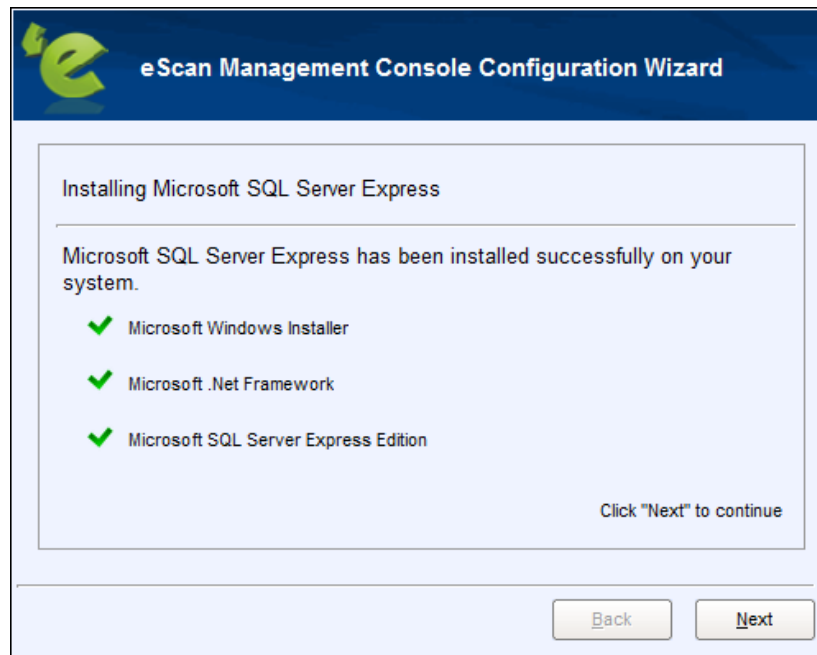
NOTE	<p>Default installation path for 32-bit PC – C:\Program Files\Microsoft SQL Server</p> <p>Default installation path for 64-bit PC – C:\Program Files (x86)\Microsoft SQL Server</p>
-------------	---

- **Choose existing**
If an SQL server hosting computer exists on your LAN, select this option. Click Browse and select the SQL server hosting computer. Select this option if you have already created an instance for eScan Database on any SQL Server installed on any computer connected to the network. Click **Browse** to locate the server. This option is being used if you already have an instance running locally or in your local area network.
9. After selecting an option, click **Next** to proceed.
If you selected the recommended option, the configuration wizard will begin installation of the Microsoft SQL Server Express.



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

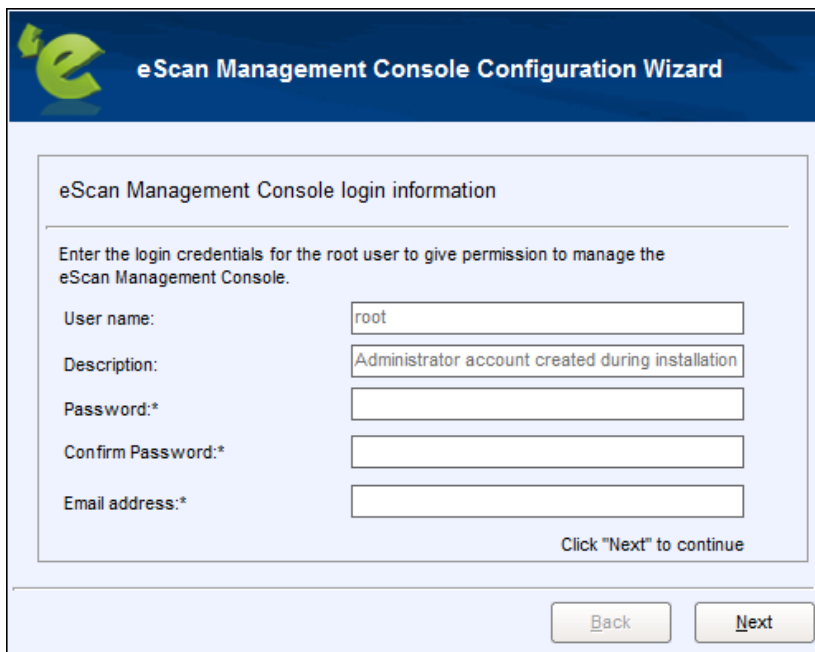
After the successful installation, the wizard displays following window.



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

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

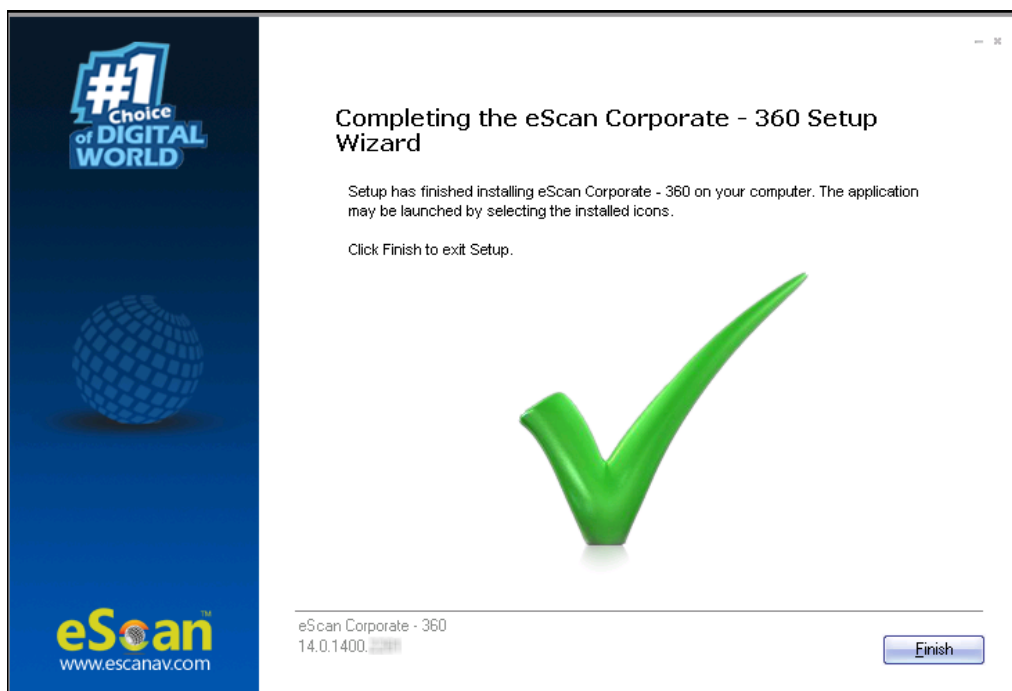
NOTE The default username for web console is **root**.

The image shows a screenshot of the 'eScan Management Console Configuration Wizard' window, specifically the 'eScan Management Console login information' step. The title bar is dark blue with the eScan logo and the text 'eScan Management Console Configuration Wizard'. The main content area has a light blue background and contains the following text: 'eScan Management Console login information', 'Enter the login credentials for the root user to give permission to manage the eScan Management Console.', and a list of five fields with labels: 'User name:', 'Description:', 'Password:*', 'Confirm Password:*', and 'Email address:*'. The 'User name' field contains the text 'root', and the 'Description' field contains the text 'Administrator account created during installation'. At the bottom right of the main content area, it says 'Click "Next" to continue'. At the bottom of the window, there are two buttons: 'Back' and 'Next'.

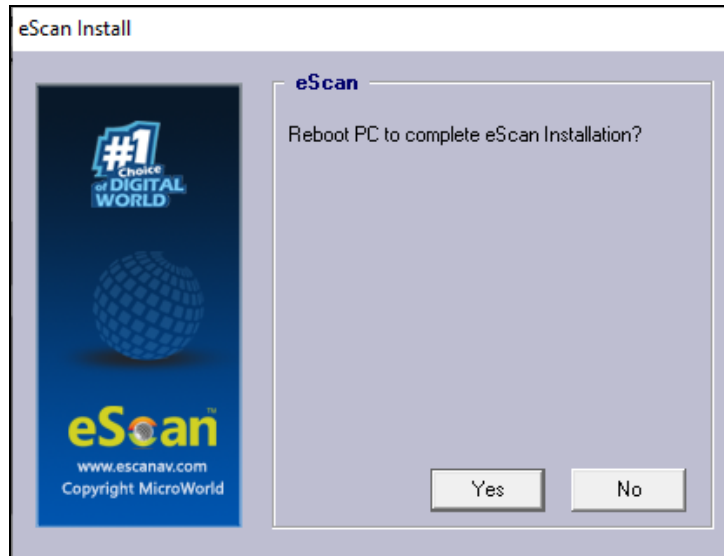
12. After filling all the details, click **Next**. The wizard displays installation successful message.



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



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



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

NOTE

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

Components of eScan Server

The eScan Server is comprised of following components:

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

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

Web Console Login

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

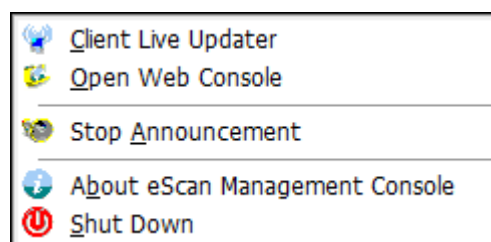
To log in to the eScan Management Console, follow the steps given below:

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

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

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

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



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

Rests of the options are explained below:

Client Live Updater

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

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

Buttons: Export To Excel, Close

Stop Announcement

Clicking this option stops broadcast from and towards the server.

About eScan Management Console

Clicking this option displays Server Up Time and general information.

Shut Down

Clicking this option shuts down the eScan Management console.

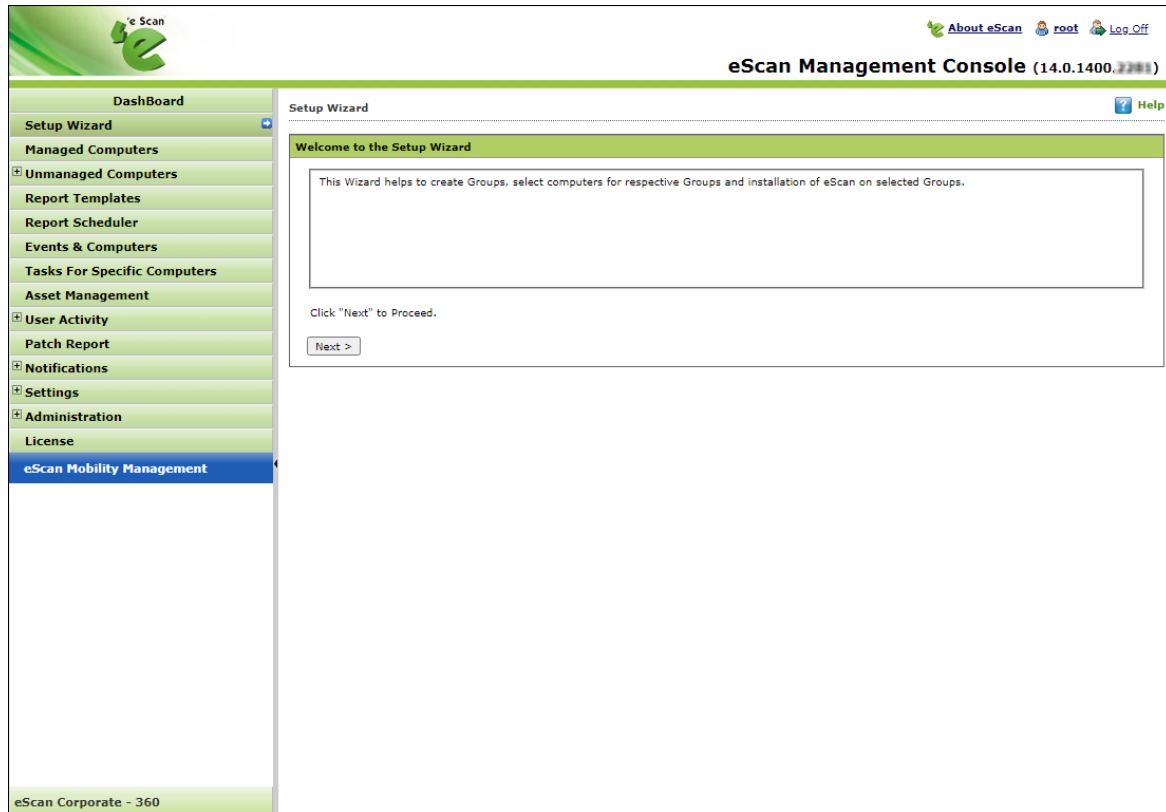
NOTE	<p>It is recommended that you do not shut down the server, as doing so will stop the communications between client and server.</p> <p>The "root" is the Superuser account created by eScan during Installation.</p>
------	---

The web console login page displays following links:

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

Main Interface

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



NOTE

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

The description of different link found on the main interface of the eScan console is listed in the table below.

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** displays your registration details.



The screenshot shows a web application window titled "Organization Details". In the top right corner, there is a "Help" link with a question mark icon. Below the title bar is a green header section labeled "Information" with an "Edit" link and a pencil icon. The main content area contains a table with the following details:

Company Id	123456789012
Company Name	ABC Corp
Full Name	John Doe
Email Address	john.doe@abc.com
Phone Number	1234567890
Number Of Employees	10
Country	USA
Registered Date	12/12/2020

At the bottom of the window, there are two buttons: "Close" and "Save".

Log off

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

Date of Virus Signatures

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

Navigation Panel



Dashboard

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

Managed Computers

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

Unmanaged Computers

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

Report Templates

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

Report Scheduler

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

Events and Computers

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

Tasks for Specific Computers

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

Asset Management

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

User Activity

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

Patch Report

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

Notifications

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

Settings

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

Administration




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

License

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

eScan Mobility Management

eScan Mobile Device Management solution is specifically designed for Mobile or Smart Phone devices. It helps you secure and protect your Mobile or Smart Phone against viruses, malwares, Trojans, and secures your confidential data. It also enables you to block applications and websites, which ensures security to your device. Using eScan Mobile Device Management Solution you can manage and secure Mobile as well as Smartphones.

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

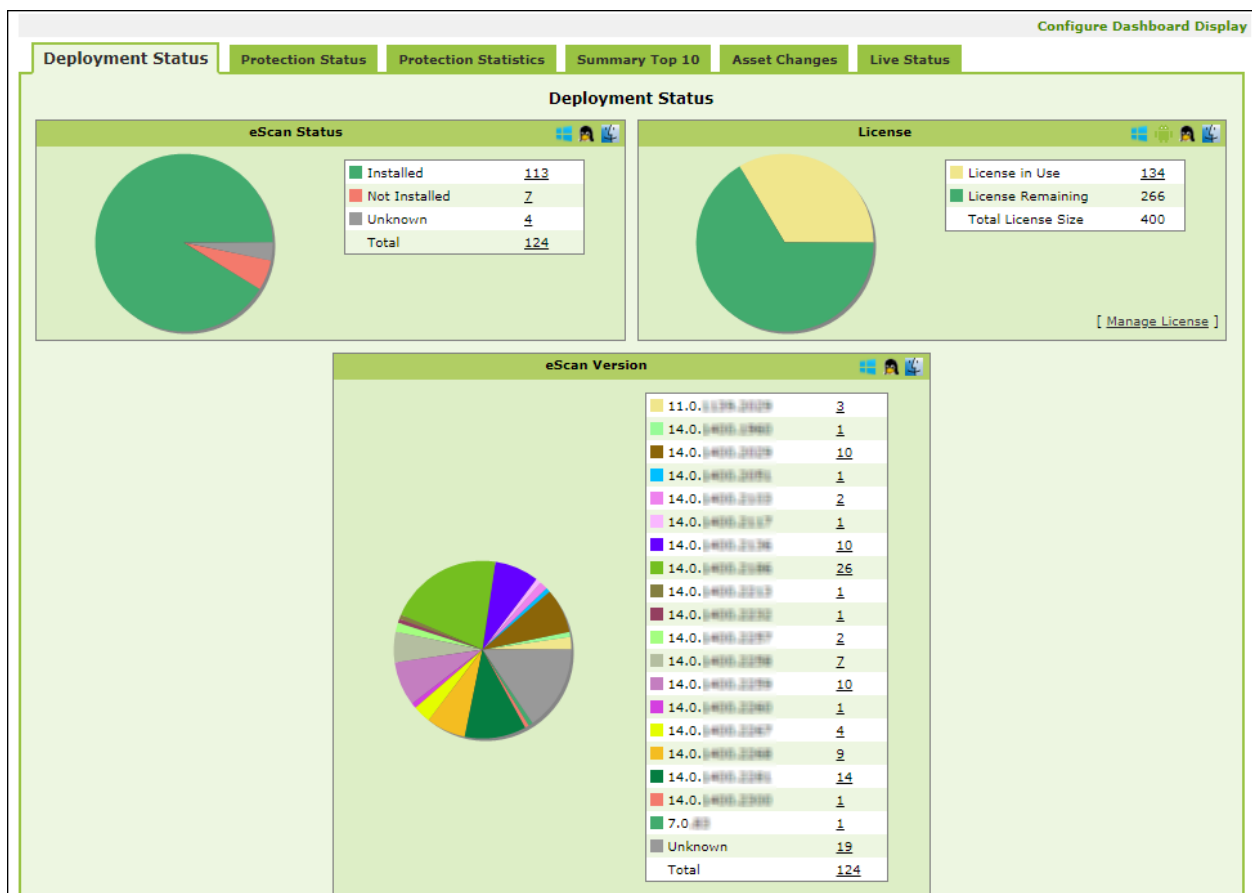
Dashboard

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

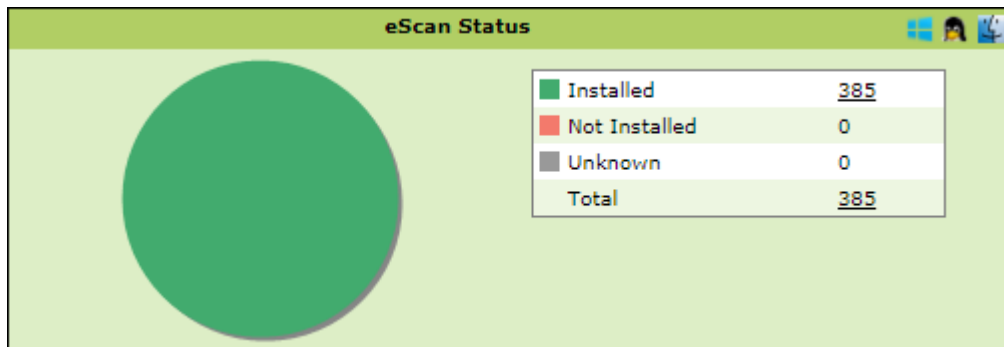
- Deployment Status
- Protection Status
- Protection Statistics
- Summary Top 10
- Asset Changes
- Live Status

Deployment Status

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



eScan Status



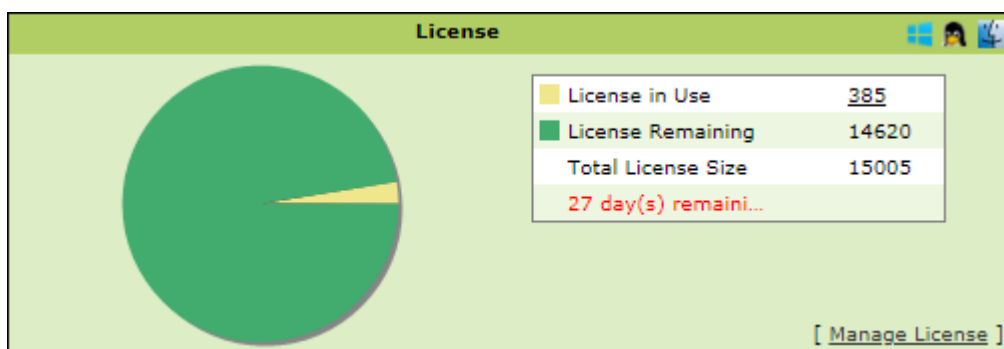
Installed – It displays the number of computers on which eScan Client is installed.

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

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

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

License



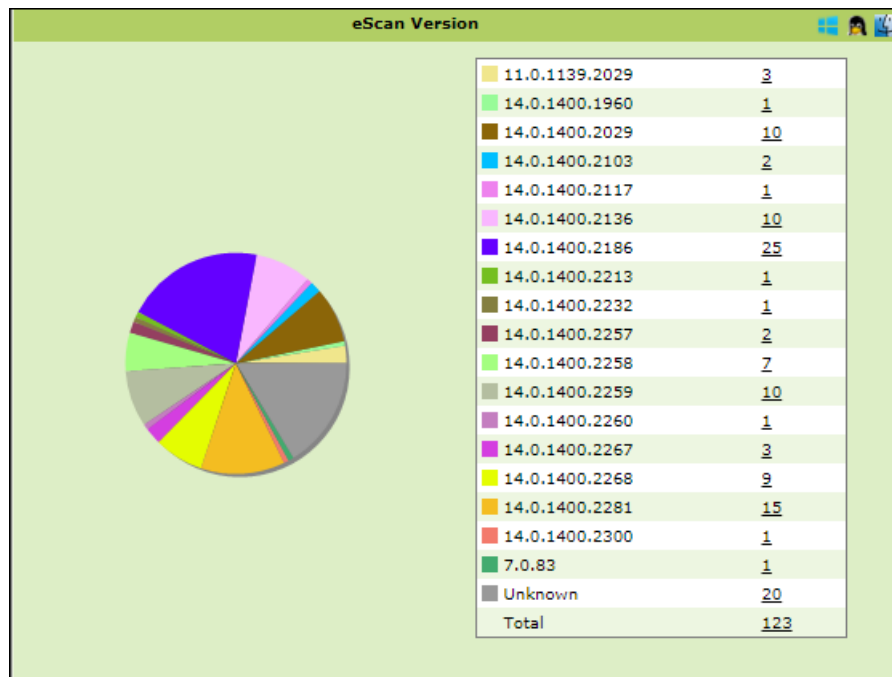
License in Use - It displays the number of licenses that are active.

Licenses Remaining - It displays the number of remaining licenses.

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

eScan version

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






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

Deployment Status >> eScan Version		
Client OS Type All		Print
Machine Name	Version	Group
COMPUTER-1	11.0.1139.2029	Managed Computers\National Sales Team-IND
EUROPE-1	11.0.1139.2029	Managed Computers\Europe Team
PRODUCTION-1	11.0.1139.2029	Managed Computers\Production Group
Close		

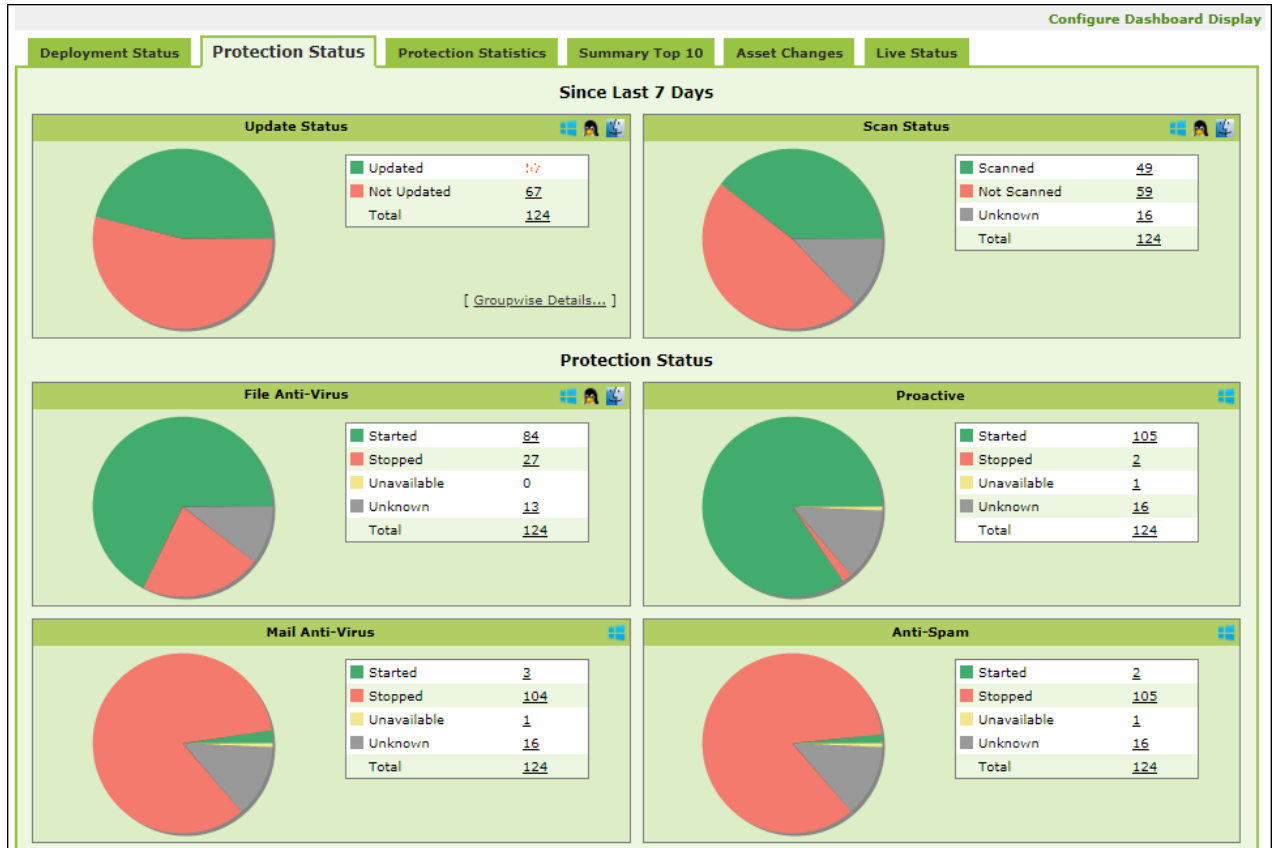
Note

Clicking underlined numerical displays detailed information for computers.

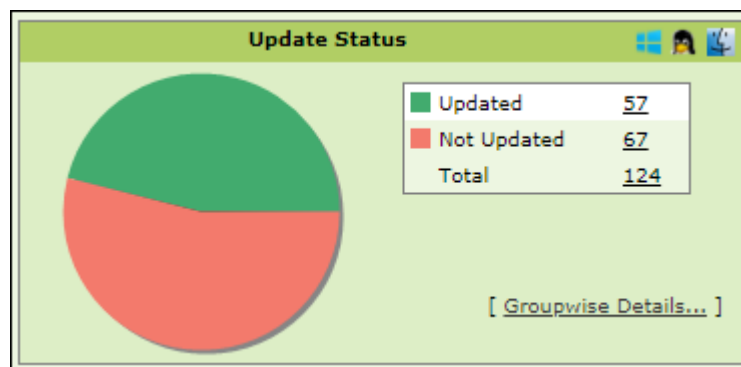
The  Windows,  Mac,  Linux Icons at the top of every chart denote that the information is displayed for the respective Operating Systems (OS).

Protection Status

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



Update Status

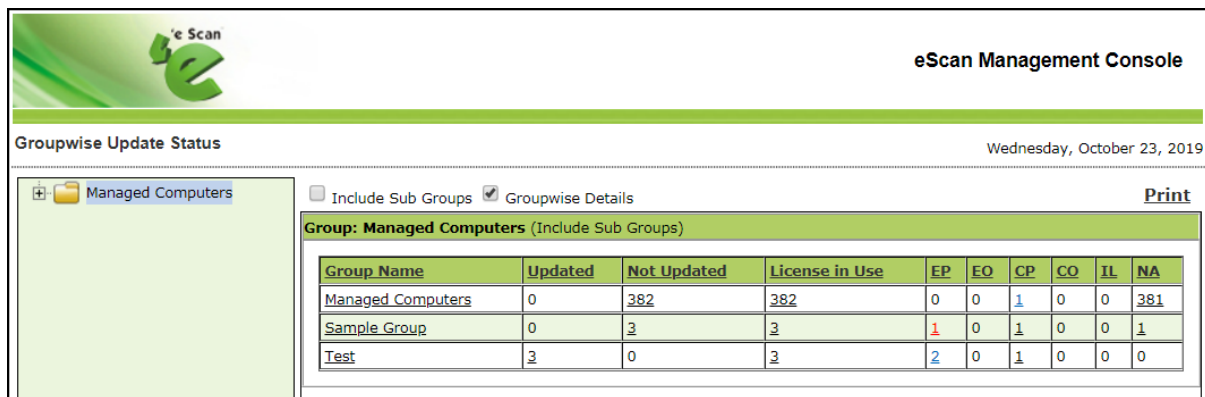


Updated – It displays the number of computers on which virus signature database is updated.

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

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

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



Groupwise Update Status Wednesday, October 23, 2019

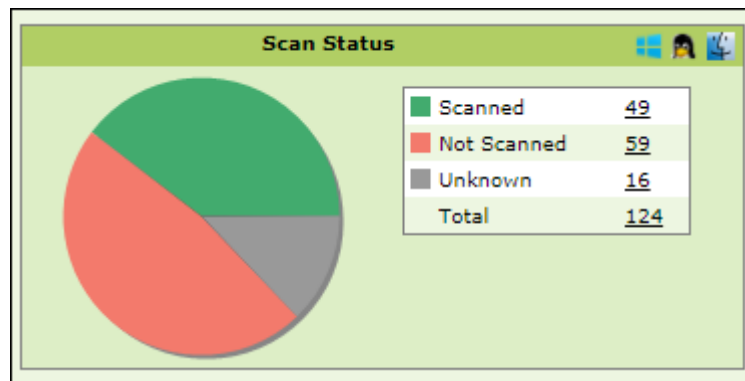
☐ Include Sub Groups ☒ Groupwise Details [Print](#)

Group: Managed Computers (Include Sub Groups)

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

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

Scan Status



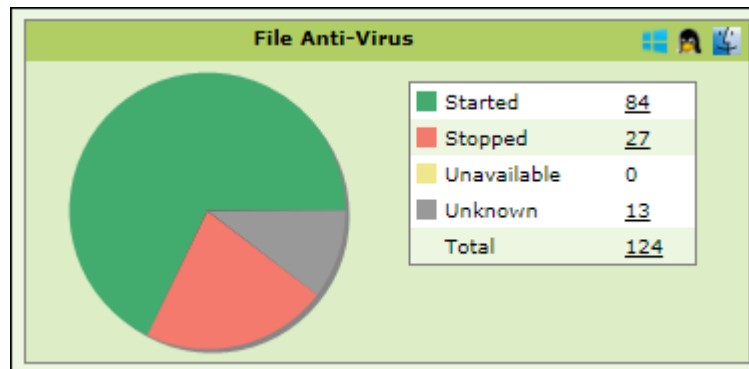
Scanned - It displays the number of computers that have been scanned in last 30 days for viruses and malware infections.

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

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

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

File Anti-Virus



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

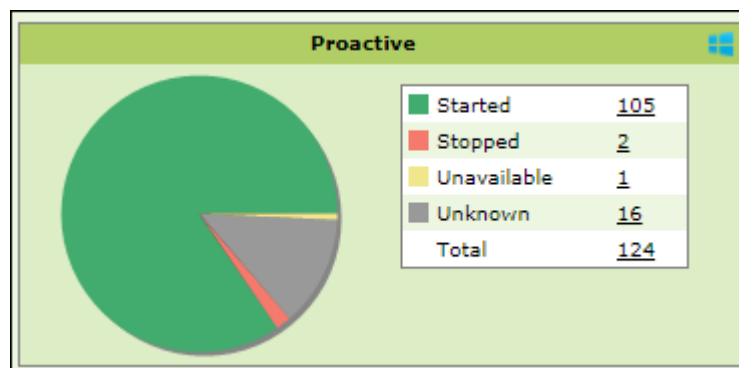
Stopped – It displays the number of computers on which the File Anti-Virus module is in Stopped state.

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

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

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

Proactive



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

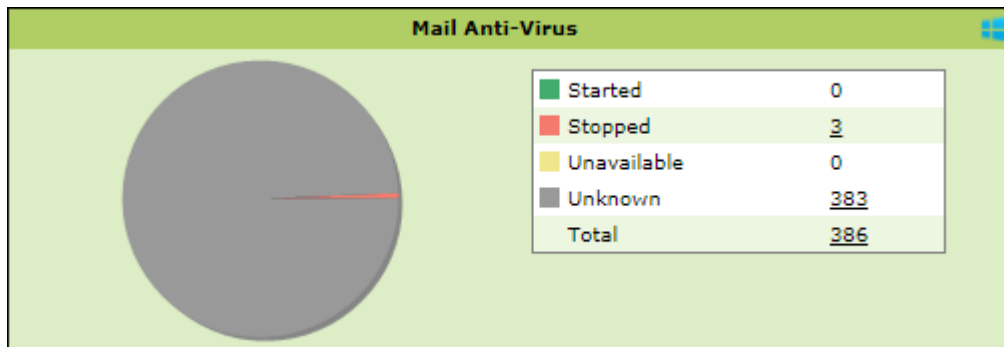
Stopped - It displays the number of computers on which Proactive scanning service is stopped.

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

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

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

Mail Anti-Virus



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

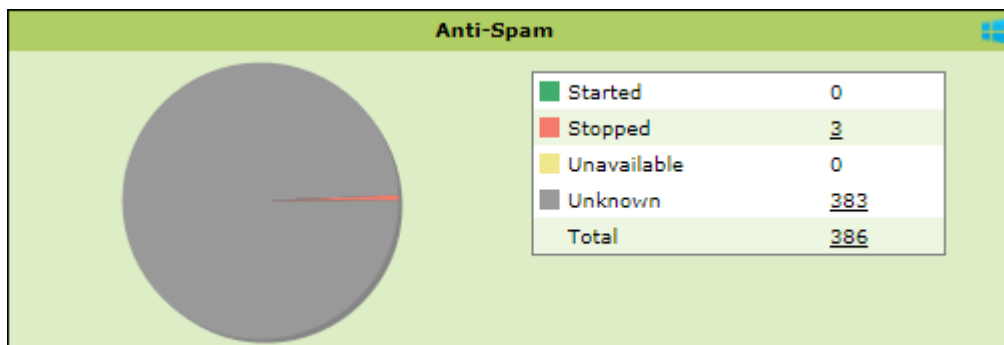
Stopped – It displays the number of computers on which the Mail Anti-Virus module is in Stopped state.

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

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

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

Anti-Spam



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

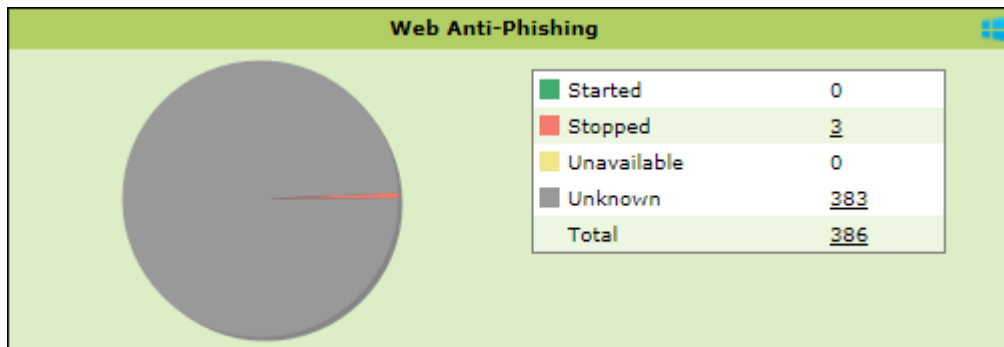
Stopped – It displays the number of computers on which the Anti-Spam module is in Stopped state.

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

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

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

Web Anti-Phishing



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

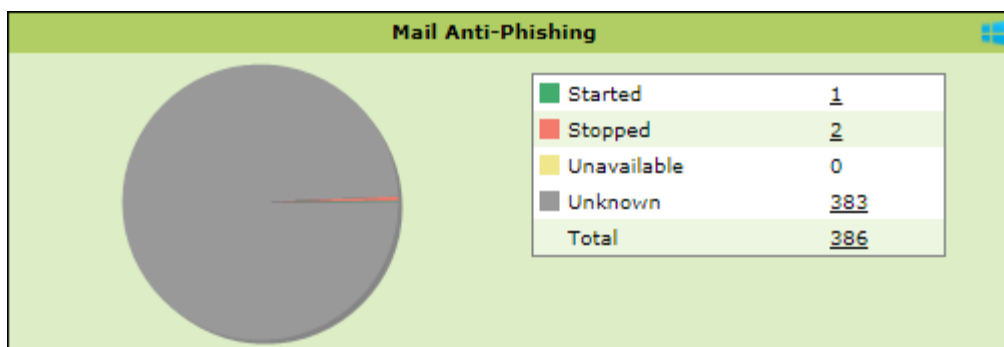
Stopped – It displays the number of computers on which the web Anti-Phishing service is stopped.

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

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

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

Mail Anti-Phishing



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

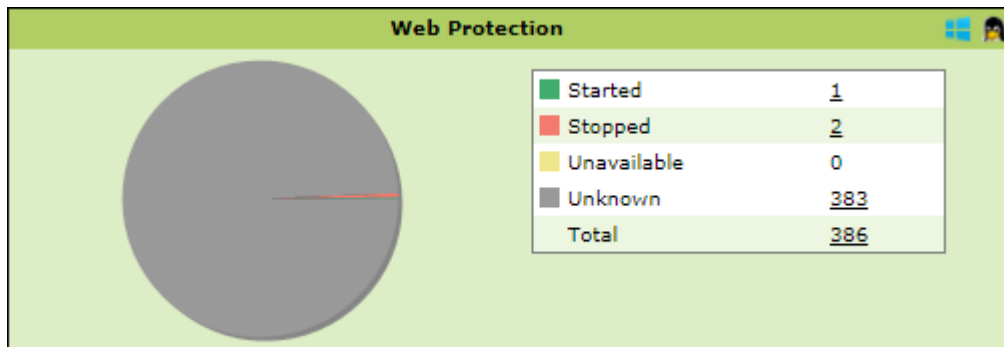
Stopped – It displays the number of computers on which the Mail Anti-Phishing service is disabled.

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

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

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

Web Protection



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

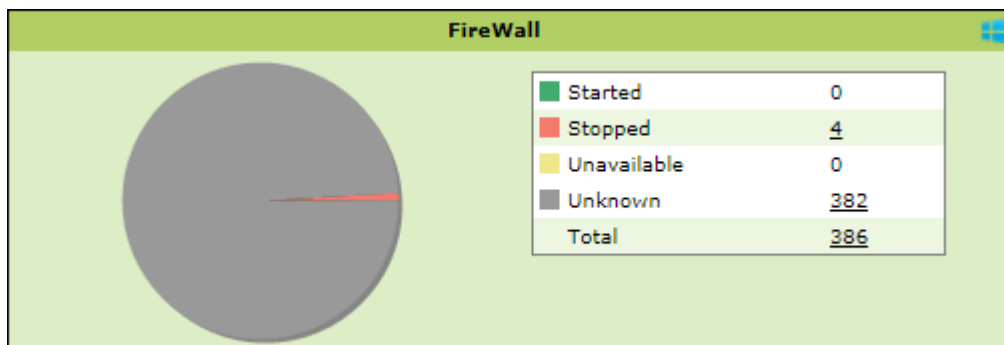
Stopped – It displays the number of computers on which the Web Protection module is in Stopped state.

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

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

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

Firewall



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

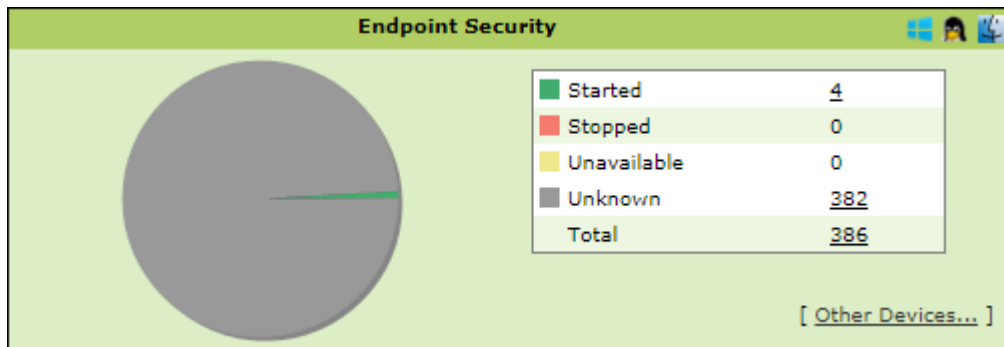
Stopped - It displays the number of computers on which the Firewall module is in Stopped state.

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

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

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

Endpoint Security



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

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

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

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

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

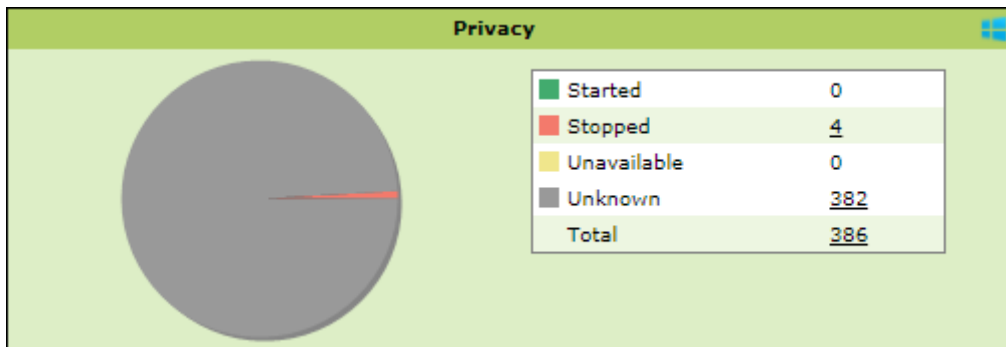
Clicking **Other Devices** displays details about other devices.

Other Devices Status

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

Close

Privacy



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

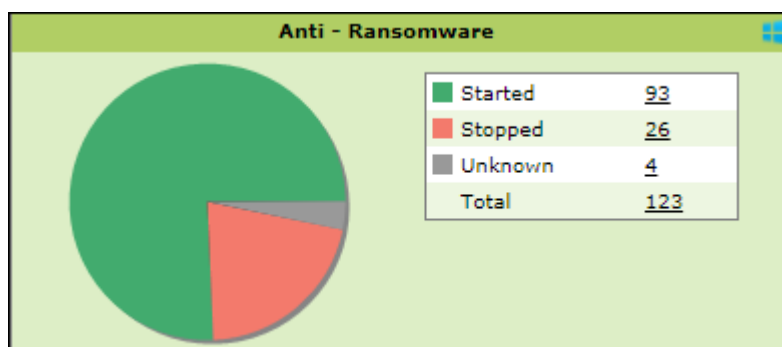
Stopped - It displays the number of computers on which the Privacy Control module is in Stopped state.

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

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

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

Anti – Ransomware



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

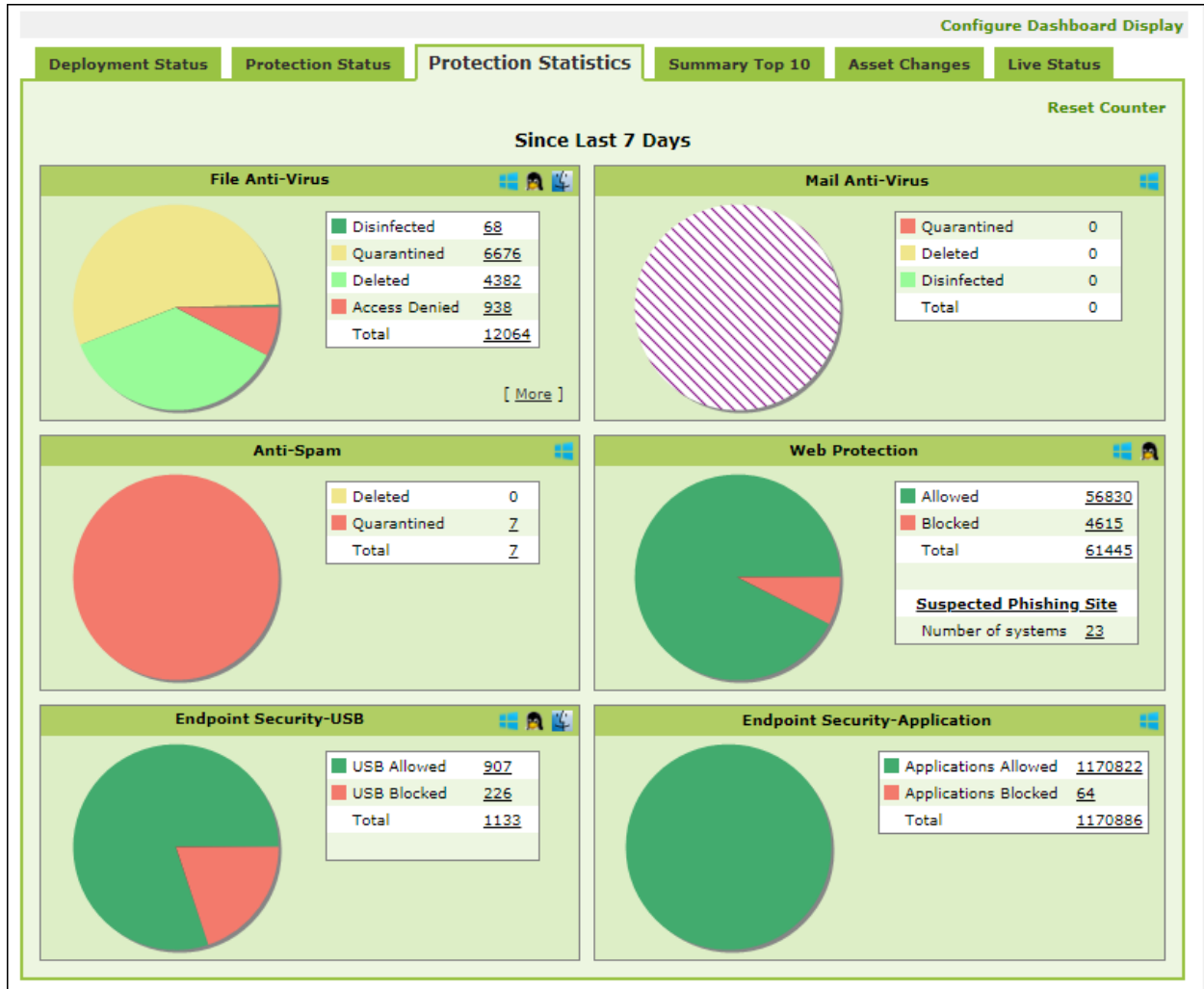
Stopped - It displays the number of computers on which the Anti – Ransomware module is in Stopped state.

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

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

Protection Statistics

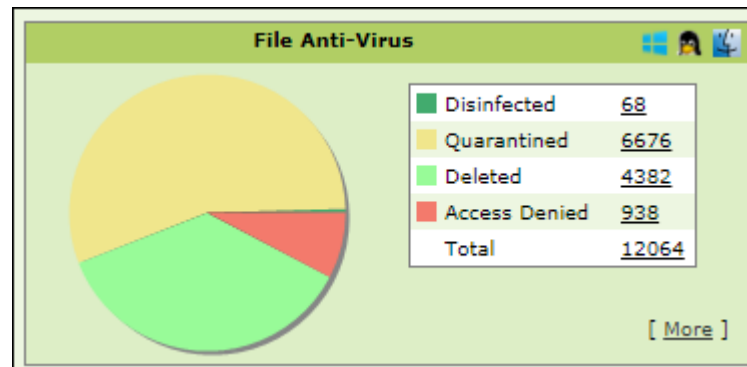
This tab displays activity statistics and action taken by all modules of eScan Client since last seven days in pie chart format.



Reset Counter

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

File Anti-Virus



Disinfected – It displays the number of files disinfected by File Anti-Virus module.


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

Deleted - It displays the number of files deleted by File Anti-Virus module.

Access Denied - It displays the number of files to which access was denied by File Anti-Virus module.

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

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


eScan Management Console

06 August 2020

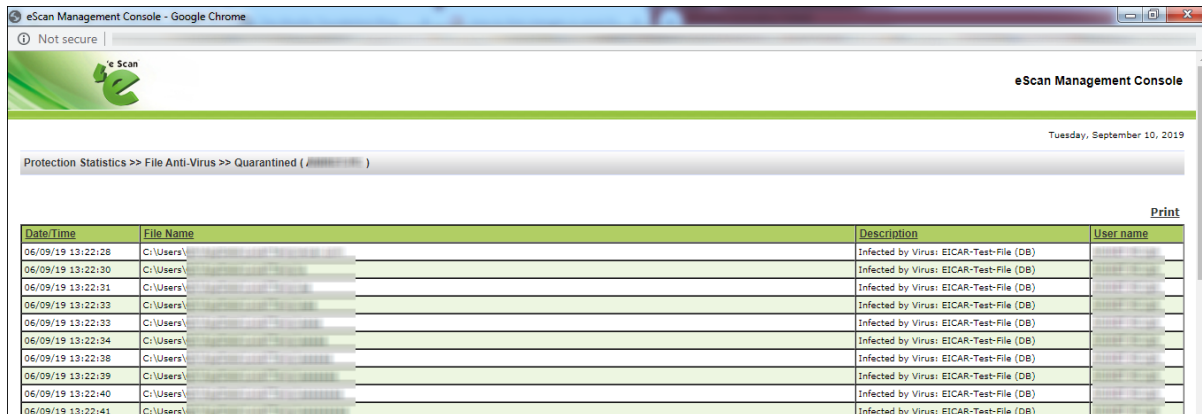
Protection Statistics >> File Anti-Virus >> Quarantined

Client OS Type All ▼ Print

Machine Name	Status	Group
WIN7-PC-001	<u>Quarantined (1)</u>	Managed Computers\Escan

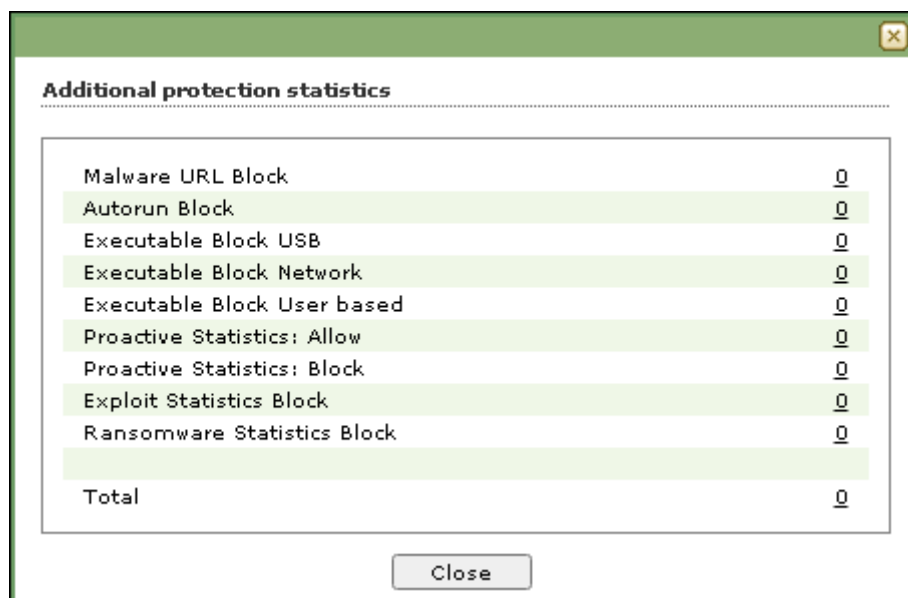
Close

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



Date/Time	File Name	Description	User name
06/09/19 13:22:38	C:\Users\... \...	Infected by Virus: EICAR-Test-File (DB)	...
06/09/19 13:22:38	C:\Users\... \...	Infected by Virus: EICAR-Test-File (DB)	...
06/09/19 13:22:38	C:\Users\... \...	Infected by Virus: EICAR-Test-File (DB)	...
06/09/19 13:22:38	C:\Users\... \...	Infected by Virus: EICAR-Test-File (DB)	...
06/09/19 13:22:38	C:\Users\... \...	Infected by Virus: EICAR-Test-File (DB)	...
06/09/19 13:22:38	C:\Users\... \...	Infected by Virus: EICAR-Test-File (DB)	...
06/09/19 13:22:38	C:\Users\... \...	Infected by Virus: EICAR-Test-File (DB)	...
06/09/19 13:22:38	C:\Users\... \...	Infected by Virus: EICAR-Test-File (DB)	...
06/09/19 13:22:38	C:\Users\... \...	Infected by Virus: EICAR-Test-File (DB)	...
06/09/19 13:22:38	C:\Users\... \...	Infected by Virus: EICAR-Test-File (DB)	...

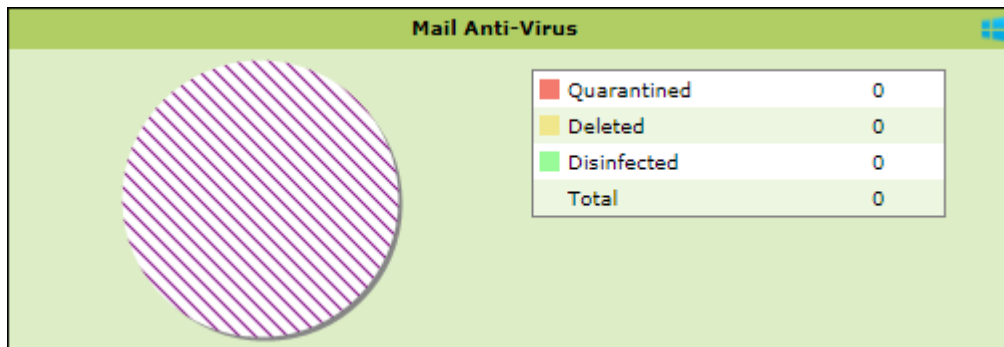
Clicking **[More]** displays additional protection statistics.



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

Close

Mail Anti-Virus



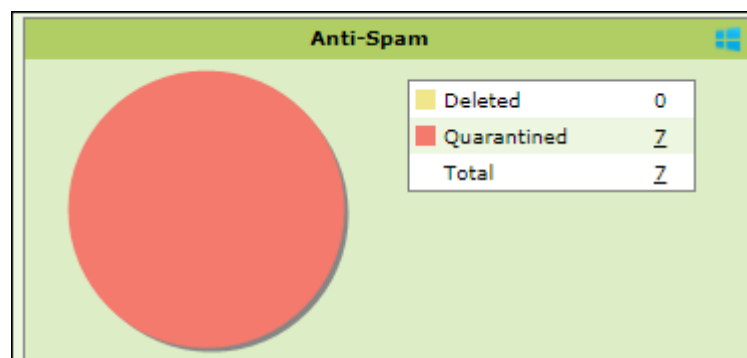
Quarantined – It displays the number of files/emails quarantined by Mail Anti-Virus module.

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

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

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

Anti-Spam

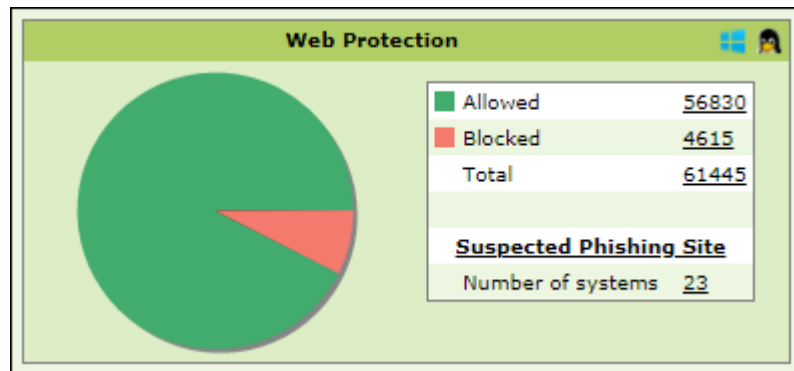


Deleted – It displays the number of files deleted by Anti-Spam module.

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

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

Web Protection



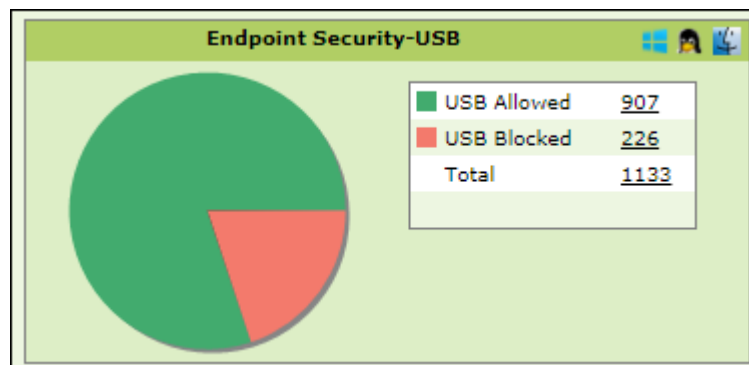
Allowed – It displays the number of websites to which access was allowed by Web Protection module.

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

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

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

Endpoint Security-USB

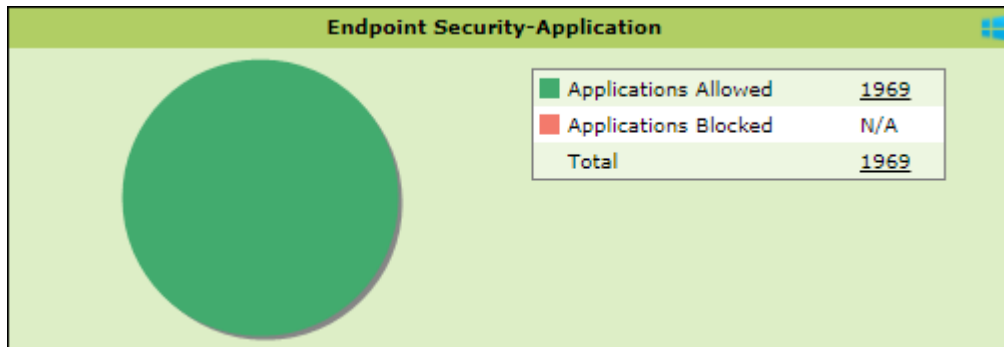


USB Allowed – It displays the number of USB access allowed along with the details for the same by Endpoint Security-USB module.

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

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

Endpoint Security-Application



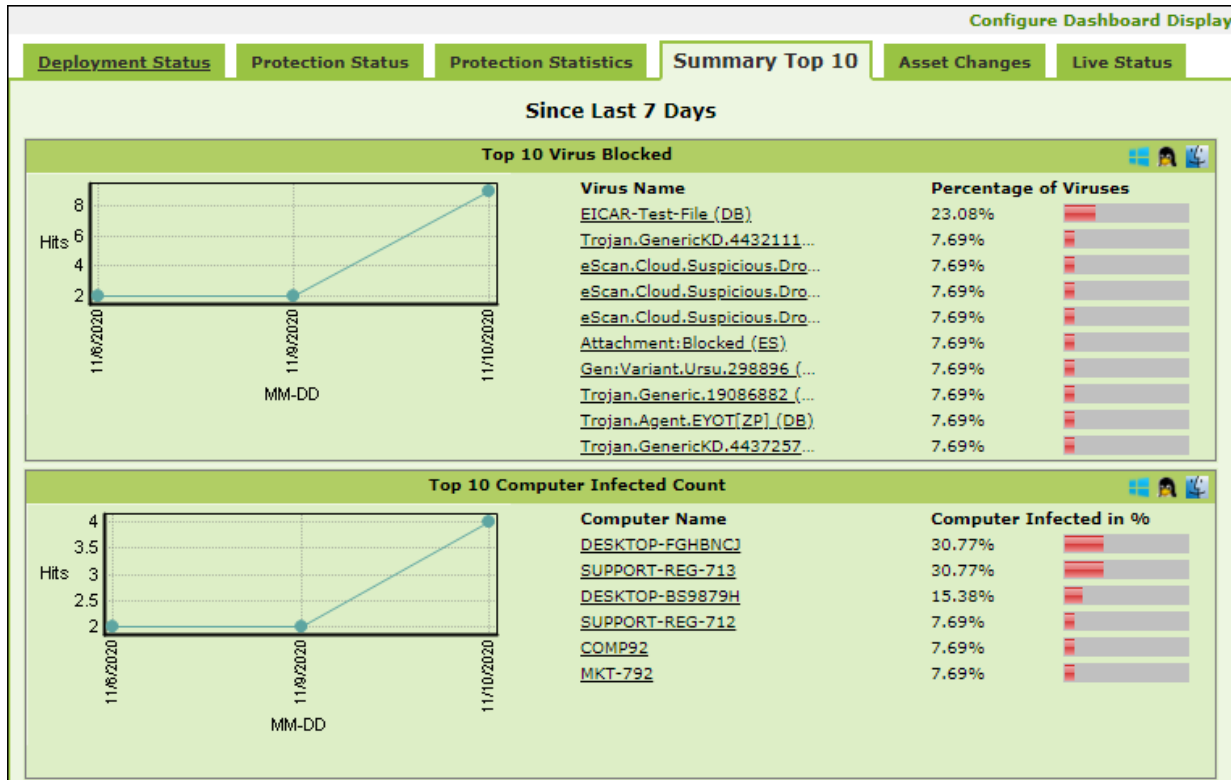
Applications Allowed – It displays the number of applications allowed by Endpoint Security-Application module.

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

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

Summary Top 10

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

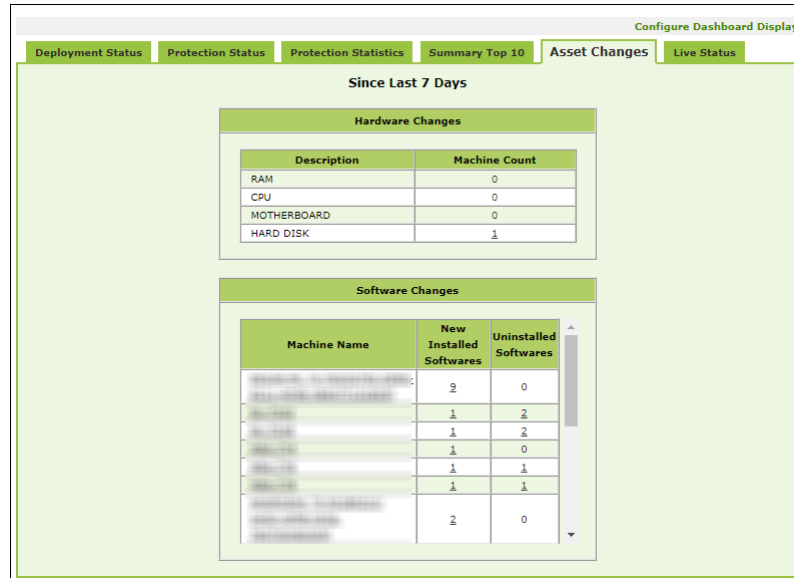


The tab displays the summary for following parameters:

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

Asset Changes

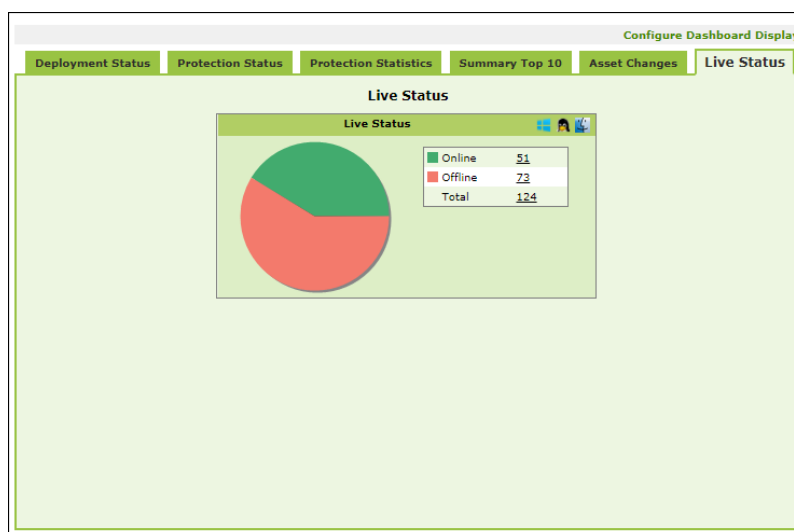
This tab displays all hardware and software changes carried out on the endpoints since last seven days.



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

Live Status

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



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

Configure the Dashboard Display

To configure the Dashboard display

1. In the Dashboard screen, at the upper right corner, click **Configure Dashboard Display**.

Configure Dashboard Display window appears displaying tabs and their parameters.

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

- Deployment Status**
 - ☒ eScan Status
 - ☒ License Summary
 - ☐ eScan Version
- Protection Status**
 - ☒ Update Status
 - ☒ File Anti-Virus
 - ☐ Mail Anti-Virus
 - ☐ FireWall
 - ☐ Web Protection
 - ☒ Endpoint Security
 - ☒ Anti-Ransomware
 - ☐ Scan Status
 - ☐ Proactive
 - ☐ Anti-Spam
 - ☐ Mail Anti-Phishing
 - ☐ Web Anti-Phishing
 - ☐ Privacy
- Protection Statistics**
 - ☒ File Anti-Virus
 - ☐ Anti-Spam
 - ☒ Endpoint Security-USB
 - ☐ Mail Anti-Virus
 - ☐ Web Protection
 - ☐ Endpoint Security-Application
- Summary Top 10**
 - ☒ Machine Infected
 - ☒ Application Allowed by Computer
 - ☒ Website Blocked by Computer
 - ☐ Application Blocked by App Name
 - ☐ Website Blocked by Sites
 - ☒ Website Blocked by Username
 - ☐ Infected Emails
 - ☐ Virus Blocked
 - ☒ USB Blocked
 - ☒ Application Blocked by Computer
 - ☒ Website Allowed by Computer
 - ☐ Application Allowed by App Name
 - ☐ Website Allowed by Sites
 - ☒ Website Allowed by Username
 - ☐ Spam Emails
 - ☒ Exploit Blocked
- Live Status**
 - ☒ Live Status

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

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

The tabs will be updated according to the changes.

Managed Computers

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

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

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

Managed Computers

Refresh Help

Search Update Agent

Action List Client Action List Policy Templates Policy Criteria Templates QR Code for 2FA

Managed Computers

- Policy
- Group Tasks
- Client Computers (1)
- Roaming Users
- sample
 - Policy
 - Group Tasks
 - Client Computers

Name	
Policy	
Group Tasks	
Client Computers	
Group Information	
AD Sync	Not Configured
Total Subgroups	2
Total Computers	1

The screen consists of following buttons:

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

Search

The Search feature lets you find any computer added in Managed Computers. After clicking **Search**, Search for Computers window appears.

The Filter section displays following fields:

Computer Name/IP

Enter a computer name or IP address.

Username

Enter a username.

Click **Find Now**.

The console will display the result.

Update Agent

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

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


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


Adding an Update Agent

To add an Update Agent

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

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

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

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

The Update Agent will be set for the selected group.

Delete an Update Agent

To delete an Update Agent

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

Update Agent

Select Group Name and Update Agent

Update Agent:

...

Group Name:

...

Add

Update Agent	IP Address	Assigned to Group(s)
10443	10.10.10.10	Managed Computers\Sample Group

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

10443:10443 says

Do you want to remove update agent?

OK

Cancel

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

Action List

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

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

Creating a Group

To create a group, follow the steps given below:

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

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

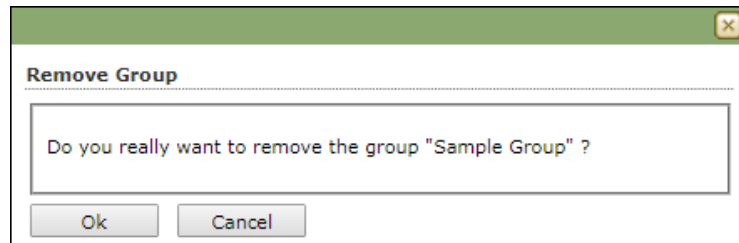
A new group will be created under the Managed Computers.

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

Removing a Group

To remove a group, follow the steps given below:

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



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

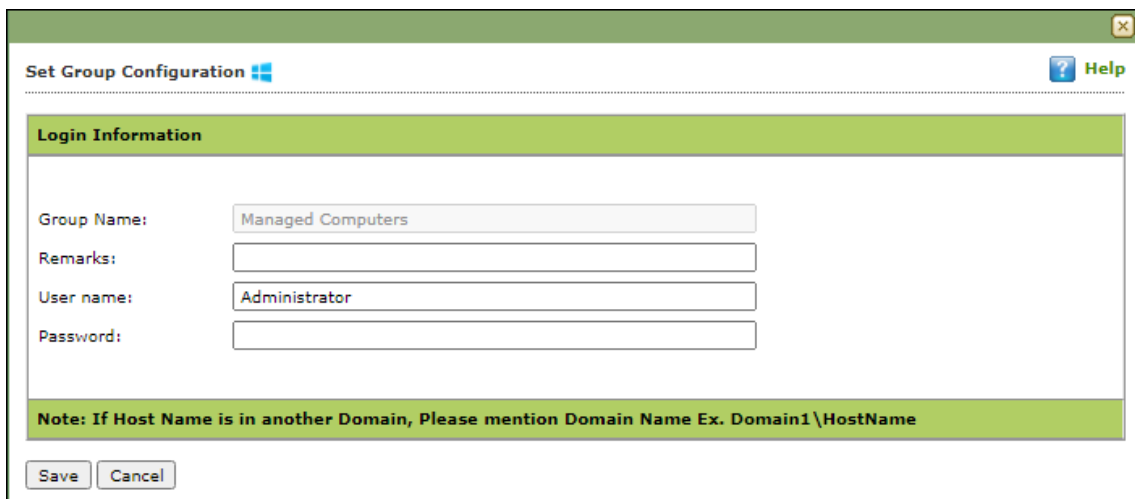
NOTE A group will be removed only if it contains no computers.

Set Group Configuration

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

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

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



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

Managing Installations

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

This section will give you an overview on following activities:

Installing eScan Client

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

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

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

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

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

Remote Installation of eScan Client

Pre-Installation

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

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

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

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

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

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

For Windows XP Home

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

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

1. Launch **Run**.
2. Enter **secpol.msc**, and then click **OK**. **Local Security Settings** window appears.
3. On the navigation pane, click **Local Policies** folder, and then double-click **Security Options** folder. The security policy appears.
4. Double-click **Network access: Sharing and security model for local accounts** policy.

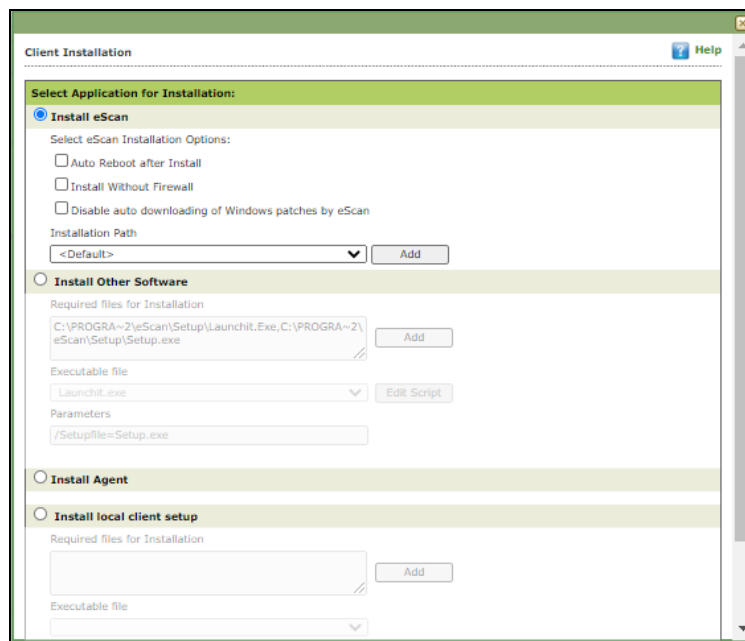
5. Select **Classic - Local users authenticate as themselves** option present in the drop-down.
6. Click **Apply > OK**.
7. Double-click **Accounts: Limit local account use of blank passwords to console logon only** policy.
8. Select **Disabled** option.
9. Click **Apply > OK**.
10. If the firewall is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

Deploy/Upgrade Client

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

Installing eScan Client on a Group

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



3. Select **Install eScan** option.

By Default eScan is installed at the following Path on a Client computer.

C:\Program Files\eScan (default path for 32-bit computer)

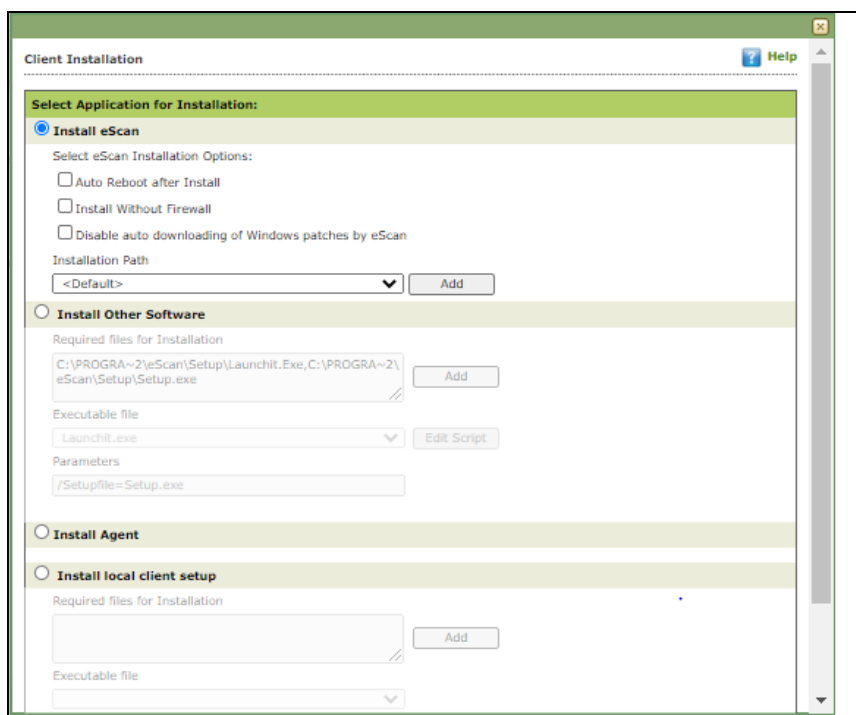
OR

C:\Program Files (x86)\eScan (default path for 64-bit computers).

4. To define a different installation path, click **Add**. (Skip this step if default path chosen).
5. Click **Install**. A window displays File transfer progress. After Installation, the eScan status will be updated in Managed Computers list.

Installing eScan Client on an Individual Computer in a Group

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











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

Refresh Client

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

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

Understanding the eScan Client Protection Status

 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 Enabled	This status is displayed when a computer is added to RMM license and the computer can be connected via RMM service.
 Two-FA Enabled	This status is displayed when a computer is added to 2FA license.
 DLP	This status is displayed when a computer is added to DLP license.
 Ebackup	This status is displayed when a computer is added to eBackup license.

Moving computer from one group to other

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

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

The computers will be moved to the selected group.

Viewing installed software (on Client computer)

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

1. In folder tree, click **Managed Computers**.
2. Select the desired computer.
3. Click **Client Action List > Show Installed Software**.
A list of all the Software installed on that computer will be displayed on pop up window in an instant.

Removing computers from a group

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

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

Installing eScan on Linux and MAC Computers

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

Installing Agent on Linux (Debian based Operating System) –

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

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

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

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

Installing eScan Agent on Mac Computers

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

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



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



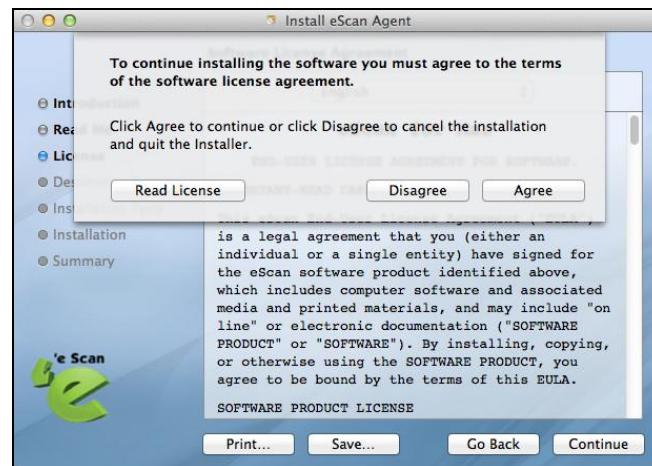
The installation wizard displays Read Me window.

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

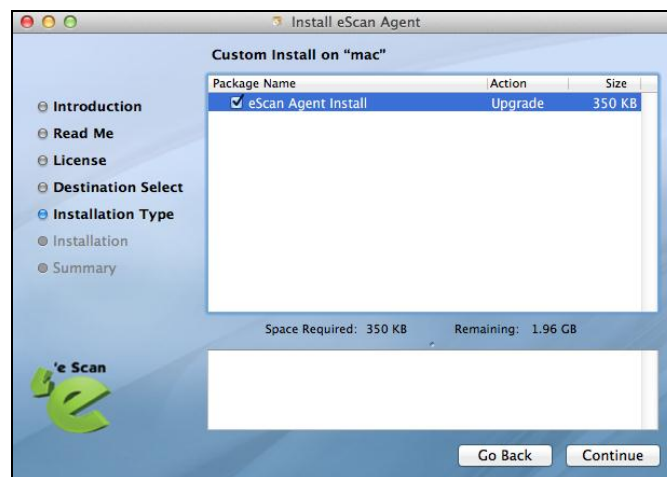


7. Please read the agreement completely and then click **Continue**.

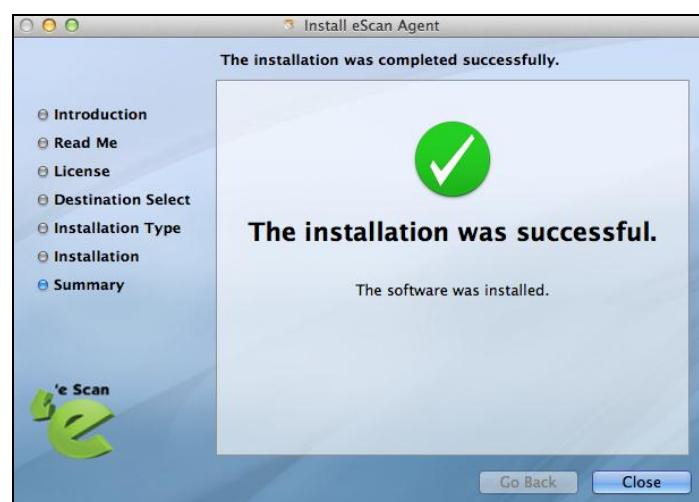
8. Agree to terms and conditions by clicking **Agree**.



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



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

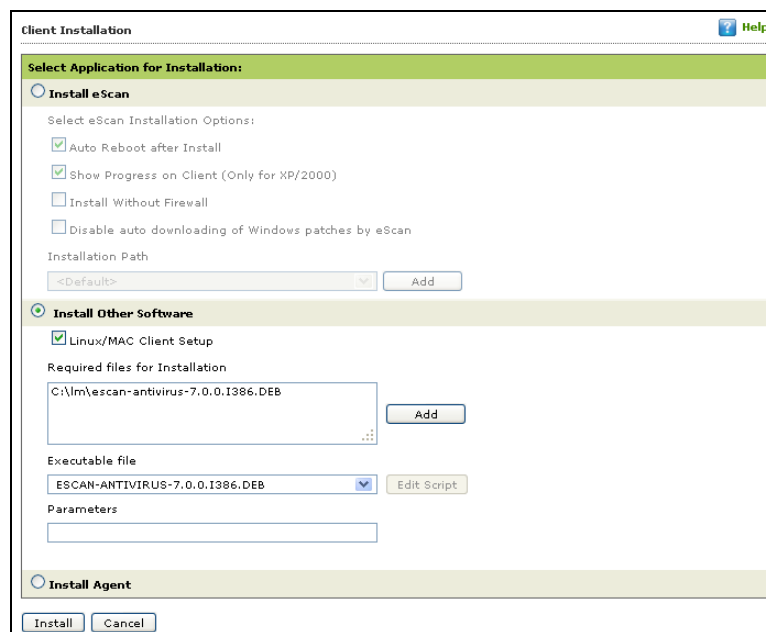


11. To exit the installation wizard, click **Close**.

Installing eScan Client on Linux or Mac computers

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

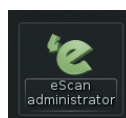
1. Select the desired computer.
2. Refresh the Client by clicking **Refresh Client**.
A link will be created for downloading the setup file of eScan Client for that computer; you will be redirected to escanav.com from where you can download the setup file.
3. Download the Client setup from the link on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



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

In Linux

- eScan Administrator Icon will be displayed on desktop.



In Mac

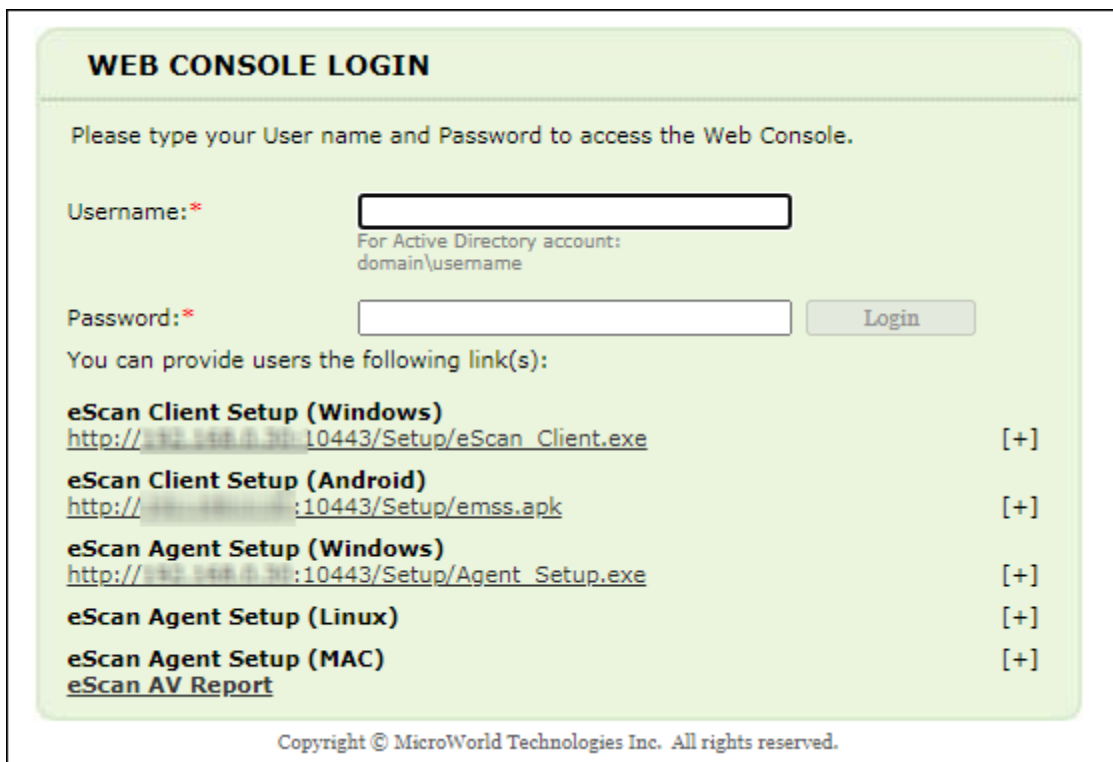
- An Icon of eScan will be displayed in the **Dock**. Double-click it to launch eScan.



Manual installation of eScan Client on network computers

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

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



The screenshot shows the 'WEB CONSOLE LOGIN' interface. It includes a text prompt 'Please type your User name and Password to access the Web Console.' followed by input fields for 'Username:*' and 'Password:*'. A 'Login' button is positioned to the right of the password field. Below the login fields, a message states 'You can provide users the following link(s):' followed by a list of download links for eScan Client and Agent setups for Windows, Android, Linux, and MAC, along with an eScan AV Report link. Each link is followed by a '[+]' icon. At the bottom, a copyright notice reads 'Copyright © MicroWorld Technologies Inc. All rights reserved.'

Link	Action
http://192.168.1.104:10443/Setup/eScan_Client.exe	[+]
http://192.168.1.104:10443/Setup/emss.apk	[+]
http://192.168.1.104:10443/Setup/Agent_Setup.exe	[+]
eScan Agent Setup (Linux)	[+]
eScan Agent Setup (MAC)	[+]
eScan AV Report	

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** of eScan Management Console to the users of the Client computer on mail.

WEB CONSOLE LOGIN

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

Username:*
For Active Directory account:
domain\username

Password:*

You can provide users the following link(s):

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

eScan Client Setup (Android) [-]
[http://\[redacted\]](http://[redacted])
[http://\[redacted\]](http://[redacted])
[http://\[redacted\]](http://[redacted])

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

eScan Agent Setup (Linux) [-]
[http://\[redacted\]](http://[redacted])
[http://\[redacted\]](http://[redacted])
[http://\[redacted\]](http://[redacted])
[http://\[redacted\]](http://[redacted])
[http://\[redacted\]](http://[redacted])
[http://\[redacted\]](http://[redacted])

eScan Agent Setup (MAC) [-]
[http://\[redacted\]](http://[redacted])
[http://\[redacted\]](http://[redacted])
[http://\[redacted\]](http://[redacted])
[http://\[redacted\]](http://[redacted])

eScan AV Report

Copyright © MicroWorld Technologies Inc. All rights reserved.

Installing other Software (Third Party Software)

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

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

4. Select **Install Other Software** option.

The screenshot shows the eScan installation wizard with the following fields and options:

- ☐ Disable auto downloading of Windows patches by eScan
- Installation Path: <Default> [Add]
- Install Other Software** (Selected)
 - ☐ Linux/MAC Client Setup
 - Required files for Installation: C:\Documents and Settings\Remya\My Documents\Downloads\snagit.exe [Add]
 - Executable file: snagit.exe [Edit Script]
 - Parameters: [Empty field]
- ☐ Install Agent
- ☐ Install local client setup
 - Required files for Installation: [Empty field] [Add]
 - Executable file: [Empty dropdown]
 - Parameters: [Empty field]

[Install] [Cancel]

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

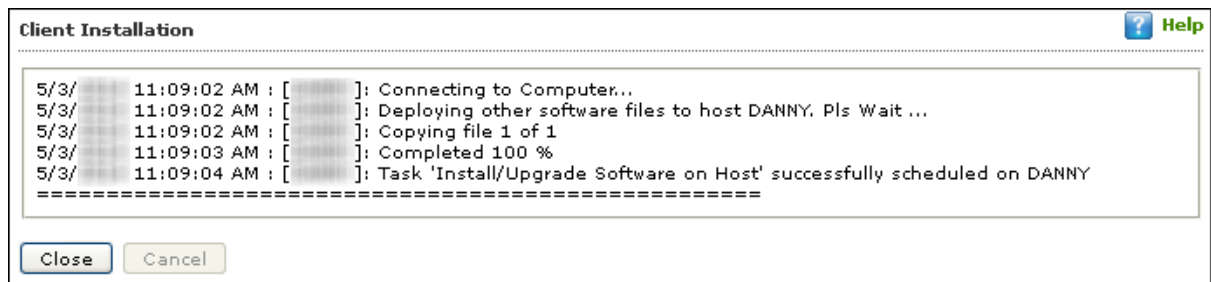
The screenshot shows the 'Add Files' dialog box in the eScan Management Console. It contains a text input field for the file path and two buttons: [Add] and [Cancel].

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

The screenshot shows the eScan installation wizard with the following fields and options:

- Install Other Software** (Selected)
 - Required files for Installation: C:\Users\QA\Downloads\tnw4ksmk.exe [Add]
 - Executable file: tnw4ksmk.exe [Edit Script]
 - Parameters: [Empty field]

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

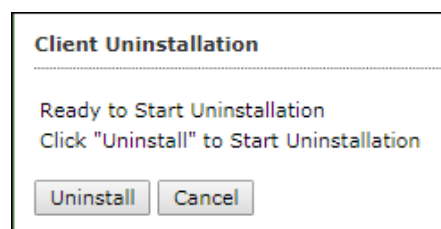


Uninstall eScan Client (Windows, Mac, and Linux)

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

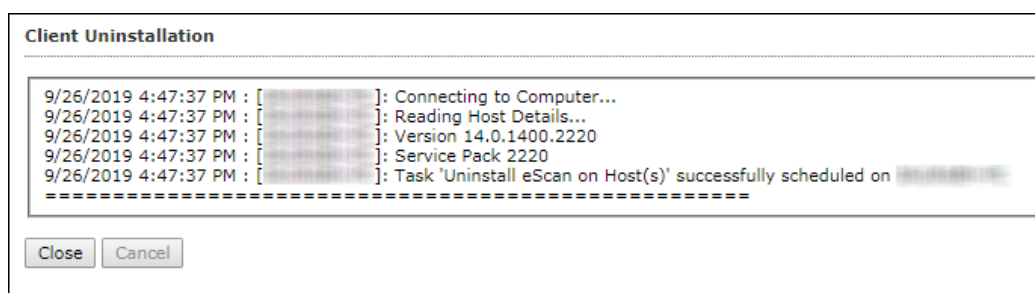
- Select the group of computers for uninstallation.
- Click **Action List > Uninstall eScan Client**.

Client Uninstallation window appears.



- Click **Uninstall**.

The Client Uninstallation window displays the progress.



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

NOTE

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

Synchronize with Active Directory

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

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

Synchronize with Active Directory window appears.

Synchronize with Active Directory

Target Groups :
Managed Computers\Sample Group

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\ADSync.log" for more details.

Source Active Directory Organization Unit

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

Synchronization Interval

Enter the preferred duration (in minutes).

Exclude from ADS Sync

This field displays a list of excluded Active Directory sources.

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

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

Search Filter

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

Install eScan manually

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

Install without Firewall

Selecting this option lets you install eScan without firewall.

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

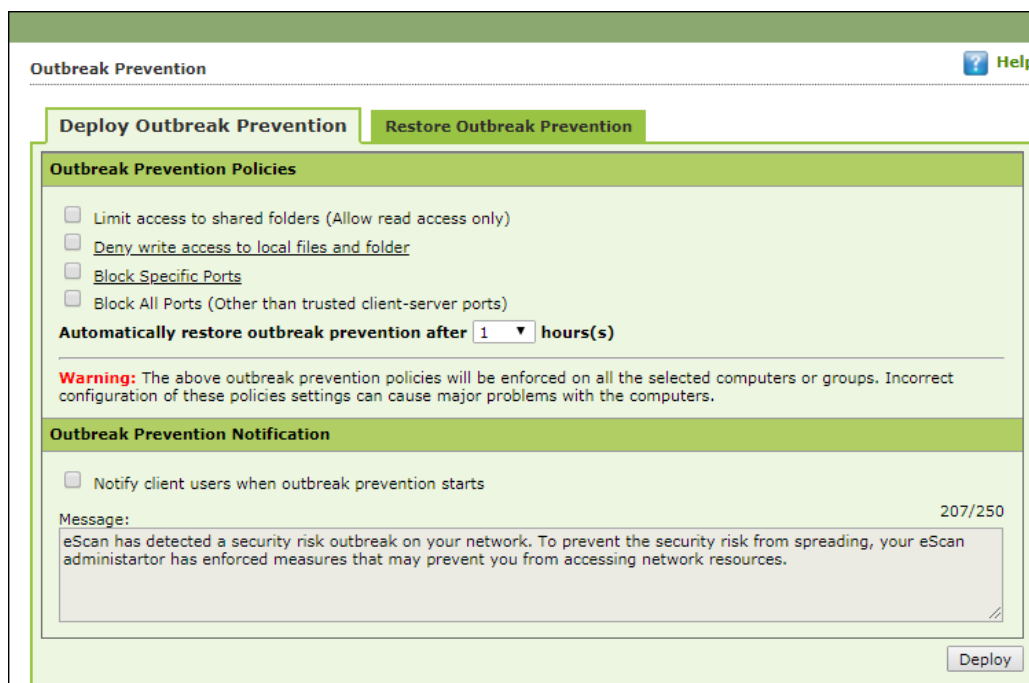
Outbreak Prevention

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

Deploying Outbreak Prevention

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

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



Limit access to shared folders

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

Deny write access to local files and folder

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

Block specific ports

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

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

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

Automatically restore the outbreak prevention after hour(s)

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

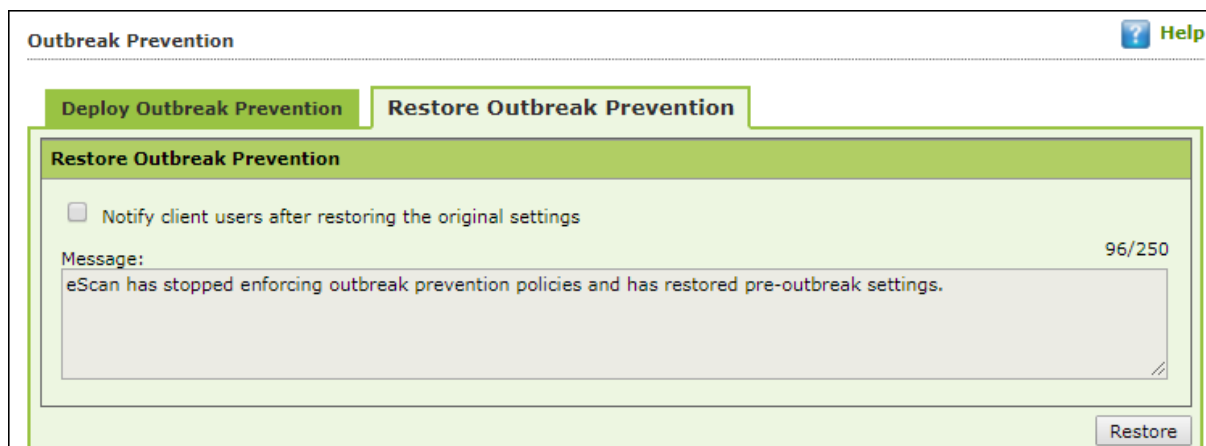
Outbreak Prevention Notification

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

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

Restore Outbreak Prevention

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



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

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

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

Create Client Setup

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

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

Create Client Setup window appears.

The 'Create Client Setup' dialog box has a title bar with a 'Help' button. It contains a 'Setup Settings' section with two checkboxes: 'Add Policy' and 'Auto add to group'. At the bottom are 'Create Setup' and 'Cancel' buttons.

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

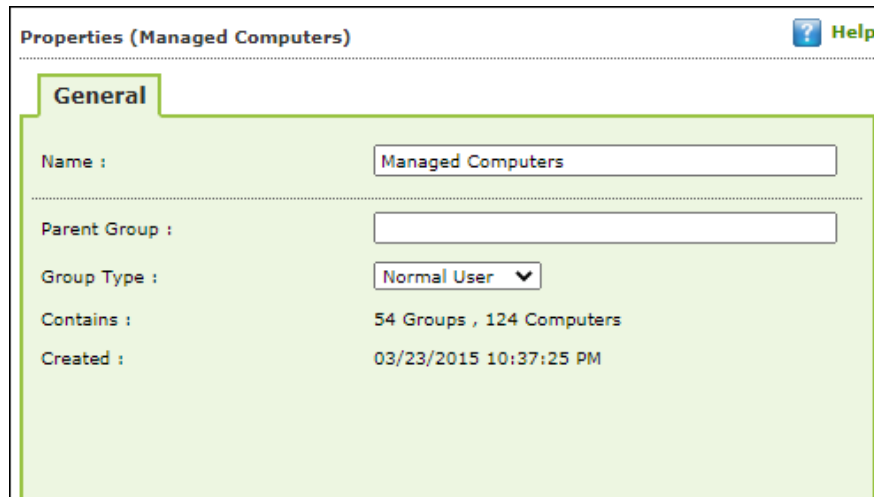
Name		Download Client Setup
	Policy	
	Group Tasks	
	Client Computers	
Group Information		
AD Sync		Not Configured
Total Subgroups		1
Total Computers		3

Properties of a group

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

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

Properties window appears.



The screenshot shows a window titled "Properties (Managed Computers)" with a "Help" button in the top right corner. The "General" tab is selected, displaying the following information:

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

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

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

Group Tasks

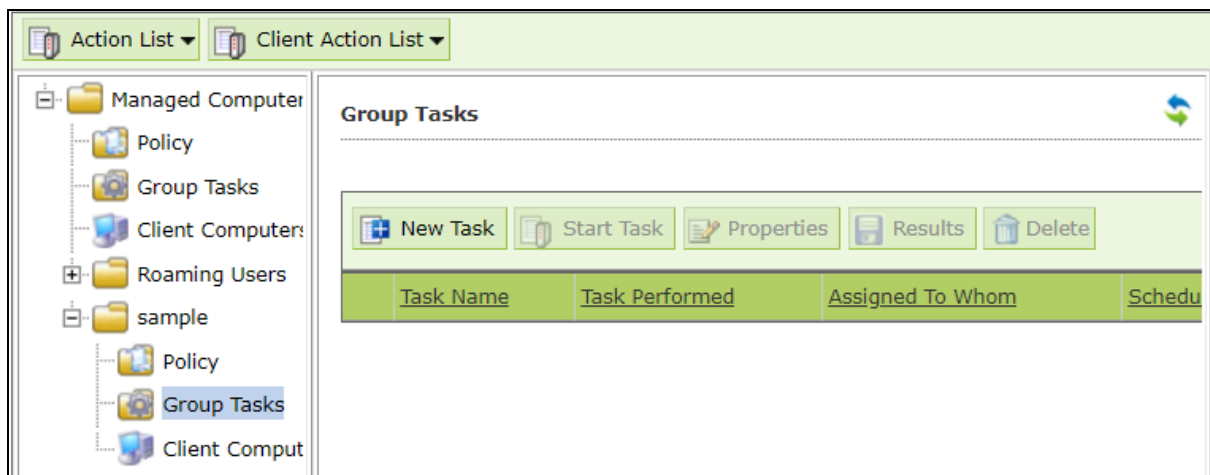
With the **Group Tasks** option, you can create a task, start a task, select a task and view its properties, view task results as well as delete an already created task. Tasks can include the following.

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

Creating a Group Task

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

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



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

New Task Template Help

Task Name

Task Name:

Assigned Tasks

- ☐ File Anti-Virus Status
 - ☐ Enabled
 - ☒ Disabled
- ☐ Mail Anti-Virus Status
 - ☐ Enabled
 - ☒ Disabled
- ☐ Anti-Spam Status
 - ☐ Enabled
 - ☒ Disabled
- ☐ Web Protection Status
 - ☐ Enabled
 - ☒ Disabled
- ☐ Endpoint Security Status
 - ☐ Enabled
 - ☒ Disabled
- ☐ Firewall Status
 - ☐ Disable Firewall
 - ☐ Enable Limited Filter Mode of Firewall
 - ☒ 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:

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

☐ Apply for Subgroups

Task Scheduling Settings

☒ Enable Scheduler ☐ Manual Start

☒ Daily ☐ Weekly ☐ Monthly

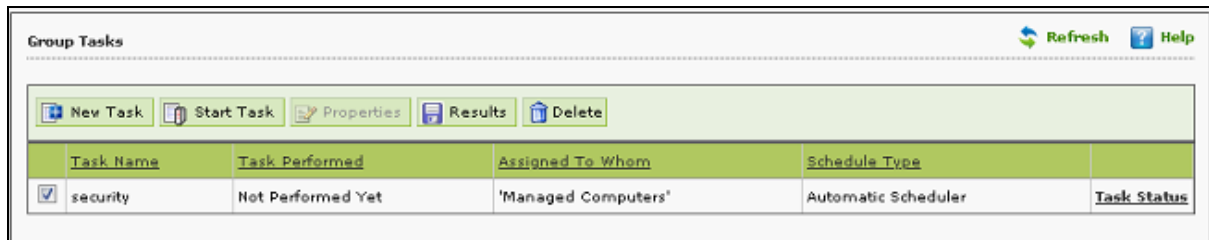
Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

At

4. Enter the Task Name and configure the desired task settings.
5. Click **Save**. The selected group will be assigned a task template.

Managing a Group Task

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



Start Task

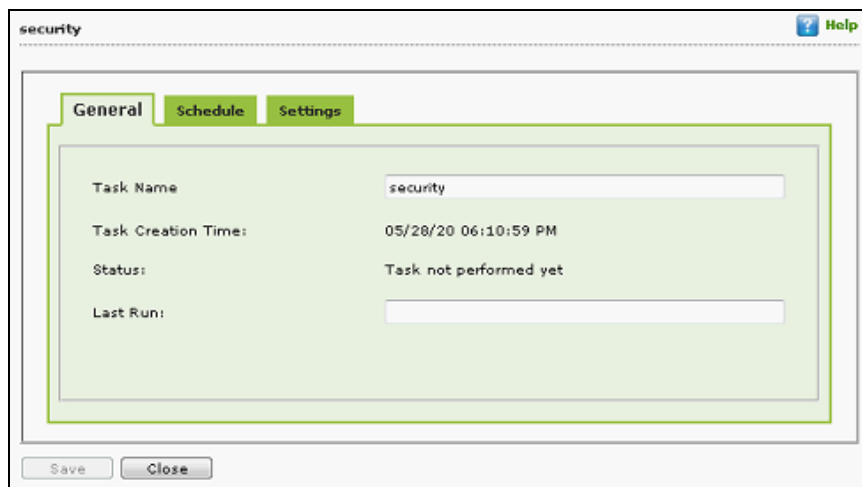
To start a task manually, select a task and then click **Start Task**.

Delete Task

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

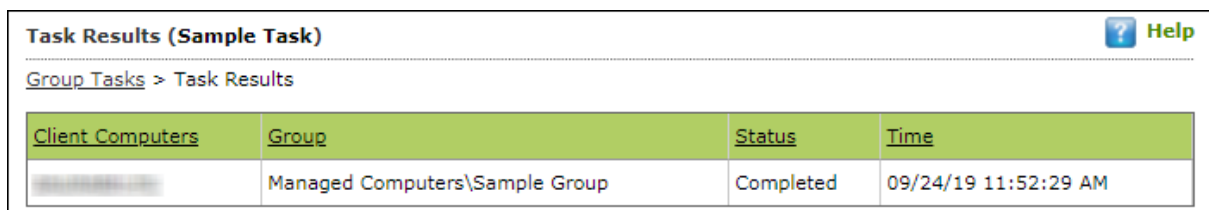
Properties

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



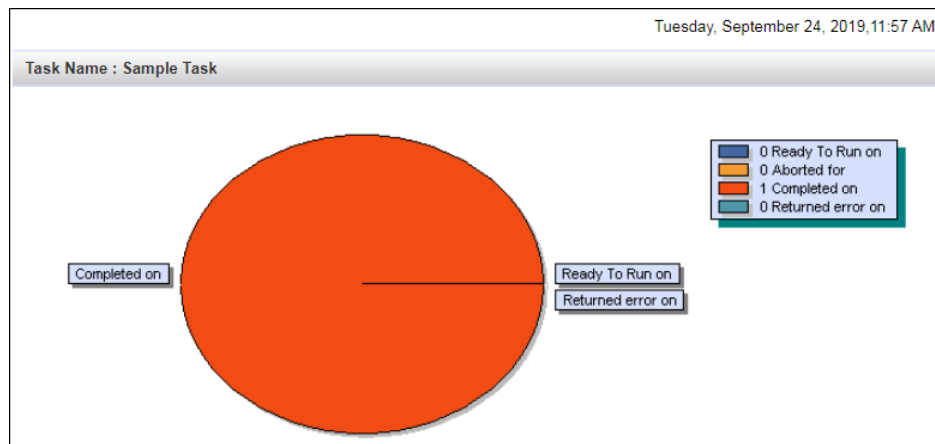
Results

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



Task Status

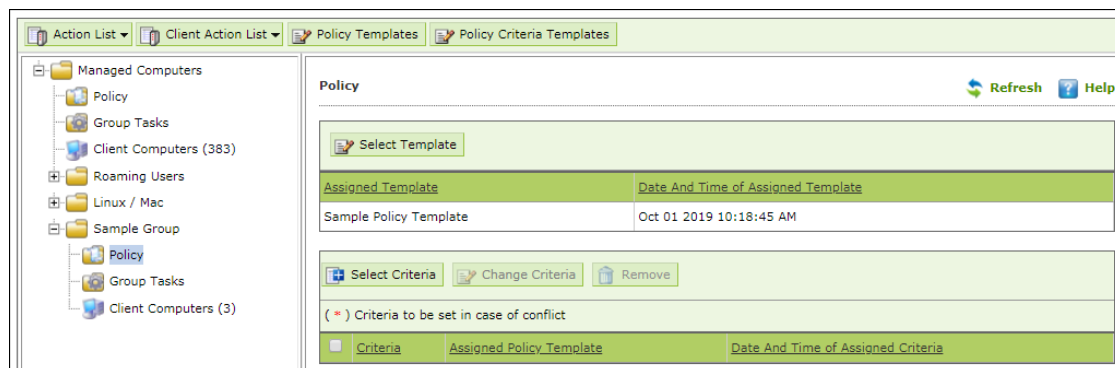
To view the status, select a task and then click **Task Status**. A brief task summary is displayed.



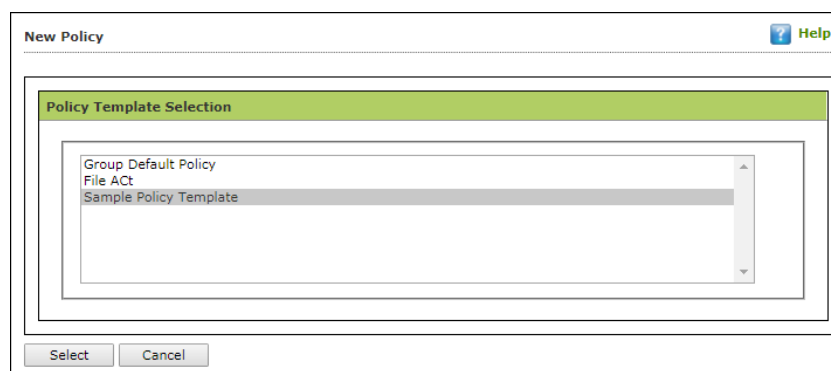
Assigning a Policy to the group

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

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



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



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

Select Policy Criteria Help

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

Policy Template Selection

- Group Default Policy
- File ACT
- Sample Policy Template**

Criteria Template Selection

- aaa**
- cr1

Select Cancel

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

Client Action List

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

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

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

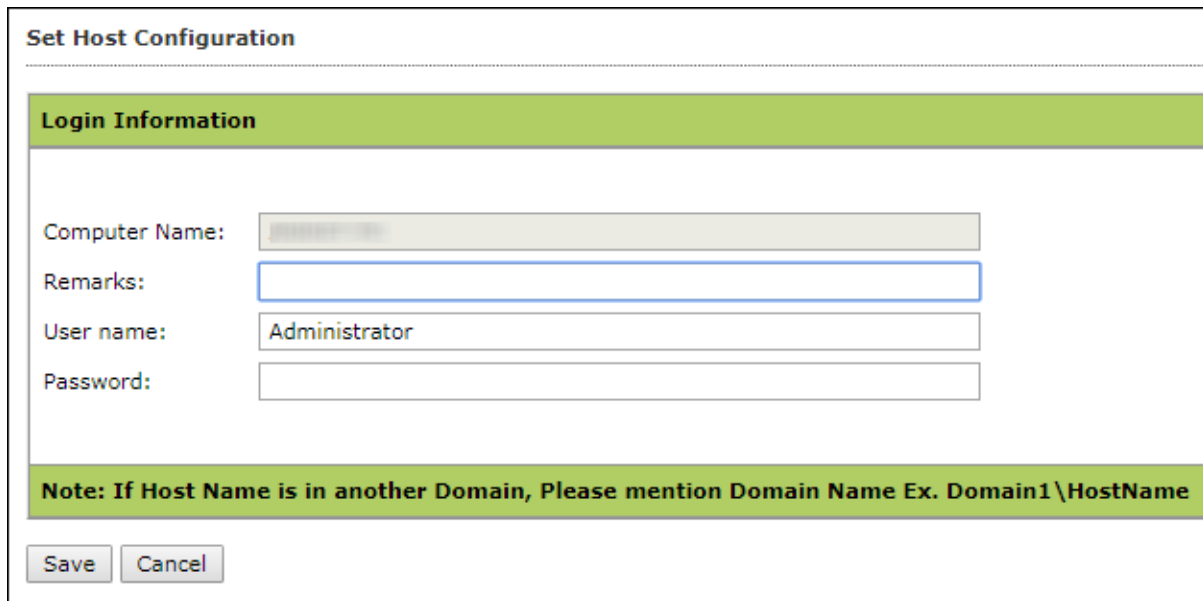
Set Host Configuration

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

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

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

Set Host Configuration window appears.



The dialog box is titled "Set Host Configuration". It features a green header bar with the title. Below the header, there is a section titled "Login Information" with a green background. This section contains four input fields: "Computer Name" (with a placeholder "localhost"), "Remarks" (empty), "User name" (with the value "Administrator"), and "Password" (empty). Below these fields, a green bar contains a note: "Note: If Host Name is in another Domain, Please mention Domain Name Ex. Domain1\HostName". At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

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

Deploy/Upgrade Client

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

Installing eScan Client on a Client Computer

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

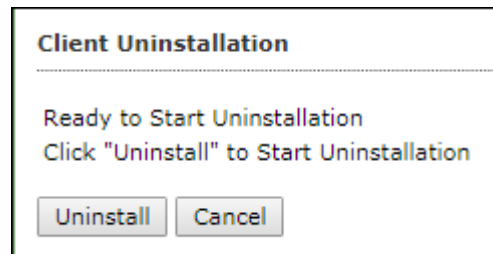
3. Select **Install eScan** option.
By Default eScan is installed at the following Path on a Client computer.
C:\Program Files\eScan (default path for 32-bit computer)
OR
C:\Program Files (x86)\eScan (default path for 64-bit computers).
4. To define a different installation path, click **Add**. (Skip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

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

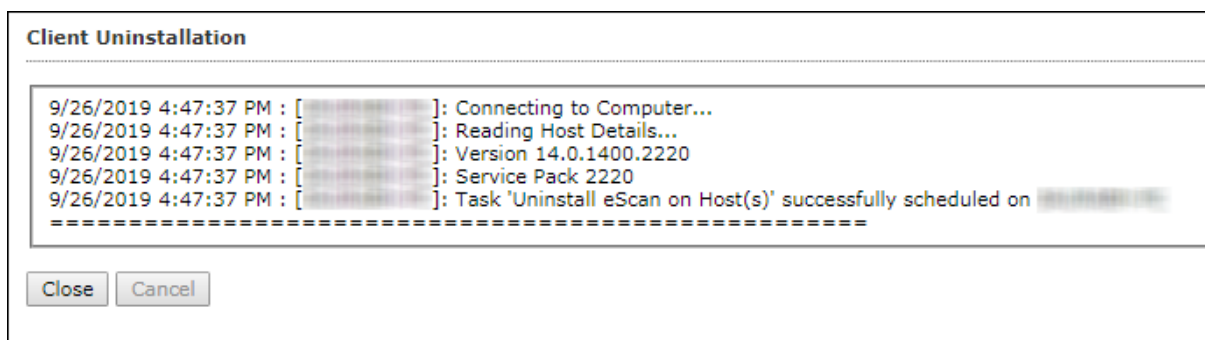
Uninstall eScan Client

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

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



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



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

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

Move to Group

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

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

Remove from Group

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

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


Connect to Client (RMM)

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

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

Add to RMM License

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

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

NOTE

After adding a client endpoint to RMM license, it is mandatory that the client endpoint should be updated with latest eScan updates.

Manage Add-On License

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

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

Manage Add-On License

☐ 2FA ☐ DLP ☐ E-Backup

☒ Add
☐ Remove

License Information

2FA
License Size : 200 License Remaining : 198
DLP
License Size : 200 License Remaining : 198
E-Backup
License Size : 200 License Remaining : 199

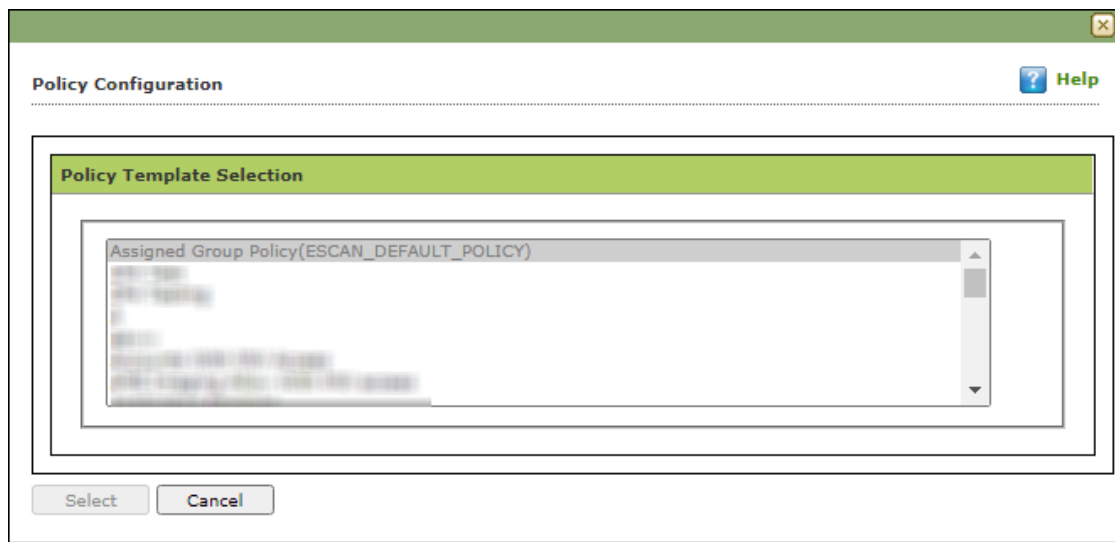
Ok Cancel

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

Assign Policy Template

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

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



5. 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:

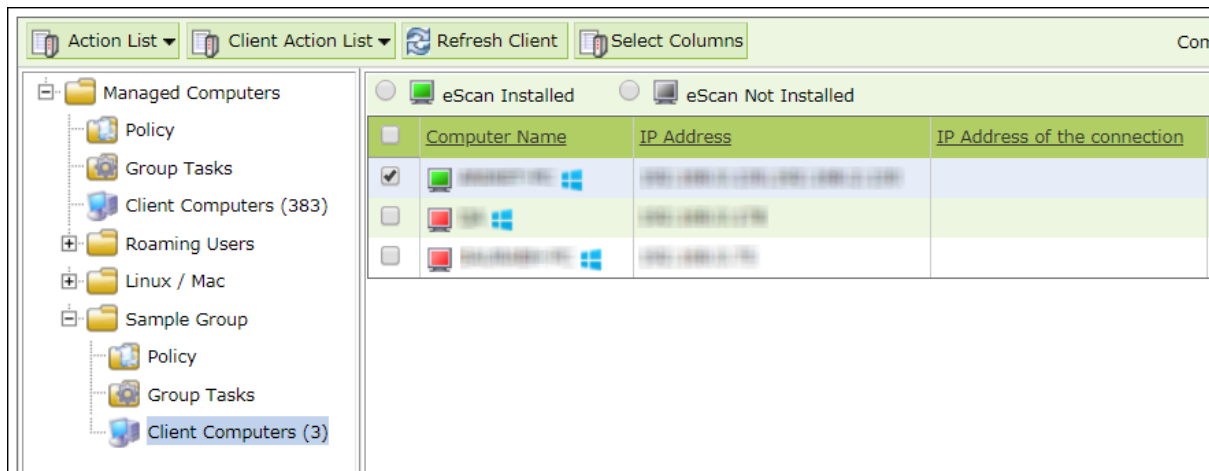
1. Go to **Managed Computers**.
2. Select the client computer which you want to assign policy template.
3. Click **Client Action List > Show Critical Events**.
This will display the list of all the critical events of the computer that can also be exported as a report.

Export

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

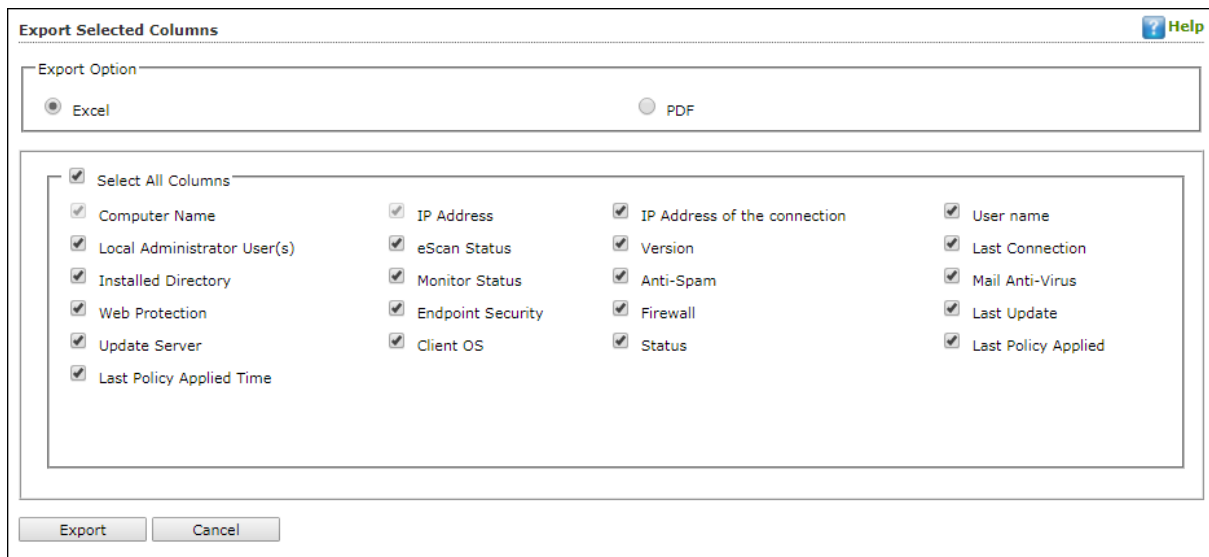
1. In the Managed Computers folder tree, select a group and then click **Client Computers**.

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



2. Select a client computer and the click **Client Action List > Export**.

Export Selected Columns window appears displaying export options and a variety of columns to be exported.



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

The report will be exported as per your preferences.

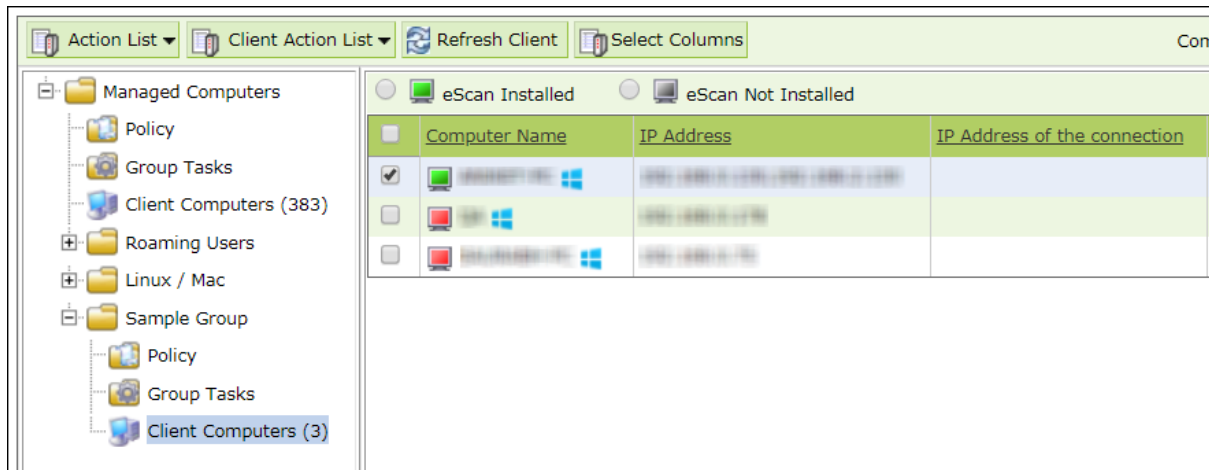
Show Installed Softwares

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

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

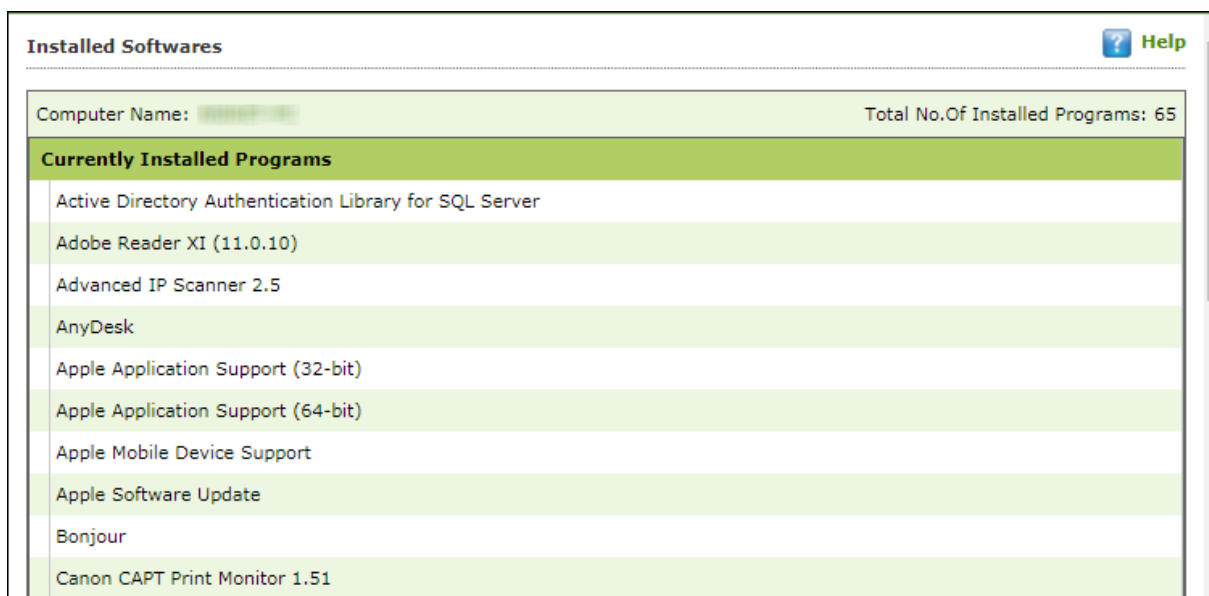
1. In the Managed Computers folder tree, select a group and then click **Client Computers**.

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



2. Select a client computer and then click **Client Action List > Show Installed Softwares**.

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



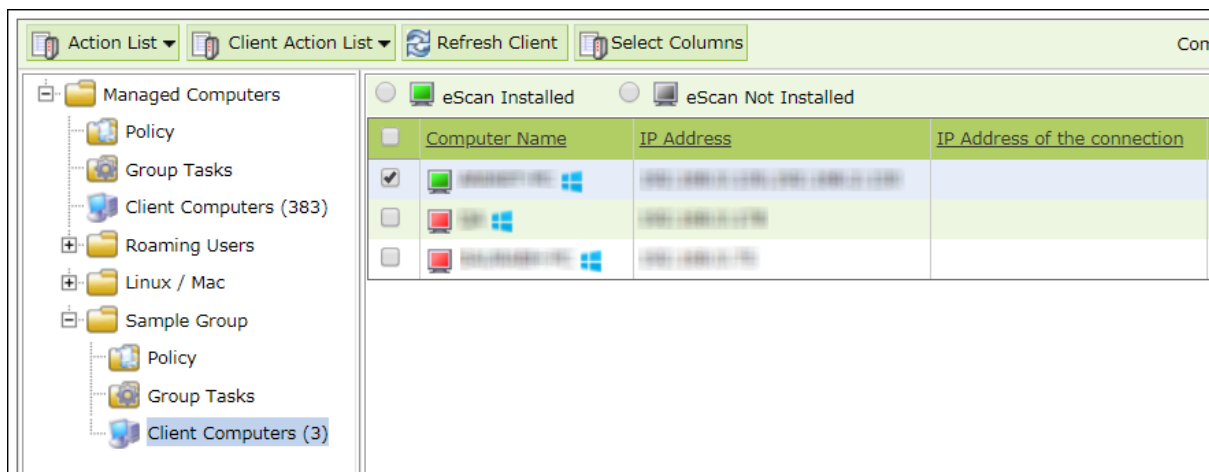
Force Download

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

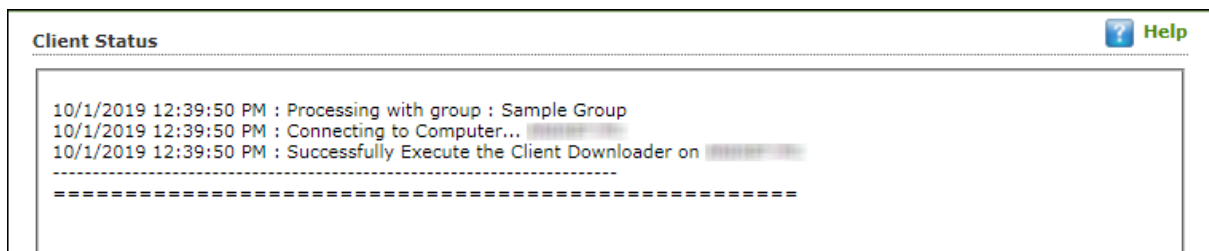
To activate this feature for computers, follow the steps given below:

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

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



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

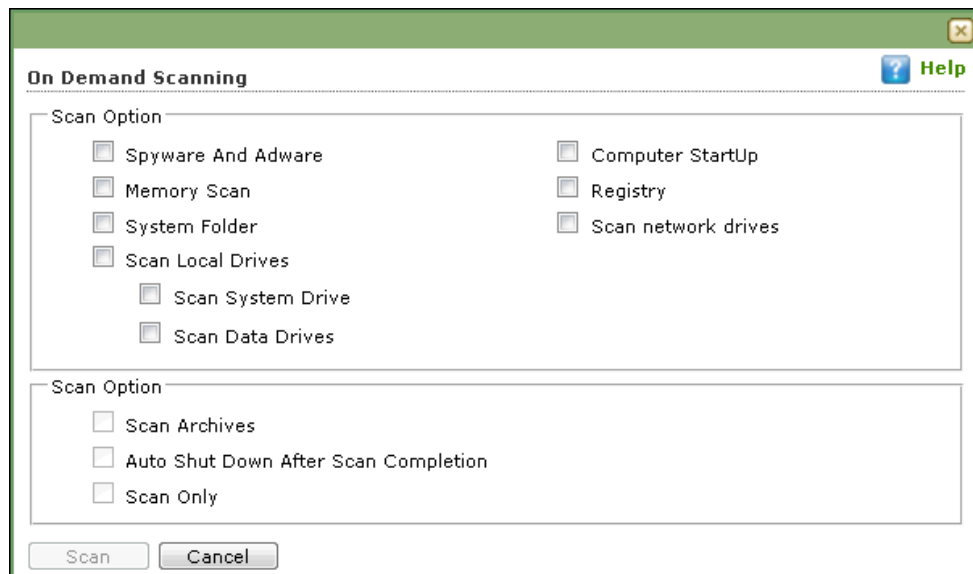


On Demand Scanning

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

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

On Demand Scanning window appears.



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

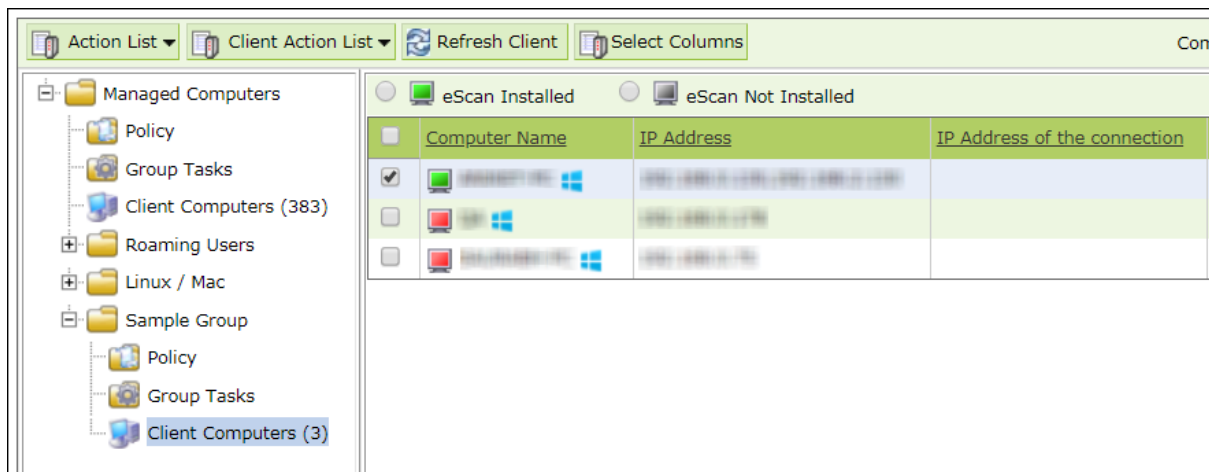
Send Message

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

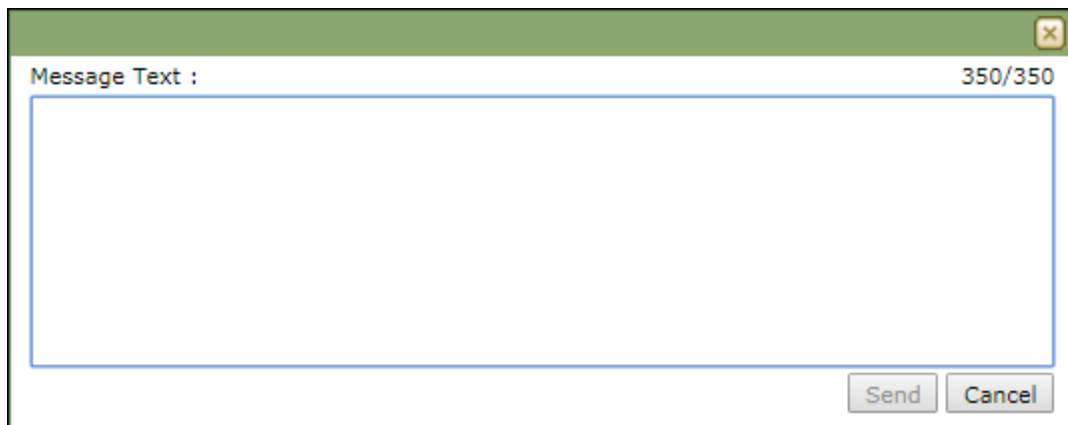
To send message to computers, follow the steps given below:

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

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



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



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

Outbreak Prevention

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

Deploying Outbreak Prevention

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

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

Limit access to shared folders

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

Deny write access to local files and folder

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

Block specific ports

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

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

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

Automatically restore the outbreak prevention after hour(s)

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

Outbreak Prevention Notification

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

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

Restore Outbreak Prevention

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

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

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

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

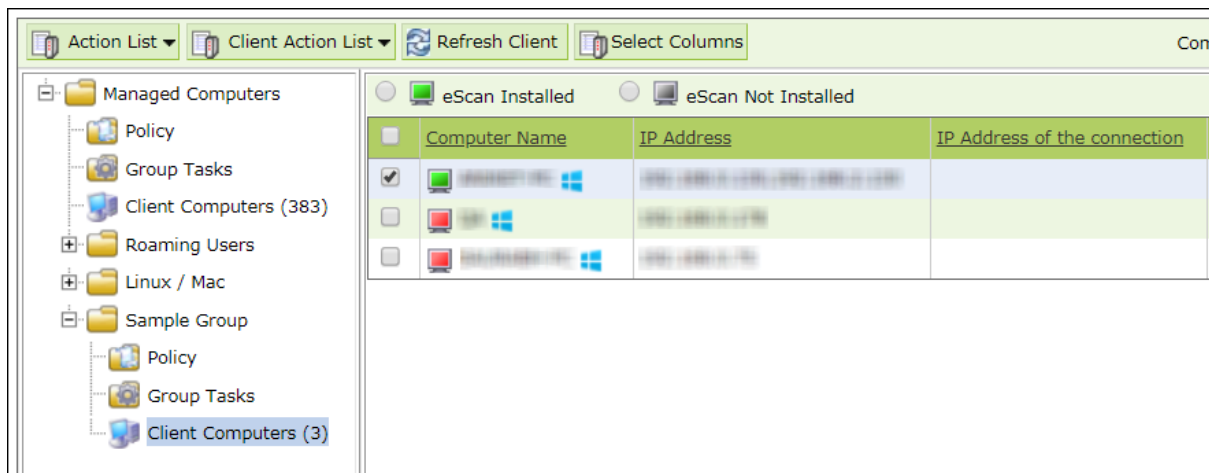
Delete All Quarantine Files

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

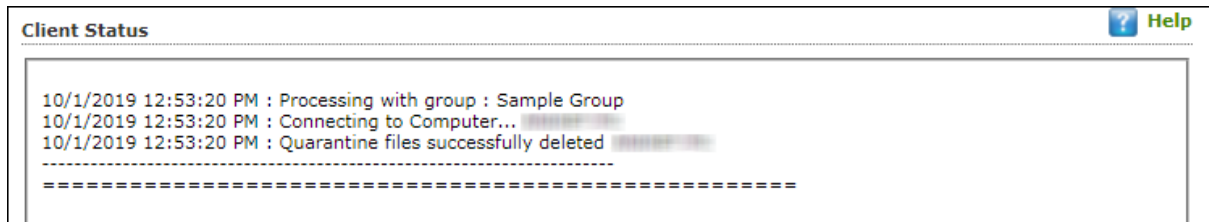
To delete all quarantine files on computers, follow the steps given below:

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

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



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



Create OTP

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

Generating an OTP

To generate an OTP, follow the steps given below:

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

Password generator

Generate One Time Password

Computer Name: *

Valid for: *

Select Option

☐ File Anti-Virus

☐ Web Protection

☐ EPS App Control

☐ Mail Anti-Virus & Anti-Spam

☐ Allow to Change Ip

☐ Firewall

☐ EPS USB

New Password

Password

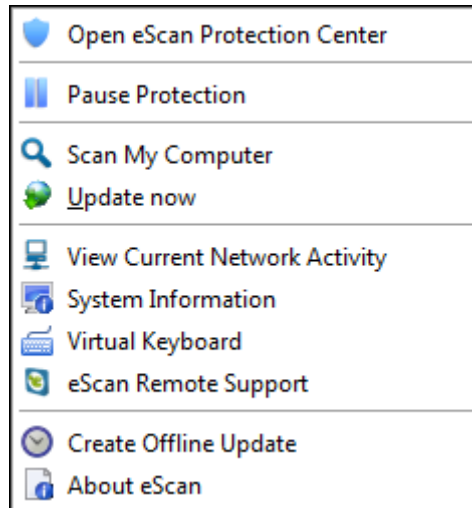
(*) Mandatory Fields

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

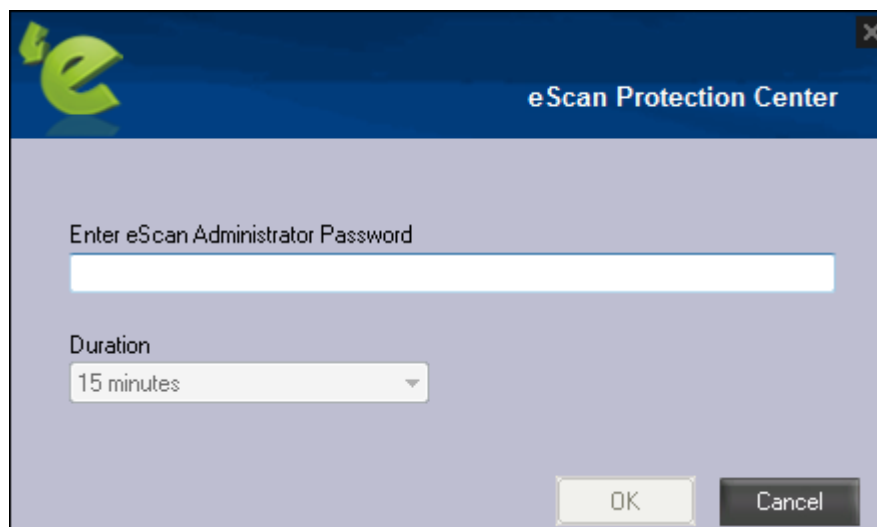
Entering an OTP

To enter an OTP, follow the steps given below:

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



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



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

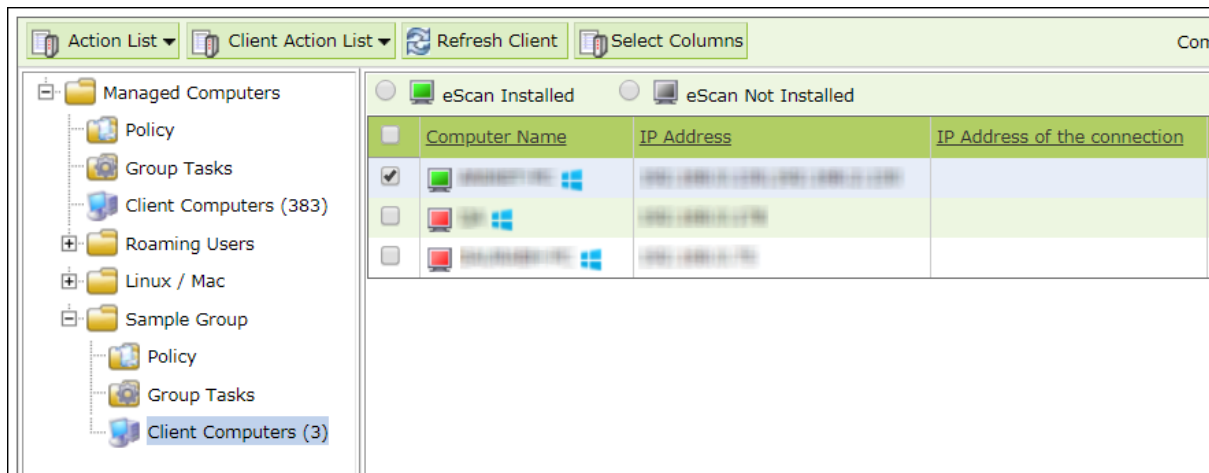
Pause Protection

The Pause Protection feature lets you pause protection for computers.

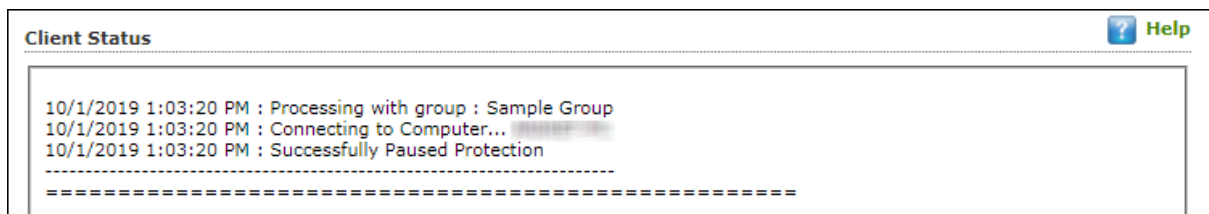
To pause the protection for computers, follow the steps given below:

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

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



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



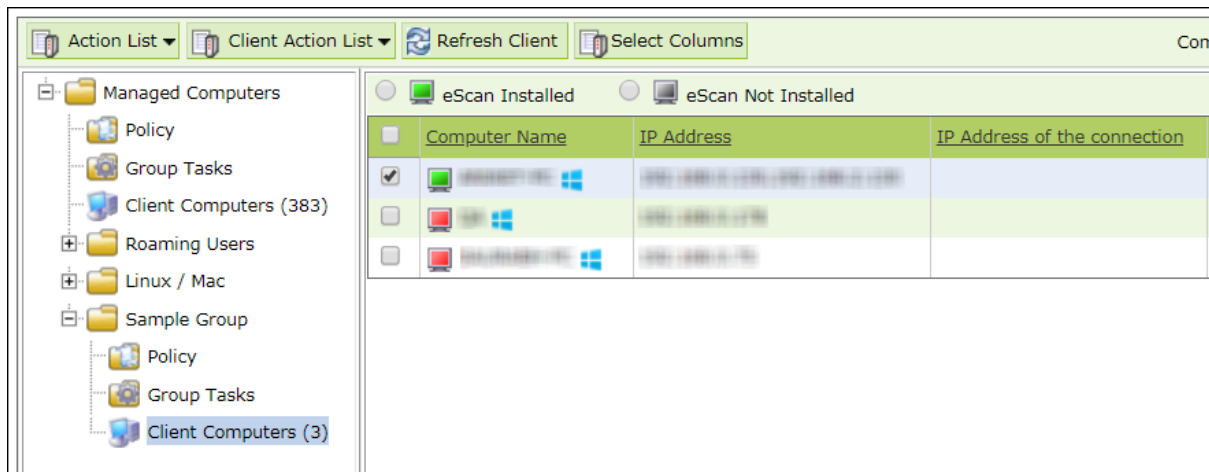
Resume Protection

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

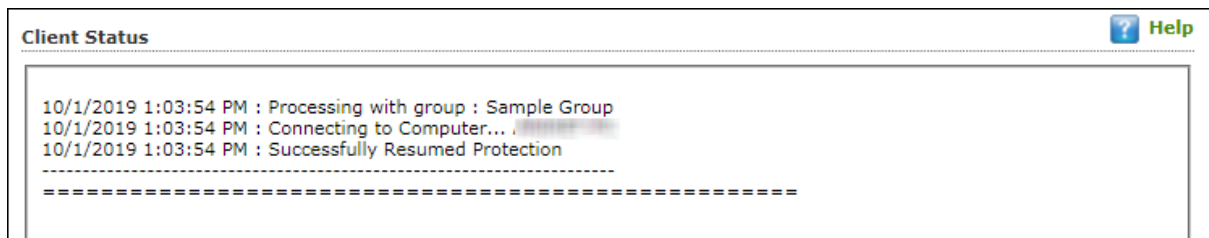
To resume protection for computers, follow the steps given below:

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

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



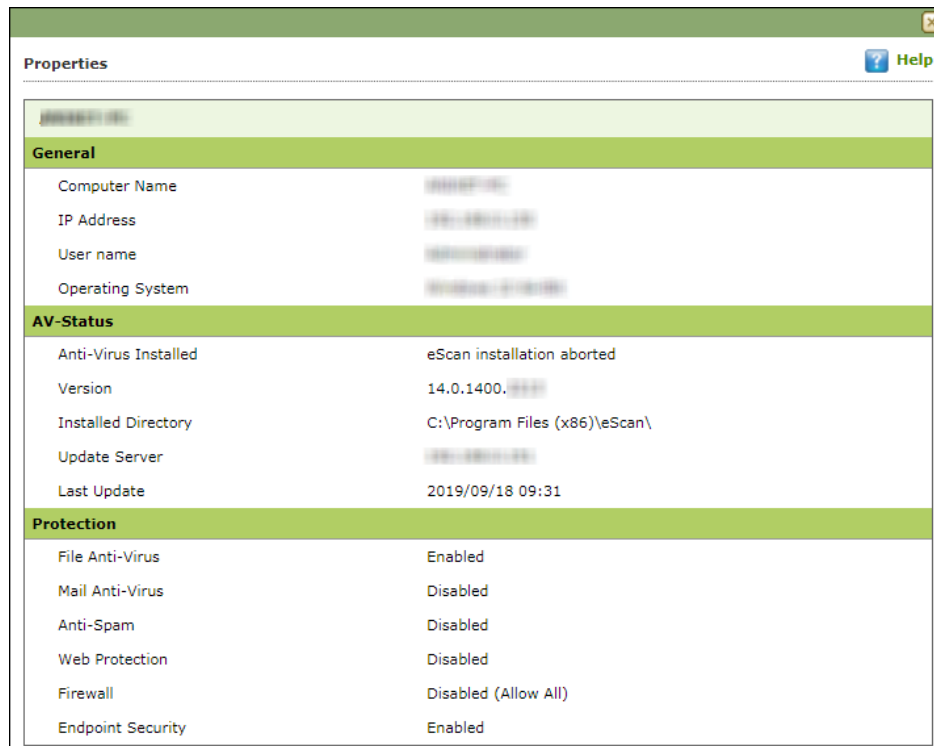
2. Select client computers and then click **Client Action List > Resume Protection**. Client Status window appears displaying the progress.



Properties of Selected Computer

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

1. Select a computer.
2. Click **Client Action List > Properties**. Properties window appears displaying details.



The screenshot shows a 'Properties' window with a green header bar and a 'Help' button. The window is divided into three main sections: General, AV-Status, and Protection. The General section lists Computer Name, IP Address, User name, and Operating System. The AV-Status section lists Anti-Virus Installed, Version, Installed Directory, Update Server, and Last Update. The Protection section lists File Anti-Virus, Mail Anti-Virus, Anti-Spam, Web Protection, Firewall, and Endpoint Security.

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

AV-Status	
Anti-Virus Installed	eScan installation aborted
Version	14.0.1400.1000
Installed Directory	C:\Program Files (x86)\eScan\
Update Server	192.168.1.100
Last Update	2019/09/18 09:31

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

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

Policy Template

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

Managing Policies

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

Defining Policies Windows computers

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

File Anti-virus

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

Mail Anti-Virus

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

Anti-Spam

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

Firewall

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

Privacy Control

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

Web Protection

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

Endpoint Security

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

Defining Policies Mac or Linux computers

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

File Anti-Virus

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

Endpoint Security

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

On Demand Scanning

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

Schedule Scan

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

Schedule Update

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

Administrator Password

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

Web Protection

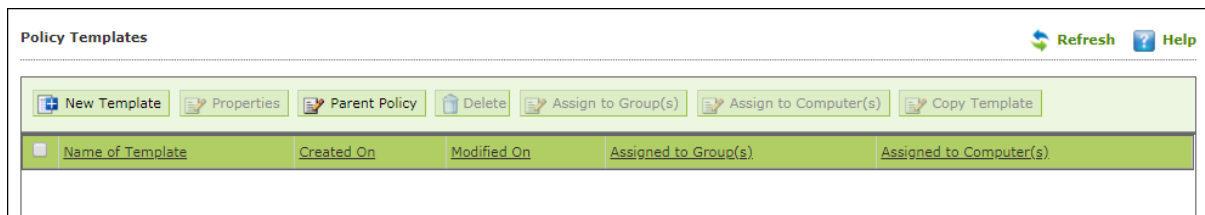
The Web Protection module for Linux feature is extremely beneficial to parents as it prevents kids from accessing websites containing harmful or restricted content. Administrators can also use this feature to prevent employees from accessing non-work-related websites during work hours.

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

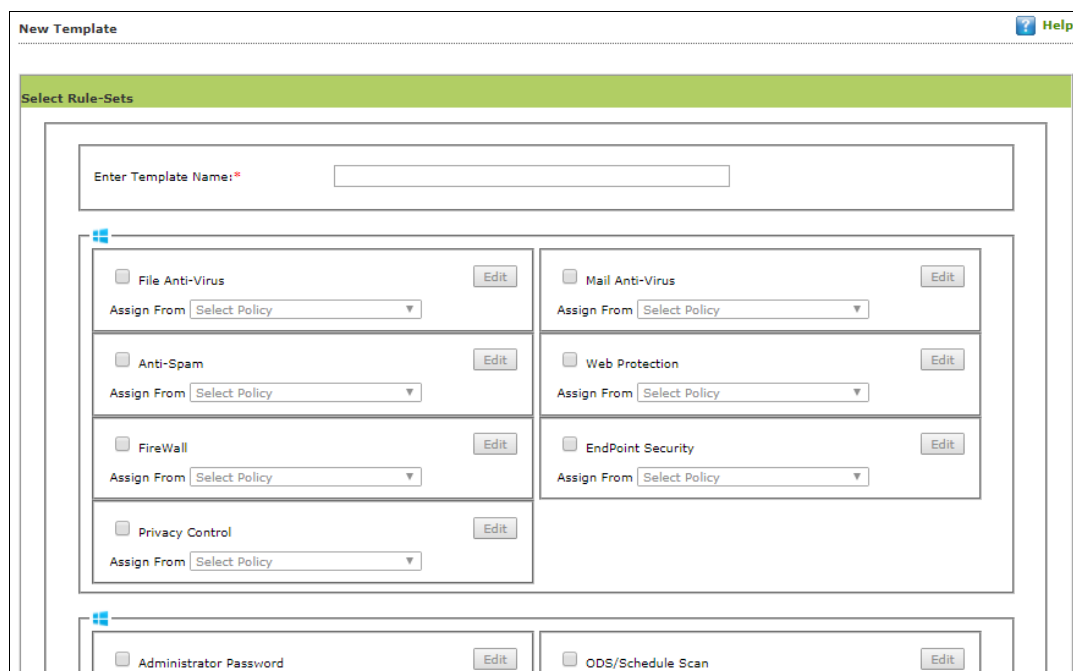
Creating Policy Template for a group/specific computer

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

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



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



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

Configuring eScan Policies for Windows Computers

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

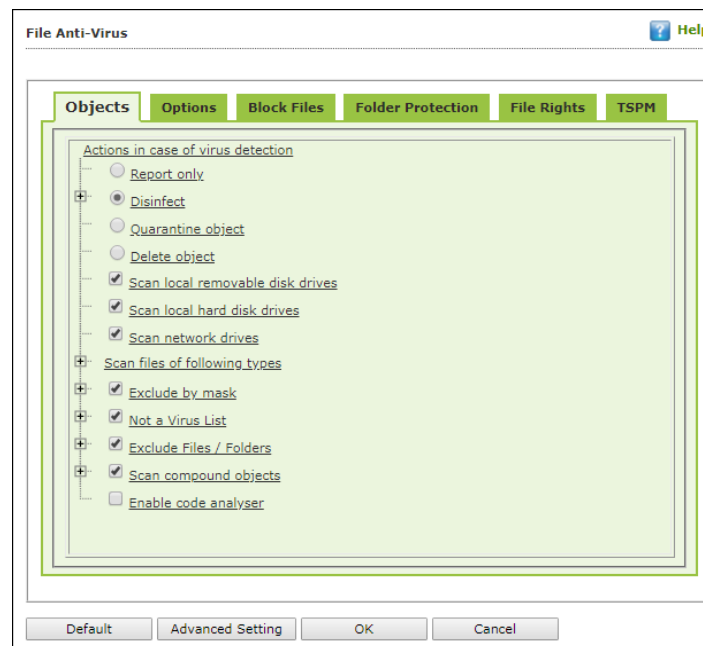
File Anti-Virus

Editing File Anti-Virus module displays following tabs:

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

Objects

The Objects tab lets you configure following options.



Actions in case of virus detection

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

Report Only

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

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

Out of these, the **Disinfect** option is selected by default. By default, the quarantined files are saved in **C:\Program Files\eScan\Infected** folder. You can select the **Make backup file**

before disinfection option if you would like to make a backup of the files before they are disinfected.

Scan local removable disk drives [Default]

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

Scan local hard disk drives [Default]

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

Scan network drives [Default]

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

Scan files of following types

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

Exclude by mask [Default]

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

Not a virus list [Default]

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

Exclude Files/Folders [Default]

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

Scan compound objects [Default]

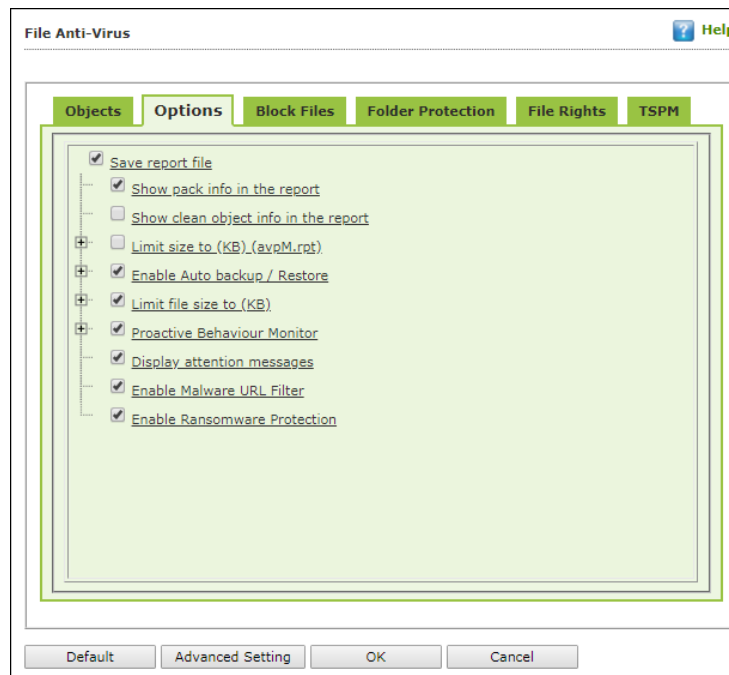
Select this check box if you want eScan to scan archives and packed files during scan operations. By default, **Packed** is selected.

Enable code Analyzer

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

Options

The Options tab lets you configure following options:



Save report file [Default]

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

Show pack info in the report [Default]

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

Show clean object info in the report

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

Limit size to (Kb) (avpM.rpt)

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

Enable Auto backup/Restore [Default]

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

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

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

Minimum disk space (MB) [Default]

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

Limit file size to (KB) [Default]

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

Proactive Behavior Monitor

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

Whitelist Option

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

Use sound effects for the following events

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

Display attention messages [Default]

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

Enable Malware URL Filter

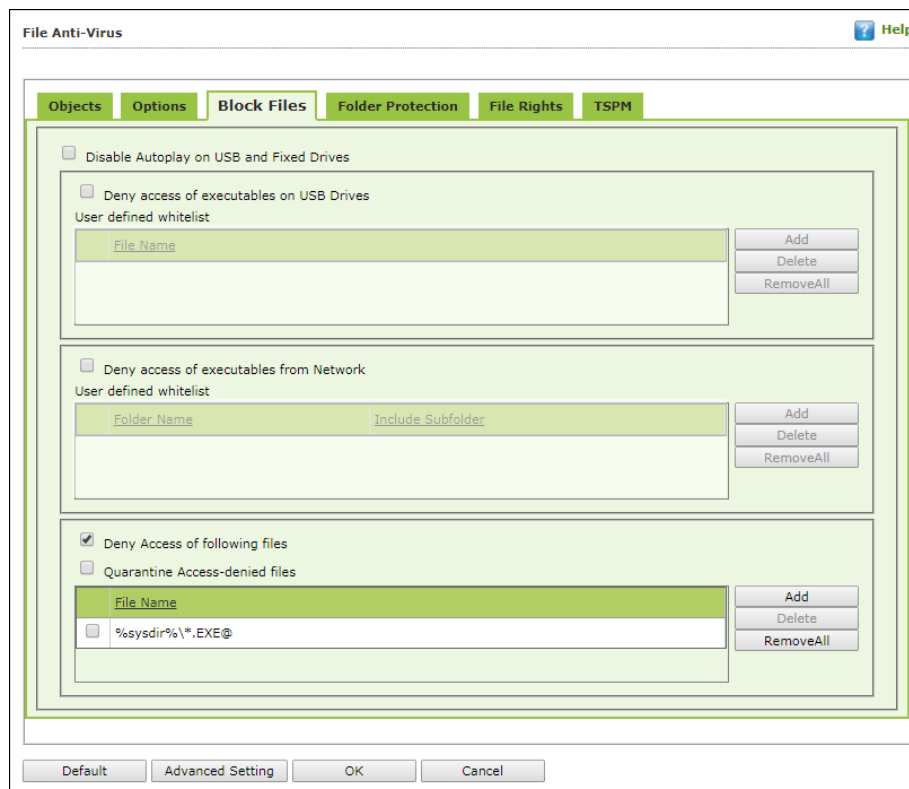
This option lets you enable a Malware URL filter where eScan blocks all URLs that are suspected to be malwares. You can exclude specific websites by whitelisting them from the eScan pop up displayed when you try to access the site.

Enable Ransomware Protection

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

Block Files

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



You can configure the following settings:

Disable AutoPlay on USB and Fixed Drives [Default]

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

Deny access of executables on USB Drives

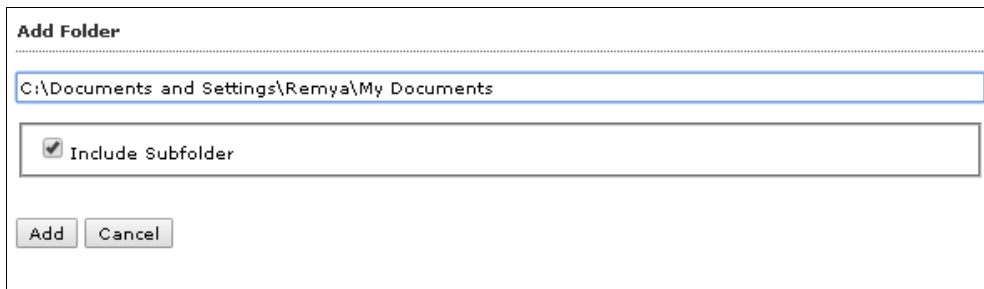
Select this check box if you want eScan to prevent executables stored on USB drives from being accessed.

Deny access of executable from Network

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

User defined whitelist

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



The image shows a dialog box titled "Add Folder". It contains a text input field with the path "C:\Documents and Settings\Remya\My Documents". Below the text field is a checkbox labeled "Include Subfolder" which is checked. At the bottom of the dialog are two buttons: "Add" and "Cancel".

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

Deny Access of following files [Default]

Select this check box if you want eScan to prevent the files in the list from running on the computers.

Quarantine Access-denied files

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

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

Folder Protection

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

File Anti-Virus

Help

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

☒ Protect files in following folders from modification and deletion

Folder Name	Include Subfolder

Add
Delete
RemoveAll

Default Advanced Setting OK Cancel

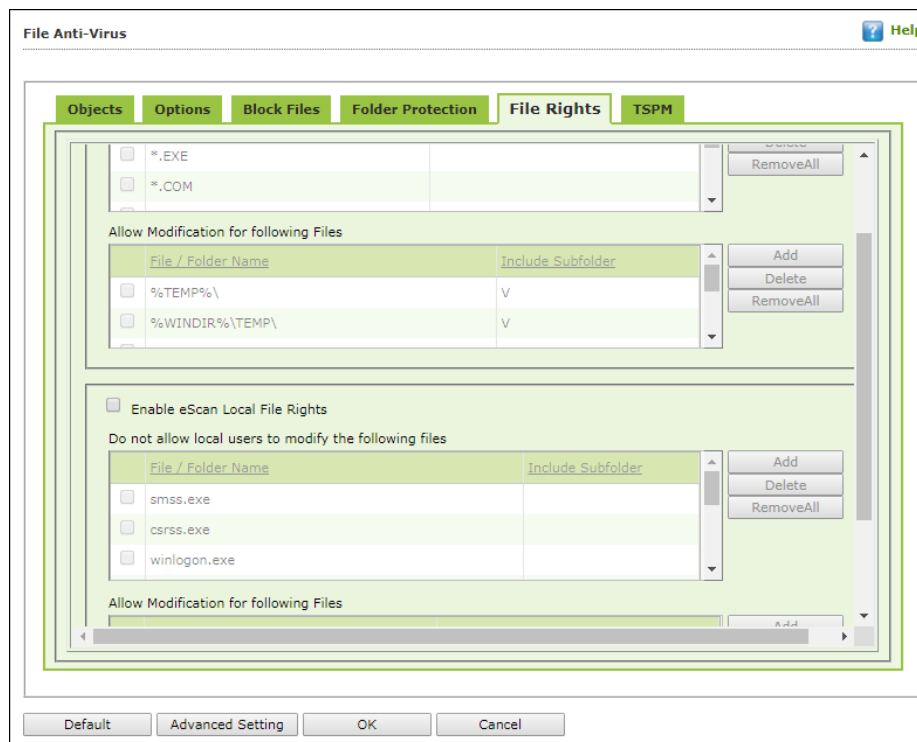
Protect files in following folders from modification and deletion [Default]

This option is selected by default.

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

File Rights

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



Enable eScan Remote File Rights

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

Do not allow remote users to modify the following local files

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

Allow modification for following files

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

Enable eScan local file rights

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

Do not allow local users to modify the following files

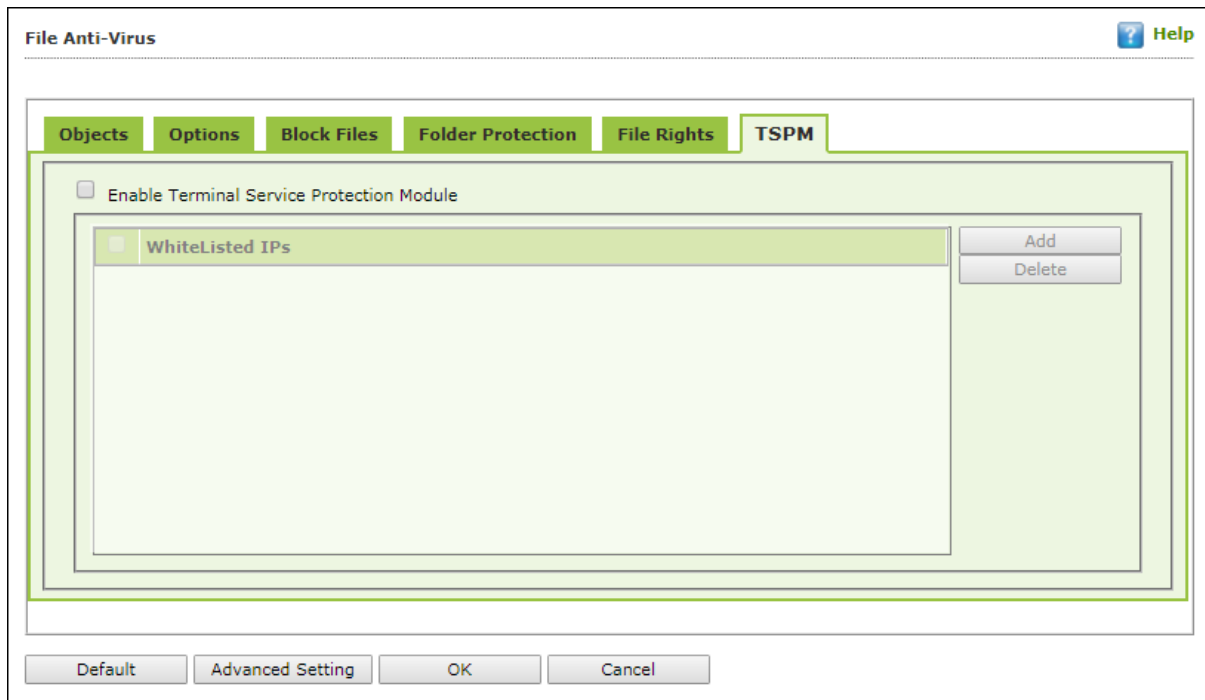
The files/folders added to this list cannot be modified by the local users.

Allow modification for files

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

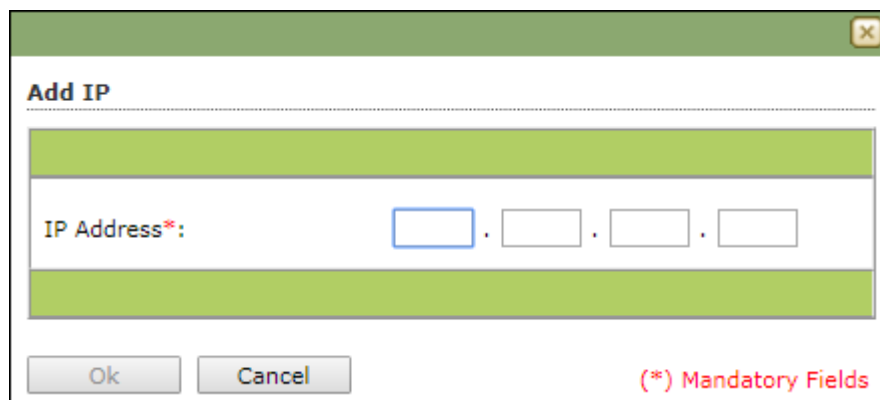
TSPM

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



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

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



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

Advanced Settings

Clicking Advanced Settings lets you configure advanced settings for console.

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

Ok

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

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

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

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

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

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

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

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

Clear Quarantine folder after Days specified

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

Clear Quarantine Folder after Size Limit specified in MB

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

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

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

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

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

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

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

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

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

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

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

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

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

Define Virus Alert Time (in seconds)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Enable Cloud (1 = Enable/0 = Disable)

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

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

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

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

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

Whitelisted AutoConfigURL

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

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

Selecting this option disables Add-ons and Extension blocking.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Selecting this option lets you disable Copy/Paste actions.

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

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

Block all RDP Session except Whitelisted under TSPM

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

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

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

PowerShell Exclusion list

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

Allow Uninstallers (1 = Enable/0 = Disable)

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

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

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

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

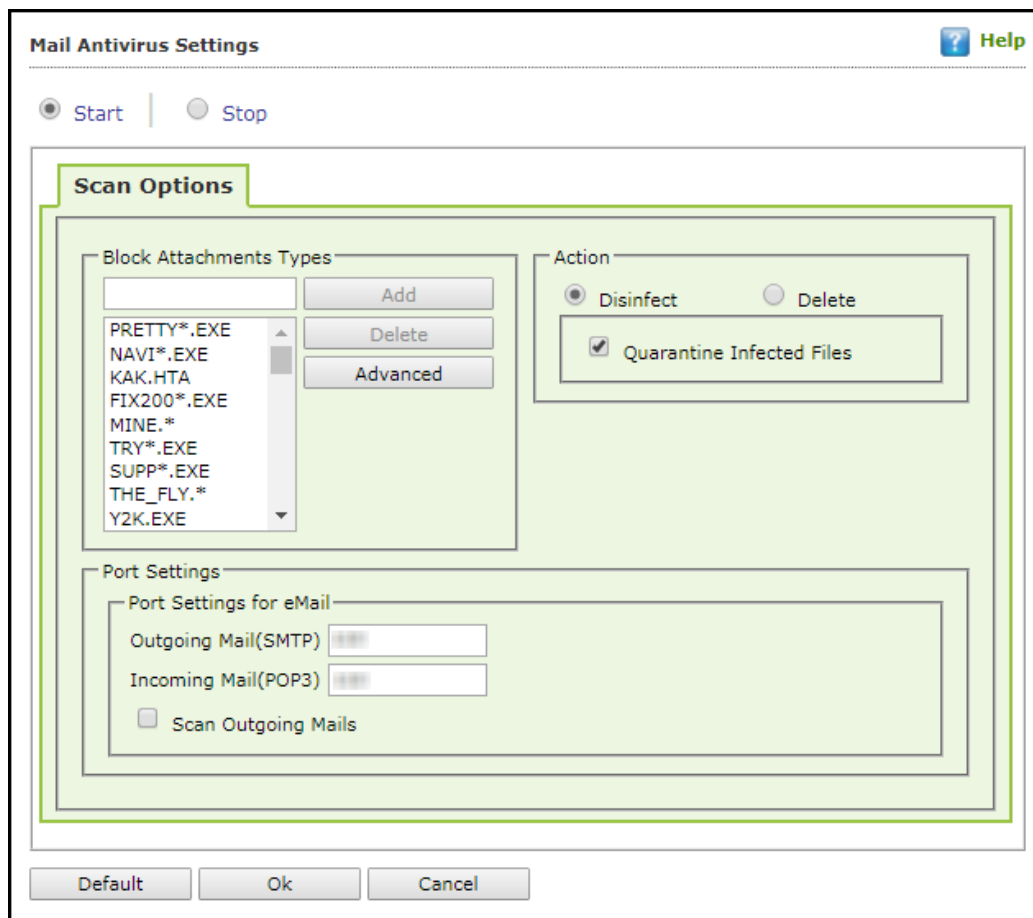
Selecting this option lets you enable/disable restrict environment settings.

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

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

Mail Antivirus

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



Scan Options

This tab lets you select the emails to be scanned and action that should be performed when a security threat is encountered during a scan operation. This tab lets you configure following settings:

Block Attachments Types

This section provides you with a predefined list of file types that are often used by virus writers to embed viruses. Any email attachment having an extension included in this list will be blocked or deleted by eScan at the gateway level. You can add file extensions to this list as per your requirements. As a best practice, you should avoid deleting the file

extensions that are present in the **Block Attachments Types** list by default. You can also configure advanced settings required to scan emails for malicious code.

Action

This section lets you configure the actions to be performed on infected emails. These operations are as follows:

Disinfect [Default]

Select this option if you want Mail Anti-Virus to disinfect infected emails or attachments.

Delete

Select this option if you want Mail Anti-Virus to delete infected emails or attachments.

Quarantine Infected Files [Default]

Select this option if you want Mail Anti-Virus to quarantine infected emails or attachments. The default path for storing quarantined emails or attachments is – C:\Program Files\eScan\QUARANT.

However, you can specify a different path for storing quarantined files, if required.

Port Settings for email

You can also specify the ports for incoming and outgoing emails so that eScan can scan the emails sent or received through those ports.

Outgoing Mail (SMTP) [Default: 25]

You need to specify a port number for SMTP.

Incoming Mail (POP3) [Default: 110]

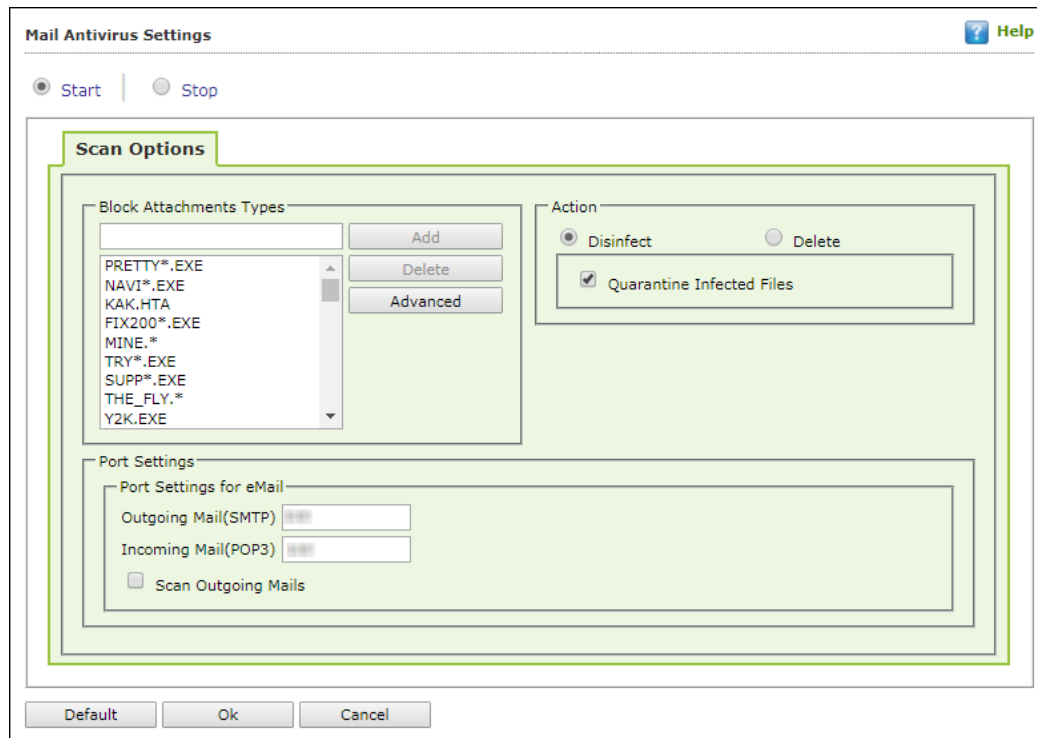
You need to specify a port number for POP3.

Scan Outgoing Mails

Select this option if you want Mail Anti-Virus to scan outgoing emails as well.

Advanced

Clicking **Advanced** displays Advanced Scan Options dialog box. This dialog box lets you configure the following advanced scanning options:



Delete all Attachment in email if disinfection is not possible

Select this option to delete all the email attachments that cannot be cleaned.

Delete entire email if disinfection is not possible [Default]

Select this option to delete the entire email if any attachment cannot be cleaned.

Delete entire email if any virus is found

Select this option to delete the entire email if any virus is found in the email or the attachment is infected.

Quarantine blocked Attachments [Default]

Select this option to quarantine the attachment if it bears extension blocked by eScan.

Delete entire email if any blocked attachment is found [Default]

Select this option to delete an email if it contains an attachment with an extension type blocked by eScan.

Quarantine email if attachments are not scanned

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

Quarantine Attachments if they are scanned

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

Exclude Attachments (White List)

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

Anti-Spam

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

Advanced

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

Send Original Mail to User [Default]

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

Do not check content of Replied or Forwarded Mails

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

Check Content of Outgoing mails

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

Phrases

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

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

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

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

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

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

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

Action List

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

Spam Filter Configuration

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

Check for Mail Phishing [Default]

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

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

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

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

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

Check content of HTML mails [Default]

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

Quarantine Advertisement mails [Default]

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

Advanced

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

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

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

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

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

Enable email Header check [Default]

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

Enable X Spam Rules check [Default]

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

Enable Sender Policy Framework (SPF) check

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

Enable Spam URI Real-time Blacklist (SURBL) check

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

Enable Real-time Blackhole List (RBL) check

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

RBL Servers

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

Auto Spam Whitelist

Unlike normal RBLs, SURBL scans emails for names or URLs of spam websites in the message body. It terminates the connection if the IP of the sender is found in any of the blacklisted categories. This contains a list of valid email addresses that can bypass the

above Spam filtering options. It thus allows emails from the whitelist to be downloaded to the recipient's inbox. You can add or delete address in the list as per your requirement.

Mail Tagging Options

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

Do not change email at all

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

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

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

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

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

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

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

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

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

Web Protection

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

Web Protection Help

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

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

Status: ☒ Active ☐ Block Web Access

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

Add Delete

Site Names: playboy.com

Add Delete Save

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

Default Advanced Setting OK Cancel

You can configure the following settings.

Filtering Options

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

Status

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

Filter Categories

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

Green

It represents an allowed websites category.

Red

It represents a blocked websites category.

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

Category Name

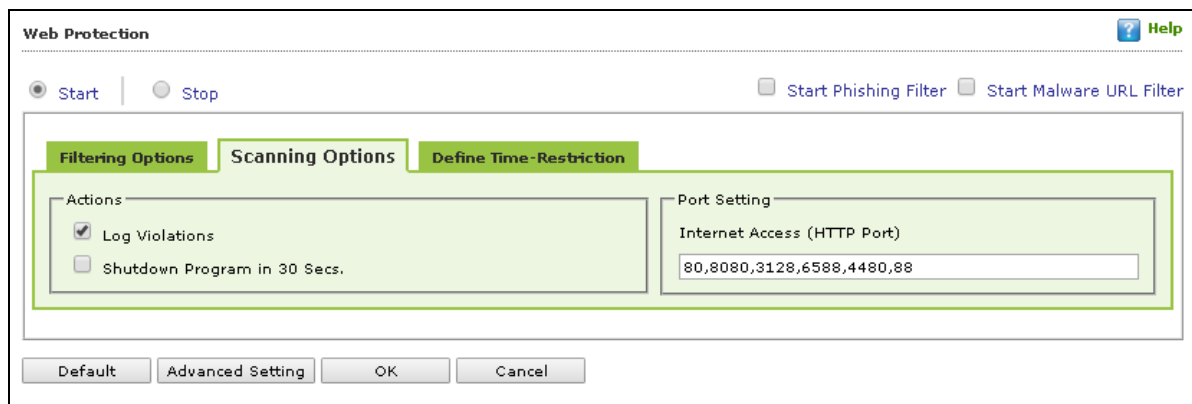
This section shows the **Words/Phrases** list. It lists the words or phrases present in the selected category. In addition, the section displays the **Site Names** list, which lists the websites belonging to the selected category. You can also add or delete filter categories depending on your requirement.

Filter Options

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

Scanning Options

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



Actions

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

Log Violations [Default]

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

Shutdown Program in 30 Secs

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

Port Setting

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

Internet Access (HTTP Port)

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

Define Time Restriction

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

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.

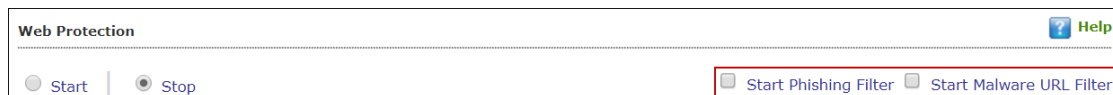
Block Web Access

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 check boxes.



Advanced Settings

Clicking **Advanced** displays Advanced Settings.

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

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

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

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

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

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

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

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

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

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

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

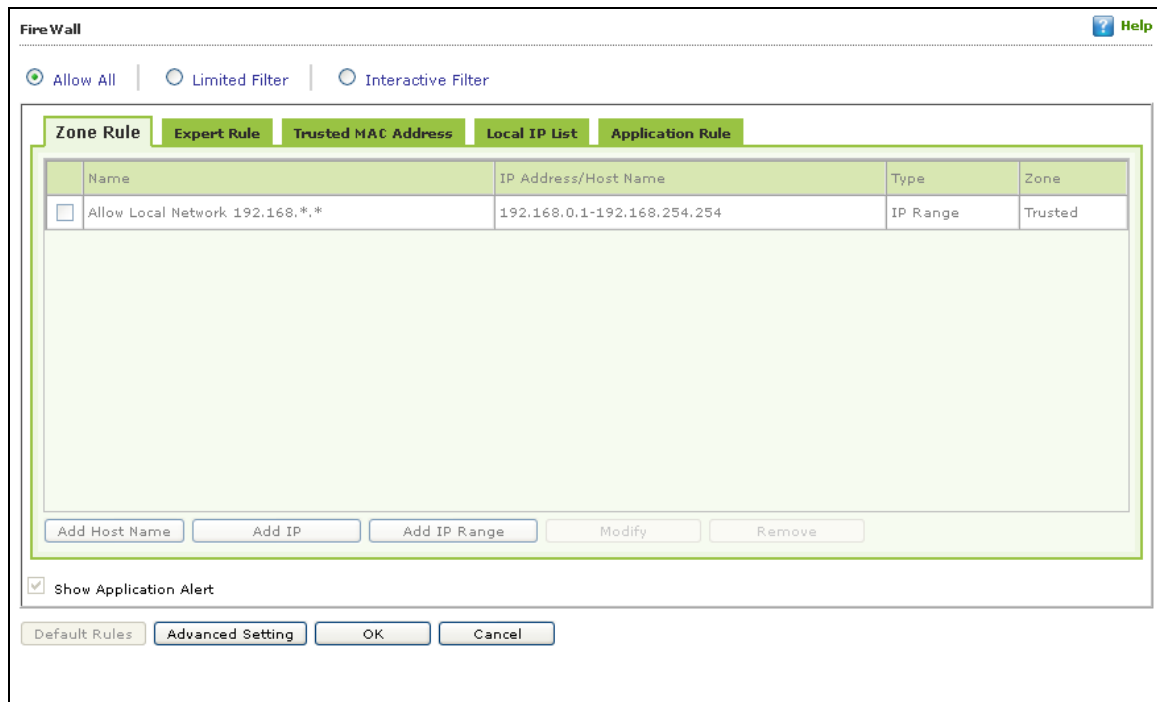
Select this option to force enable/disable web protection using filter driver.

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

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

Firewall

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



The Firewall feature of eScan protects your data when you:

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

By default, the firewall operates in the **Allow All** mode. However, you can customize the firewall by using options like **Limited Filter** for filtering only incoming traffic and **Interactive Filter** to monitor incoming and outgoing traffic. The eScan Firewall also lets you specify different set of rules for allowing or blocking incoming or outgoing traffic.

These rules include Zone Rules, Expert Rules, Trusted Media Access Control (MAC) Address, and Local IP list. This page provides you with options for configuring the module. You can configure the following settings to be deployed to the eScan client systems.

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

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

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

Following tabs are available:

Zone Rule

Expert Rule

Trusted MAC Address

Local IP List

Application Rule

Zone Rule

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

Buttons (to configure a zone rule)

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

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

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

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

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

Expert Rule

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

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

Buttons (to configure an Expert Rule)

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

The screenshot shows the 'Add Firewall Rule' window. The 'General' tab is active, showing the following configuration:

- Rule Name:** Rule1
- Rule Action:** Permit Packet (selected), Deny Packet
- Protocol:** TCP and UDP
- Apply Rule on Interface:** Any Interface

Buttons at the bottom: OK, Cancel.

General tab

In this section, specify the Rule settings:

Rule Name – Provide a name to the Rule.

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

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

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

Source tab

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

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

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

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

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

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

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

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

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

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

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

Destination tab

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

Destination IP Address –

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

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

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

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

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

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

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

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

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

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

General Source Destination **Advanced**

☐ Enable Advanced ICMP Processing

ICMP Type

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

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

☐ Log information when this rule applies

OK Cancel

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

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

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

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

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

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

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

Trusted MAC Address

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

Buttons (to configure the Trusted MAC Address)

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

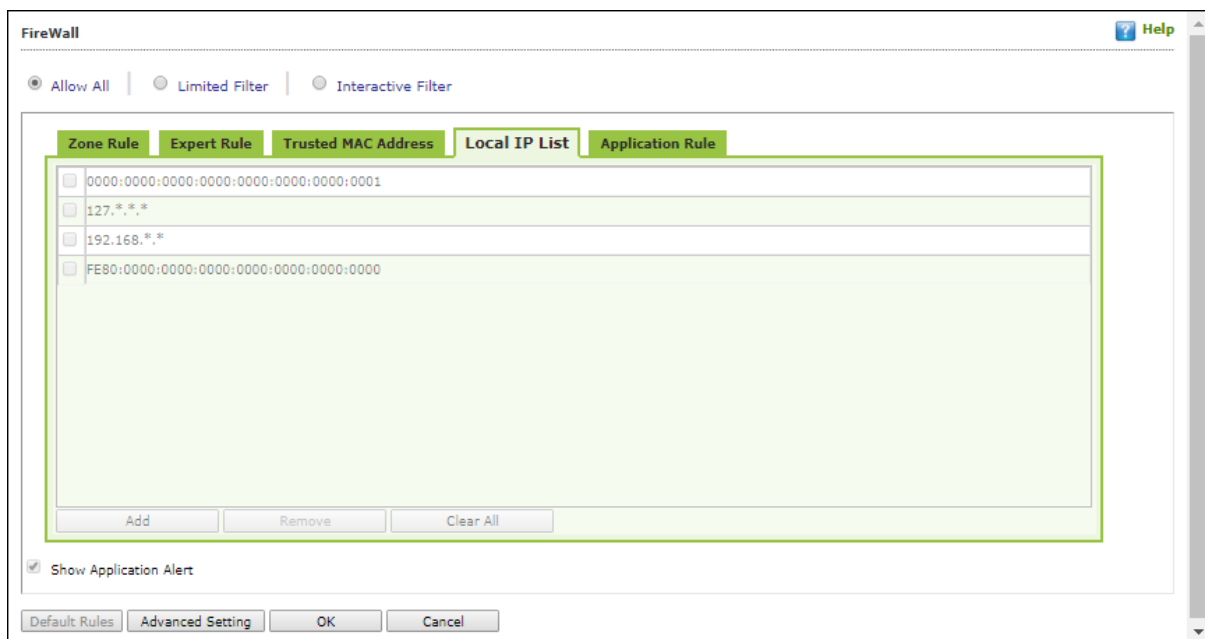
Edit – To modify/change the MAC Address, click **Edit**.

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

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

Local IP List

This section contains a list of Local IP addresses.



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

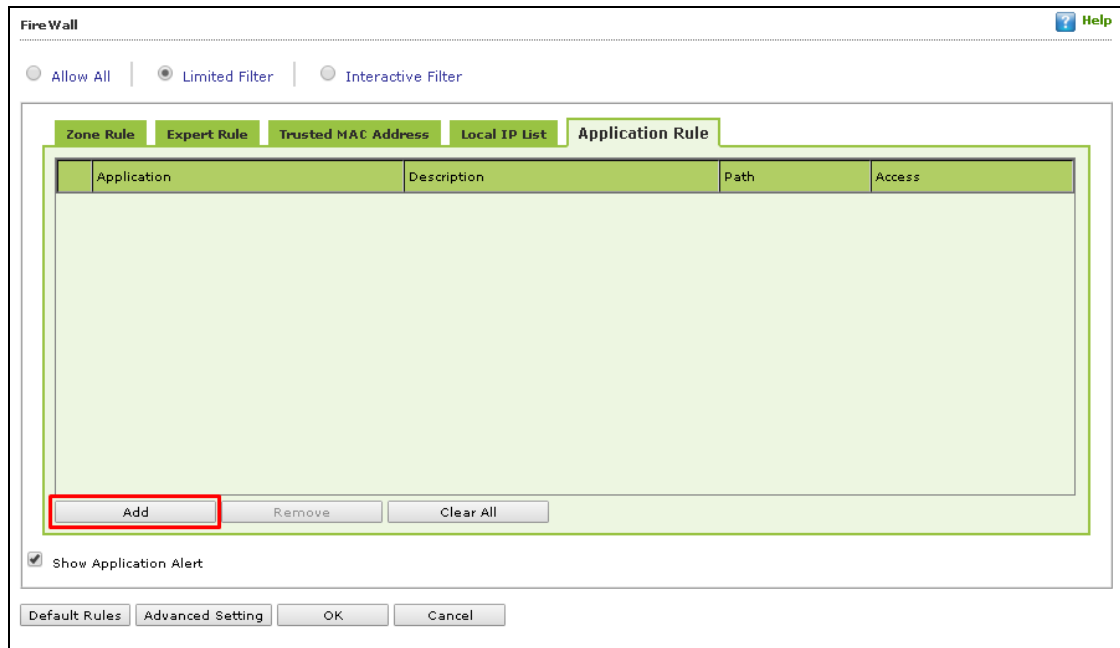
Remove – To remove a local IP address, click **Remove**.

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

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

Application Rule

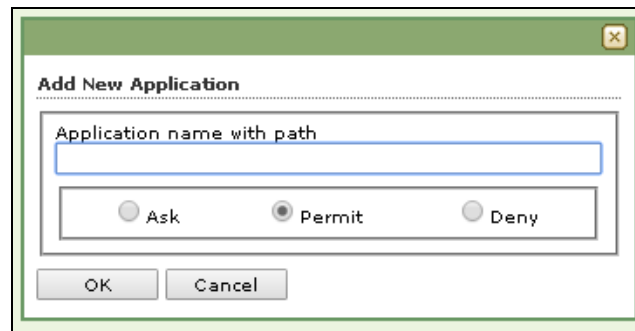
In this section you can define the permissions for different application. The application can be set to Ask, Permit or Deny mode.



Defining permission for an application

To define permission for an application,

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



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

The permission for the application will be defined.

Removing permission of an application

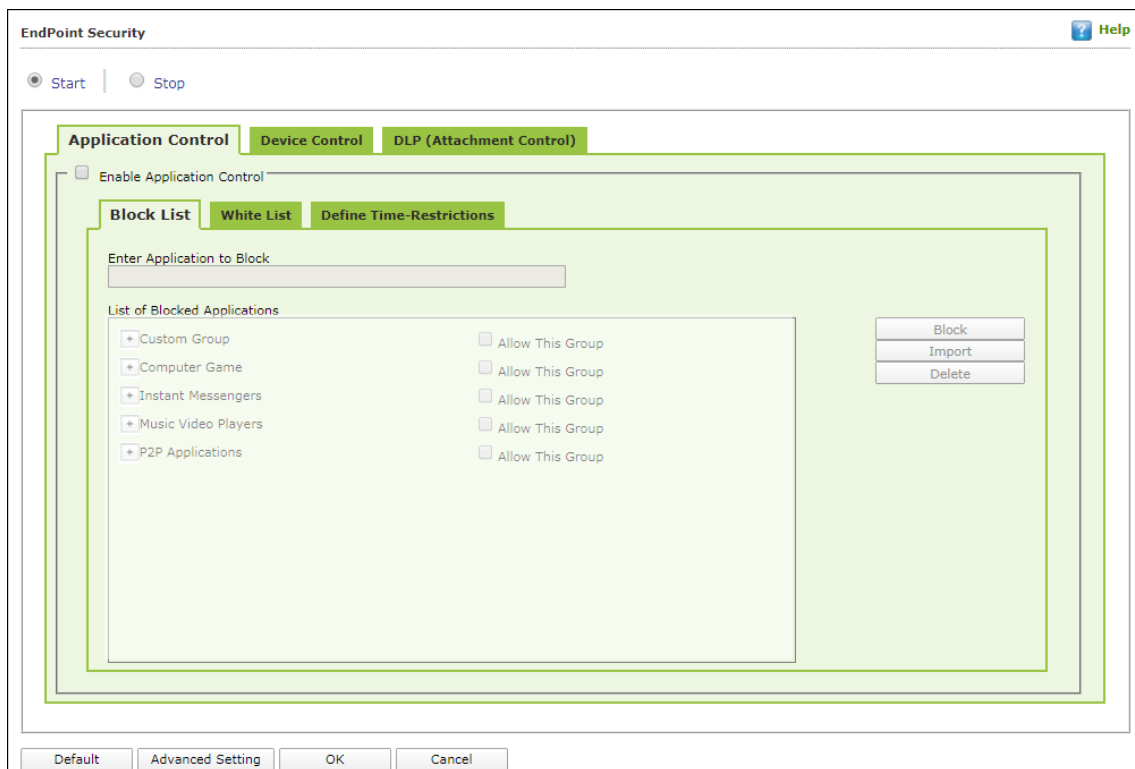
Select an application and then click **Remove**. The application will no longer have the permission.

Other Buttons

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

Endpoint Security

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



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

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

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

Application Control

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

Enable Application Control

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

Block List

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

List of Blocked Applications

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

White List

Enable White Listing

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

Enter Application to whitelist

Enter the name of the application to be whitelisted.

White Listed Applications

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

Define Time Restrictions

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

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

Datewise Restrictions

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

Device Control

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

EndPoint Security

Help

Start

Stop

Application Control

Device Control

DLP (Attachment Control)

☒ Enable Device Control

USB Settings

☐ Block USB Ports

☐ Ask for Password

☒ Use eScan Administrator Password

☐ Use Other Password

☒ Do Virus Scan

☒ Allow user to cancel scan

☐ Read Only - USB

☒ Disable AutoPlay

☐ Record Files Copied To USB / CD

☐ Record Files Copied To Local

☐ Record Files Copied To Network

☒ Ignore System Drive

Whitelist

☐ Scan Whitelisted USB Devices

Serial No.	Device Name	Description
------------	-------------	-------------

Add

Import

Edit

Delete

RemoveAll

Print

☐ Disable Web Cam

☐ Disable Bluetooth

☐ Disable SD Cards

CD / DVD Settings

☐ Block CD / DVD

☐ Read Only - CD / DVD

Default

Advanced Setting

OK

Cancel

You can configure the following settings:

Enable Device Control [Default]

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

USB Settings

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

Block USB Ports

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

Ask for Password

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

Use eScan Administrator

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

Use Other Password

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

Do Virus Scan [Default]

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

Allow user to cancel scan

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

Disable AutoPlay [Default]

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

Read Only USB

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

Record Files Copied To USB

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

Record Files Copied To Network

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

Record Files Copied To Local

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

Ignore System Drive

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

Whitelist

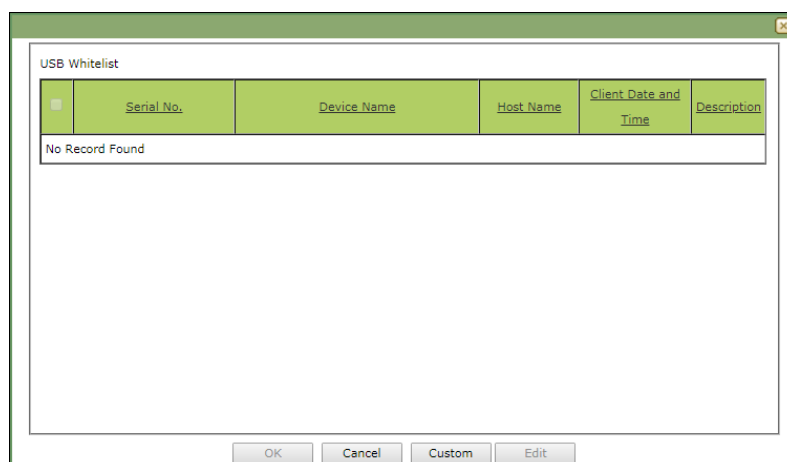
eScan provides a greater level of endpoint security by prompting you for a password whenever you connect a USB drive. To disable password protection for a specific device, you can add it along with its serial number to the whitelist. The next time you connect the device it will not ask for a password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

Scan Whitelisted USB Devices

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

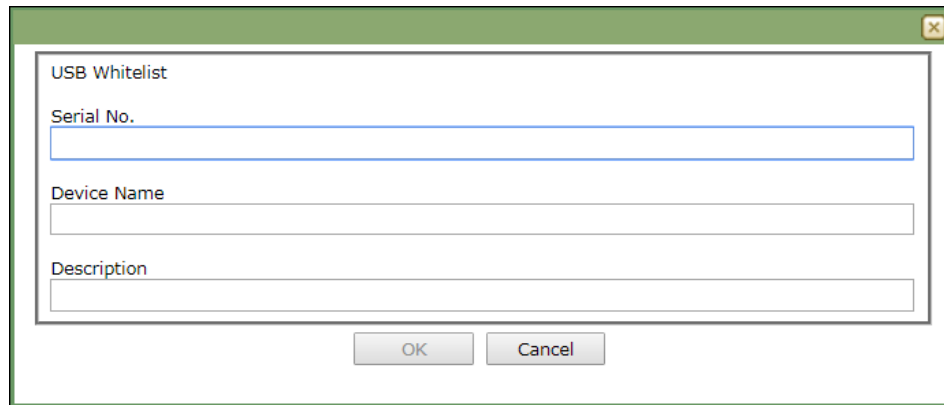
Add

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



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

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



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: SDFS677GFQW8N6CN8CBN7CXVB, USB Drive 2.5, Whitelist by
xyzDFRGHRS54456HGDF347OMCNAK, Flash Drive 2.2

Disable Web Cam: Select this option to disable Webcams.

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

Disable Bluetooth: Select this option to disable Bluetooth.

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

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

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

DLP (Attachment Control)

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

The screenshot shows the 'EndPoint Security' application window with the 'DLP (Attachment Control)' tab selected. The window has a 'Start' button and a 'Stop' button. Below these are three tabs: 'Application Control', 'Device Control', and 'DLP (Attachment Control)'. The 'DLP (Attachment Control)' tab is active and contains the following settings:

- Attachment Allowed** (selected) or **Attachment Blocked** (unselected).
- Enter Process Name :** A text box with 'Eg. Thunderbird.exe' and 'Add' and 'Delete' buttons.
- Blacklisted Process**: A list box for adding processes to the blacklist.
- Attachments will be allowed from below sites irrespective of the above settings**: A text box with 'Eg. Gmail.com, Yahoo' and 'Add' and 'Delete' buttons.
- Whitelisted sites**: A list box for adding sites to the whitelist.

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

You can configure the following settings:

Attachment Allowed

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

Attachment Blocked

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

Enter Process Name

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

Blacklisted Process

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

Whitelisted Process

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

Enter Site Name

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

Whitelisted Sites

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

Advanced Settings

Advanced Setting

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

Ok

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

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

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

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

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

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

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

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

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

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

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

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

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

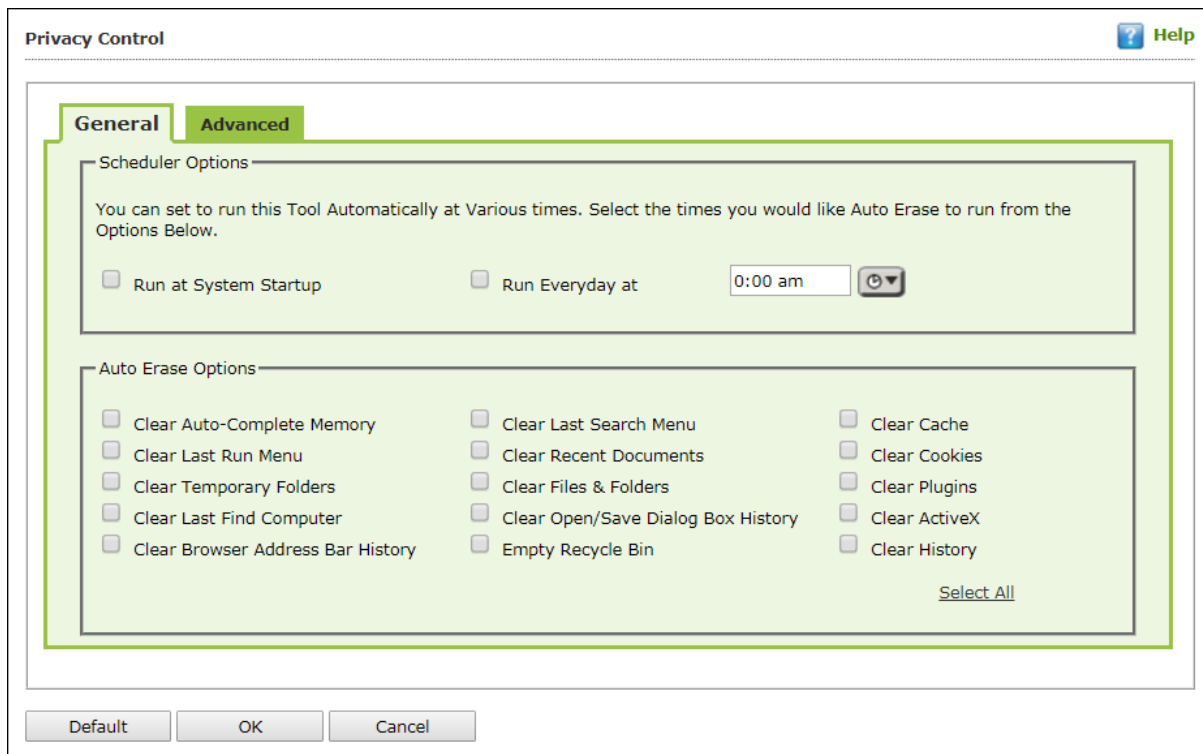
Select this option to allow/block use of network printers.

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

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

Privacy Control

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



It consists following tabs:

- General
- Advanced

General tab

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

Scheduler Options

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

Run at System Startup

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

Run Every day at

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

Auto Erase Options

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

Clear Auto Complete Memory

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

Clear Last Run Menu

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

Clear Temporary Folders

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

Clear Last Find Computer

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

Clear Browser Address Bar History

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

Clear Last Search Menu

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

Clear Recent Documents

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

Clear Files & Folders

When you select this check box, Privacy Control deletes selected Files and Folders. Use this option with caution as it permanently deletes unwanted files and folders from the computer to free space on the computer.

Clear Open/Save Dialog box History

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

Empty Recycle Bin

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

Clear Cache

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

Clear Cookies

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

Clear Plugins

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

Clear ActiveX

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

Clear History

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

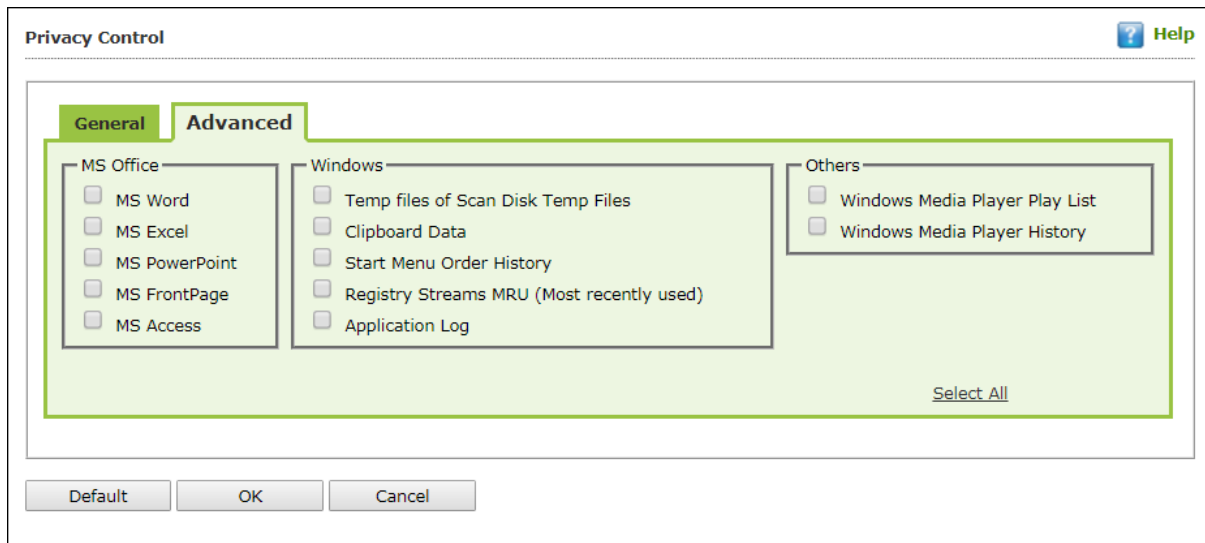
In addition to these options, the **Auto Erase Options** section has

Select All/ Unselect All

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

Advanced tab

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



MS Office

The .msi extension files will be cleared if these options are selected.

Windows

The respective unwanted files like temp files will be cleared.

Others

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

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

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

Administrator Password

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

eScan Password

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

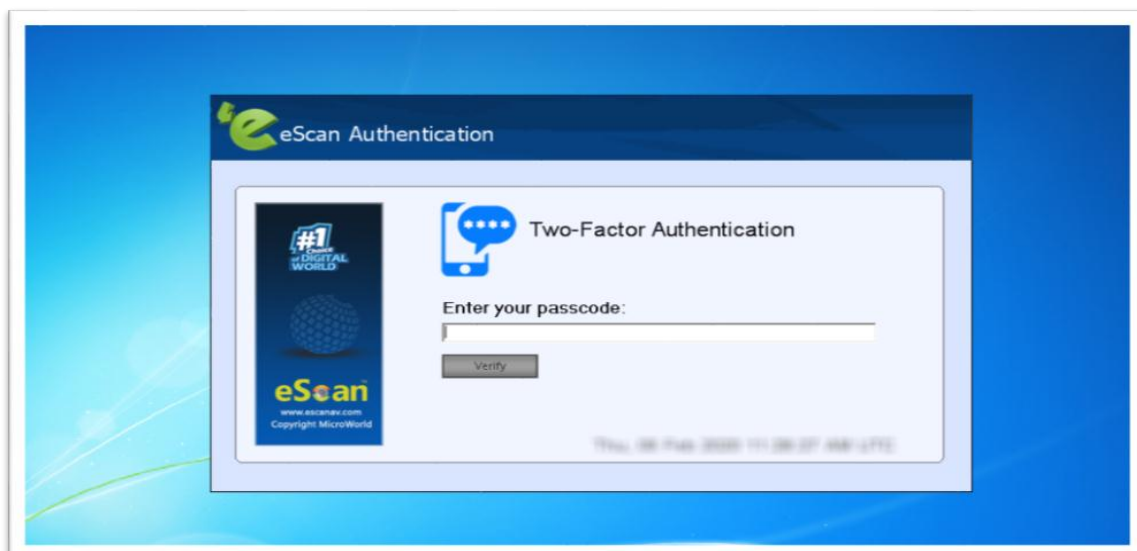
The screenshot shows the 'Add/Change Password' dialog box. It has a title bar with 'Add/Change Password' and a 'Help' icon. There are two tabs: 'eScan Password' and 'Two-Factor Authentication'. The 'eScan Password' tab is active. It contains two radio buttons: 'Set Password' and 'Blank Password'. The 'Blank Password' option is selected. Below the 'Set Password' option, there are two text input fields: 'Enter new Password' and 'Confirm new Password'. Below these fields, there is a red text label: 'Password is case-sensitive'. Below the 'Blank Password' option, there is a checkbox labeled 'Use separate uninstall password'. Below this checkbox, there are two text input fields: 'Enter uninstall password' and 'Confirm uninstall password'. At the bottom of the dialog, there are four buttons: 'Default', 'Advanced Setting', 'OK', and 'Cancel'.

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

Two-Factor Authentication

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

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



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

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

NOTE

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

3. Select **Administrator Password** check box and then click **Edit**.
4. Click **Two-Factor Authentication** tab.

Following window appears.

The screenshot shows a dialog box titled "Add/Change Password" with a "Help" icon in the top right. It has two tabs: "eScan Password" and "Two-Factor Authentication". The "Two-Factor Authentication" tab is active. Inside this tab, there is a section with five checkboxes: "Enable Two-Factor Authentication", "RDP", "Safe Mode", "Local Logon", and "Unlock". Below this section, there is another section with three options: "Use eScan Administrator Password", "Use Other Password" (which has a text input field next to it), and "Use Online Two-Factor Authentication". At the bottom of the dialog are four buttons: "Default", "Advanced Setting", "OK", and "Cancel".

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

Login Scenarios

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

RDP

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

Safe Mode

After a system is booted in Safe Mode, the personnel will have to enter system login credentials and 2FA passcode to access the system.

Local Logon

Whenever a system is powered on or restarted, the personnel will have to enter system login credentials and 2FA passcode to access the system.

Unlock

Whenever a system is unlocked, the personnel will have to enter login credentials and 2FA passcode to access the system.

Password Types

If the policy is applied to a group, the 2FA passcode will be same for all group members. The 2FA passcode can also be set for specific computer(s). You can use following all password types to log in:

Use eScan Administrator Password

You can use the existing eScan Administrator password for 2FA login. This password can be set in **eScan Password** tab besides the **Two-Factor Authentication** tab.

Use Other Password

You can set a new password which can be combination of uppercase, lowercase, numbers, and special characters.

Use Online Two-Factor Authentication

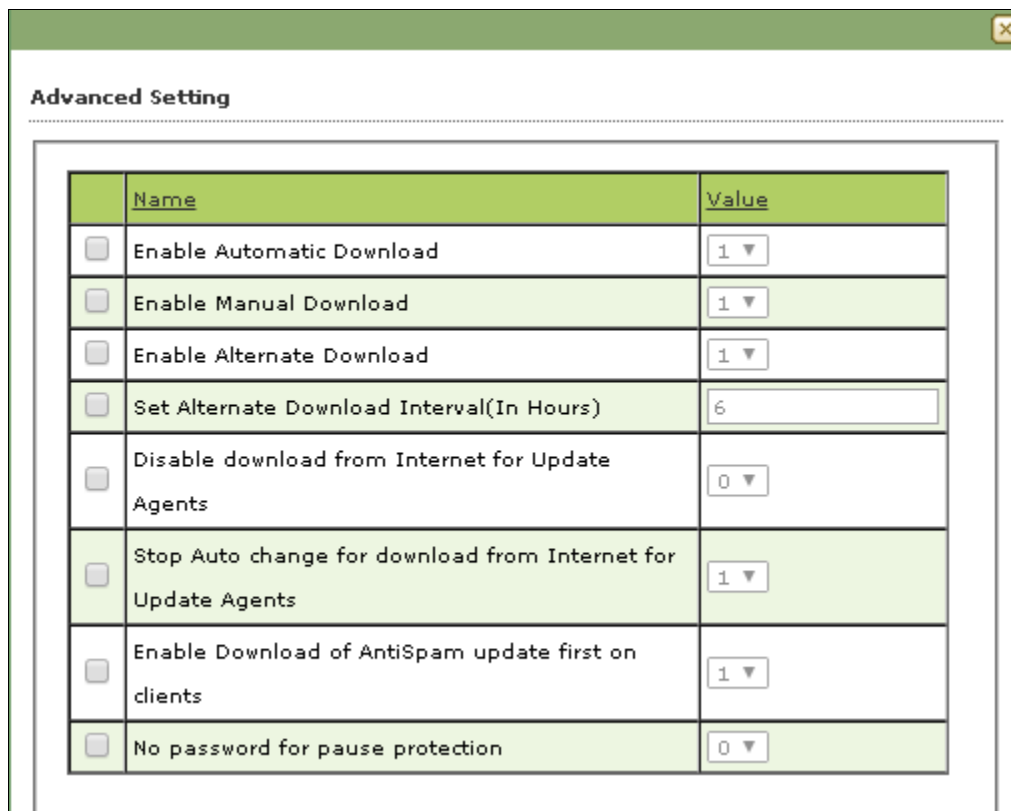
To use this feature, follow the steps given below:

1. Install the Authenticator app from Play Store for Android devices or App Store for iOS devices.
2. Open the Authenticator app and tap **Scan a barcode**.
3. Select the check box **Use Online Two-Factor Authentication**.
4. Go to **Managed Computers** and below the top right corner, click **QR code for 2FA**.
A QR code appears.
5. Scan the onscreen QR code via the Authenticator app.
A Time-based One-Time Password (TOTP) appears on smart device.
6. Forward this TOTP to personnel for login.

After selecting the appropriate Login Scenarios and Password Types, click **OK**. The Policy Template gets saved/updated.

Advanced Setting

Clicking **Advanced Setting** displays Advance setting.



The screenshot shows a window titled "Advanced Setting" with a close button in the top right corner. Inside the window is a table with two columns: "Name" and "Value". Each row in the table has a checkbox in the "Name" column. The values are either dropdown menus or text input fields.

Name	Value
<input type="checkbox"/> Enable Automatic Download	1 ▼
<input type="checkbox"/> Enable Manual Download	1 ▼
<input type="checkbox"/> Enable Alternate Download	1 ▼
<input type="checkbox"/> Set Alternate Download Interval(In Hours)	6
<input type="checkbox"/> Disable download from Internet for Update Agents	0 ▼
<input type="checkbox"/> Stop Auto change for download from Internet for Update Agents	1 ▼
<input type="checkbox"/> Enable Download of AntiSpam update first on clients	1 ▼
<input type="checkbox"/> No password for pause protection	0 ▼

Enable Automatic Download (1 = Enable/0 = Disable)

It lets you Enable/Disable Automatic download of Antivirus signature updates.

Enable Manual Download (1 = Enable/0 = Disable)

It lets you Enable/Disable Manual download of Antivirus signature updates

Enable Alternate Download (1 = Enable/0 = Disable)

It lets you Enable/Disable download of signatures from eScan (Internet) if eScan Server is not reachable.

Set Alternate Download Interval (In Hours)

It lets you define time interval to check for updates from eScan (Internet) and download it on managed computers.

Disable download from Internet for Update Agents (1 = Enable/0 = Disable)

Selecting this option lets you disable Update Agents from downloading the virus signature from internet.

Stop Auto change for download from Internet for Update Agents (1 = Enable/0 = Disable)

This option is used when an Update Agent didn't find the primary server to download virus signature, then it tries to get virus signature from internet, so to stop Update Agent from downloading from internet this option is to be set to 1(one).

Enable Download of Anti-Spam update first on clients (1 = Enable/0 = Disable)

Normally while updating a system for virus signatures, we first download the anti-virus signature and then anti-spam signature. This option lets you first download Anti-spam updates on clients.

No password for pause protection

Selecting this option lets you pause eScan protection without entering password.

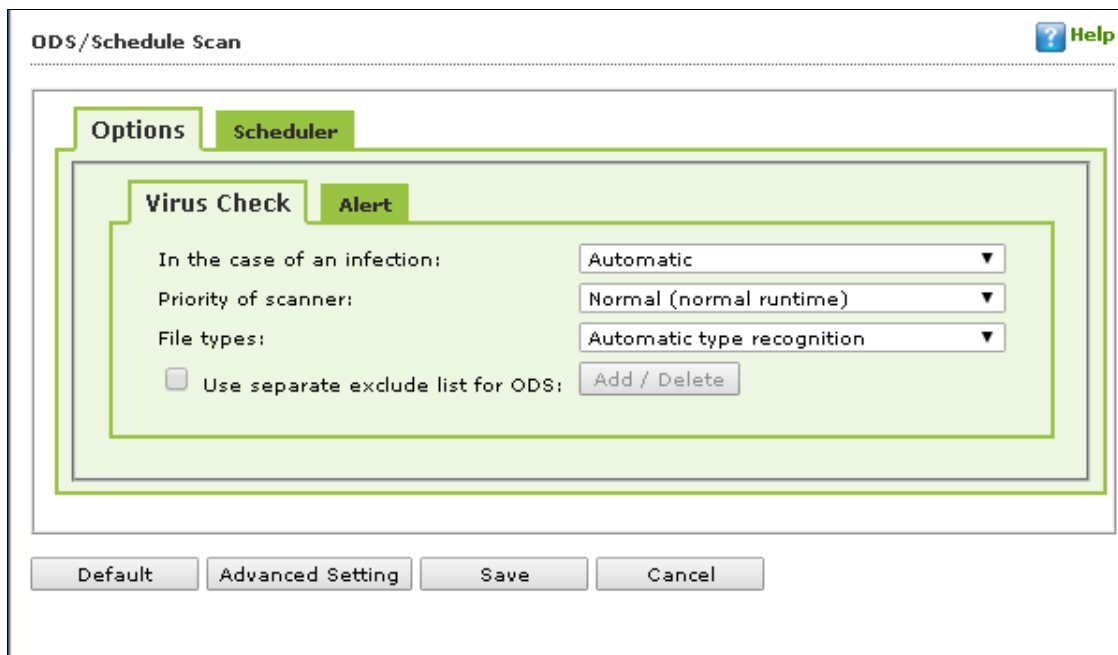
ODS/Schedule Scan

ODS (On Demand Scanning)/Schedule Scan provides you with various options like – checking for viruses, and making settings for creating logs and receiving alerts. You can also create task in the scheduler for automatic virus scanning.

NOTE Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.

It consists following tabs:

- Options
- Scheduler



The screenshot shows the 'ODS/Schedule Scan' window. It has a 'Help' button in the top right corner. The main area contains two tabs: 'Options' and 'Scheduler'. The 'Options' tab is active and contains two sub-tabs: 'Virus Check' and 'Alert'. The 'Virus Check' sub-tab is selected and shows the following settings:

- 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

At the bottom of the window, there are four buttons: 'Default', 'Advanced Setting', 'Save', and 'Cancel'.

Options

Options tab lets you make the settings for checking viruses and receiving alerts. There are two tabs – Virus Check and Alerts. You can do the following activities.

- Virus check
- Alerts

Virus Check

It lets you configure the settings for checking viruses.

To set virus check,

1. Specify the following field details.
 - **In the case of an infection:** Select an appropriate option from the drop-down list. For example, Log only, Delete infected file, and [Default] Automatic.
 - **Priority of scanner:** Select an appropriate option from the drop-down list. For example,
 - High (short runtime)
 - Normal (normal runtime) [Default]
 - Low (long runtime)
 - **File types:** Select an appropriate option from the drop-down list. For example, \[Default\] Automatic type recognition and only program files.
 - **Use separate exclude list for ODS:** Select this option to add a list of file/folders that should be excluded from scan.
2. Click **Save**.

Alerts tab

It lets you configure the settings for virus alert. You can also create a log of the infected viruses.

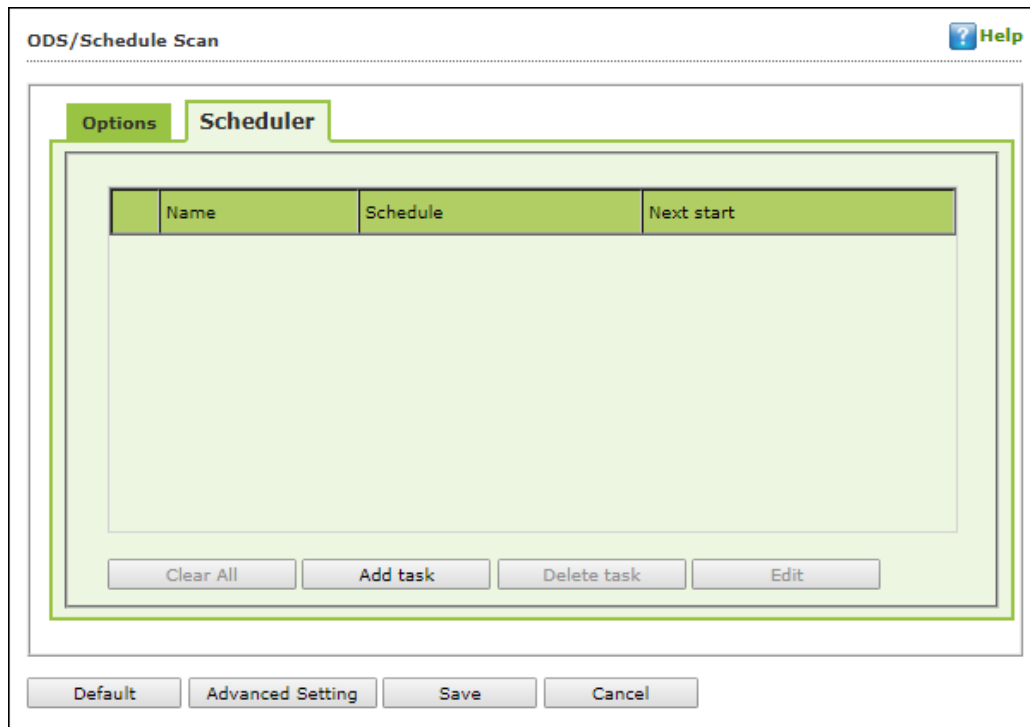
To set alerts,

1. Under **Alert** section, Select the [Default] **Warn**, if virus signature is more than x days old check box, and then enter the number of days in the x days old field, if you want to receive alerts when virus signature exceeds the specified days. By default, value 3 appears in the field.
2. Select the **Warn**, if the last computer analysis was more than x days ago check box, and then enter the number of days in the x days ago field, if you want to receive alerts when last computer analysis exceeds the specified days. By default, 3 appears in the field.
3. Under **Log Settings** section, select the [Default] **Prepare Log** check box, if you want to prepare log of the infected files, and then select an appropriate option.
4. Click **Save**.

NOTE	Click Default to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.
-------------	--

Scheduler

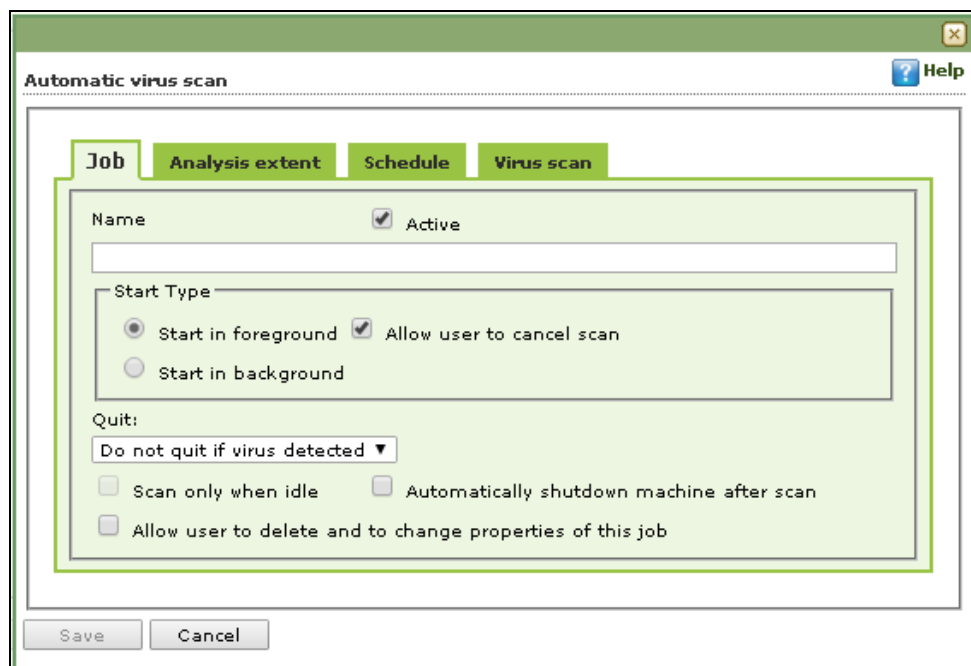
Scheduler tab lets you create/delete various tasks in the scheduler for automatic virus scanning.



NOTE Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.

Clear All - This button will clear all the listed tasks.

Add Task



Automatic Virus Scan lets you do following activities:

- a) Creating job
- b) Setting analysis extent
- c) Scheduling virus execution
- d) Scheduling virus scan

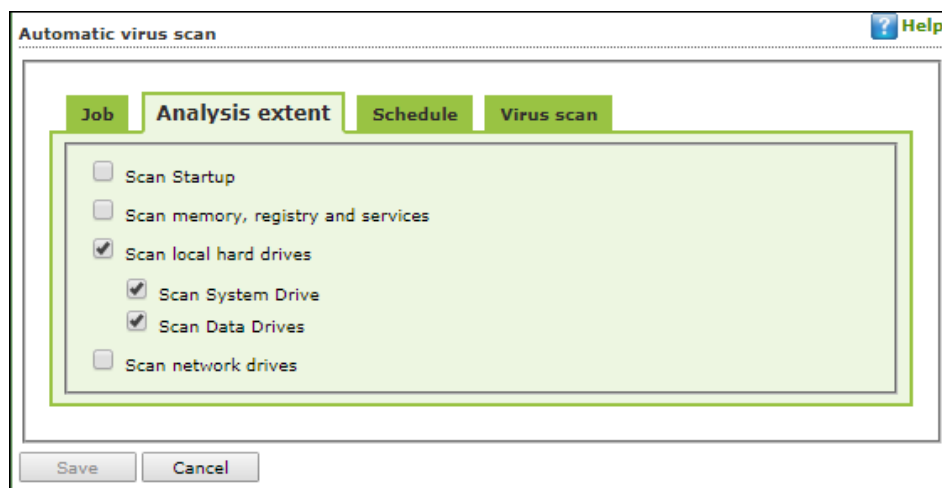
a) Job

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 check box, if you want to allow the client to schedule the task.
 - **Start in foreground [Default]:** Click this option if you want to view scanning process running in front of you.
When this option is selected, the **Scan only when idle** option becomes unavailable.
 - **Start in background:** Click this option if you want scanning process to run in the background. By default, Do not quit if virus is detected option is selected. When you select this option, the Quit drop-down list becomes unavailable.
3. Click **Save**.

b) Analysis Extent

It lets you configure analysis extent settings for virus scanning.



1. Click the **Analysis Extent** tab.
2. Select the **Scan Startup** option, if you want to scan all startup entries.
3. Select the **Scan memory, registry and services** option, if you want to scan memory, registry and services.

4. Select the [Default] **Scan local hard drives** option, if you want to scan local hard drives.
5. Select **Scan network drives** option, if you want to scan network drives. Users should note that scanning a network drive may affect system performance.
6. Click **Save**.

c) Scheduling

It lets you schedule the date and time of execution for virus scanning.

The screenshot shows the 'Automatic virus scan' dialog box with the 'Schedule' tab selected. The 'Execute' section contains six radio button options: 'Once' (selected), 'Hourly', 'Daily', 'Weekly', 'Monthly', and 'With system startup'. Below this, the 'Date and time' section features a date input field showing '09/26/2019', a time input field showing '12:00 pm', and a clock icon. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

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 Help

Job **Analysis extent** **Schedule** **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

Save Cancel

1. Click the **Virus Scan** tab.
2. Specify the following field details.
 - **In the case of an infection:** Select an appropriate option from the drop-down list. For example, Log only, Delete infected file, and [Default] Automatic.
 - **Priority of scanner:** Select an appropriate priority from the drop-down list.
 - **File types:** Select an appropriate option from the drop-down list. For example, [Default] Automatic type recognition and Only program files.
3. Under Log Settings section, select the [Default] Prepare Log check box, if you want to prepare log of the infected files, and then click an appropriate option.
4. Click **Save**.

Delete Task – Clicking **Delete Task** lets you delete the particular task from the list.

Edit – Clicking **Edit** lets you edit the properties of the particular task from the list.

MWL (MicroWorld WinSock Layer)

eScan's "MicroWorld-WinSock Layer" (MWL) is a revolutionary concept in scanning Internet traffic on a real-time basis. It has changed the way the world deals with Content Security threats. Unlike the other products and technologies, MWL tackles a threat before it reaches your applications. MWL is technically placed above the WinSock layer and acts as a "Transparent Gatekeeper" on the WinSock layer of the operating system. All content passing through WinSock has to mandatorily pass through MWL, where it is checked for any security violating data. If such data occurs, it is removed and the clean data is passed on to the application.

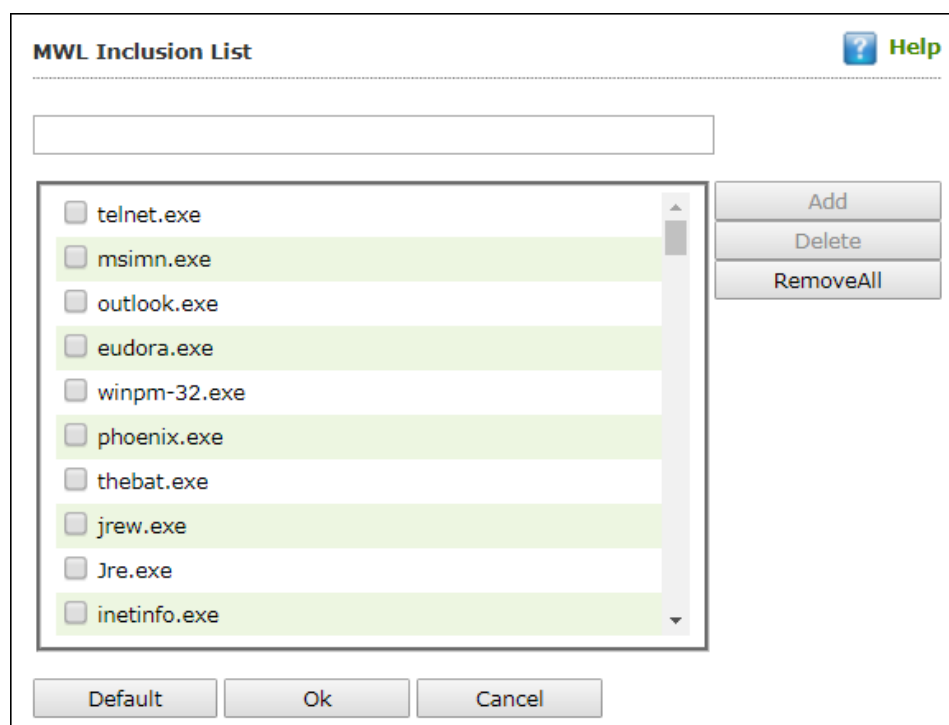
MWL Inclusion List

Inclusion List contains the name of all executable files which will bind itself to MWTSP.DLL. All other files are excluded.

NOTE Click **Default** to apply default settings, done during eScan installation. It loads and resets the values to the default settings.

You can do the following activities.

- **Adding files** to Inclusion List
- **Deleting files** from Inclusion List
- **Removing all files** from Inclusion List



Add files to Inclusion List

To add executable files to the Inclusion List,

1. Enter the executable file name and then click **Add**.
The executable file will be added to the Inclusion List.
2. Click **OK**.

Delete files from Inclusion List

To delete executable files from the Inclusion List, follow the steps given below:

1. Select executable files, and then click **Delete**.
A confirmation prompt appears.
2. Click **OK**.
The executable file will be deleted from the Inclusion List.

Remove all files from Inclusion List

To remove all executable files from the Inclusion List,

1. Click **Remove All**.
A confirmation prompt appears.
2. Click **OK**.
All executable files will be removed from the Inclusion List.

MWL Exclusion List

MWL (MicroWorld WinSock Layer) Exclusion List contains the name of all executable files which will not bind itself to **MWTSP.DLL**.

NOTE

Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.

You can do the following activities.

- **Adding files** to Exclusion List
- **Deleting files** from Exclusion List
- **Removing all files** from Exclusion List

The dialog box titled "MWL Exclusion List" features a "Help" icon in the top right corner. Below the title bar is a text input field. The main area contains a list of files with checkboxes: INETINFO.EXE, VHTTDP32.DLL, NS-ADMIN.EXE, NS-SLAPD.EXE, TCPSVCS.EXE, SVCHOST.EXE, ESERV.EXE, DOWNLOAD.EXE, RP.EXE, and SPOOLER.EXE. To the right of the list are three buttons: "Add", "Delete", and "RemoveAll". At the bottom of the dialog are three buttons: "Default", "Ok", and "Cancel".

Adding files to Exclusion List

To add executable files to the Exclusion List,

1. Enter the executable file name and then click **Add**.
The executable file gets added to the Exclusion List.
2. Click **OK**.

Deleting files from Exclusion List

To delete executable files from the Exclusion List,

1. Select the appropriate file check box, and then click **Delete**.
A confirmation prompt appears.
2. Click **OK**.
The executable file gets deleted from the Exclusion List.

Removing all files from Exclusion List

To remove all executable files from the Exclusion List,

1. Click **Remove All**.
A confirmation prompt appears.
2. Click **OK**.
All executable files get removed from the Exclusion List.

Notifications and Events

The screenshot shows the 'Notifications & Events' configuration window. The 'Notifications' tab is selected. The 'Warning Notification Settings' section includes 'Virus Alerts' with a checked 'Show Alert Dialog-box' option, 'Mail Server Settings' with fields for SMTP Mail Server, SMTP Port, User Authentication (Opt.), and Authentication Password (Opt.), and a list of notification types: 'Attachment Removed Warning To Sender' (checked), 'Attachment Removed Warning To Recipient' (checked), 'Virus Warning To Sender' (checked), 'Virus Warning To Recipient' (checked), 'Content Warning To Sender' (unchecked), and 'Content Warning To Recipient' (checked). The 'Warning Mails' section has 'From' and 'To' fields, both set to 'postmaster'. The 'Delete Mails From User' section has a list box and buttons for 'Add', 'Delete', and 'RemoveAll'. A preview box at the bottom shows a sample email notification with the following content:

```
attrem.snd
#Lines starting with # are comment lines.
#This file specifies warning sent to Mail-Sender by
#eScan when it deletes attachments.
#
The attachment(s) that you sent with the following mail
was deleted by eScan (not delivered to the recipient)
=====
The Mail came from : %f
The Mail recipient : %t
Subject of the Mail : %s
Message-ID : %i
Received : %r
```

Notifications

Notifications tab lets you configure the notification settings. It lets you send emails to specific recipients when malicious code is detected in an email or email attachment. It also lets you send alerts and warning messages to the sender or recipient of an infected message. You can configure the following settings:

Virus Alerts [Default]

This section contains **Show Alert Dialog box** option. Select this option if you want Mail Anti-Virus to alert you when it detects a malicious object in an email.

Warning Mails

Configure this setting if you want Mail Anti-Virus to send warning emails and alerts to a given sender or recipient. The default sender is **postmaster** and the default recipient is **postmaster**.

Attachment Removed Warning to Sender [Default]

Select this check box if you want Mail Anti-Virus to send a warning message to the sender of an infected attachment. Mail Anti-Virus sends this email when it encounters a virus infected attachment in an email. The email content is displayed in the preview box.

Attachment Removed Warning to Recipient [Default]

Select this check box if you want Mail Anti-Virus to send a warning message to the recipient when it removes an infected attachment. The email content is displayed in the preview box.

Virus Warning to Sender [Default]

Select this check box if you want Mail Anti-Virus to send a virus warning message to the sender. The email content is displayed in the preview box.

Virus Warning to Recipient [Default]

Select this check box if you want Mail Anti-Virus to send a virus warning message to the recipient. The email content is displayed in the preview box.

Content Warning to Sender

Select this check box if you want Mail scanner to send a content warning message to the sender. The email content is displayed in the preview box.

Content Warning to Recipient [Default]

Select this check box if you want Mail scanner to send a content warning message to the recipient. The email content is displayed in the preview box.

Delete Mails from User

You can configure eScan to automatically delete emails that have been sent by specific users. For this, you need to add the email addresses of such users to the **Delete Mails From User** field. The **Add**, **Delete**, and **Remove All** buttons appear as dimmed. After you enter text in the **Delete Mails From User** field, the buttons get enabled.

Events

Events tab lets you define the settings to allow/restrict clients from sending alert for following events:

- Executable Allowed
- Website Allowed
- Cleaned Mail

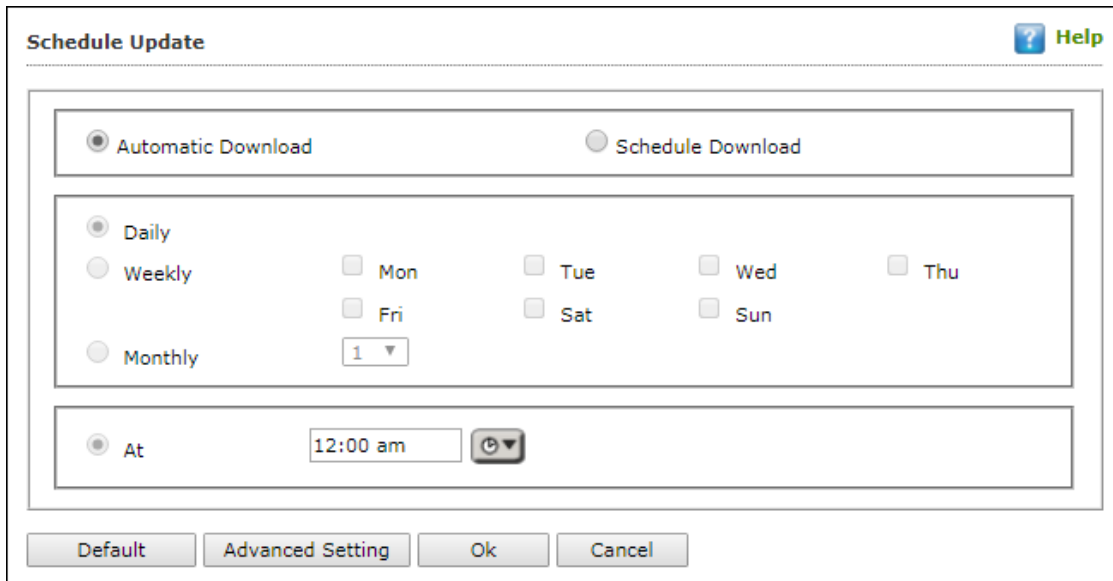
By default, all events are selected.

The screenshot shows a window titled "Notifications & Events" with a "Help" icon in the top right. It has two tabs: "Notifications" and "Events", with "Events" being the active tab. Inside the "Events" tab, there is a section titled "Do not allow client to send event for" followed by a list of three items, each with a checked checkbox: "Executable Allowed", "WebSite Allowed", and "Cleaned Mail". At the bottom of the window, there are four buttons: "Default", "Advanced Setting", "OK", and "Cancel".

NOTE	Click Default to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.
-------------	--

Schedule Update

The Schedule Update lets you schedule eScan database updates.



The screenshot shows the 'Schedule Update' dialog box. It has a title bar with a 'Help' button. The dialog is divided into three main sections. The top section has two radio buttons: 'Automatic Download' (selected) and 'Schedule Download'. The middle section has three radio buttons: 'Daily' (selected), 'Weekly', and 'Monthly'. To the right of these are checkboxes for days of the week: Mon, Tue, Wed, Thu, Fri, Sat, and Sun. The 'Monthly' option has a dropdown menu showing '1'. The bottom section has a radio button for 'At' (selected), a text box showing '12:00 am', and a clock icon. At the bottom of the dialog are four buttons: 'Default', 'Advanced Setting', 'Ok', and 'Cancel'.

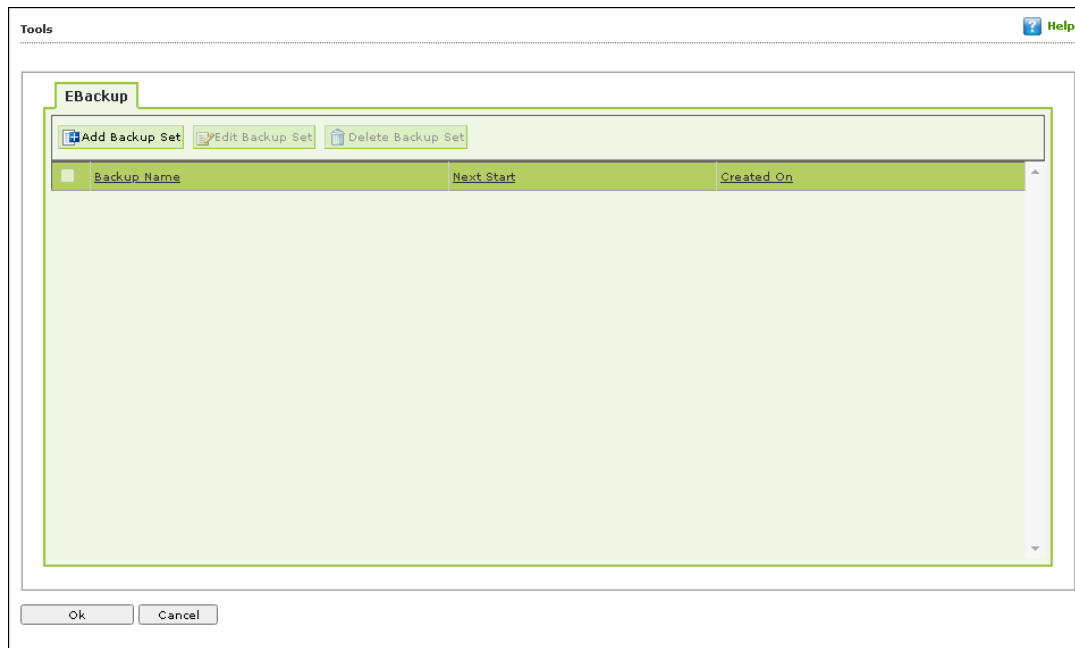
The updates can be downloaded automatically with **Automatic Download** option.

-OR-

The updates can be downloaded on a schedule basis with **Schedule Download** option. Select intervals and time basis as per your preferences.

Tools

The Tools lets you configure eBackup Settings.



eBackup

Taking regular backup of your critical files stored on your computer is very important, as files may get misplaced or damaged due to issues such as virus outbreak, modification by a ransomware or another user. This feature of eScan allows you to take backup of your important files stored on your computer such as documents, Photos, media files, music files, contacts and so on. It allows you to schedule the backup process by creating tasks. The backed up data is stored in an encrypted format in a folder secured by eScan's real-time protection. You can create Backup jobs by adding files, folders to take a backup either manually or schedule the backup at a defined time or day.

With eBackup feature you can:

- Create, schedule, edit, and delete backup jobs as per requirement.
- Take a backup of specific folder(s)/file extension(s) on local endpoint, external drives or network drive.
- Exclude specific folder(s)/file extension(s) from being backed up.
- Add specific file extensions to be backed up along with regular backup as per requirement.
- Save the backup data in external hard drive or local drive.

Add Backup Set

To create a Backup Set,

1. Go to **Managed Computers**.
2. Click **Policy Templates > New Template**.

NOTE

You can add the backup set for existing Policy Templates by selecting a Policy Template and then clicking **Properties**. Then, follow the steps given below:

3. Select **Tools** check box and then click **Edit**.
4. Click **Add Backup Set**.

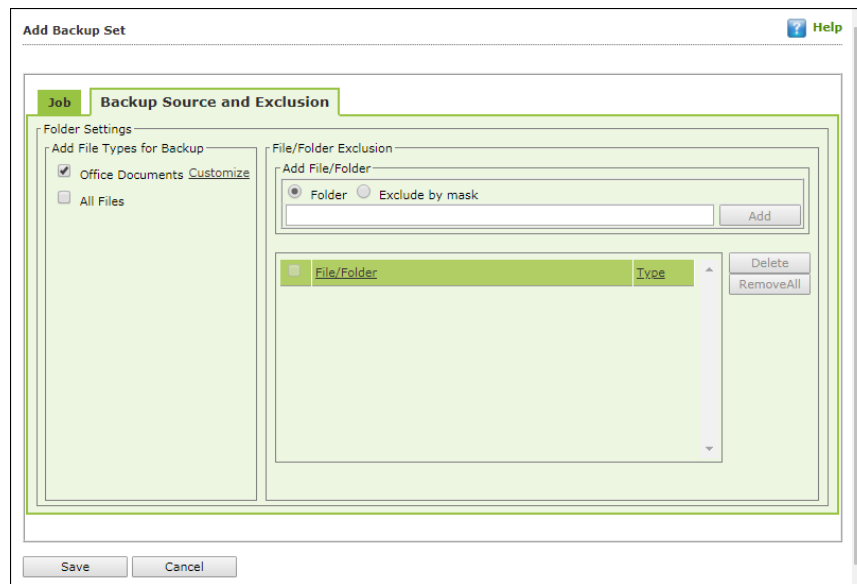
Add Backup Set window appears.

5. Enter a name.
6. In the Scheduler section, select a preferred interval for backup execution.
7. Administrator can save the backup set in the Network Drive by providing the path of the drive and Username and password for the network drive.

NOTE

Network storage of backup set will be available in the trail period. To continue the use of this feature user need to avail the license for the same.
In case of system crash or hardware failure, user can recover the created data backup, so storing the backup in the network drive, mapped drive, or NAS drive would be useful in such scenarios.

8. Click **Backup Source and Exclusion** tab.



9. Select the type of files for backup. By default, Office Documents option is selected.
10. Under the File/Folder Exclusion section, you can exclude a specific folder or a file format from getting backed up.
11. Click **Save**.
The Backup Set will be created.

NOTE

By default, **Active** option is selected. If **Active** option is not selected, a Backup Set will be created but eScan won't backup data.

Edit Backup Set

To edit a Backup Set,

1. Select a Backup Set.
2. Click **Edit Backup Set**.
3. After making the necessary changes, click **Save**.
The Backup Set will be edited and saved.

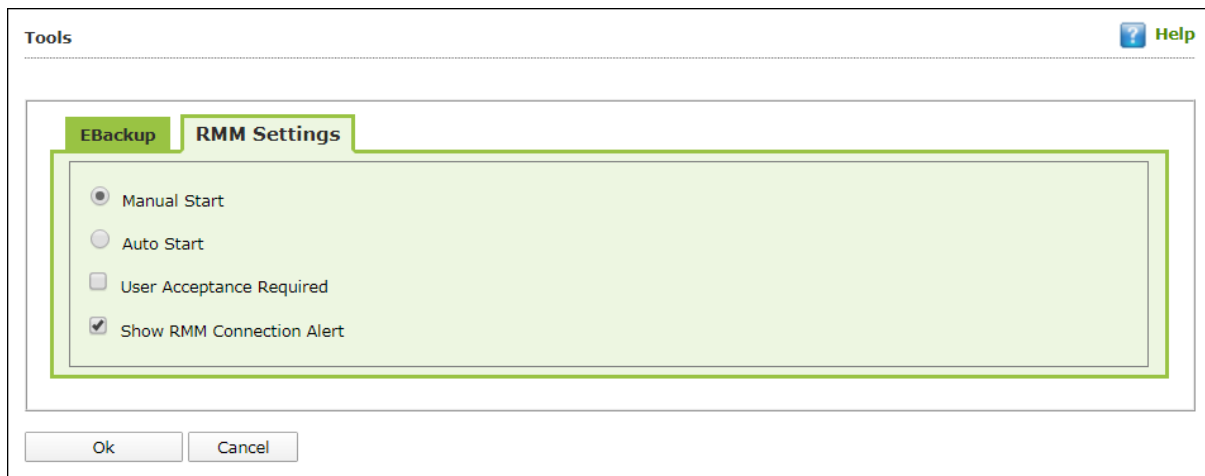
Delete Backup Set

To delete a Backup Set,

1. Select a Backup Set.
2. Click **Delete Backup Set**.
A confirmation prompt appears.
3. Click **OK**.
The Backup Set will be deleted.

RMM Settings

The RMM settings let you configure default connection settings for connecting to client computers. You will get the following configuration options:




- **Manual Start:** If this option is selected, client endpoint users have to manually start the RMM service to establish a RMM connection.
- **Auto Start:** If this option is selected, RMM service will be started automatically and all client endpoints will be connected to your main eScan server.
- **User Acceptance Required:** If this check box is selected, a pop-up appears on client endpoint for RMM connection acceptance. If left unselected, pop-up doesn't appear and you get direct access to the client endpoint.
- **Show RMM Connection Alert:** If this check box is selected, a notification appears on client endpoint informing about active RMM connection. If left unselected, notification doesn't appear on client endpoint.

After making the necessary changes click **OK**.
Click **Save**. The Policy Template gets saved.

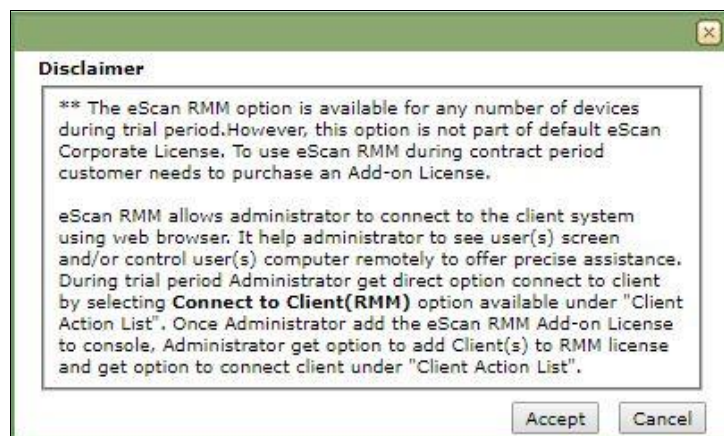
RMM - Manual Start

To take a remote connection by using **Manual Start** option

1. Tell the client endpoint user to right-click the eScan Protection Center icon  and click **Start eScanRMM**.



2. After the client endpoint user has clicked **Start eScanRMM**, select the target endpoint and then click **Client Action List > Connect to Client (RMM)**.
Following disclaimer appears.

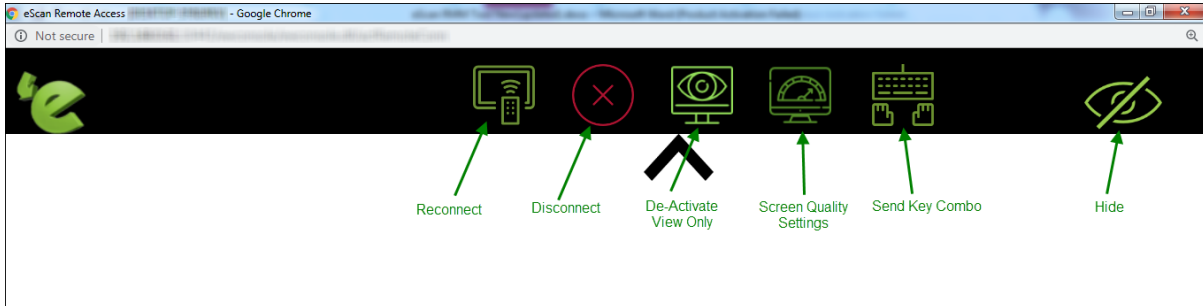


NOTE

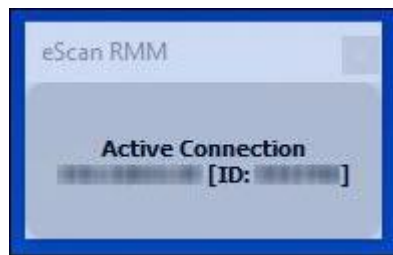
If you are using eScan product in Trial version, this disclaimer will appear each time you are connecting to an endpoint via RMM feature.

A local server won't be part of RMM and can't be connected via RMM.

3. Read the disclaimer thoroughly and then click **Accept**.
Your default browser opens eScan Remote Access window (Google Chrome, Mozilla Firefox, MS Edge, etc.)



Following notification appears on client endpoint displaying IP address of RMM connecting endpoint and connection ID (If **Show RMM Connection Alert** option is selected).



RMM - Auto Start

If **Auto Start** option is selected, then client endpoints get automatically connected to your eScan server.

1. Go to **Managed Computers**, select the target endpoint and then click **Client Action List > Connect to Client (RMM)**.
RMM disclaimer appears.
2. Read the disclaimer thoroughly and then click **Accept**.
Your default browser opens eScan Remote Access window (Google Chrome, Mozilla Firefox, MS Edge, etc.)

After you are done performing an activity, click the **Disconnect** icon to end remote connection.

NOTE	To get detailed information about RMM feature, click here .
-------------	---

Configuring eScan Policies for Linux and Mac Computers

eScan lets you define settings for File Anti-Virus, Endpoint Security, On Demand scanning and Schedule Scan module for Linux and Mac computers connected to the network. Click **Edit** to configure the eScan module settings for computers with respective operating systems.

<input type="checkbox"/> File Anti-Virus Assign From <input type="text" value="Select Policy"/>	<input type="checkbox"/> EndPoint Security Assign From <input type="text" value="Select Policy"/>
<input type="checkbox"/> On Demand Scanning Assign From <input type="text" value="Select Policy"/>	<input type="checkbox"/> Schedule Scan Assign From <input type="text" value="Select Policy"/>
<input type="checkbox"/> Schedule Update Assign From <input type="text" value="Select Policy"/>	<input type="checkbox"/> Administrator Password Assign From <input type="text" value="Select Policy"/>
<input type="checkbox"/> Web Protection Assign From <input type="text" value="Select Policy"/>	

NOTE	<p>Icons next to every module displays that the settings are valid for the respective operating systems only.</p> <p>It lets you define settings for Scanning; you can also define action to be taken in case of an infection. It also lets you define the number of days for which the logs should be kept as well as create list for Masks, Files or Folders to be excluded from scanning.</p>
-------------	--

File Anti-Virus 🐼 🐼

File Anti-Virus 🐼 🐼 ? Help

In the case of an infection: Disinfect (if not possible, quarantine) ▼

Scan Settings

☐ Archives 🐼 🐼
☒ Packed 🐼 🐼
☐ Follow symbolic links 🐼

☐ Mails 🐼
☐ Cross file system 🐼

☒ Display attention messages
 Number of days log should be kept 365

☐ Exclude by mask 🐼

Add
Delete
RemoveAll

☐ Exclude Files / Folders 🐼 🐼

Add
Delete
RemoveAll

☒ Add Directory for realtime scan 🐼

Add
Delete
RemoveAll

Default
OK
Cancel

Actions in case of infection [Drop-down]

It displays a list of actions eScan should take, in case of virus detection.

File Anti-Virus 🐼 🐼

In the case of an infection: Disinfect (if not possible, quarantine) ▼

☐ Archives 🐼 🐼
☒ Packed 🐼 🐼
☐ Follow symbolic links 🐼

Disinfect (if not possible, quarantine) ▼
 Log only
 Disinfect (if not possible, log)
 Disinfect (if not possible, delete file)
Disinfect (if not possible, quarantine)
 Delete
 Quarantine

By default, Disinfect (if not possible, quarantine file) option is selected. Following are the types of actions:

- **Log Only:** This option indicates or alerts the user about the infection detected (No Action is taken; only logs are maintained).
- **Disinfect (if not possible, log):** This option tries to disinfect and if disinfection is not possible it logs the information of only the infected object.
- **Disinfect (if not possible, delete file):** This option tries to disinfect and if disinfection is not possible it deletes the infected object.
- **Disinfect (if not possible, quarantine file):** This option tries to disinfect and if disinfection is not possible it quarantines the infected object.
- **Delete:** This option deletes the infected object.
- **Quarantine:** This option quarantines the infected object.

Scan Settings

- **Mails** - It indicates scanning the mail files. By default, it is selected. Select this check box if you want eScan real-time protection to scan mails.
- **Archives** - It indicates the archived files, such as zip, rar, and so on. Select this check box if you want eScan real-time protection to scan archived files.
- **Packed** - It indicates the compressed executable. Select this check box if you want eScan real-time protection to scan packed files.
- **Cross File System** that facilitates scanning of files over cross-file systems.
- **Follow Symbolic Links:** scans the files following the symbolic links.

Exclude by Mask (file types) - Select this option if you want eScan real-time protection to exclude specific file extensions.

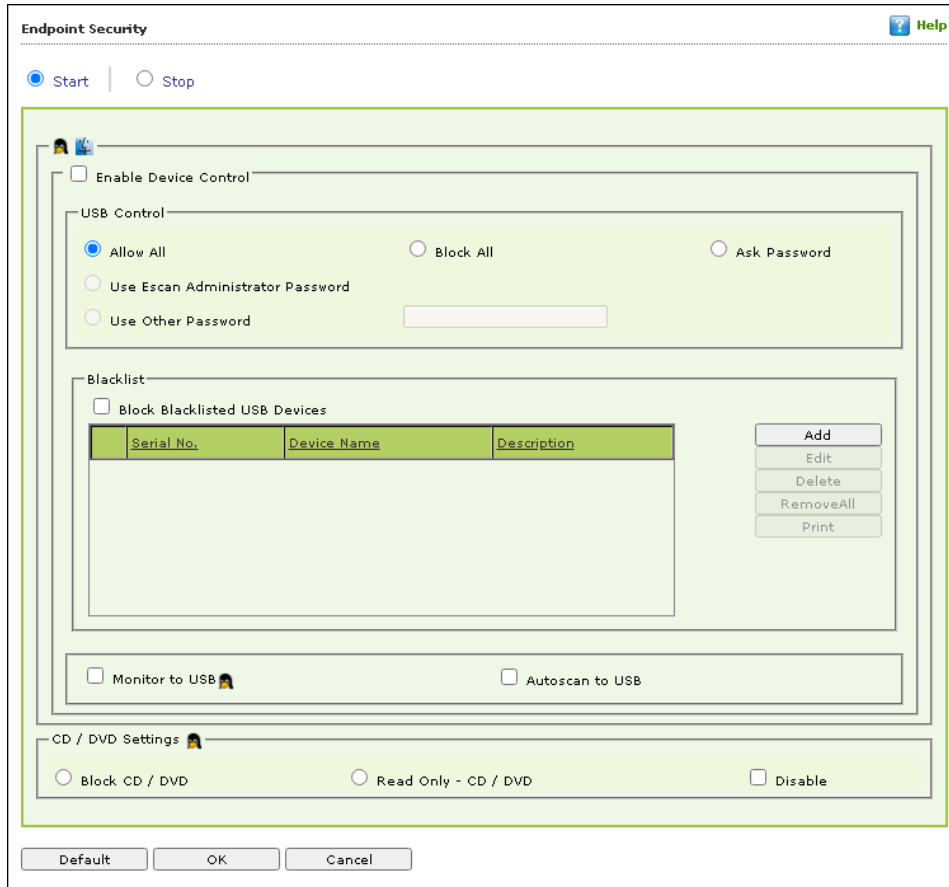
Exclude Folders and files - Select this option if you want eScan real-time protection to exclude Folders and files from scanning. eScan lets you add; Remove any or all Added Files or Folders whenever required.


Add Directory for Real-Time Scan: If you want eScan to perform real-time scan on any of the directories add them in this list.

You can restore default eScan settings by clicking **Default**.

Endpoint Security

The Endpoint Security module lets you centrally manage all endpoints on your network and closely monitor all USB activities in real-time. With eScan USB control, you can prevent data theft by blocking all except your trusted USB storage devices and Stop your files from being taken away on thumb drives, iPod, mp3 players and portable USB hard drives.



Endpoint Security  Help

☒ Start | ☐ Stop

☐ Enable Device Control

USB Control

☒ Allow All ☐ Block All ☐ Ask Password


☐ Use Escan Administrator Password


☐ Use Other Password

Blacklist

☐ Block Blacklisted USB Devices

Serial No.	Device Name	Description

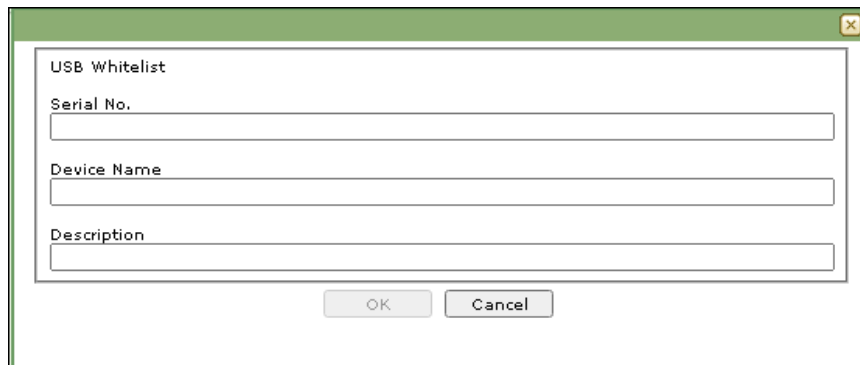
☐ Monitor to USB  ☐ Autoscan to USB

CD / DVD Settings 

☐ Block CD / DVD ☐ Read Only - CD / DVD ☐ Disable

Enable Device Control: Select this check box to configure the Device Control settings.

- **USB Control:** This option lets you to allow, block, or ask password for the USB device connected to the endpoint. It has following options:
 - **Allow All:** Select this option to allow all the connected USB devices.
 - **Block All:** Select this option to block all the connected USB devices.
 - **Ask Password:** Select this option to set password for the connected USB devices. This will ask password before allowing USB devices to connect to the system. You can either set a password or use the administrator password using options **Use Other Password** and **Use Escan Administrator Password** respectively.
- **Blacklist:** This option let's you to add USB devices to the blacklist. You can add, delete, modify using the following options:
 - **Add:** Click **Add** to add the USB serial number, name, and description of the USB devices. The USB will be added to the list.



- **Edit:** Click **Edit** to edit the details of the USB devices.
- **Delete:** Select the USB device and click **Delete** to remove the device from the list.
- **Remove All:** To remove all the USB devices from the list, click **Remove All**.
- **Print:** This will print all the USB devices in the list along with details for the same.
- **Monitor to USB:** Select this check box to monitor all the connected USB devices connected to the endpoints.
- **Autoscan to USB:** Select this option to auto-scan all the USB devices connected to the endpoints.

CD/DVD Settings

This option lets administrator to block, allow, and disable the CD/DVD. You have following options to configure:

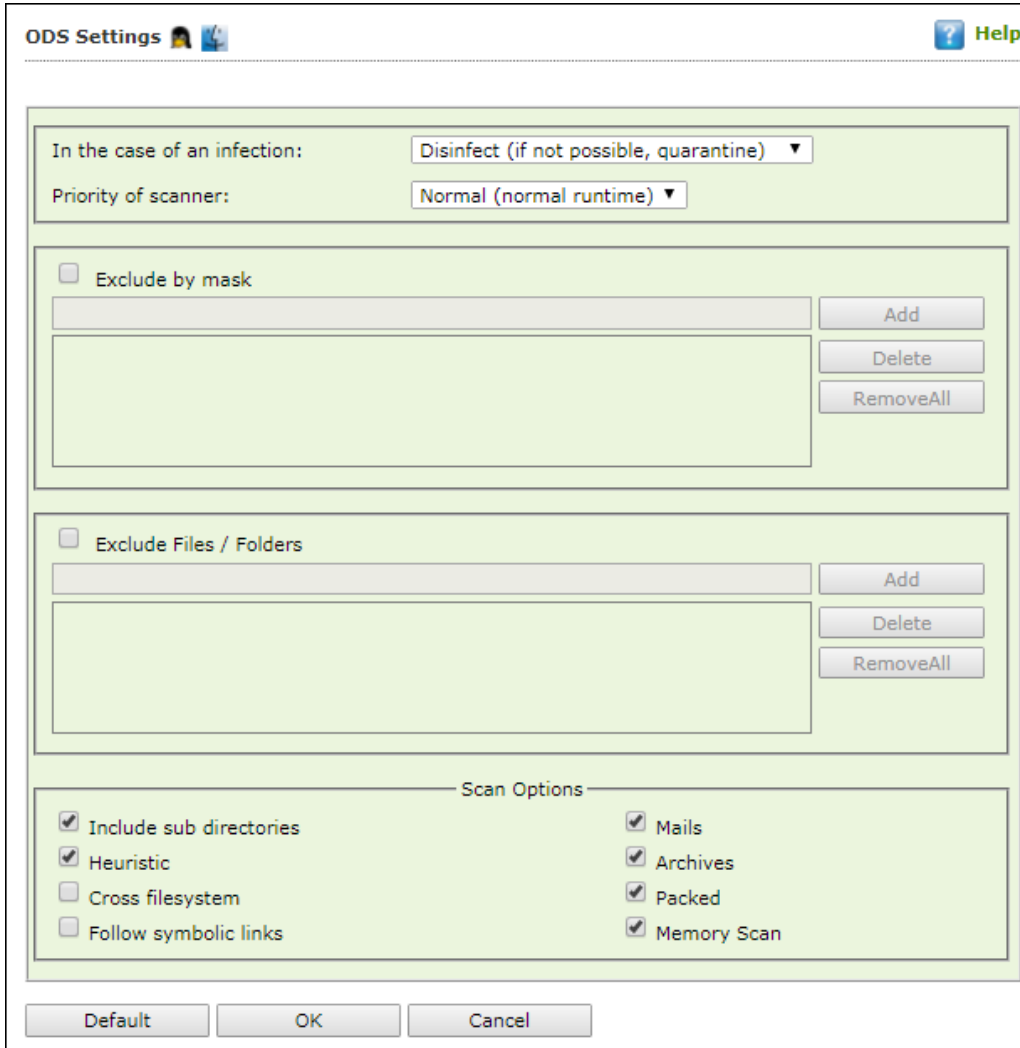
- **Block CD/DVD:** This option block all the CD and DVD.
- **Read Only CD/DVD:** This option allows user to only read the content CD and DVD.
- **Disable:** This option disables all the CD and DVD.

Default

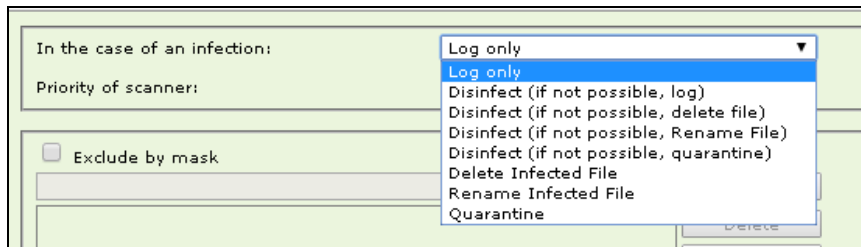
This button resets all the setting to default.

ODS Settings

With ODS Settings you can define actions in case of infection, you can also define list of files by mask, Files or Folders to be excluded from Scanning. It also lets you configure settings for various other Scan options like Include Sub directories, Mails, Archives Heuristic Scanning etc. by selecting respective options.



Actions in case of infection [Drop-down]



It indicates a type of action which you want eScan real-time protection to take, in case of virus detection.

By default, Disinfect (if not possible, quarantine file) option is selected. Following actions can be taken:

- **Log Only:** It indicates or alerts the user about the infection detected.
- **Disinfect (if not possible, log):** It tries to disinfect and if disinfection is not possible it logs the information of only the infected object.
- **Disinfect (if not possible, delete file):** It tries to disinfect and if disinfection is not possible it deletes the infected object.
- **Disinfect (if not possible, Rename file):** It tries to disinfect and if disinfection is not possible it renames the infected object.
- **Disinfect (if not possible, quarantine):** It tries to disinfect and if disinfection is not possible it quarantines the infected object.
- **Delete Infected File:** It directly deletes the infected object.
- **Rename Infected File:** It directly renames the infected object.
- **Quarantine:** It directly quarantines the infected object.

Priority of Scanner – You can select the priority of scanning as **High (short runtime)**, **Normal (normal runtime)**, or **Low (long runtime)**.

- **High (short runtime)** – Has a short runtime.
- **Normal (normal runtime)** – Has a normal runtime.
- **Low (long runtime)** – Has a long runtime.

Exclude by Mask – Select this check box if you want eScan real-time protection to exclude specific files, and Remove any or all Added Files whenever required.

Exclude Folders and Files – Select this check box if you want eScan real-time protection to exclude Folders and files from scanning. eScan lets you add; Remove any or all Added Files or Folders whenever required during On Demand Scanning.

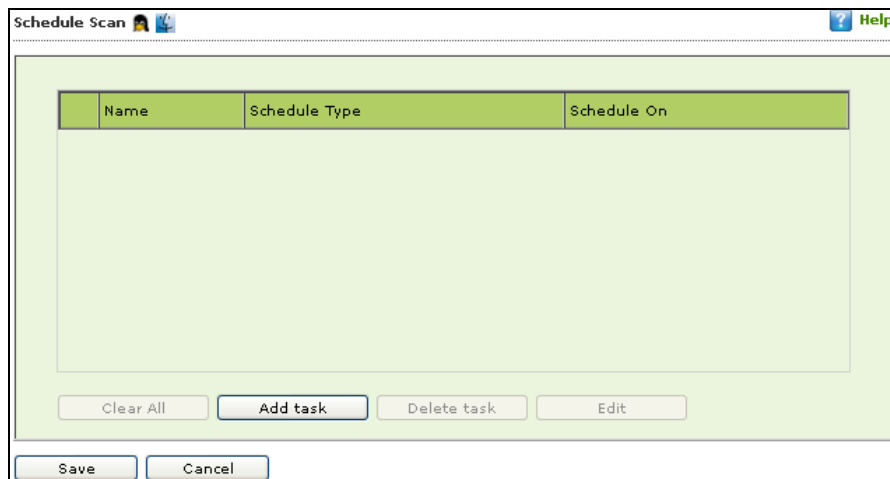
Scan options

- **Mails** – It indicates scanning the mail files. By default, it is selected. Select this check box if you want eScan real-time protection to scan mails.
- **Archives** – It indicates the archived files, such as zip, rar, and so on. Select this check box if you want eScan real-time protection to scan archived files.
- **Packed** – It indicates the compressed executable.
- **Memory Scan** – This option ensures eScan scans the system's memory for any infection from malwares.
- **Include Sub Directories** – This option ensures eScan scans all the sub directories recursively under every directory and not only the first level of directories.
- **Heuristic** – Heuristic scanning is almost identical to signature scanning, which instead of looking for specific signatures looks for certain instructions or commands within a program/application. This results in the detection of potentially malicious function in program/application.
- **Cross File System** that facilitates scanning of files over cross-file systems.

- **Follow Symbolic Links:** scans the files following the symbolic links.
- **Memory Scan:**

You can restore default eScan settings by clicking **Default**.

Schedule Scan

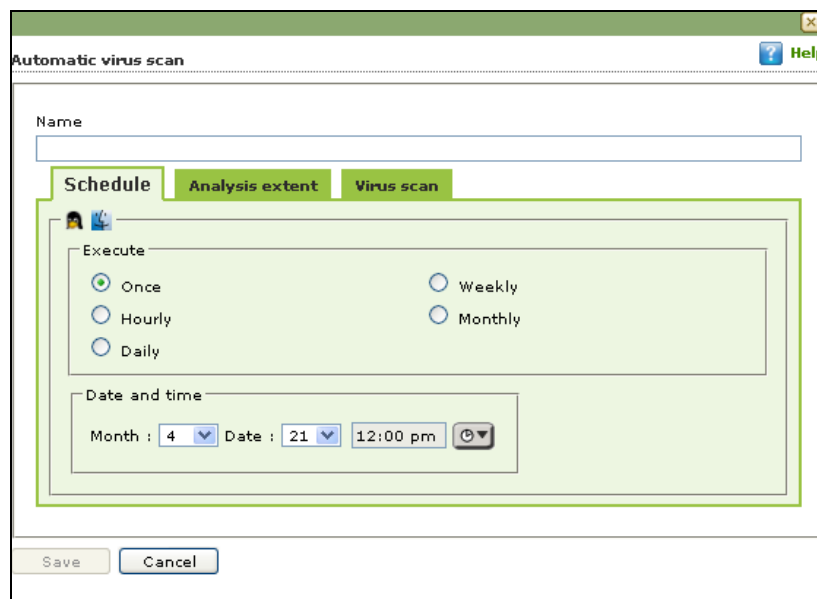


It lets you add a task for scheduling a scan.

Adding a task - It lets you schedule and define options for Analysis extent and the files or folders to be scanned.

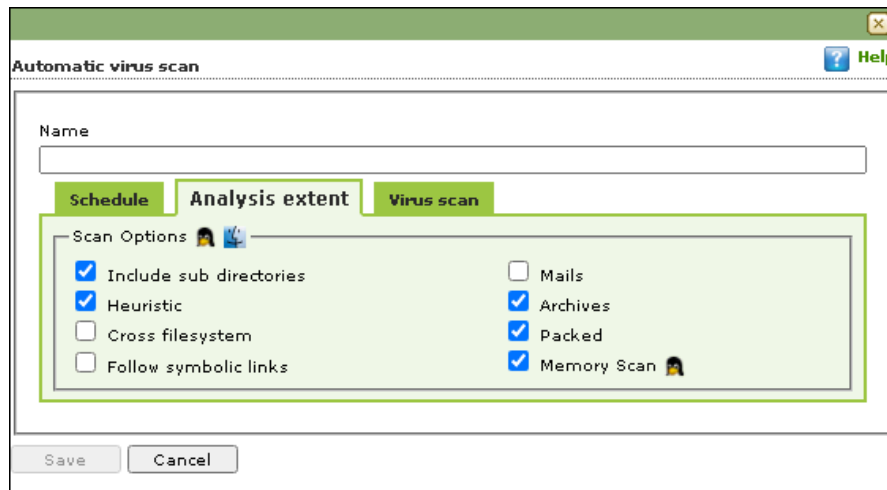
Automatic Virus Scan

Schedule



Using this tab you can define the task name and schedule it as desired. You can schedule once, Weekly basis, every hour, monthly or daily. It also lets you schedule virus scan at desired date and time.

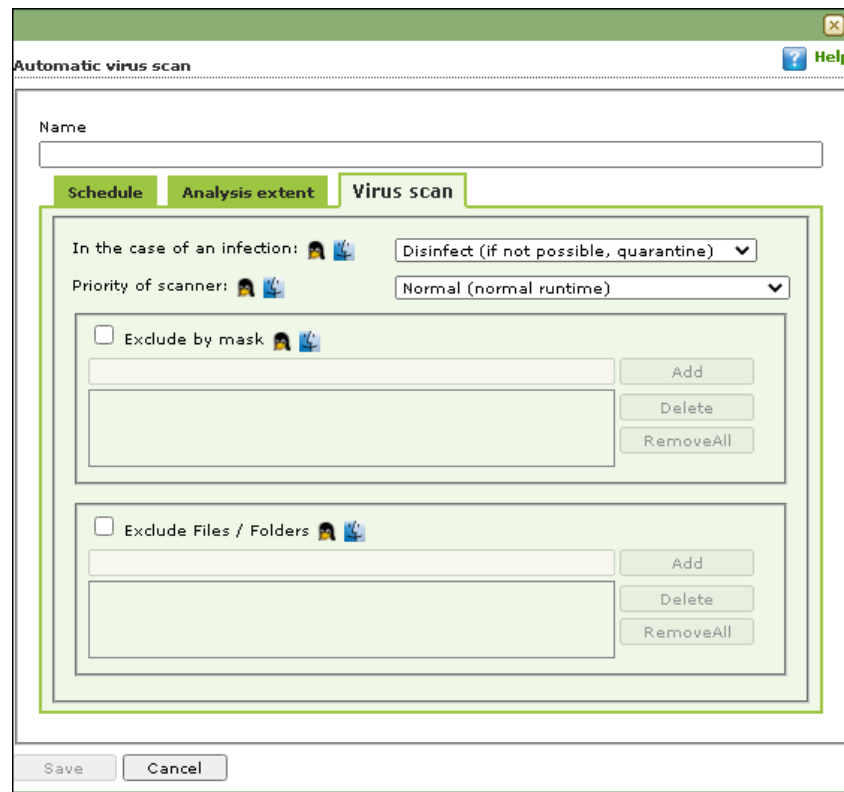
Analysis Extent



Using this tab you can define the scan options for Linux and Mac computers connected to the network.

- **Include sub Directories** – This option lets you include sub directories while conducting an automatic scan.
- **Heuristic Scan** – Heuristic scanning is almost identical to signature scanning, which instead of looking for specific signatures looks for certain instructions or commands within a program/application. This results in the detection of potentially malicious function in program/application.
- **Cross File System** that facilitates scanning of files over cross-file systems.
- **Symbolic Link Scanning** scans the files following the symbolic links.
- **Mails** - It indicates scanning the mail files. By default, it is selected. Select this check box if you want eScan real-time protection to scan mails.
- **Archives** - It indicates the archived files, such as zip, rar, and so on. Select this check box if you want eScan real-time protection to scan archived files.
- **Packed** - It indicates the compressed executable. Select this check box if you want eScan real-time protection to scan packed files.
- **Memory Scan** -

Virus Scan



Actions in case of Infection [Drop-down]

It displays a list of actions eScan should take, in case of virus detection. By default, Disinfect (if not possible, quarantine file) option is selected. Following are the types of actions:

- **Log Only:** It indicates or alerts the user about the infection detected.
- **Disinfect (if not possible, log):** It tries to disinfect and if disinfection is not possible it logs the information of only the infected object.
- **Disinfect (if not possible, delete file):** It tries to disinfect and if disinfection is not possible it deletes the infected object.
- **Disinfect (if not possible, quarantine file):** It tries to disinfect and if disinfection is not possible it quarantines the infected object.
- **Delete:** Infected objects are deleted with this option.
- **Quarantine:** Infected objects are quarantined with this option.

Exclude file types (Mask) - Select this check box if you want eScan real-time protection to exclude specific files, and then add the directories and files that you want to exclude by clicking **Add**. eScan lets you Remove any or all Added Files whenever required.

Exclude Folders and files - Select this check box if you want eScan real-time protection to exclude Folders and files from scanning. eScan lets you add; Remove any or all Added Files or Folders whenever required.

Schedule Update 🐧

This module lets you schedule the updates for Linux computers.

Schedule Update Help

☐ Automatic Download

Start at Every hours(s)

☒ Schedule Download

☒ Once
 ☐ Weekly
☐ Hourly
 ☐ Monthly
☐ Daily

Date and time

Month : Date :

- The updates can be downloaded automatically with **Automatic Download** option.
- The updates can be downloaded on a schedule basis with **Schedule Download** option. Select intervals and time basis as per your preferences.

Administrator Password 🐼

Administrator Password lets you create and change password for administrative login of eScan protection center for Linux computers. It also lets you keep the password as blank, wherein you can login to eScan protection center without entering any password. It also lets you define uninstallation password which will be required before uninstalling eScan Client from managed computers manually. The user will not be able to uninstall eScan Client without entering uninstallation password.

To Add/Change eScan administrator password

Set Password

Click this option, if you want to set password.

Blank Password

Click this option, if you do not want to set any password for login.

When you click this option, the **Enter new Password** and **Confirm new Password** fields become unavailable.

Enter new Password

Enter the new password.

Confirm new Password

Re-enter the new password for confirmation.

Use separate uninstall password

Click this option, if you want to set password before uninstallation of eScan Client.

Enter uninstall Password

Enter the uninstallation password.

Confirm uninstall Password

Re-enter the uninstallation password for confirmation.

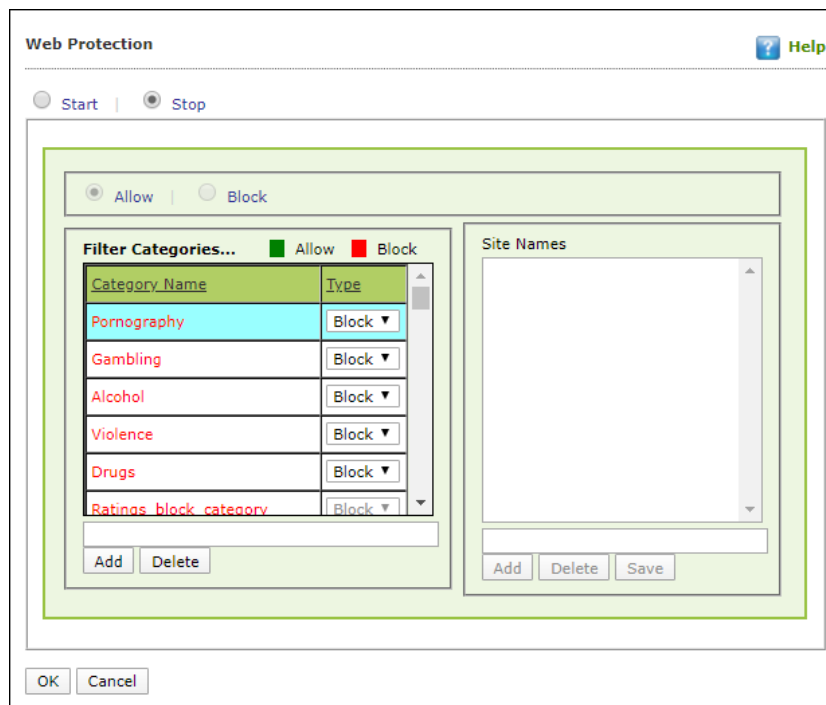
After filling all fields, click **OK**. The Password will be saved.

Web Protection

Web Protection module lets you block websites containing pornographic or offensive material for Linux computers. This feature is extremely beneficial to parents because it prevents kids from accessing websites containing harmful or restricted content. Administrators can also use this feature to prevent employees from accessing non-work-related websites during work hours. You can configure the following settings.

Start/Stop

It lets you enable/disable **Web-Protection** module. Click the appropriate option.



The screenshot shows the 'Web Protection' configuration window. At the top, there are radio buttons for 'Start' and 'Stop', with 'Stop' selected. Below this, there are radio buttons for 'Allow' and 'Block', with 'Allow' selected. The main area is divided into two sections: 'Filter Categories...' and 'Site Names'. The 'Filter Categories...' section contains a table with columns 'Category Name' and 'Type'. The table lists several categories: Pornography, Gambling, Alcohol, Violence, Drugs, and Ratings block category, all with 'Block' selected in the 'Type' column. Below the table are 'Add' and 'Delete' buttons. The 'Site Names' section is empty, with 'Add', 'Delete', and 'Save' buttons below it. At the bottom of the window are 'OK' and 'Cancel' buttons.

Category Name	Type
Pornography	Block
Gambling	Block
Alcohol	Block
Violence	Block
Drugs	Block
Ratings block category	Block

You can configure the following settings.

Filtering Options

This tab has predefined categories that help you control access to the Internet.

Status

This section lets you allow or block access to specific websites based on Filter Categories. You can set the status as **Active** or **Block** web access. Select the **Block Web Access** option if you want to block all the websites except the ones that have been listed in the **Filter Categories**. When you select this option, only **Filtering Options** and **Pop-up Filter** tabs are available.

Filter Categories

This section uses the following color codes for allowed and blocked websites.

- **Green:** It represents an allowed websites category.
- **Red:** It represents a blocked websites category.

The filter categories used in this section include categories like Pornography, Gambling, Chat, Alcohol, Violence, Drugs, Ratings block category, Websites Allowed, etc. You can also add or delete filter categories depending on your requirement.

Category Name

This section shows the **Words/Phrases** list. It lists the words or phrases present in the selected category. In addition, the section displays the **Site Names** list, which lists the websites belonging to the selected category. You can also add or delete filter categories depending on your requirement.

Filter Options

This section includes the **Add sites rejected by the filter to Block category** check box. Select this option if you want eScan to add websites that are denied access to the Block category database automatically.

Network Security 🐼

Network Security module helps to prevent the Reverse Shell Exploit and blocks the Port Scan. Enabling this features will prevents Zero-day attacks and all other cyber threats.

Network Security ⓘ Help

Reverse Shell Exploit Prevention

☐ Start ☒ Stop

☐ Enable White List

☐ bash ☐ python ☐ perl

Add Delete RemoveAll

☐ Enable Black List

☐ apache ☐ apache2 ☐ httpd

Add Delete RemoveAll

Block Port Scan

☐ Enable Block Port Scan

Excluded IP(Port Scan)

Add Delete RemoveAll

Default Save Cancel

Start/Stop

It lets you enable/disable **Network Security** module. Click the appropriate option.

After enabling this, you can configure the following settings:

Enable White List

Select this checkbox to whitelist the scripting languages, such as bash, Python, Perl, and more. You can add and delete the scripting languages from whitelisting.

- **Add:** To add a scripting language, select the language and click **Add**.
- **Delete:** To delete a scripting language, select a language and click **Delete**.
- **Remove All:** To remove all the whitelisted scripting language, click **Remove All**.

Enable Black List

Select this checkbox to blacklist the scripting languages, such as bash, Python, Perl, and more. You can add and delete the scripting languages from blacklisting.

- **Add:** To add a scripting language, select the language and click **Add**.
- **Delete:** To delete a scripting language, select a language and click **Delete**.
- **Remove All:** To remove all the blacklisted scripting language, click **Remove All**.

Block Port Scan

Enable Block Port Scan

Select this checkbox to enable the port scan option. You can add and delete the IP addresses that need to exclude from the port scan.

- **Add:** To add an IP, enter the IP address and click **Add**.
- **Delete:** To delete an IP, select the IP address and click **Delete**.
- **Remove All:** To remove all the excluded IP addresses, click **Remove All**.

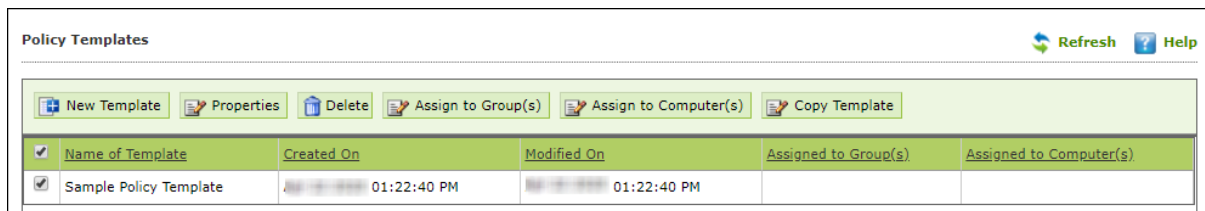
Assigning Policy Template to a group

There are two ways to assign the policy template to group.

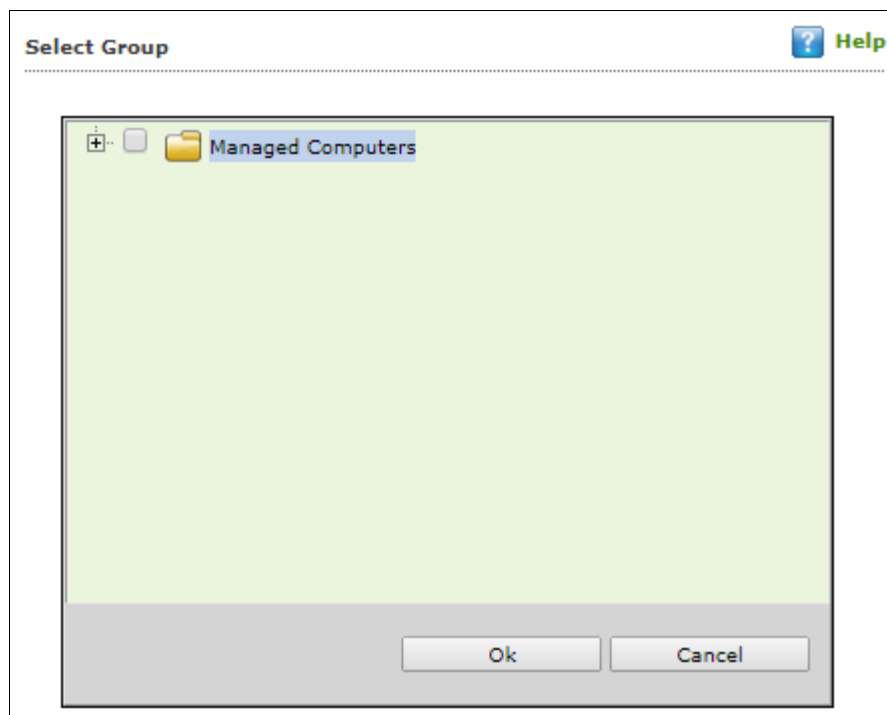
Method 1

To assign a Policy to a group,

1. In the Managed Computers screen, click **Policy Templates**.
Policy Templates window appears.
2. In the **Policy Templates** window, select a policy template.



3. Click **Assign to Group(s)**.
Select Group window appears.

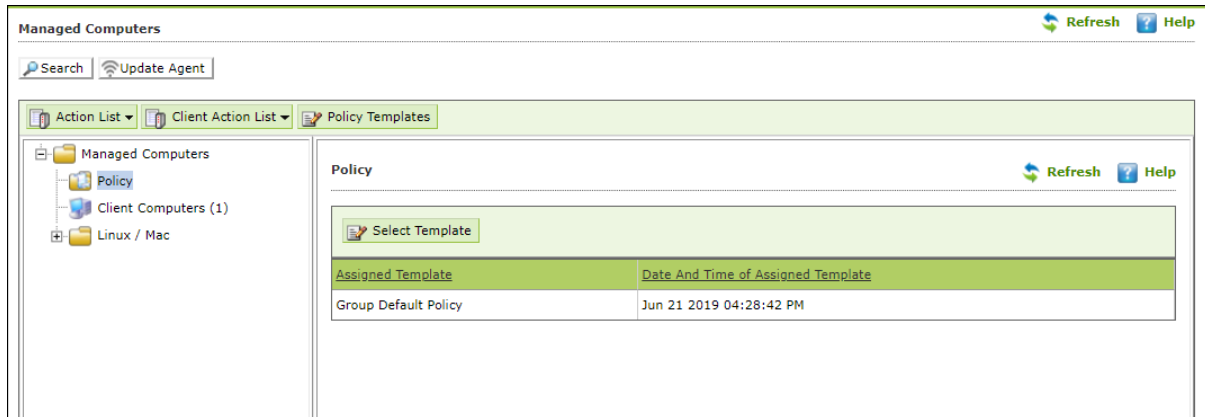


4. Select the group(s) and then click **OK**.
The policy will be assigned to the selected group(s).

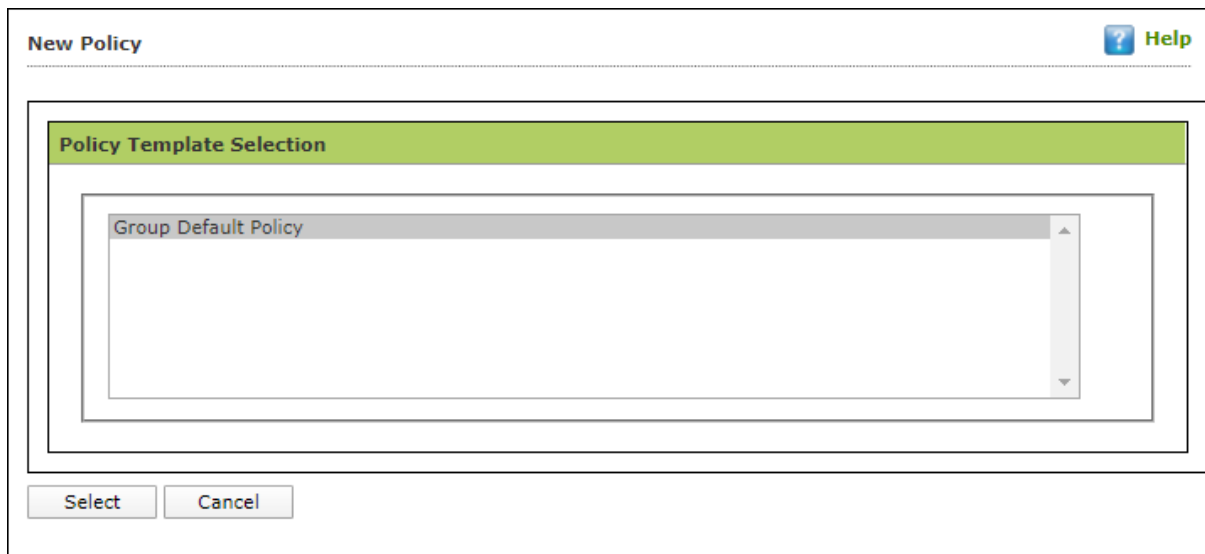
Method 2

To assign a Policy to the group:

1. In the Managed Computers folder tree, select a group.
2. Under the group, click **Policy**.
Policy pane appears on the right side.



3. In the right pane, click **Select Template**.
New Policy window appears.

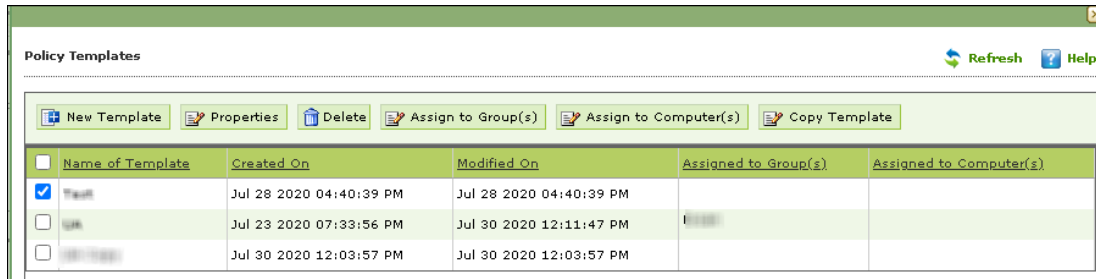


4. Select a policy template and then click **Select**.
The default Policy Template for group will be saved and updated.

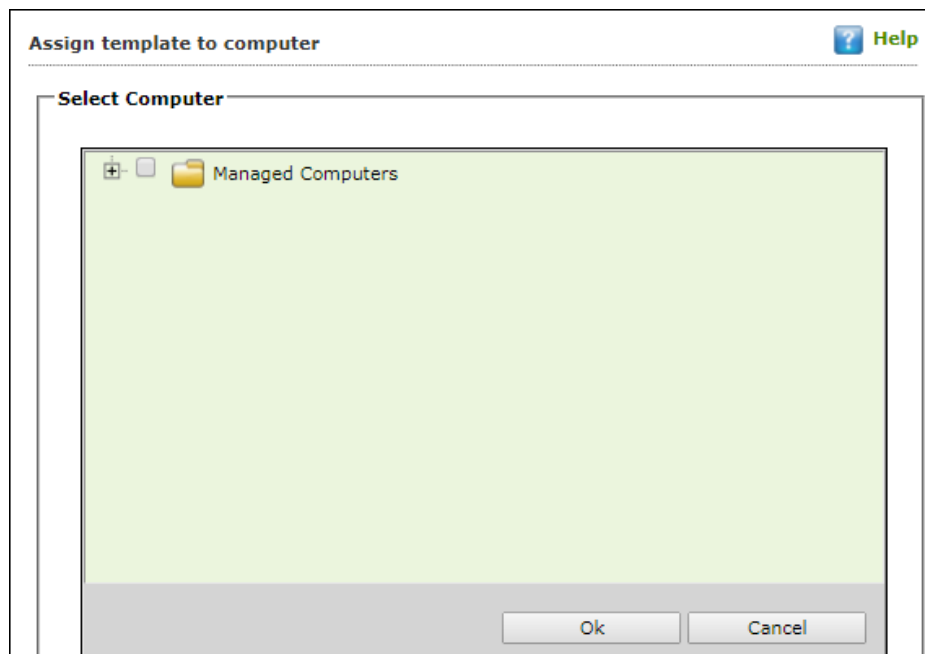
Assigning Policy Template to Computer(s)

To assign a policy template to computers,

1. In the **Policy Templates** window, select a policy.



2. Click **Assign to Computer(s)**.
3. Assign Template to computer window appears.

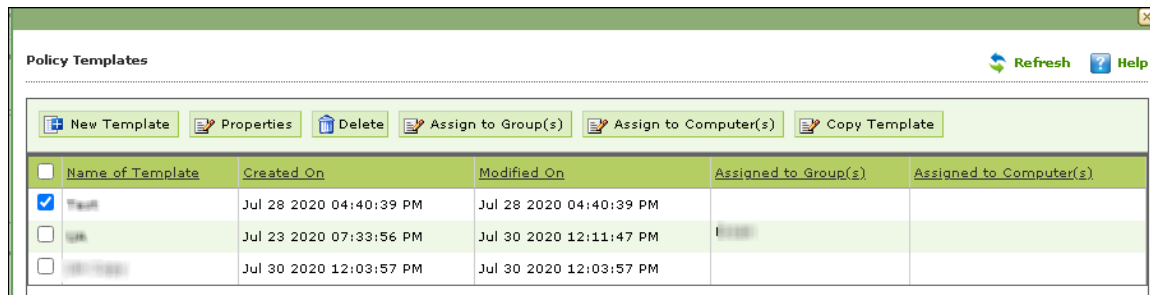


4. Click **Managed Computers**.
 5. Select the computer(s) and then click **OK**.
- The policy template will be assigned to the selected computers.

Copy a Policy Template

To copy a Policy Template,

1. In the Policy Templates window, select a policy.



3. Click **Copy Template**.
New Template window appears displaying settings from the original template.
4. Enter a name for the template.
5. Make the necessary changes and then click **Save**.
The template will be copied.

Parent Policy

The **Parent Policy** lets you to implement a change in policy setting to multiple policies at the same time. For example, if you want to make a policy change in a single module like **File Anti-Virus** in multiple policies; you can do this all at a time using Parent Policy.

To configure Parent Policy, follow the steps given below:

4. In the Managed Computers screen, click **Policy Templates**.
Policy Templates window appears.
5. In the Policy Template window, click **Parent Policy**.

Policy Templates				
<div> <input type="button" value="New Template"/> <input type="button" value="Properties"/> <input type="button" value="Parent Policy"/> <input type="button" value="Delete"/> <input type="button" value="Assign to Group(s)"/> <input type="button" value="Assign to Computer(s)"/> <input type="button" value="Copy Template"/> </div>				
<input type="checkbox"/>	Name of Template	Created On	Modified On	Assigned to Group(s)
<input type="checkbox"/>	Sample Policy Template	Sep 24 2019 12:33:42 PM	Sep 24 2019 12:33:42 PM	

Properties (Parent Policy) window appears displaying all the policies.

Properties (Parent Policy)

Policy Details

☐ File Anti-Virus

Assign To

☐ Anti-Spam

Assign To

☐ FireWall

Assign To

☐ Privacy Control

Assign To

☐ Mail Anti-Virus

Assign To

☐ Web Protection

Assign To

☐ EndPoint Security

Assign To

☐ Administrator Password

Assign To

☐ ODS/Schedule Scan

Assign To

☐ MWL Inclusion List

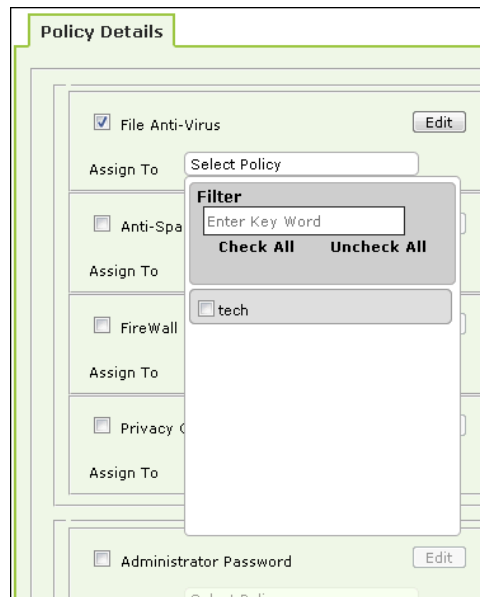
Assign To

☐ MWL Exclusion List

Assign To

6. Select and edit the required module according to your preferences.

7. Click **Assign To** drop-down and select the policies for which the parent policy changes should be applied.



8. Click **OK**. The Parent policy will be updated and changes will be applied to all the policies selected.

NOTE	Before disabling a module in Parent Policy, ensure that policies are unchecked from Assign To drop-down.
-------------	---

Data Encryption

The Data Encryption module lets you protect sensitive and confidential data from unauthorized access and data leak. With this module, the user can create a Vault that stores data in encrypted format.

The Vault is encrypted using 256-bit Advanced Encryption Standard (AES) and HMAC-SHA 256-bit key. A password is required to access the vault. After you access the vault, the data stored will be automatically decrypted. Vice versa, after you close the vault, the data stored will be automatically encrypted.

How to Create a Vault?

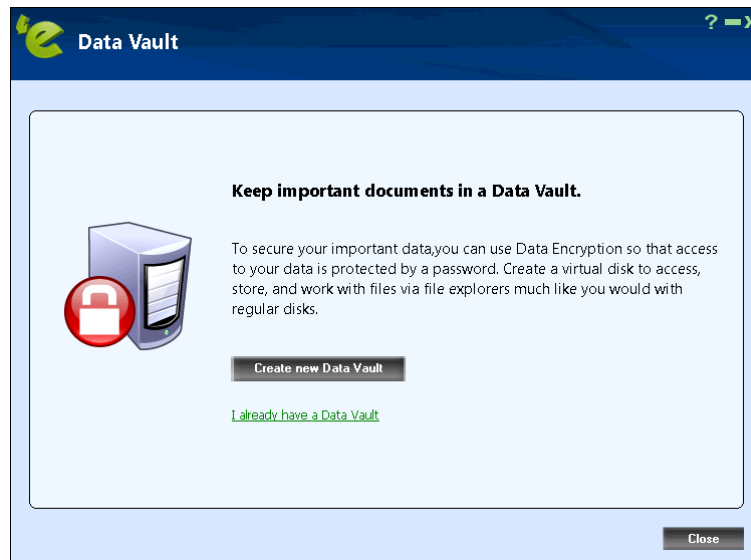
To create a vault, follow the steps given below:

1. Launch eScan.
2. Click **data encryption**.

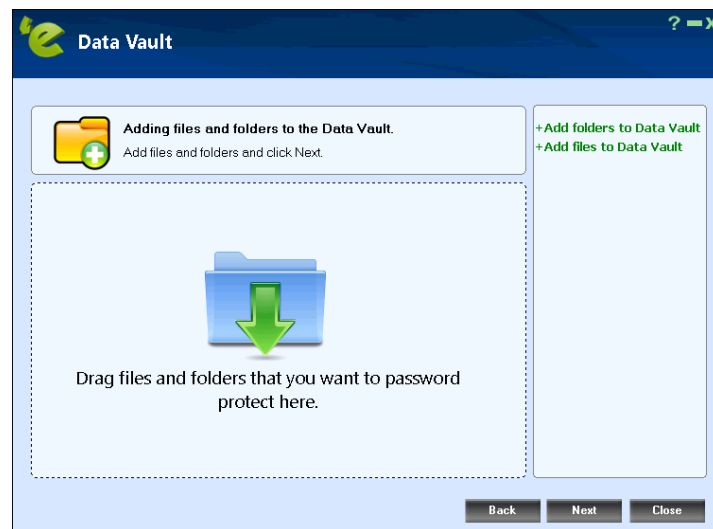


Data Vault window appears.

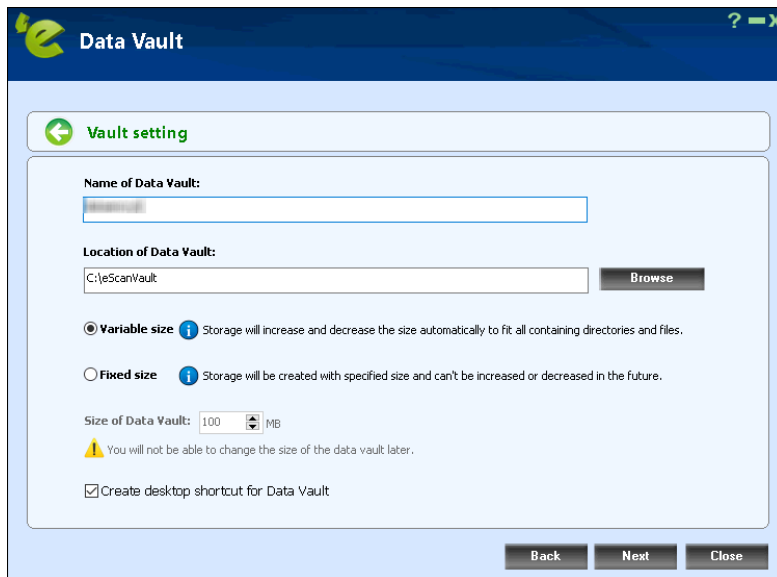
3. Click **Create new Data Vault**.



4. To add files or folders in Data Vault, click **Add folders to Data Vault** or **Add files to Data Vault**.



5. After adding required files and folder, click **Next**.
6. Configure the Data Vault:
 - **Name of Data Vault:** Enter a name for the vault.
 - **Location of Data Vault:** To select a custom location for Data Vault, click **Browse**. The default path for vault is **c:\eScanVault**.
 - Select a size for Data Vault, **Variable size** or **Fixed size**. If selected **Fixed size** enter the size in below field or use the arrow buttons to specify size.
 - Optionally, select the checkbox **Create desktop shortcut for Data Vault**.



Data Vault

← **Vault setting**

Name of Data Vault:

Location of Data Vault:
 Browse

☒ **Variable size** ⓘ Storage will increase and decrease the size automatically to fit all containing directories and files.
☐ **Fixed size** ⓘ Storage will be created with specified size and can't be increased or decreased in the future.

Size of Data Vault: MB

⚠ You will not be able to change the size of the data vault later.

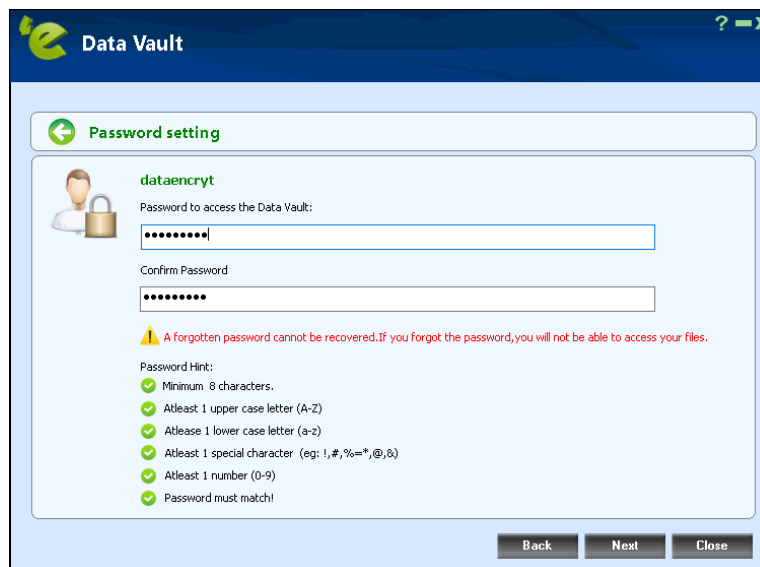
☒ Create desktop shortcut for Data Vault

Back **Next** **Close**

7. After filling all the details, click **Next**.
8. Read the **Password Hint** and then enter the password.

NOTE

A forgotten password cannot be recovered.
If you forgot the password, you cannot access your files.



Data Vault

← **Password setting**

dataencrypt

Password to access the Data Vault:

Confirm Password:

⚠ A forgotten password cannot be recovered.If you forgot the password,you will not be able to access your files.

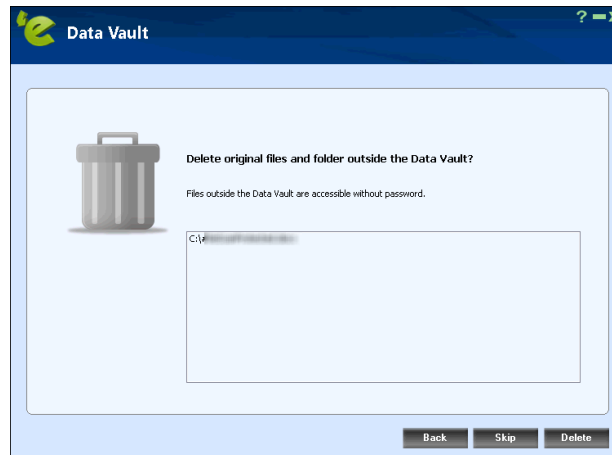
Password Hint:

- ✓ Minimum 8 characters.
- ✓ Atleast 1 upper case letter (A-Z)
- ✓ Atleast 1 lower case letter (a-z)
- ✓ Atleast 1 special character (eg: !, #, %, =, *, @, &)
- ✓ Atleast 1 number (0-9)
- ✓ Password must match!

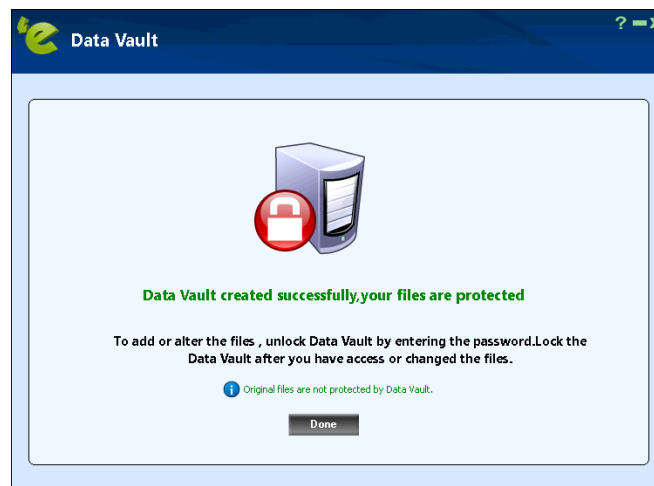
Back **Next** **Close**

9. Click **Next**.

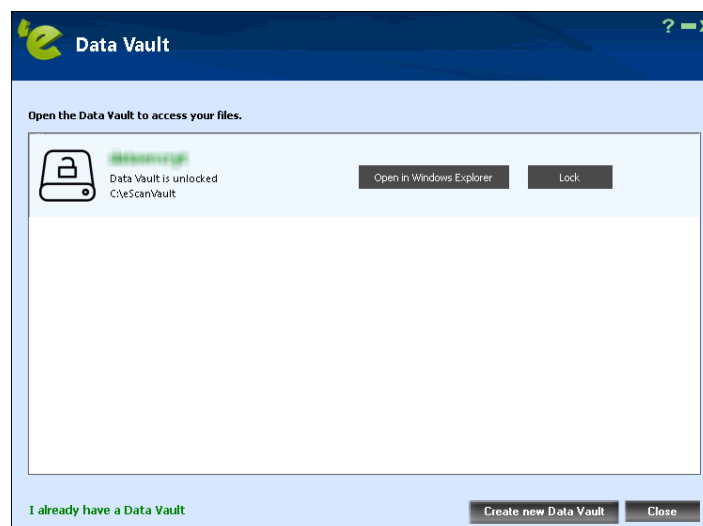
10. Data will be copied to the Data Vault. If you wish to delete the original files and folders outside the data vault by clicking **Delete** or else click **Skip**.



11. Click **Finish**. You will be forwarded to the following screen. Click **Done**.

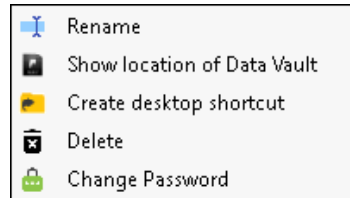


12. The Data Vault will be created and get displayed on the data encryption list. To encrypt your data, click **Lock**.



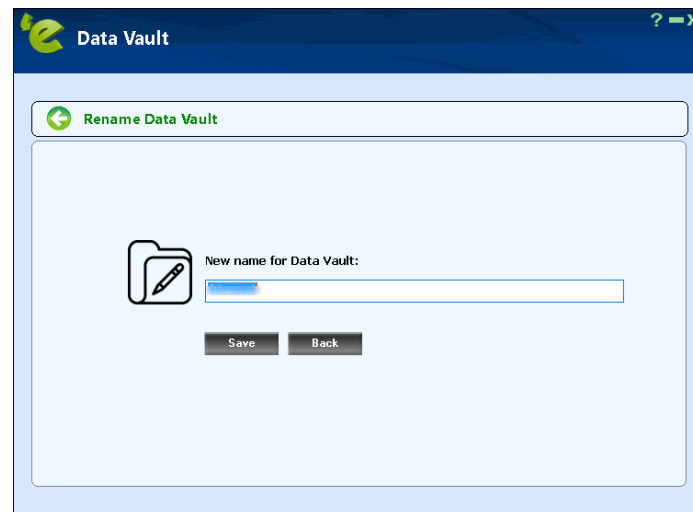
13. Click **Close**. The created Data Vault will be encrypted.

After the data vault is locked, you will get **More** button displayed the right-hand side of the screen. Through this option, you will get the following setting to configure the data vault:



Rename

You can rename the existing data vault. After clicking on this option, you will get the following screen, where you can rename the vault.



After renaming, click **Save**.

Show location of Data Vault

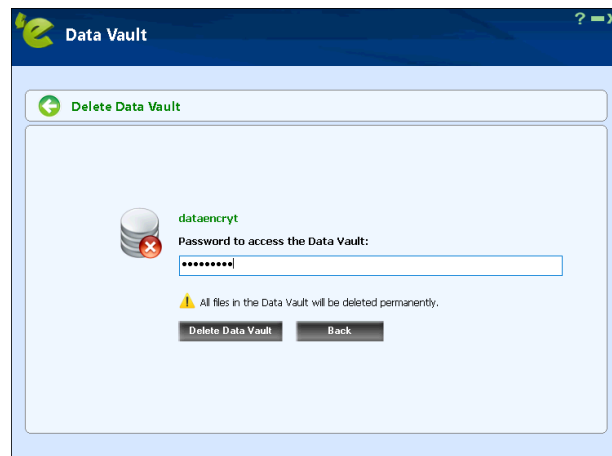
This option will open the location where data vault is created.

Create desktop shortcut

This option will create shortcut for the created vault for accessing it easily.

Delete

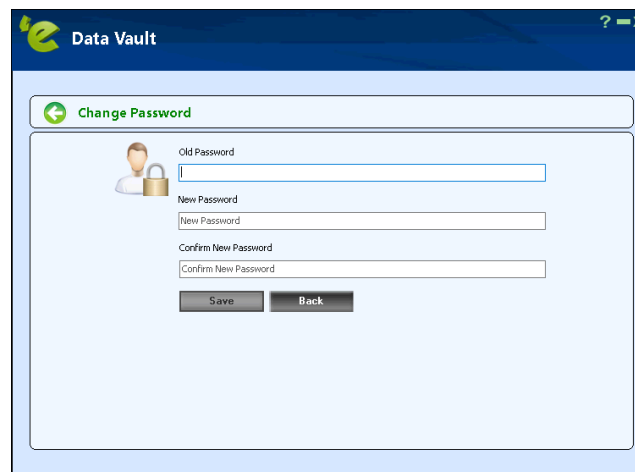
You can delete the existing data vault. Click on this option, you will get the following screen prompting for password.



After entering the password, click **Delete Data Vault**. This will delete the selected data vault.

Change Password

This option allows you to change the password set for the data vault. Click this option, you will be forwarded to the following screen.



Enter the **Old Password**, **New Password**, and **Confirm New Password**. Click **Save**. This will change the password of the data vault.

Note

If you selected **Create desktop shortcut for Data Vault** checkbox, it will create a shortcut of data vault (.

Policy Criteria Templates

This button allows to add criteria template based on the endpoints conditions.

Adding a Policy Criteria Template

To define Policy Criteria Template, follow the steps given below:

1. In the Managed Computers screen, click **Policy Criteria Templates**.
Policy Criteria screen appears.

Name of Criteria	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
------------------	------------	-------------	----------------------	-------------------------

2. Click **New Criteria**.
Policy Criteria screen displays parameter for creation.

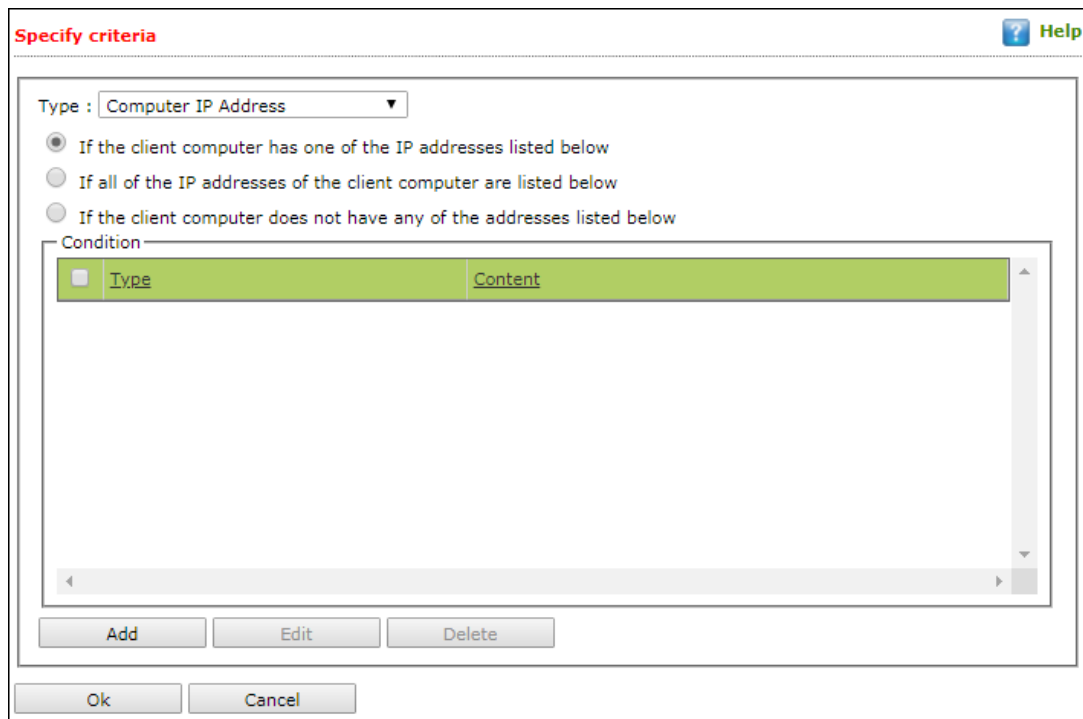
Criteria Name:

Description:

Conditions for criteria:

3. Enter **Name** and **Description**.
4. Click **Add** drop-down.
5. Click **Add AND Condition**.

Specify Criteria screen appears.



Specify criteria ? Help

Type : Computer IP Address ▼

☒ If the client computer has one of the IP addresses listed below
☐ If all of the IP addresses of the client computer are listed below
☐ If the client computer does not have any of the addresses listed below

Condition

Type	Content
------	---------

Add Edit Delete

Ok Cancel

6. Click the **Type** drop-down. It displays following options:

- Computer IP Address
- Management Server Connection
- Users
- Machine Name

Depending upon the option, the conditions and settings vary.

Computer IP Address

1. Select the appropriate condition.
2. Click **Add**.

Address window appears.



Address

Type : IP Address ▼

IP Address :

Ok Cancel

3. Enter the IP address.
4. Click **OK**.

The Policy Criteria Template for an IP Address will be saved.

Management Server Connection

Specify criteria

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

Ok Cancel

1. Select the appropriate condition.
2. Click **OK**.

The Policy Criteria Template for Management Server Connection will be saved.

Users

Specify criteria Help

Type : **Users** ▼

☒ If the client computer has one of the Username listed below

Condition

☐ Username▲

Add Add AD users Edit Delete

Ok Cancel

Adding Local Users

1. To add local users, click **Add**.
Username window appears.

Username

Username

Ok Cancel

2. Enter a Username.
 3. Click **OK**.
- The local user will be added.

Adding Active Directory Users

To add Active Directory users, follow the steps given below:

1. Click **Add AD Users**.
- Add Active Directory Users window appears.

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*:

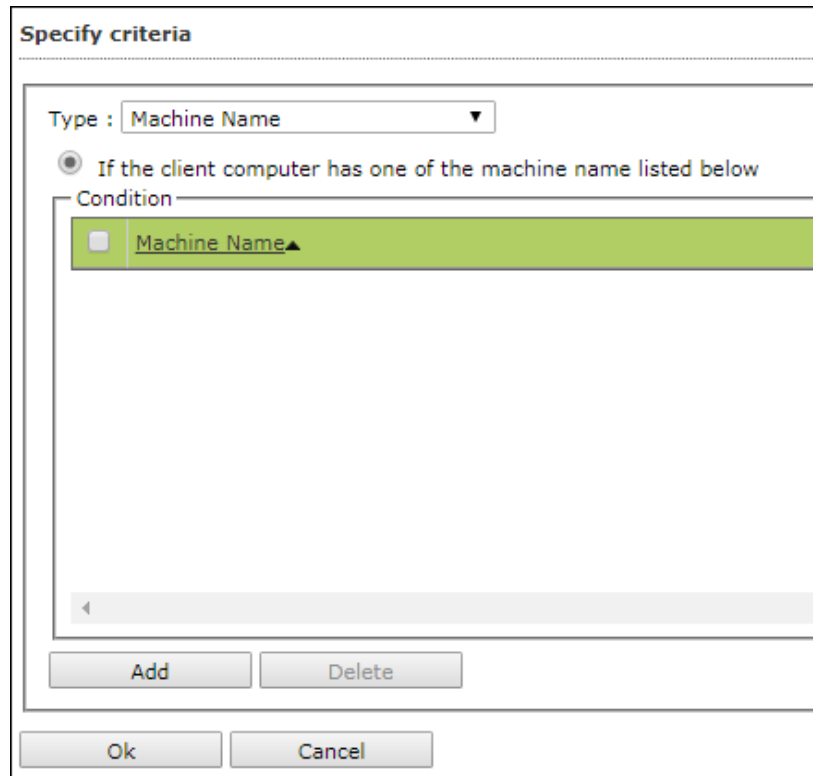
Search Results

Users

Selected Users

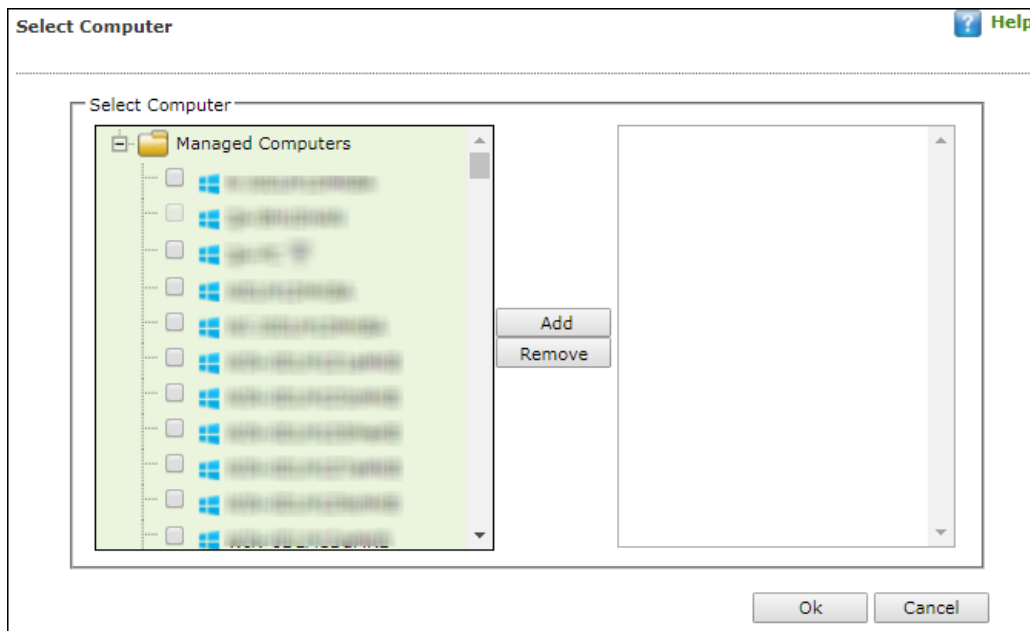
2. Enter data in mandatory fields.
 3. Click **Search**.
 4. Search Results section displays a list of discovered users in **Users** list. Select a user and then click button to add the user to **Selected Users** list. Vice versa the added user can be moved from Selected Users to Users by clicking .
 5. Click **OK**.
- The Policy Criteria Template for Users will be saved.

Machine Name



The 'Specify criteria' dialog box is shown. It has a title bar 'Specify criteria'. Inside, there is a 'Type' dropdown menu set to 'Machine Name'. Below it, a radio button is selected with the text 'If the client computer has one of the machine name listed below'. Under this, there is a 'Condition' section with a list box containing one item: 'Machine Name' with a small upward arrow icon. At the bottom of the list box are 'Add' and 'Delete' buttons. At the very bottom of the dialog are 'Ok' and 'Cancel' buttons.

1. Click **Add**. Select Computer screen appears displaying all managed computers.



The 'Select Computer' dialog box is shown. It has a title bar 'Select Computer' and a 'Help' button. Inside, there is a 'Select Computer' section. On the left, there is a tree view showing 'Managed Computers' with a list of computer names, each preceded by a checkbox. To the right of this list are 'Add' and 'Remove' buttons. On the far right, there is an empty list box. At the bottom of the dialog are 'Ok' and 'Cancel' buttons.

2. Select the computer(s) to be added under this criterion and click **Add > OK**.
The Policy Criteria Template for selected machines will be saved.

Viewing Properties of a Policy Criteria template

To view the properties of a Policy Criteria Template, follow the steps given below:

1. Select a policy criteria template.
2. Click **Properties**.

Policy Criteria				
<div> New Criteria Properties Delete Criteria Assign To </div>				
<input checked="" type="checkbox"/>	Name of Criteria	Created On	Modified On	Assigned to Group(s)
<input checked="" type="checkbox"/>	aaa	Sep 26 2019 03:44:12 PM	Sep 26 2019 03:44:12 PM	Group Default Policy Managed Computers

Policy Criteria window appears.

Policy Criteria

Criteria Name: aaa

Description:

Conditions for criteria:

Add

Edit

Delete

Condition

☐ If all of the IP addresses of the client computer are listed below

- 192.168.0.01

Save

Close

3. Make the necessary changes and click **Save**.
The Policy Criteria template will be saved and updated.

Copying a Policy Template

To copy a Policy Template, follow the steps given below:

1. In the Policy Templates window, select a policy.

Policy Templates				
<div> New Template Properties Parent Policy Delete Assign to Group(s) Assign to Computer(s) Copy Template </div>				
<input checked="" type="checkbox"/>	Name of Template	Created On	Modified On	Assigned to Group(s)
<input checked="" type="checkbox"/>	Sample Policy Template	Sep 24 2019 12:33:42 PM	Sep 24 2019 12:33:42 PM	

2. Click **Copy Template**.
New Template window appears displaying settings from the original template.
3. Enter a name for the template.

4. Make the necessary changes and click **Save**.
The template will be copied.

Deleting a Policy Criteria template

To delete assigned policy criteria template, follow the steps given below:

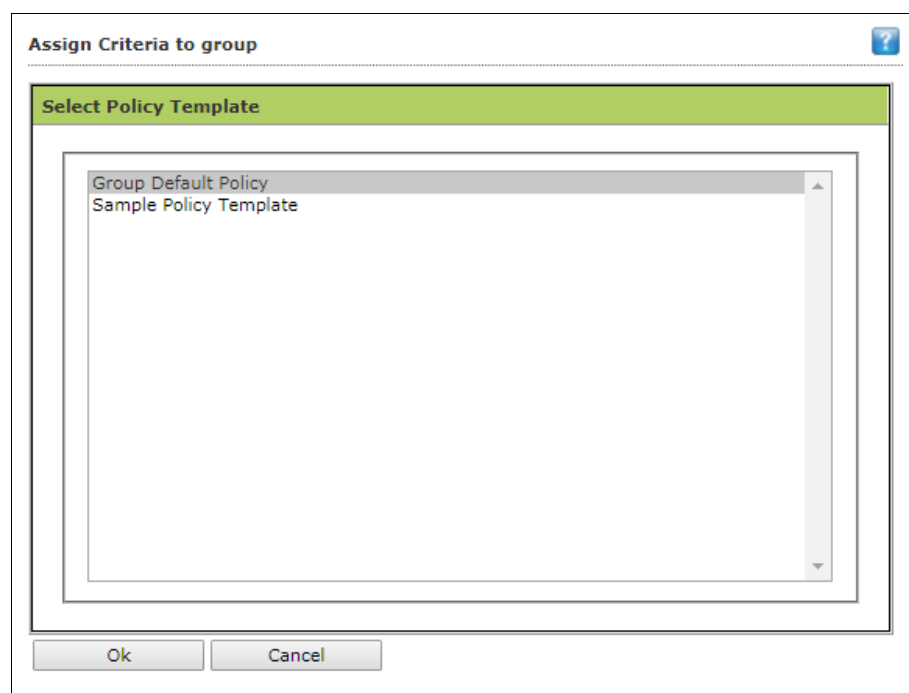
The Policy Criteria window displays to which group or computer the template is assigned in Assigned to Group(s) or Assigned to Computer(s) column.

For explanation, we are following the procedure as per the screenshot below

1. Select a policy criteria template.
2. Click **Assign To > Groups**.

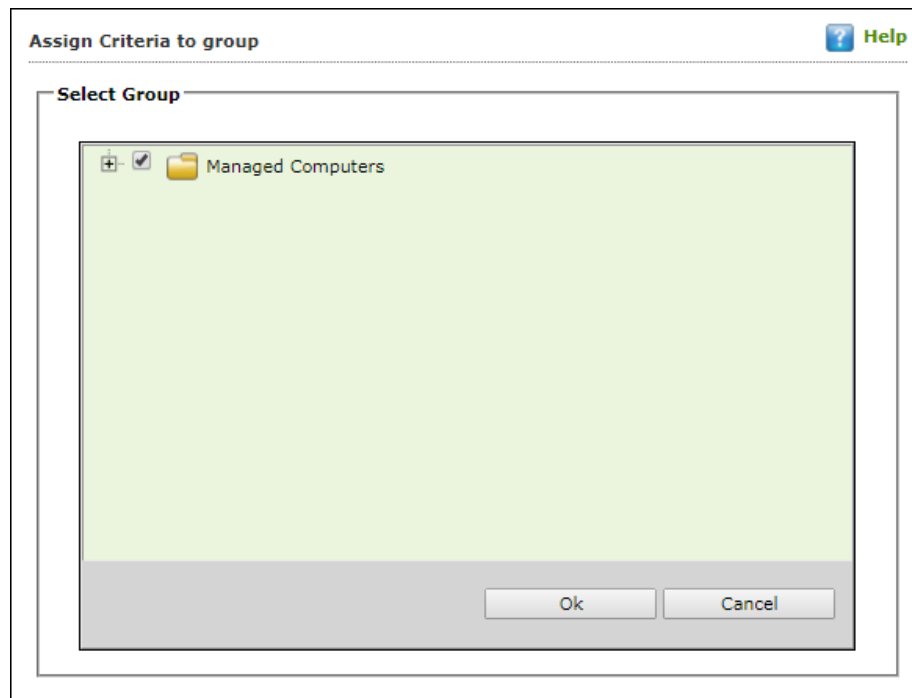
Policy Criteria Refresh Help				
New Criteria Properties Delete Criteria Assign To ▼				
<input checked="" type="checkbox"/>	Name of Criteria	Created On	Modified On	
<input checked="" type="checkbox"/>	aaa	Sep 26 2019 03:44:12 PM	Sep 26 2019 03:44:12 PM	Group Default Policy Managed Computers

Assign Criteria to Group window appears.



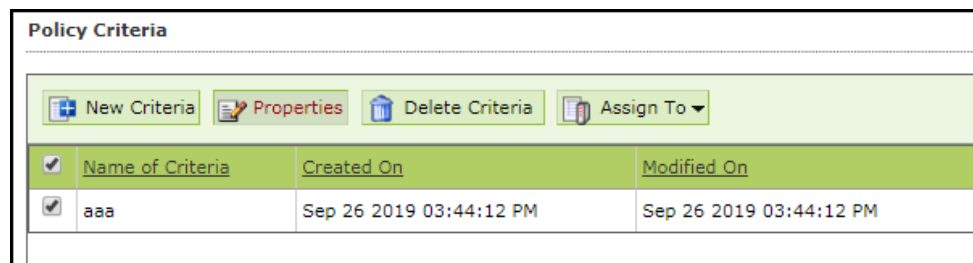
3. Click **Group Policy Template > OK**.

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.



6. Select the template.
 7. Click **Delete Criteria**.
- The Policy Criteria Template will be deleted.

Unmanaged Computers

To install eScan Client, define policies and tasks on the basis of group, it is necessary to move computers to the created groups. You can move the computers from **Unmanaged Computers** to desired groups created in the **Managed Computers** using the following submodules:

- Network Computers
- IP Range
- Active Directory
- New Computers Found

Network Computers

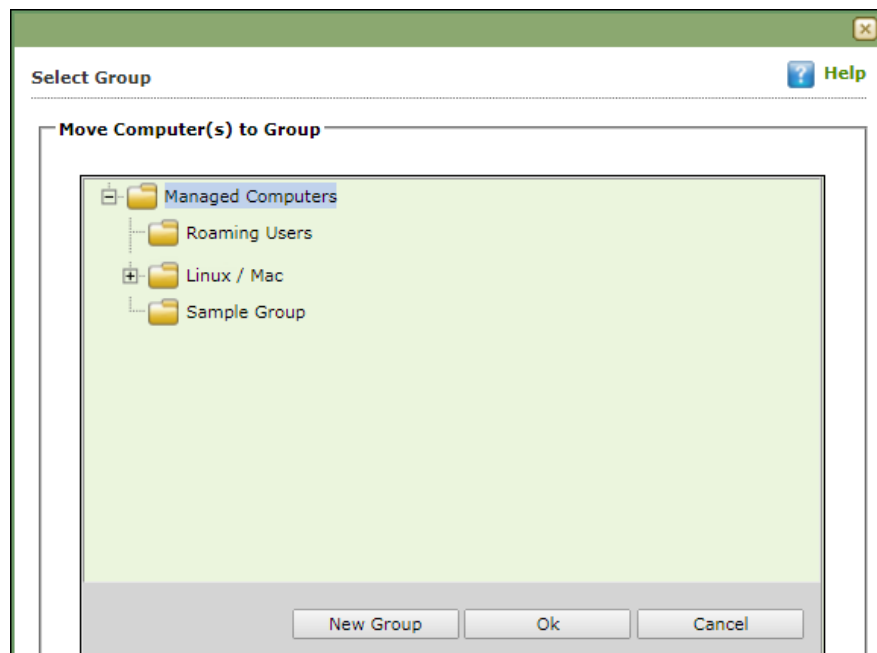
This submodule displays a list of available networks. You can move the computers from the list of computers present in the Network Computers using the following steps –

1. In the navigation panel, click **Unmanaged Computers > Network Computers**.
2. Click **Microsoft Windows Network**.
3. Select the workgroup from where you want to move computers to the group created in Managed Computers section. A list of computers appears.



4. Select the computer(s) you want to move to the desired groups.
5. Click **Action List > Move to Group**. Select Group window appears.

6. Click **Managed Computers** tree to view the groups.

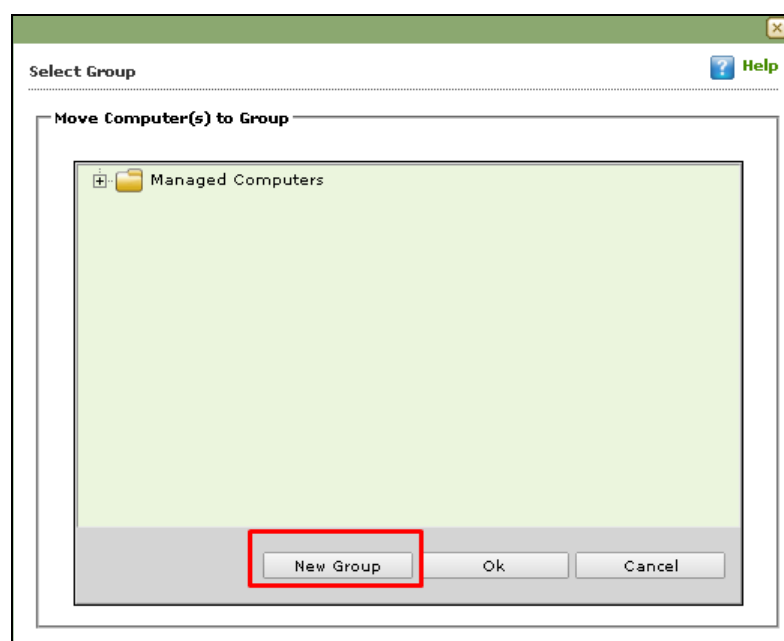


7. Select the group where you wish to move the selected computer(s) and click **OK**.
The selected computer(s) will be moved to the group.

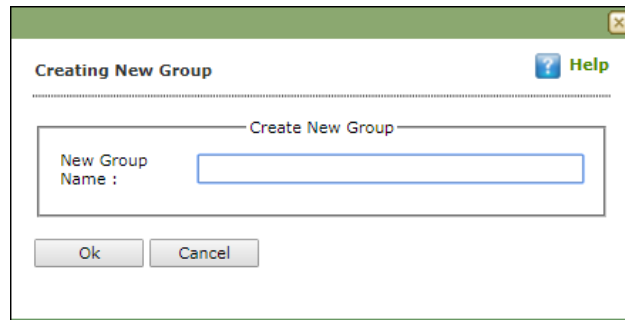
Creating a New Group from the Select Group window

To create a new group from the Select Group window, follow the steps given below:

1. In the Select Group window, click **Managed Computers > New Group**.



Creating New Group window appears.



The 'Creating New Group' dialog box has a title bar with a green gradient and a close button. Below the title bar is a 'Help' button with a question mark icon. The main area contains a label 'New Group Name :' followed by a text input field. At the bottom are 'Ok' and 'Cancel' buttons.

2. Enter a name for the group.
3. Click **OK**. A new group will be created.

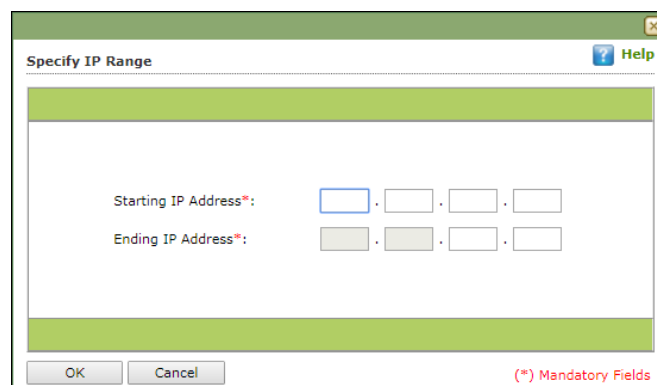
IP Range

The **IP Range** submodule lets you scan the desired IP address or range of IP address and add the required computers to any of the managed groups. It also lets you add, search and delete an IP range.

Adding New IP Range

To add an IP range, follow the steps given below:

1. In the IP range screen, click **New IP Range**.
Specify IP Range window appears.



The 'Specify IP Range' dialog box has a title bar with a green gradient and a close button. Below the title bar is a 'Help' button with a question mark icon. The main area contains two rows of IP address input fields. The first row is labeled 'Starting IP Address*' and the second row is labeled 'Ending IP Address*'. Each row has four input boxes separated by dots. At the bottom are 'OK' and 'Cancel' buttons. A red note at the bottom right says '(*) Mandatory Fields'.

2. Enter the Starting and Ending IP address.
3. Click **OK**. The IP Range will be added.

NOTE

Please enter the start and end IP address even if you want to search for single IP address, both the entries will have the same IP address in such a case. The selected IP Range will be added to the IP Range tree.
When you select the IP Range all computers present in that IP Range will be displayed on the interface in the right.

Other details like IP Address of the computer, its group, Protection status (Unmanaged/Unknown/Protected/Not installed, Critical/Unknown); the table also displays Status of all modules of eScan.

Moving an IP Range to a Group

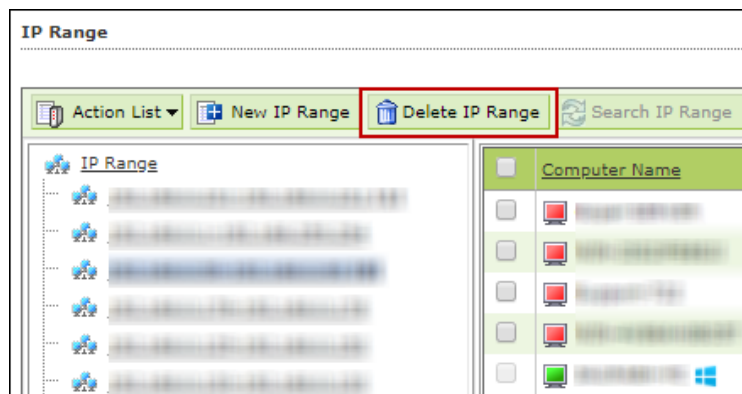
To move an entire IP range to a group, follow the steps given below:

1. Select an IP range.
2. Select the checkbox next to Computer Name column.
3. Click **Action List** > **Move to Group**. Select Group window appears.
4. Select the destination group.
5. Click **OK**. The IP range will be moved to the specified group.

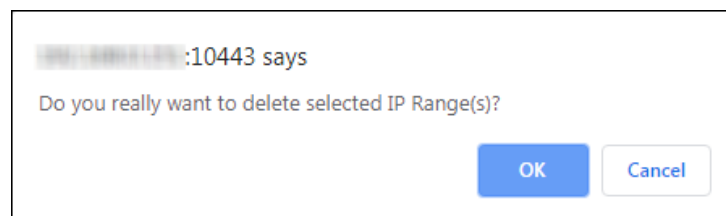
Deleting an IP Range

To delete an IP range, follow the steps given below:

1. Select an IP Range.
2. Click **Delete IP Range**.



A confirmation prompt appears.



3. Click **OK**. The IP range will be deleted.

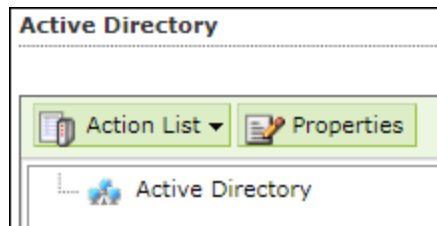
Active Directory

The Active Directory submodule lets you add computers from an Active Directory.

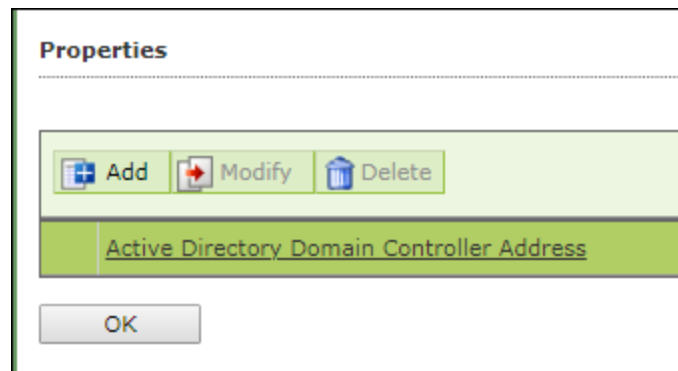
Adding an Active Directory

To add an Active Directory, follow the steps given below:

1. Click **Unmanaged Computers > Active Directory**.
2. Click **Properties**.



Properties window appears.

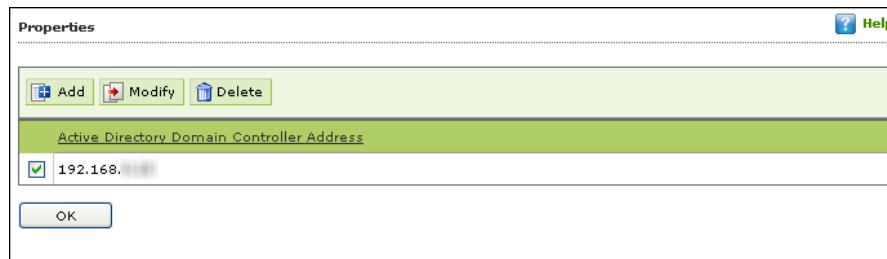


3. Click **Add**. Login Settings window appears.

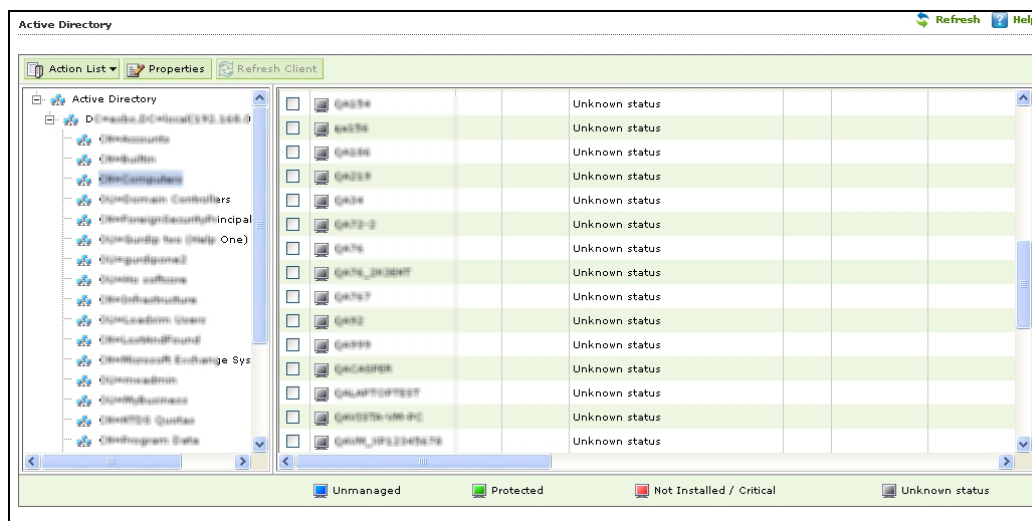
The screenshot shows a window titled "Login Settings" with a green header bar and a "Help" button. The main area has a green background. It contains several input fields with red asterisks indicating mandatory fields: "AD IP Address", "User name", "Password", "Confirm Password", "Use SSL Auth." (checkbox), and "AdsPort" (with the value "389" entered). At the bottom, there are "OK" and "Cancel" buttons. A red note at the bottom right says "(*) Mandatory Fields".

4. Fill in the required Login Credentials and click **OK**.

The details including IP Addresses from active directory will be added instantly.



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**.



Moving Computers from an Active Directory

To move computers from an Active Directory, follow the steps given below:

1. Click an Active Directory.
2. Select the computers you want to move to other group.
3. Click **Action List > Move to Group**.
Select Group window appears.
4. Select the Group and Click **OK**.

The selected computers will be moved to the selected group.

New Computers Found

The New Computers Found submodule displays list of all new computers connected to the network. With the Action List drop-down you can set Host Configuration, Move Computers to a Group, view Properties and Refresh Client. You can also export the New Computers List to .xls file format.

After the computers are moved from Unmanaged Computers to groups under Managed Computers, you can assign it tasks, Set host configuration, Manage Policies, Deploy/Upgrade Client or deploy a Hotfix on all or any of the Managed Computer individually or in group.

New Computers Found						
<input type="text" value="Search"/>						
<div> <div>Action List</div> <div>Filter Criteria</div> </div>						
	Computer Name	IP Address	User name	Last Seen	Belongs To	eScan Status
<input type="checkbox"/>	192.168.1.101	192.168.1.101		23 Sep 2019 10:59:59	Server	Unknown status
<input type="checkbox"/>	192.168.1.102	192.168.1.102		23 Sep 2019 10:59:54	Server	Unknown status
<input type="checkbox"/>	192.168.1.103	192.168.1.103		23 Sep 2019 11:00:12	Server	Unknown status
<input type="checkbox"/>	192.168.1.104	192.168.1.104		23 Sep 2019 11:00:12	Server	Unknown status
<input type="checkbox"/>	192.168.1.105	192.168.1.105		23 Sep 2019 10:59:54	Server	Unknown status
<input type="checkbox"/>	192.168.1.106	192.168.1.106		23 Sep 2019 10:59:54	Server	Unknown status
<input type="checkbox"/>	192.168.1.107	192.168.1.107		23 Sep 2019 11:00:01	Server	Unknown status

Filter Criteria

The Filter Criteria lets you filter new computers found according to date range.

New Computers Found	
<input type="text" value="Search"/>	
<div> <div>Action List</div> <div>Filter Criteria</div> </div>	
<div>Filter Criteria</div> <div> <div>Date Range</div> <div> <div>From (MM/DD/YYYY)</div> <div>11/06/2019</div> </div> <div> <div>To (MM/DD/YYYY)</div> <div>11/06/2019</div> </div> </div> <div> <div>Search</div> <div>Reset</div> </div>	

1. Select appropriate date in **From** and **To** fields.
2. Click **Search**.

A list of computers discovered by eScan in the date range will be displayed.

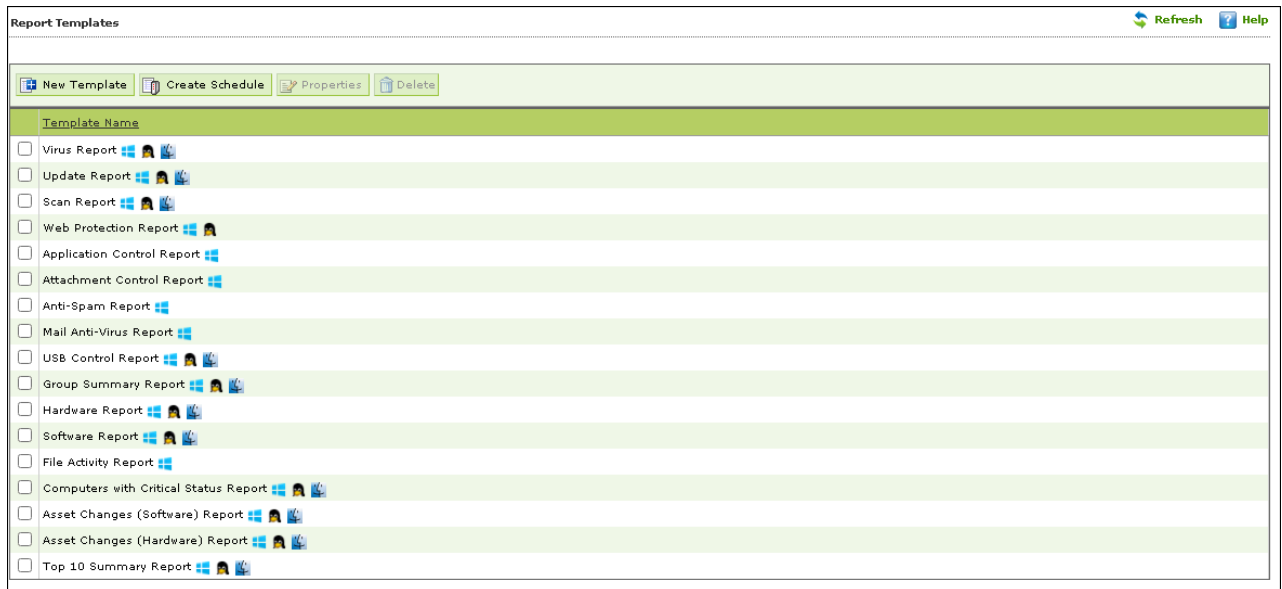
Action List

This drop-down provides following options:

- **Set Host Configuration:** To learn more, [click here](#).
- **Deploy/Upgrade Client:** To learn more, [click here](#).
- **Move to Group:** To learn more, [click here](#).
- **Refresh Client:** To learn more, [click here](#).
- **Export to Excel:** This option lets you to export the status of particular system into Excel reports.
- **Properties:** To learn more, [click here](#).

Report Templates

The Report Templates module lets you create template and schedule them according to your preferences. The module also consists of pre-loaded templates according to which the report can be created and scheduled.



Creating a Report Template

To create a Report Template, follow the steps given below:

1. In the navigation panel, click **Report Templates**.
2. Click **New Template**.

New Template screen appears.

3. Enter a name for the template.
4. Select a report enter.
Depending upon the report enter, the additional setting varies.
5. After making the necessary selections/filling data, click **Save**.
The template will be created according to your preferences.

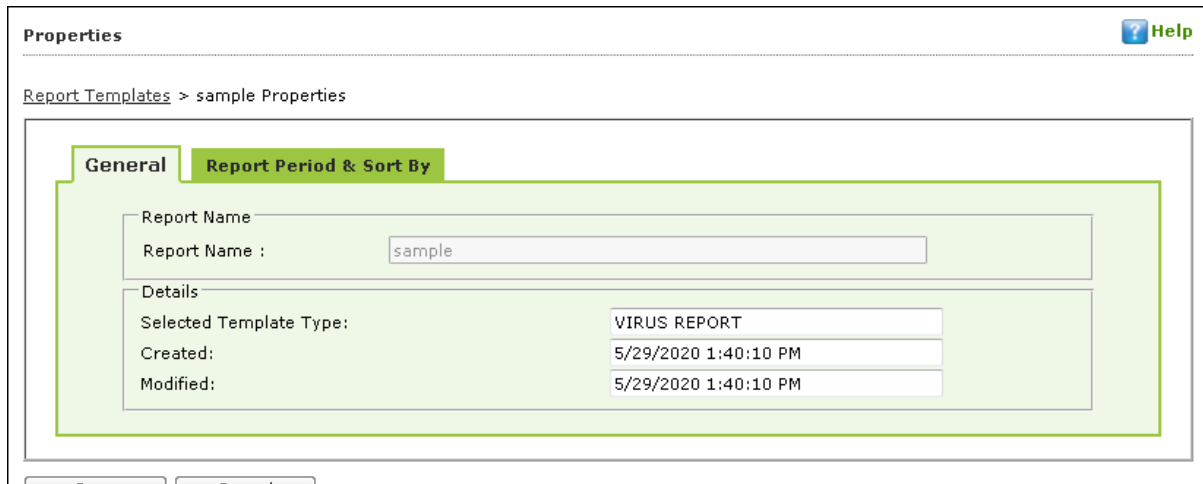
Creating Schedule for a Report Template

The Report Template module lets you create a new schedule for the report templates.
To learn more, [click here](#).

Viewing Properties of a Report Template

To view the properties of Report Template, follow the steps given below:

1. Select the Report Template whose properties you want to view.
2. Click **Properties**. Properties screen appears.



Properties Help

[Report Templates](#) > sample Properties

General **Report Period & Sort By**

Report Name
Report Name :

Details
Selected Template Type:
Created:
Modified:

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.

Report Scheduler > New Schedule

Report Name

New Report Name : *

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

2. In the Settings section, select preferred templates.
3. In the Select Condition section, select a condition for groups or specific computers.

Select Condition

☒ Generate a Report for Groups

☐ Generate a Report for a List of Computers

Select Target Groups

- ☐ Managed Computers

4. In the Send Report by email section, fill the required information to receive reports via email.

Send Report by Email

Report Sender*:

Report Recipient*:

Add

▲

▼

Delete

Mail Server IP Address:

Mail Server Port:

User Authentication:

Password Authentication:

* For Example: user@yourcompany.com

Select the Report Format

HTML page ▼

5. Select the preferred report format.
6. In Report Scheduling Settings section, make the necessary changes.

Report Scheduling Settings

☒ Enable Scheduler

☐ Manual Start

☒ Daily

☐ Mon ☐ Tue ☐ Wed ☐ Thu

☐ Weekly

☐ Fri ☐ Sat ☐ Sun

☐ Monthly

1 ▼

☐ Last Day of Month

☒ At

12:00 pm

Save

Cancel

7. Click **Save**.
New schedule will be created.

Viewing Reports on Demand

To view a report or a set of reports immediately,

1. Click **Report Scheduler > View & Create**.

New Schedule screen appears.

2. Select the **Template** options, the **Condition** and the **Target Groups**.
3. Click **View**.
4. A new window appears displaying the created report.

Clicking **Create Schedule** lets you create a new Schedule.

Managing Existing Schedules

The Report Scheduler module lets you manage the existing schedules.

Report Scheduler

Start Task
 Results
 Properties
 Delete
 New Schedule
 View & Create

<input type="checkbox"/>	Schedule Name	Report Recipient	Scheduler Type
<input checked="" type="checkbox"/>	Hardware	Hardware - 10/1/2019	Manually Start
<input type="checkbox"/>	New Report	New Report - 10/1/2019	Manually Start
<input type="checkbox"/>	New Report_1	New Report_1 - 10/1/2019	Automatic Scheduler

Generating Task Report of a Schedule

To generate a task report, select the preferred report schedule name and then click **Start Task**.

A task window appears displaying the name of the report being generated.

Viewing Results of a Schedule

To see the results of a schedule and its time stamp, select the report schedule and then click **Results**.

Results screen appears.

Results(Hardware)

[Report Scheduler](#) > Results

Status	Time
Completed	9/21/2019 12:25:25 PM

Cancel

Viewing Properties of a Schedule

To view the properties of a schedule,

1. Select a schedule.
 2. Click **Properties**.
- Properties screen appears.

Properties Help

Report Scheduler > Properties

General | Schedule | Settings | Groups

Schedule Name :*

Created:

Status:

(*) Mandatory Fields

The properties screen displays general properties and lets you configure Schedule, Settings and Groups settings.

Deleting a Schedule

To delete a report schedule

1. Select a schedule.
 2. Click **Delete**.
- A confirmation prompt appears.

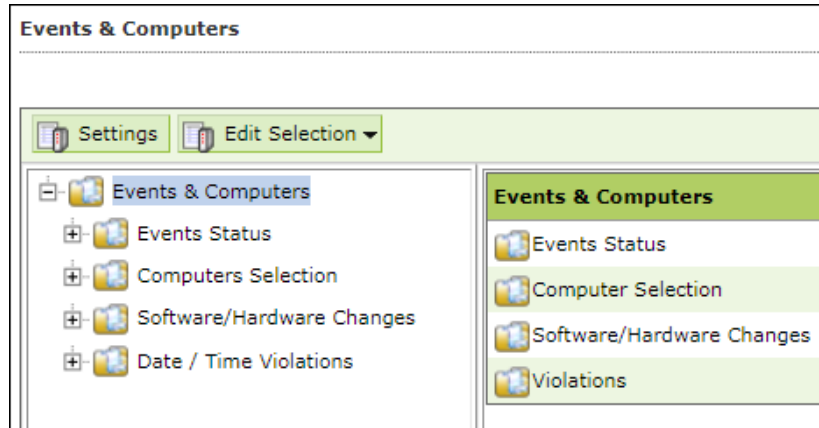
Report Scheduler

Do you want to Delete the Selected Task(s) ?

3. Click **OK**.
- The schedule will be deleted.

Events and Computers

eScan Management Console maintains the record of all the events sent by the client computer. Through the events & computers module, the administrator can monitor the Events and Computers; the module lets you sort the computer with specific properties.



Events Status

The Event Status subfolder is divided into following sections:

- Recent
- Critical
- Information

Recent

The Recent section displays both Information and Critical events.

Critical

The Critical section displays Critical events and immediate attention.

For example, Virus detection, Monitor disabled.

The Critical events can be filtered on the basis of date range and the report can be exported in .xls or .html format.

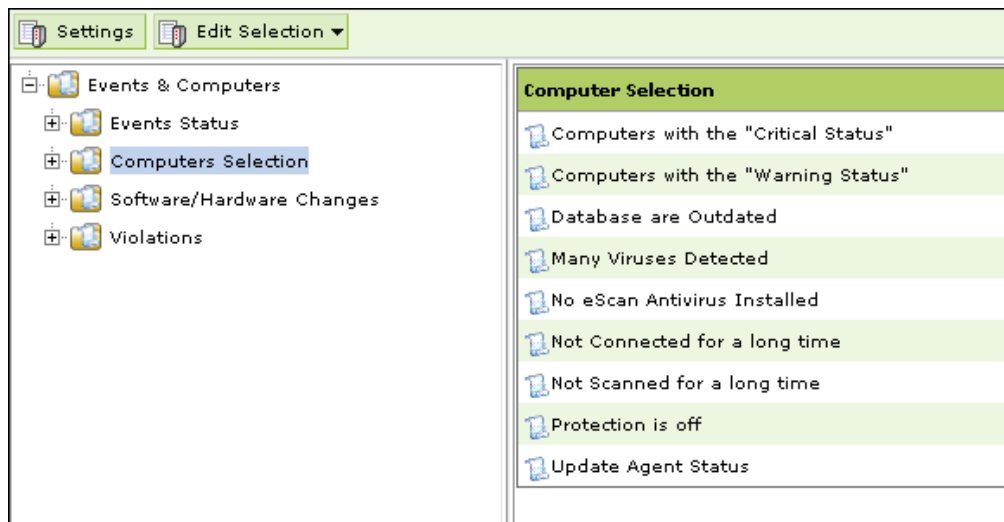
Information

The Information section displays basic information events.

For example, Virus database update, Status.

Computer Selection

The Computer Selection subfolder displays computers that fall under different categories. It lets you select the computer and take the preferred action. You can also set the criteria for each section and sort the computer accordingly.



The Computer Selection subfolder consists following sections:

- Computers with the "Critical Status"
- 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

Computers with the "Critical Status"

This section displays computers marked with Critical status.

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 Staus

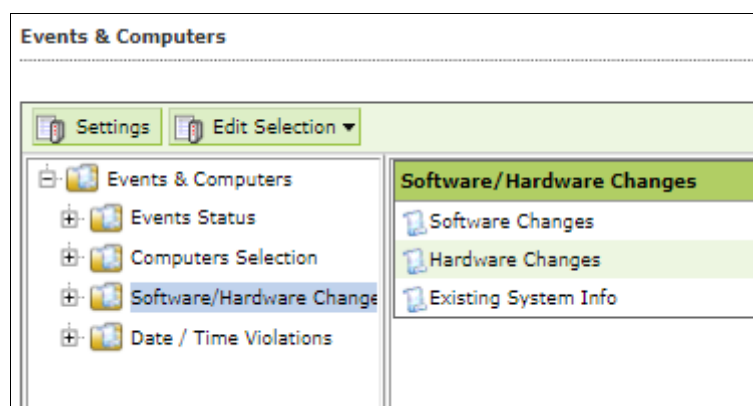
This section displays the status of computers assigned as Update Agent.

The additional settings vary depending upon the Computer Status.

Software/Hardware Changes

This subfolder displays all software/ hardware changes that occurred on computers. It consists following sections:

- Software Changes
- Hardware changes
- Existing System Info



Software Changes

This section displays software changes i.e. installation, uninstallation or software upgrades.

Hardware changes

This section displays hardware changes that occurred on computers. For example, IP address. Hard Disk, RAM etc.

Existing System Info

This section displays a computer's existing hardware information.

Violations

Date/Time Violations

This subfolder consists Date/Time Violations that displays client computers whose users attempted to modify date and time.

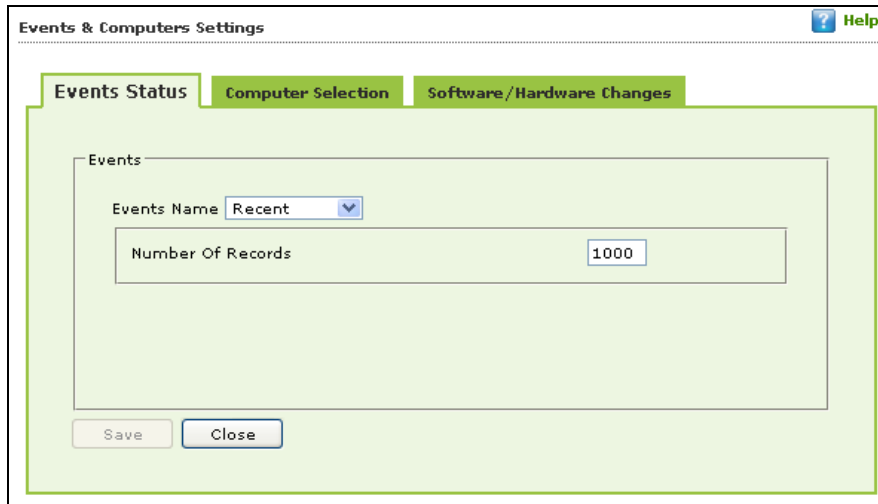
Date	Time	Machine Name	IP Address	User name	Event Id	Module Name	Description
3/6/2018	15:58:18	COMPSS1	192.168.0.106	COMPSS1	File Anti-Virus (1818)	eScan Monitor	Date/Time Modification Disabled
3/6/2018	15:58:04	COMPSS1	192.168.0.106	COMPSS1	File Anti-Virus (1818)	eScan Monitor	Date/Time Modification Disabled
3/6/2018	15:58:02	COMPSS1	192.168.0.106	COMPSS1	File Anti-Virus (1818)	eScan Monitor	Date/Time Modification Disabled
3/6/2018	14:50:16	WEAD17	192.168.7.79	WEAD17\Tom	File Anti-Virus (1818)	eScan Monitor	Date/Time Modification Disabled
3/6/2018	12:30:35	WEAD18	192.168.0.107	WEAD18\Sur	File Anti-Virus (1818)	eScan Monitor	Date/Time Modification Disabled
3/6/2018	12:30:15	WEAD18	192.168.7.79	WEAD18\Tom	File Anti-Virus (1818)	eScan Monitor	Date/Time Modification Disabled
3/6/2018	12:30:15	WEAD18	192.168.7.79	WEAD18\Tom	File Anti-Virus (1818)	eScan Monitor	Date/Time Modification Disabled
3/6/2018	12:30:14	WEAD18	192.168.7.79	WEAD18\Tom	File Anti-Virus (1818)	eScan Monitor	Date/Time Modification Disabled
3/6/2018	12:30:14	WEAD18	192.168.7.79	WEAD18\Tom	File Anti-Virus (1818)	eScan Monitor	Date/Time Modification Disabled

Settings

You can define the Settings for Events, Computer Selection and Software/Hardware changes by clicking on the **Settings** option and defining the desired settings using the Tabs and options present on the Events and Computer settings window.

Event Status Setting

Basically, events are activities performed on client's computer.



On the basis of severity, the events are categorized in to the following types:

- **Recent:** It displays both critical and information events that occurred recently on managed client computers.
- **Critical:** It displays all critical events occurred on managed client computers, such as virus detection, monitor disabled status, and so on.
- **Information:** It displays all informative types of events, such as virus database update, status, and so on.

Steps to define event status settings:

Perform the following steps to save the event status settings:

1. Select the appropriate **Events Name**.
2. Enter the number of events that you want to view in a list, in the **Number of Records** field.
3. Click **Save**. The settings get saved.

Computer Selection

The **Computer Selection** lets you select and save the computer status settings. This module lets you do the following activities:

Critical Status: It displays a list of computers that are critical in status, as per the criteria's selected in computer settings. Specify the following field details.

- **Check for eScan Not Installed:** Select this checkbox to view the list of client systems under managed computers on which eScan has not been installed.
- **Check for Monitor Status:** Select this checkbox to view the client systems on which eScan monitor is not enabled.
- **Check for Not Scanned:** Select this checkbox to view the list of client systems which has not been scanned.
- **Check for Database Not Updated:** Select this checkbox to view the list of client systems on which database has not been updated.
- **Check for Not Connected:** Select this checkbox to view the list of eScan client systems that have not been communicated with eScan server.
- **Database Not Updated from more than:** Enter the number of days from when the database has not been updated.
- **System Not Scanned for more than:** Enter the number of days from when the system has not been scanned.
- **System Not Connected for more than:** Enter the number of days from when the client system has not been connected to eScan server.
- **Number Of Records:** Enter the number of client systems that you want to view in the list.

Warning Status: It displays the list of systems which are warning in status, as per the criteria's selected in computer settings. Specify the following field details:

- **Check for Not Scanned:** Select this checkbox to view the list of client systems which has not been scanned.
- **Check for Database Not Updated:** Select this checkbox to view the list of client systems on which database has not been updated.
- **Check for Not Connected:** Select this checkbox to view the list of eScan client systems that have not been communicated with eScan server.
- **Check for Protection off:** Select this checkbox to view the list of client systems on which protection for any module is inactive.
- **Check for Many Viruses:** Select this checkbox to view the list of client systems on which maximum viruses are detected.
- **Database Not Updated from more than:** Enter the number of days from when the database has not been updated.
- **System Not Scanned for more than:** Enter the number of days from when the system has not been scanned.
- **System Not Connected for more than:** Enter the number of days from when the client system has not been connected to eScan server.
- **Number Of Virus:** Enter the number of viruses detected on client system.
- **Number Of Records:** Enter the number of client system that you want to view in the list.

Database are Outdated: It displays a list of systems on which virus database is outdated. Specify the following field details:

- **Database Not Updated from more than:** Enter the number of days from when the database has not been updated.
- **Number of Records:** Enter the number of client system that you want to view in the list.

Many viruses Detected: It displays a list of systems on which number of viruses exceeds the specified count in computer settings. Specify the following field details:

- **Number of Virus:** Enter the number of viruses detected on client system.
- **Number of Records:** Enter the number of client system that you want to view in the list.

No eScan Antivirus Installed: It displays the list of systems on which eScan has not been installed. Specify the following field detail:

- **Number of Records:** Enter the number of client system that you want to view in the list.

Not connected to the eScan server for a long time: It displays the list of systems which have not been connected to the server from a long time. Specify the following field detail:

- **Number of Records:** Enter the number of client system that you want to view in the list.

Not scanned for a long time: It displays the list of systems which have not been scanned from a long time, as specified in computer settings. Specify the following field details:

- **System Not Scanned for more than:** Enter the number of days from when the system has not been scanned.
- **Number of Records:** Enter the number of client system that you want to view in the list.

Protection is off: It displays the list of systems on which protection is inactive for any module, as per the protection criteria's selected in computer settings. It shows the status as "Disabled" in the list. Specify the following field details.

- **Check for Monitor Status:** Select this checkbox if you want to view the client systems on which eScan monitor is not enabled.
- **Check for Mail Anti-Phishing:** Select this checkbox if you want to view the list of client systems on which **Mail Anti-Phishing** protection is inactive.
- **Check for Mail Anti-Virus:** Select this checkbox if you want to view the list of client systems on which **Mail Anti-Virus** protection is inactive.
- **Check for Mail Anti-Spam:** Select this checkbox if you want to view the list of client systems on which **Mail Anti- Spam** protection is inactive.
- **Check for Endpoint Security:** Select this checkbox if you want to view the list of client systems on which **Endpoint Security** protection is inactive.
- **Check for Firewall:** Select this checkbox if you want to view the list of client systems on which **Firewall** protection is inactive.
- **Check for Proactive:** Select this checkbox if you want to view the list of client systems on which **Proactive** protection is inactive.
- **Check for Web Protection:** Select this checkbox if you want to view the list of client systems on which protection of
- **Web Protection** module is inactive.
- **Number of Records:** Enter the number of client system that you want to view in the list.

Steps to define computer settings

To save the computer settings, follow the steps given below:

1. Click **Computers Selection** tab.
2. Select a type of status for which you want to set criteria, from the **Computer status** drop-down.
3. Select the appropriate checkboxes, and then enter field details in the available fields. For more information, refer [Types and criteria of computer status] section.
4. Click **Save**. The settings will be saved.

Software/ Hardware Changes Setting

You can set these settings, if you want to get updates on any changes made in the software, hardware, and to existing system.

The **Software/ Hardware Changes** enable you to do the following activities:

Type of Software/Hardware Changes

- **Software changes**
- **Hardware changes**
- **Existing system info**

To Change software/hardware settings, follow the steps given below:

1. Click the **Software/Hardware Changes** tab.
2. Specify the following field details.
 - **Software/Hardware Changes:** Click the drop-down and select the changes made.
 - **Number of Days:** Enter the number of days, to view changes made within the specified days.
 - **Number of Records:** Enter the number of client systems that you want to view in the list.
3. Click **Save**. The settings get saved.

Performing an action for computer

To perform an action for a computer, follow the steps given below:

1. Select a computer.
2. Click **Edit Selection** drop-down.
3. Click the preferred action.

Tasks for Specific Computers

The Tasks for Specific Computers module lets you create a new task for computer(s) according to your preferences.

Creating a task for specific computers

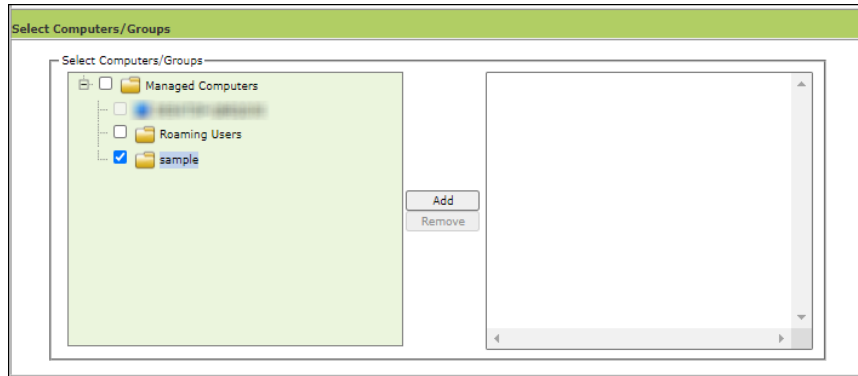
To create a task for specific computer(s), follow the steps given below:

1. In the navigation panel, click **Tasks for Specific Computers**.
2. Click **New Task**.

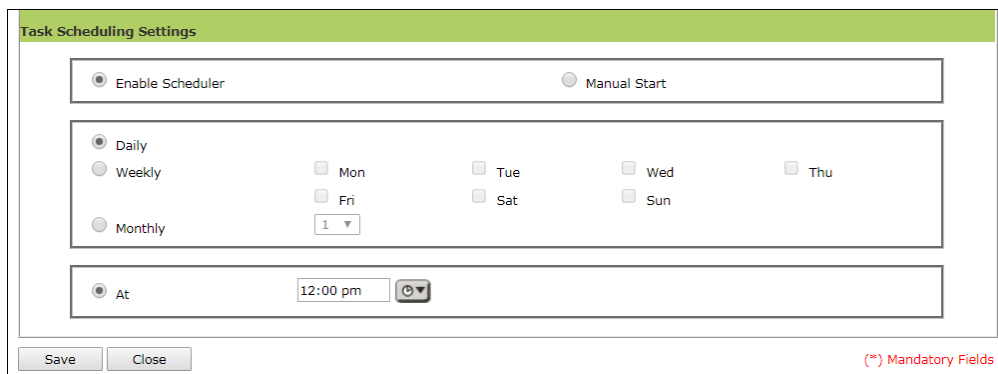
New Task Template form appears.

3. Enter a name for task.
4. In the **Assigned Tasks** section, select the modules and scans to be run.

- In the **Select Computers/Groups** section, select the computers/groups on which the tasks should be run and then click **Add**.



- In the **Tasks Scheduling Settings** section, configure the schedule settings.



- Click **Save**. The task will be saved and run for specific computers according to your preferences.

Viewing Properties of a task

To view Properties of a task, select the task and click **Properties**.

sample

Tasks For Specific Computers > Properties

General Schedule Machines Settings

Task Name: sample

Task Creation Time: 05/29/20 03:15:34 PM

Status: Task not performed yet

Last Run:

Save Close

This section will have following tabs to configure:

- **General:** This tab allows to change the task name and provides details about the task creation, status, and last run.
- **Schedule:** This tab allows to change the scheduler setting for the particular task.
- **Machines:** This tab allows to add or remove the endpoints added to the particular task.
- **Settings:** This tab allows to modify or select the modules and scans to be run.

NOTE To run a scheduled task manually, select the task and then click **Start Task**.

Viewing Results of a task

To view Results of a task, select the task and click **Results**.

Task Results (sample)

Tasks For Specific Computers > Task Results

Client Computers	Group	Status	Date/Time
Managed Computers\TestGroup	Managed Computers\TestGroup	Not Performed Yet	

This option will provide the summary details about the task like clients computers, group to which computers belong, status of the task, and more.

Deleting a task for specific computers

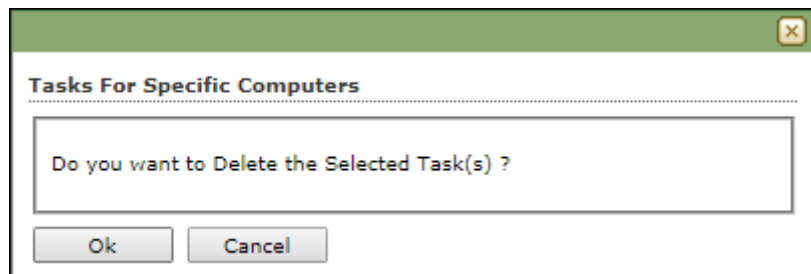
To delete a task, follow the steps given below:

1. In the Tasks for Specific Computers screen, select the task you want to delete.

Tasks For Specific Computers					Refresh	Help
<input type="button" value="New Task"/> <input type="button" value="Start Task"/> <input type="button" value="Properties"/> <input type="button" value="Results"/> <input type="button" value="Delete"/>						
<input type="checkbox"/>	Task Name	Pending	Completed	Schedule Type	Task Status	
<input checked="" type="checkbox"/>	New Task	1	0	Manually Start	Task Status	
<input type="checkbox"/>	New Task_1	1	0	Automatic Scheduler	Task Status	

2. Click **Delete**.

A confirmation prompt appears.



3. Click **OK**. The task will be deleted.

Asset Management

This module displays list of hardware configuration, software installed, software version number and a Software report for Microsoft software installed on **Managed Computers**.

The Asset Management module consists following tabs:

- **Hardware Report**
- **Software Report**
- **Software License**
- **Software Report (Microsoft)**

Hardware Report

The Hardware Report tab displays hardware configuration of all Managed Computers.

Asset Management				
Refresh Help				
Hardware Report Software Report Software License Software Report (Microsoft)				
Filter Criteria			Export Option	
Computer Details				
Computer Name	Group	IP Address	User's name	Operating System
Computer-001	Managed Computers	192.168.1.101	Administrator	Windows 2008 R2 Standard Edition 64-bit
Computer-002	Managed Computers	192.168.1.102	Administrator	Windows 7 Professional 32-bit
Computer-003	Managed Computers	192.168.1.103	Administrator	Windows 7 Professional 64-bit
Computer-004	Managed Computers	192.168.1.104	Administrator	Windows 7 Professional 32-bit
Computer-005	Managed Computers	192.168.1.105	Administrator	Windows 10 Professional 64-bit
Computer-006	Managed Computers	192.168.1.106	Administrator	Windows 7 Professional 32-bit
Computer-007	Managed Computers	192.168.1.107	Administrator	Windows 10 Professional 64-bit

The tab displays following details of managed computers:

- Computer Name
- Group
- IP Address
- User name
- Operating System
- Service Pack
- OS Version
- OS Installed Date
- Internet Explorer
- Processor
- Motherboard
- RAM
- HDD
- Local MAC Adapter(s)
- Wi-Fi MAC [Adapter]
- USB MAC [Adapter]
- PC Identifying Number

- Motherboard Serial No
- Network Speed
- Disk Free Space
- PC Manufacturer
- PC Model
- MB Manufacturer
- Graphic Card Details
- Machine Type
- BitLocker Status
- Keyboard Vendor
- Software

To view the list of Software along with the installation dates, click **View** in **Software** column.

Filtering Hardware Report

To filter the Hardware Report as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.

Select the parameters you want to be included in the filtered report.

Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After making the necessary selections, click **Search**.

The Hardware Report will be filtered according to your preferences.

Exporting Hardware Report

To export the Hardware Report, click **Export Option**.

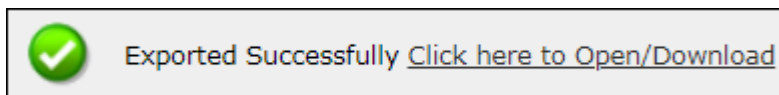
Export Option field expands.

▲ Filter Criteria ▼ Export Option

Export Option

☐ Excel ☐ PDF ☒ HTML

Select the preferred option and then click **Export**. A success message appears.



Click the link to open/download the file.

Software Report

The Software Report tab displays list of Software along with the number of computers on which they are installed.

Asset Management Refresh Help

Hardware Report Software Report Software License Software Report (Microsoft)

▲ Filter Criteria ▲ Export Option

Software Details 1 - 100 of 1000 page 1 of 10 Rows per page: 100

Software Name	Computer Count
1ClickDownloader	1
2007 Microsoft Office system	16
2in1 Coundition Zero 1.1&Counter-Strike 1.6(build 2738)	1
3.5G Connect V3.1	1
3.75G Digiconnect v2.0.8.1884	1
3DP Chip Lite v17.05	1
3DP Chip Lite v18.05	4

To view the computers on which the specific software is installed, click the numerical in Computer Count column.

Computer list window appears displaying following details:

- Computer Name
- Group
- IP Address
- Operating System
- Software Version
- Installed Date

Filtering Software Report

To filter Software Report, click **Filter Criteria** field.

Filter Criteria field expands.

The Software Report can be filtered on the basis of **Software Name** or **Computer Name**.

Software Name

Entering the Software name displays suggestions. Select the appropriate software.

Computer Name

Click the drop-down and select the preferred computer(s).

OS Type

Enter the OS type.

Group By

The results can be grouped by Software name, Computer name or Group.

If Group option is selected, the report can be filtered for a specific group.

After entering data in all fields, click **Search**.

The Software Report will be filtered according to your preferences.

Exporting Software Report

To export the Software Report, click **Export Option**.

Export Option field expands.

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.

A success message appears.



Exported Successfully [Click here to Open/Download](#)

Click the link to open/download the file.

Software License

The Software License tab displays list of Software Licenses of managed computers.

Asset Management

Refresh

Help

Hardware Report

Software Report

Software License

Software Report (Microsoft)

▲ Filter Criteria

▲ Export Option

1 - 3 of 3

◀◀ page 1 of 1 ▶▶

Rows per page: 100 ▼

License Key	Software Name	Computer Count
W269K-W269K-W269K-W269K-W269K	Windows 10 Professional 32-bit 	<u>1</u>
W269K-W269K-W269K-W269K-W269K	Windows 10 Professional 64-bit 	<u>1</u>
W269K-W269K-W269K-W269K-W269K	Windows XP Professional 32-bit 	<u>1</u>

The log displays License Key, Software Name and Computer Count.

To see more details of the computer's license key installed, click the numerical value in License Key or Computer Count column.

Filtering Software License Report

To filter Software Report, click **Filter Criteria** field.

Filter Criteria field expands.

Filter Criteria		Export Option	
Filter Criteria			
Software License Key	*	Include	
Software Name	*	Include	
Computer Name	*	Include	
IP Address	*	Include	
OS Type	*	Include	
<input type="button" value="Search"/> <input type="button" value="Reset"/>		<div>Group By</div> <div><input type="checkbox"/> Group</div>	
		(*) View All Items	

Software License Key

Entering the license key displays suggestions. Select the appropriate key.

Software Name

Entering the Software name displays suggestions. Select the appropriate software.

Computer Name

Click the drop-down and select the preferred computer(s).

IP Address

Entering the IP address displays suggestions. Select the appropriate IP address.

OS Type

Enter the OS type.

Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After entering data in all fields, click **Search**.

The Software License Report will be filtered according to your preferences.

Exporting Software License Report

To export the Software License Report, click **Export Option**.

Export Option field expands.

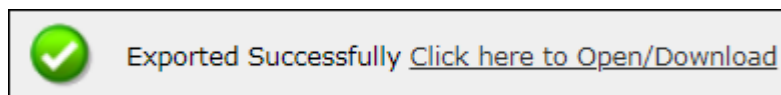
Select whether you want report for Windows OS and Microsoft Office.

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.

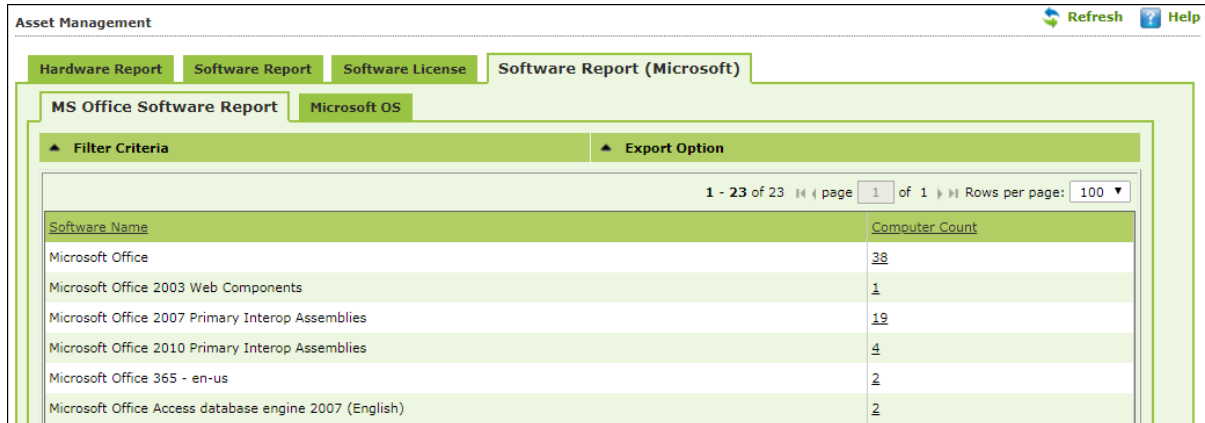
A success message appears.



Click the link to open/download the file.

Software Report (Microsoft)

The Software Report (Microsoft) displays details of the Microsoft Software installed on the computers.



Software Name	Computer Count
Microsoft Office	38
Microsoft Office 2003 Web Components	1
Microsoft Office 2007 Primary Interop Assemblies	19
Microsoft Office 2010 Primary Interop Assemblies	4
Microsoft Office 365 - en-us	2
Microsoft Office Access database engine 2007 (English)	2

The tab consists following subtabs:

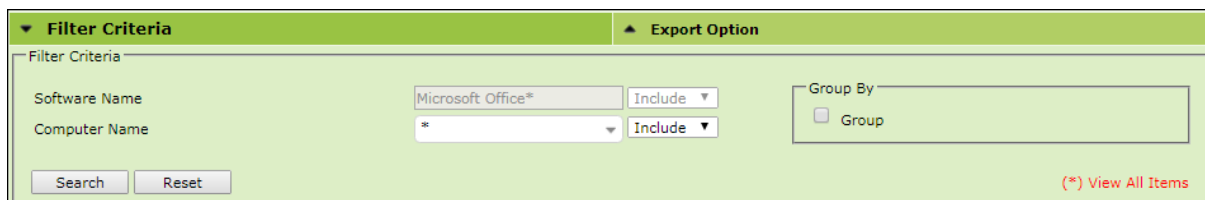
MS Office Software Report – It displays Microsoft software name and computer count.

Microsoft OS – It displays Operating System, Service Pack, OS version and computer count.

Filtering Software Report (Microsoft)

To filter Software Report (Microsoft), click **Filter Criteria** field.

Filter Criteria field expands.



Computer Name

Click the drop-down and select the preferred computer(s).

Group By

If Group option is selected, the report can be filtered for a specific group.

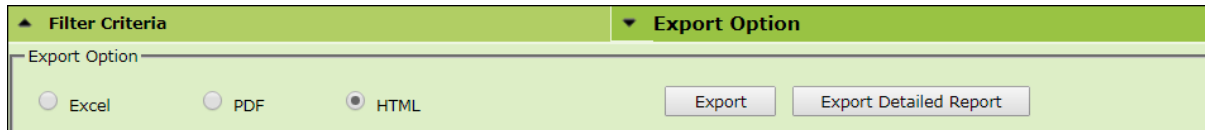
After entering data in all fields, click **Search**.

The Software Report (Microsoft) will be filtered according to your preferences.

Exporting Software Report (Microsoft)

To export the Software Report (Microsoft), click **Export Option**.

Export Option field expands.



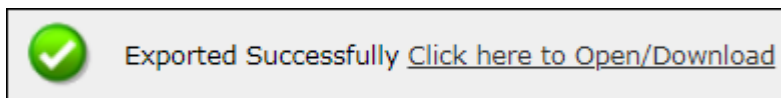
The screenshot shows the 'Export Option' field expanded. It contains three radio buttons: 'Excel', 'PDF', and 'HTML'. The 'HTML' option is selected. To the right of the radio buttons are two buttons: 'Export' and 'Export Detailed Report'.

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.

A success message appears.

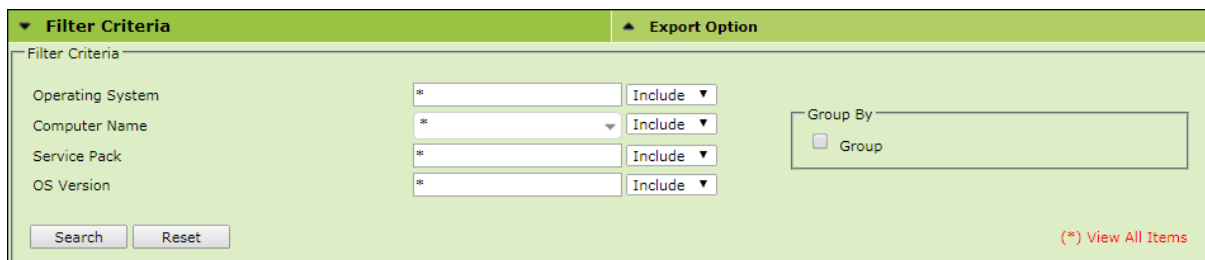


Click the link to open/download the file.

Filtering Microsoft OS Report

To filter the Microsoft OS report, click **Filter Criteria** field.

Filter Criteria field expands.



The screenshot shows the 'Filter Criteria' field expanded. It contains four rows of filter criteria: 'Operating System', 'Computer Name', 'Service Pack', and 'OS Version'. Each row has a text input field and a dropdown menu set to 'Include'. To the right of these rows is a 'Group By' section with a checkbox labeled 'Group'. At the bottom left are 'Search' and 'Reset' buttons. At the bottom right is a link '(*) View All Items'.

Operating System

Entering the operating system name displays list of suggestions. Select the appropriate OS.

Computer Name

Click the drop-down and select the preferred computer(s).

Service Pack

Entering the service pack name displays list of suggestions. Select the appropriate Service Pack.

OS Version

Entering the OS version displays list of suggestions. Select the appropriate OS version.

Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

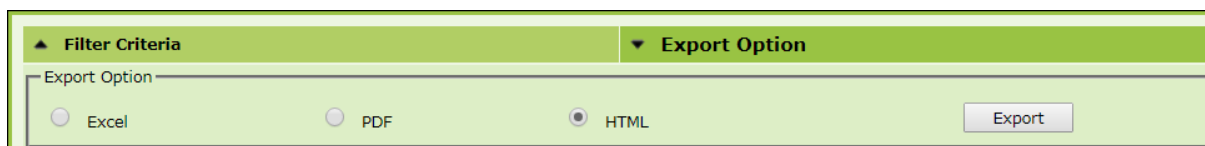
After filling all the fields, click **Search**.

The Microsoft OS report will be filtered according to your preferences.

Exporting Microsoft OS Report

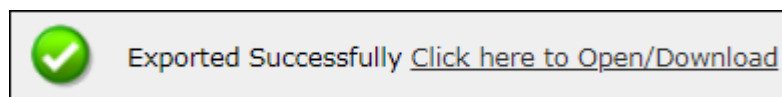
To export the Microsoft OS Report, click **Export Option**.

Export Option field expands.



The screenshot shows a web interface with two tabs: "Filter Criteria" and "Export Option". The "Export Option" tab is active, showing three radio button options: "Excel", "PDF", and "HTML". The "HTML" option is selected. To the right of the radio buttons is an "Export" button.

Select the preferred option and then click **Export**. A success message appears.



Click the link to open/download the file.

User Activity

The User Activity module lets you monitor Print, Session and File activities occurring on the client computers. 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 consists Print Date, Machine Name, IP Address, Username, Printer Name, Document Name along with number of Copies and Pages.

Print Activity

Settings

Refresh

Help

▲ Filter Criteria

▲ Export Option

1 - 10 of 10 1 of 1 Rows per page: 10

Printer Name	Copies	Pages
Burton's HP OfficeJet	3	3
Microsoft Print	28	34
Microsoft Office	10	192

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.

Print Activity >> Burton's HP OfficeJet

Machine Name : *(Include)

Export To: ---Select---

Export

1 - 3 of 3 page 1 of 1 Rows per page: 10

Client Date	Machine Name	IP Address	User name	Printer Name	Document Name	Copies	Pages
18/09/19 1:33:43 PM	Microsoft Office	192.168.1.100	Microsoft Office	Burton's HP OfficeJet	http://internal-network.com/officejet/officejet.html	1	1
18/09/19 12:40:41 PM	Microsoft Office	192.168.1.100	Microsoft Office	Burton's HP OfficeJet	http://internal-network.com/officejet/officejet.html	1	1
18/09/19 12:37:01 PM	Microsoft Office	192.168.1.100	Microsoft Office	Burton's HP OfficeJet	http://internal-network.com/officejet/officejet.html	1	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.



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	Group By <input checked="" type="radio"/> Printer <input type="radio"/> User name
Printer	==	Include	
User name	==	Include	
<input checked="" type="checkbox"/> Date Range From (MM/DD/YYYY) 11/02/2019 To (MM/DD/YYYY) 11/02/2019			
<input type="button" value="Search"/> <input type="button" value="Reset"/>		(**) View All Items	

Computer Name

Click the drop-down and select the preferred computer.

Printer

Enter the printer's name.

User Name

Enter the User's name.

Include/Exclude

Selecting Include/Exclude for a Machine or Printer lets you include or exclude it from the log.

Date Range

To search the log between specific dates, select **Date Range** check box. Afterwards, click the calendar icon and select **From** and **To** dates.

After filling all fields, click **Search**.

The Print activity log will be filtered and generated according to your preferences.

Group By

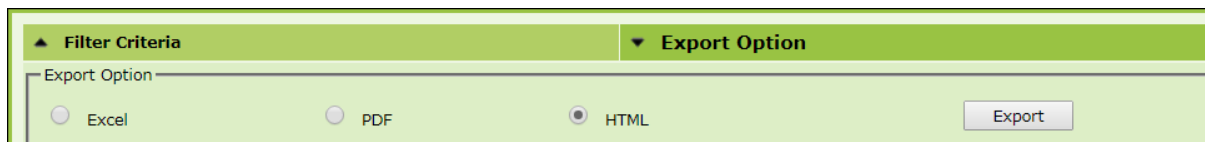
To view results by specific printer, select **Printer**, Date Range and then click **Search**.

To view results by specific user name, select **User name**, Date Range and then click **Search**.

Exporting Print Activity Report

To export the generated log, click **Export Option**.

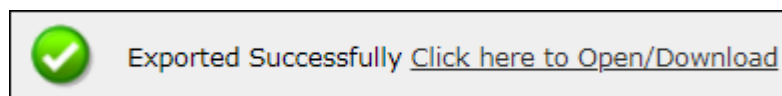
Export Option field expands.



The screenshot shows a web interface with two tabs: 'Filter Criteria' and 'Export Option'. The 'Export Option' tab is active, showing three radio button options: 'Excel', 'PDF', and 'HTML'. The 'HTML' option is selected. An 'Export' button is located to the right of the options.

Select the preferred option and then click **Export**.

A success message appears.



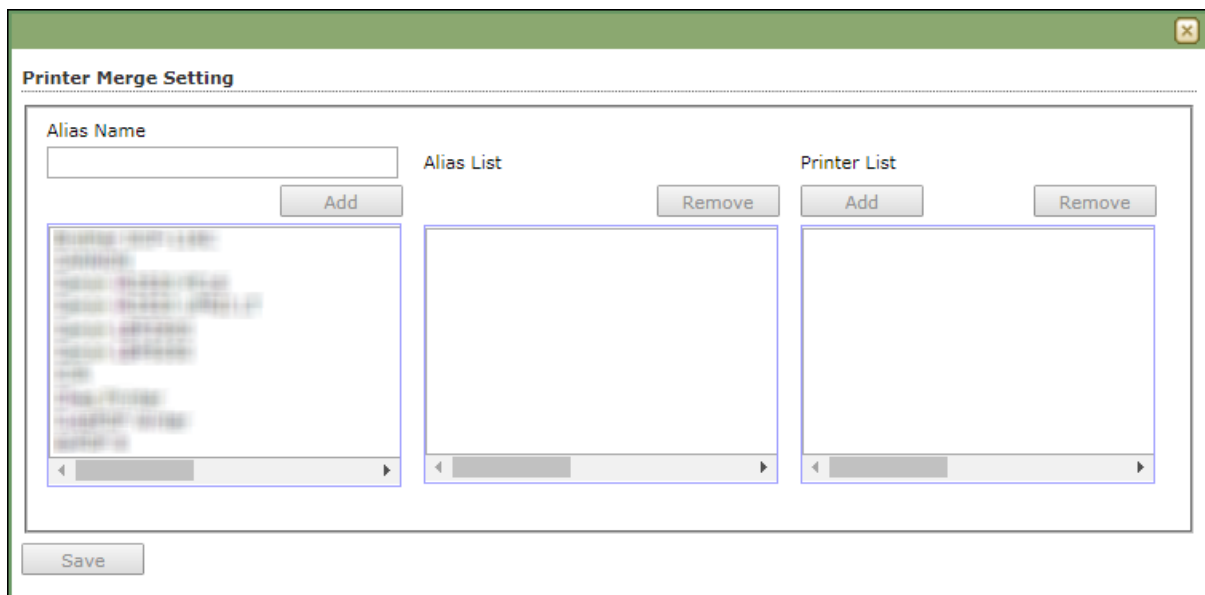
Click the link to open/download the file.

Print Activity Settings

Print Activity Settings lets you keep track of printers by adding them in a group and assigning it an alias name. The printers can be added or removed from this alias group.

To configure Print Activity Settings:

1. In the Print Activity screen, at the top right corner, click **Settings**.
Printer Merge Setting window appears.



The screenshot shows the 'Printer Merge Setting' window. It has a title bar with a close button. Inside, there's a section titled 'Printer Merge Setting'. Below this, there are three main areas: 'Alias Name' with a text input field and an 'Add' button; 'Alias List' with a list box and a 'Remove' button; and 'Printer List' with a list box and 'Add' and 'Remove' buttons. Each list box contains several printer names. At the bottom left, there is a 'Save' button.

2. Enter name in Alias Name field.
3. Select printer(s) for the alias.
4. Click **Add**.
The printer(s) will be added to the alias.
5. Click **Save**. The Print Activity Settings will be saved.

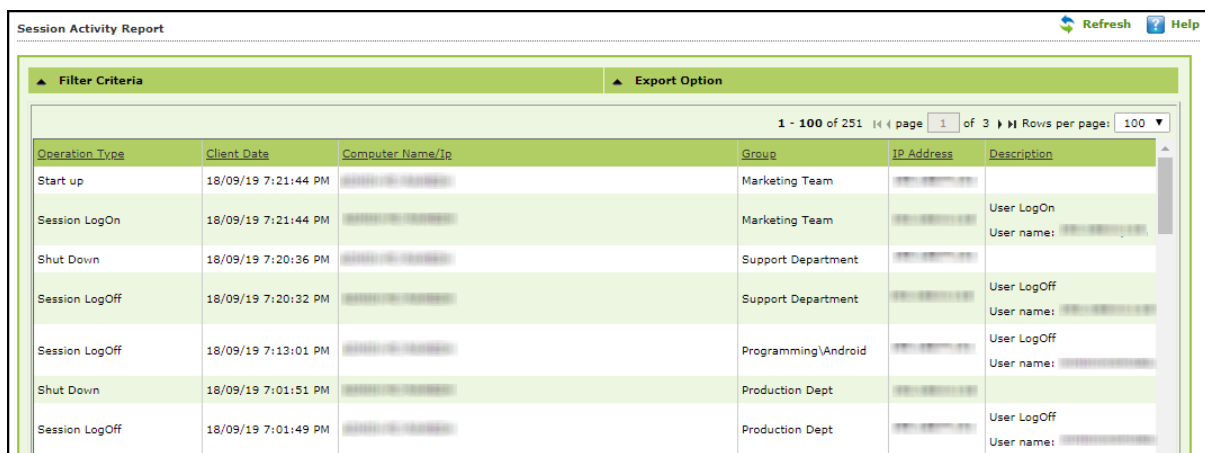
Session Activity Report

This submodule monitors and logs the session activity of the managed computers. It displays a report of the Operation type, Date, Computer name, Group, IP address and event description. With this report the administrator can trace the user Logon and Logoff activity along with remote sessions that took place on all managed computers.

Viewing Session Activity Log

In the navigation panel, click **User Activity > Session Activity Report**.

The log displays list of session activities and type of operation performed. Options for Filtering or Exporting the log in desired formats are also present on the same interface.



Session Activity Report

Refresh Help

Filter Criteria Export Option

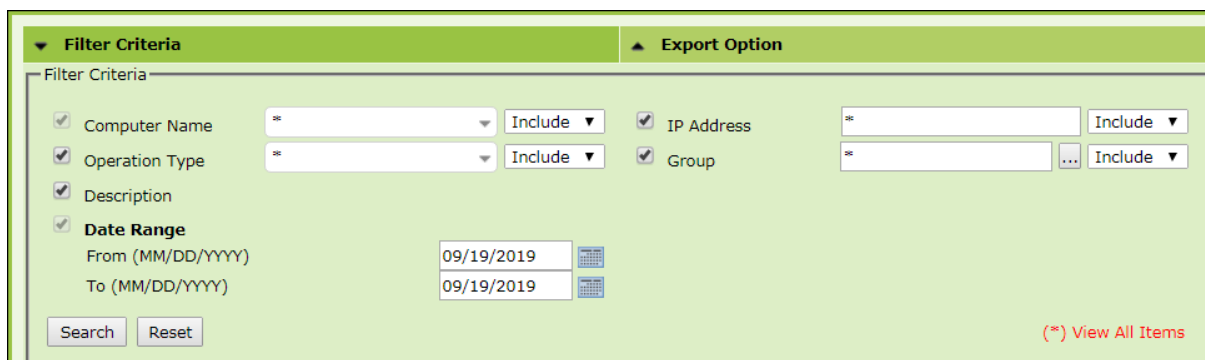
1 - 100 of 251 | page 1 of 3 | Rows per page: 100

Operation Type	Client Date	Computer Name/Ip	Group	IP Address	Description
Start up	18/09/19 7:21:44 PM	XXXXXXXXXX	Marketing Team	XXXXXXXXXX	
Session LogOn	18/09/19 7:21:44 PM	XXXXXXXXXX	Marketing Team	XXXXXXXXXX	User LogOn User name: XXXXXXXX
Shut Down	18/09/19 7:20:36 PM	XXXXXXXXXX	Support Department	XXXXXXXXXX	
Session LogOff	18/09/19 7:20:32 PM	XXXXXXXXXX	Support Department	XXXXXXXXXX	User LogOff User name: XXXXXXXX
Session LogOff	18/09/19 7:13:01 PM	XXXXXXXXXX	Programming\Android	XXXXXXXXXX	User LogOff User name: XXXXXXXX
Shut Down	18/09/19 7:01:51 PM	XXXXXXXXXX	Production Dept	XXXXXXXXXX	
Session LogOff	18/09/19 7:01:49 PM	XXXXXXXXXX	Production Dept	XXXXXXXXXX	User LogOff User name: XXXXXXXX

Filtering Session Activity Log

To filter session activities, click **Filter Criteria** field.

Filter Criteria field expands.



Filter Criteria Export Option

Filter Criteria

☒ Computer Name Include
☒ Operation Type Include
☒ Description
☒ Date Range
 From (MM/DD/YYYY) 09/19/2019
 To (MM/DD/YYYY) 09/19/2019

☒ IP Address Include
☒ Group ... Include

(*) View All Items

Filter Criteria lets you filter and generate the log according to your preferences. The check box selected will be added as a column in the report.

Computer Name

Click the drop-down and select the preferred computers.

Operation Type

Click the drop-down and select the preferred activities.


Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the log.

IP Address

Enter the IP address in this field.

Group

Enter the group's name or click  and select a group.

Date Range

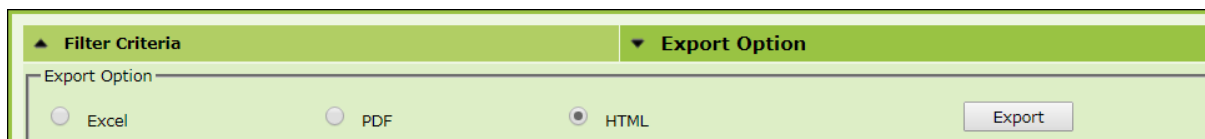
To search the log between specific dates, select **Date Range** check box. Afterwards, click the calendar icon and select **From** and **To** dates.

After filling all fields, click **Search**.

Exporting Session Activity Report

To export the generated log, click **Export Option**.

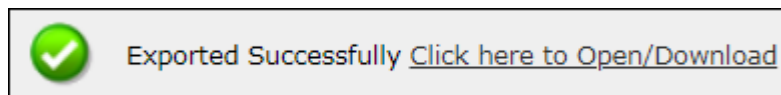
Export Option field expands.



The screenshot shows a web interface with two tabs: 'Filter Criteria' and 'Export Option'. The 'Export Option' tab is active, showing three radio buttons labeled 'Excel', 'PDF', and 'HTML'. The 'HTML' radio button is selected. To the right of the radio buttons is an 'Export' button.

Select the preferred option and then click **Export**.

A success message appears.



Click the link to open/download the file.

File Activity Report

The File Activity module displays a report of the files created, copied, modified, and deleted on managed computers. Additionally in case of a misuse of any official files can be tracked down to the user through the details captured in the report. Select and filter the report based on any of the details captured.

Viewing File Activity Log

In the navigation panel, click **User Activity > File Activity Report**.

The log displays list of files and the type of operation performed on them. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

1 - 10 of 112848 page 1 of 11285 Rows per page: 10							
Client Date	Computer Name/Ip	Group	IP Address	User's name	File Action Type	Drive Type	Source File
4/20/2019 12:00:25 AM	192.168.1.100	Admin	192.168.1.100	Administrator	CREATE	DRIVE_NETWORK	NewFile
4/20/2019 12:00:25 AM	192.168.1.100	Admin	192.168.1.100	Administrator	CREATE	DRIVE_NETWORK	NewFile
4/20/2019 12:01:52 AM	192.168.1.100	Admin	192.168.1.100	Administrator	CREATE	DRIVE_NETWORK	NewFile
4/20/2019 12:01:52 AM	192.168.1.100	Admin	192.168.1.100	Administrator	CREATE	DRIVE_NETWORK	NewFile
4/20/2019 12:04:15 AM	192.168.1.100	Admin	192.168.1.100	Administrator	CREATE	DRIVE_NETWORK	NewFile
4/20/2019 12:04:15 AM	192.168.1.100	Admin	192.168.1.100	Administrator	CREATE	DRIVE_NETWORK	NewFile

Filtering File Activity Log

To filter file activities, click **Filter Criteria** field. Filter Criteria field expands.

Filter Criteria

Export Option

☒ Computer Name
 Include

☒ User's name
 Include

☒ File Action Type
 Include

☒ Source File
 Include

☒ Application
 Include

☒ Date Range
 From (MM/DD/YYYY) To (MM/DD/YYYY)

☒ IP Address
 Include

☒ Group
 Include

☒ Drive Type
 Include

☒ Destination File
 Include

(*) View All Items

Filter Criteria lets you filter and generate the log according to your preferences. The check box selected will be added as a column in the report.

Computer Name

Click the drop-down and select the preferred computers.

Username

Enter the username of the computer.

File Action type

Click the drop-down and select a preferred file action.

Source File

Enter the source file's name.

Application

Enter an application's name.


Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the log.

IP Address

Enter an IP address.

Group

Enter the group's name or click  and select a group.

Drive Type

Click the drop-down and select the drive type.

Destination File

Enter the file path.

Date Range

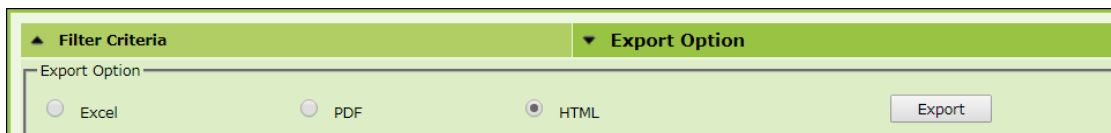
To search the log between specific dates, select **Date Range** check box. Afterwards, click the calendar icon and select **From** and **To** dates.

After filling all fields, click **Search**.

Exporting File activity Report

To export the generated report, click **Export Option**.

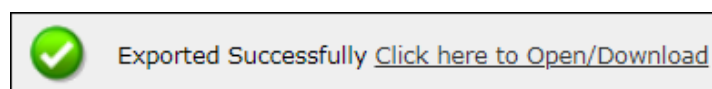
Export Option field expands.



The screenshot shows a green header bar with two tabs: 'Filter Criteria' and 'Export Option'. Below the 'Export Option' tab, there is a section labeled 'Export Option' containing three radio buttons: 'Excel', 'PDF', and 'HTML'. The 'HTML' radio button is selected. To the right of these options is a button labeled 'Export'.

Select the preferred option and then click **Export**.

A success message appears.



Click the link to open/download the file.

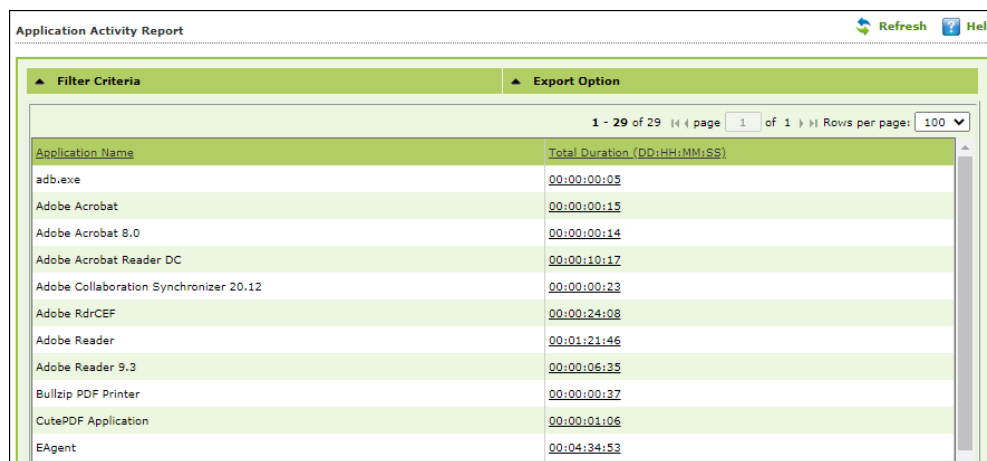
Application Access Report

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.



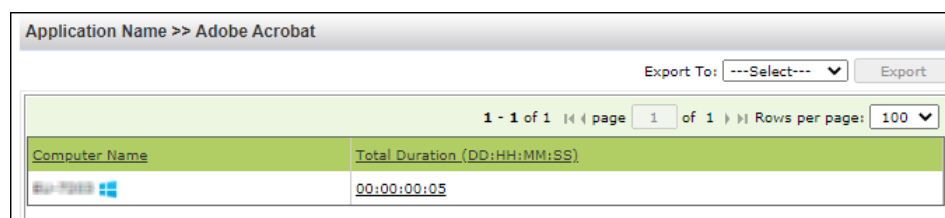
Application Activity Report

Filter Criteria Export Option

1 - 29 of 29 |< < page 1 of 1 > > Rows per page: 100

Application Name	Total Duration (DD:HH:MM:SS)
adb.exe	00:00:00:05
Adobe Acrobat	00:00:00:15
Adobe Acrobat 8.0	00:00:00:14
Adobe Acrobat Reader DC	00:00:10:17
Adobe Collaboration Synchronizer 20.12	00:00:00:23
Adobe RdrCEF	00:00:24:08
Adobe Reader	00:01:21:46
Adobe Reader 9.3	00:00:06:35
Bullzip PDF Printer	00:00:00:37
CutePDF Application	00:00:01:06
EAgent	00:04:34:53

By clicking on the duration present under **Total Duration (DD:HH:MM:SS)** column, you will get the details of the computer name accessed the app and duration.



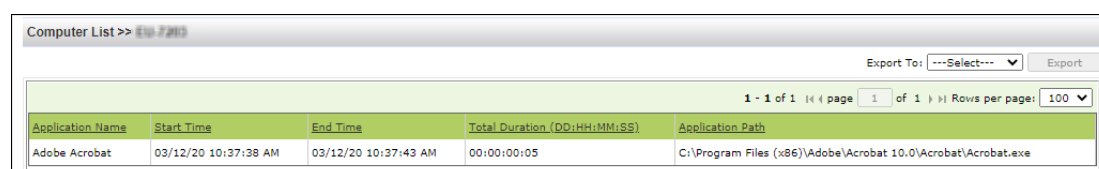
Application Name >> Adobe Acrobat

Export To: ---Select--- Export

1 - 1 of 1 |< < page 1 of 1 > > Rows per page: 100

Computer Name	Total Duration (DD:HH:MM:SS)
WIN-7213	00:00:00:05

Again, if you click on the duration, you will get detailed view of the app accessed by the computer along with the date, time, and application path.



Computer List >> WIN-7213

Export To: ---Select--- Export

1 - 1 of 1 |< < page 1 of 1 > > Rows per page: 100

Application Name	Start Time	End Time	Total Duration (DD:HH:MM:SS)	Application Path
Adobe Acrobat	03/12/20 10:37:38 AM	03/12/20 10:37:43 AM	00:00:00:05	C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\Acrobat.exe

You can export this report in various format such as PDF, CSV, and HTML.

Filtering Application Access Report

To filter file activities, click **Filter Criteria** field. Filter Criteria field expands.

Filter Criteria lets you filter and generate the log according to your preferences. The check box selected will be added as a column in the report.

Application Name

Entering the Application name displays suggestions. Select the appropriate application.

Computer Name

Click the drop-down and select the preferred computer(s).

Group By

The results can be grouped by Application name or Computer name.

Date Range

To search the log between specific dates, select **Date Range** check box. Afterwards, click the calendar icon and select **From** and **To** dates.

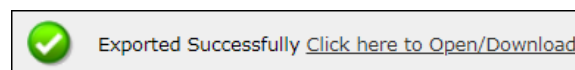
After entering data in all fields, click **Search**. The Application Access Report will be filtered according to your preferences.

Exporting Application Access Report

To export the generated report, click **Export Option**. Export Option field expands.

Select the preferred option and then click **Export**.

A success message appears.



Click the link to open/download the file.

Patch Report

The Patch Report module displays the number of windows security patches installed and not installed on managed computers. This will help an administrator identify the number of vulnerable systems in the network and install the critical patches quickly.

Patch Management Refresh Help

Patch Report All Patch Report

Filter Criteria Export Option

1 - 10 of 255 1 of 26 10 Rows per page: 10

Patch Name	Applied Count	Not Applied Count	Not Applicable Count
KB2207566	0	0	2
KB2286198	0	0	2
KB2305420	0	0	2
KB2347290	0	0	2
KB2393802	0	0	2
KB2412687	0	0	2
KB2419632	0	0	2
KB2419635	0	0	2
KB2419640	0	0	2
KB2425227	0	0	2

Patch report

The Patch report tab displays the Patch Name, Applied Count, Not Applied Count and Not Applicable Count. Clicking the numerical displays the patch name, details about the computer, the group it belongs to, IP address and User's name.

Computer List >> KB958644 Export To: ---Select--- Export

1 - 2 of 2 1 of 1 10 Rows per page: 10

Computer Name	Group	IP Address	User's name	Operating System
Managed Computers	Managed Computers			Windows 10 Professional 32-bit
Managed Computers\TestGroup	Managed Computers\TestGroup			Windows XP Professional x64 Edition 64-bit

Filtering Patch Report

To filter the Patch Report as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.

Patch Report All Patch Report

Filter Criteria Export Option

Filter Criteria

Patch Name * Include ▼

Computer Name * Include ▼

Search Reset

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

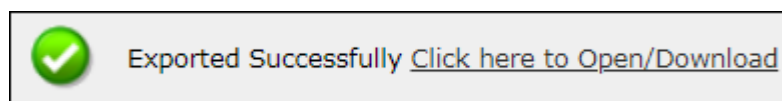
Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After making the necessary selections, click **Search**.

The Patch Report will be filtered according to your preferences.

Exporting Patch Report

To export the Patch Report, click **Export Option**. Export Option field expands. Select the preferred option and then click **Export**. A success message appears.



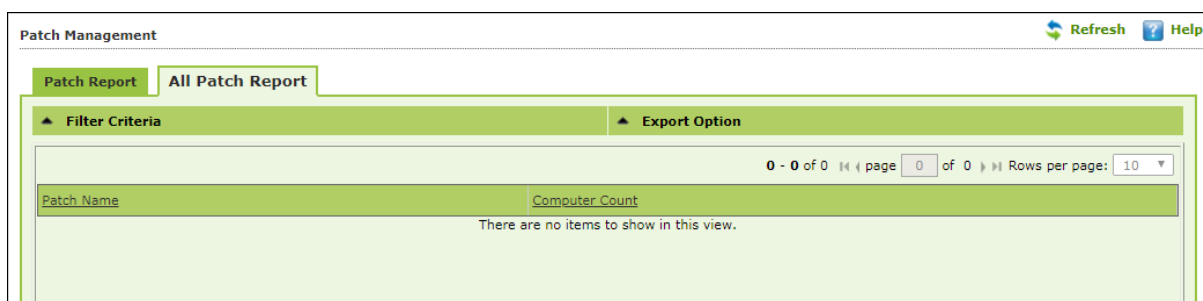
Click the link to open/download the file.

Other than security patch – for all patch Microsoft patch based on events
File AV > Advanced Settings

All Patch Report

The All Patch Report tab displays all Microsoft patches based on following specific events.

- 1-KB patches
- 2-Security Update
- 4-Hotfix
- 8-Update
- 16-Service Pack
- 31-All



Filtering All Patch Report

To filter the All Patch Report as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.

The screenshot shows the 'All Patch Report' interface. It has two tabs: 'Patch Report' and 'All Patch Report'. The 'All Patch Report' tab is active. Below the tabs, there are two main sections: 'Filter Criteria' and 'Export Option'. The 'Filter Criteria' section is expanded, showing input fields for 'Patch Name' and 'Computer Name', each with a dropdown menu set to 'Include'. There are 'Search' and 'Reset' buttons. The 'Export Option' section is collapsed. A note at the bottom states: 'Note : To enable All Patch Report Configure policy under File Antivirus-->Advanced Setting-->Send Windows Security Patch Events.' A link '(*) View All Items' is also present.

Enter the **Patch Name** and **Computer Name** to be included in the filtered report.

NOTE	To enable All Patch Report Configure policy by going to File Antivirus-->Advanced Setting-->Send Windows Security Patch Events.
------	--

Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

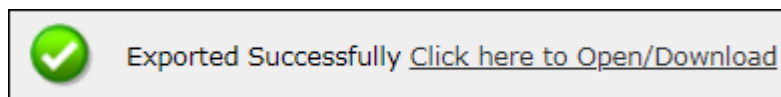
After making the necessary selections, click **Search**.

The Patch Report will be filtered according to your preferences.

Exporting All Patch Report

To export the All Patch Report, click **Export Option**. Export Option field expands.

Select the preferred option and then click **Export**. A success message appears.



Click the link to open/download the file.

Notifications

This module lets you configure notifications for different actions/incidents that occur on the server. The Notifications module consists following submodules:

- Outbreak Alert
- Event Alert
- Unlicensed Move Alert
- New Computer Alert
- Configure SIEM
- SMTP Settings

Outbreak Alert

If the virus count exceeds the limits set by you, an outbreak email notification will be sent to the recipient.

To set an outbreak alert, follow the steps given below:

1. In the navigation panel, click **Notifications > Outbreak Alert**.
Outbreak Notification screen appears.

2. Select the checkbox **Send notification**.
3. Enter the preferred values in Number and Time Limit field.
4. Click **Save**. Outbreak Alert Settings will be saved.

NOTE	In order to receive notification emails, it is necessary to configure SMTP settings. Learn more about SMTP Settings by clicking here .
-------------	--

Event Alert

This submodule lets you enable email notifications about any event that occurs on the client computers connected to the server.

Event Notification

Events Alert Settings

☐ Enable email alert Notification
 [Configure SMTP Settings](#)

Save

Cancel

To enable the event alert,

1. In the navigation panel, click **Notifications > Event Alert**.
2. Select the check box Enable email alert Notification.
3. Select the events from the list for which you prefer an alert.

Events Alert Settings

☒ Enable email alert Notification
 [Configure SMTP Settings](#)

☒ Send Information only in subject line

Select Event Ids

Select activities for which email alert is required

<input type="checkbox"/>	Event Id	Description
<input checked="" type="checkbox"/>	154	AVPMAPP_UPDATES_DONE
<input type="checkbox"/>	100	ESCAN_DUMMY_EVENT
<input type="checkbox"/>	1	MWAV_FOUND_MALWARE
<input type="checkbox"/>	2	MWAV_FOUND_VIRUS_AND_DELETED
<input type="checkbox"/>	3	MWAV_FOUND_VIRUS_AND_CLEARED
<input type="checkbox"/>	4	MWAV_FOUND_ADWARE
<input type="checkbox"/>	5	MWAV_FOUND_ERROR
<input type="checkbox"/>	6	MWAV_FOUND_VIRUS_AND_RENAMED
<input type="checkbox"/>	7	MWAV_FOUND_ADWARE_AND_DELETED
<input type="checkbox"/>	8	MWAV_LAST_COMPUTER_SCAN
<input type="checkbox"/>	9	MWAV_START
<input type="checkbox"/>	10	MWAV_SUMMARY
<input type="checkbox"/>	501	SCHED_MWAV_FOUND_MALWARE
<input type="checkbox"/>	502	SCHED_MWAV_FOUND_VIRUS_AND_DELETED
<input type="checkbox"/>	503	SCHED_MWAV_FOUND_VIRUS_AND_CLEARED
<input type="checkbox"/>	504	SCHED_MWAV_FOUND_ADWARE

4. Select the required hosts or group.
 5. Click **Save**.
- The Event Alert Settings will be saved.

Unlicensed Move Alert

This submodule lets you enable notification alert when a computer automatically moves to Unlicensed Computers category based on the setting done (under events and computers) for the computer which is not connected to the server for a long time.

To enable the unlicensed move alert,

1. In the navigation panel, click **Notifications > Unlicensed Move Alert**.
2. Select the check box **Send notification for unlicensed computers**.
3. Click **Save**.

The Unlicensed Move Alert Settings will be saved.

New Computer Alert

This submodule lets eScan send you a notification alert when a new computer is connected to the server within the IP range mentioned under the Managed Computers.

To enable the new computer alert, follow the steps given below:

1. In the navigation panel, click **Notifications > New Computer Alert**.
2. Select the checkbox **Send new Computers added notification within the shown time**.
3. Enter the preferred values in Time limit field.
4. Click **Save**.

The New Computer Alert Settings will be saved.

Configure SIEM

SIEM technology provides real-time management of security events generated for hardware changes and applications installed/uninstalled/upgraded where eScan is installed. eScan is equipped with variety of features that facilitate real-time monitoring, correlating captured events, notifications and console views and provides long-term storage, analysis and reporting of data.

To configure SIEM, follow the steps given below:

1. In the navigation panel, click **Notification > Configure SIEM**.
2. Select the **Enable event forward to SIEM/SYSLOG Server** checkbox.
3. After selecting the checkbox, it will enable the rest of the options that can be configured. You can enter the details of the SIEM/SYSLOG Server.
4. Click **Save**.

The SIEM settings will be saved.

SMTP Settings

This submodule lets you configure the SMTP settings for all the email notifications.

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

This setting lets you approve the log upload from client computers. It also lets you set the maximum FTP download sessions allowed for client computers. (Note: 0 means unlimited)

Bind IP Settings

This setting lets you bind an IP address. Click the drop-down and select the preferred IP address for binding. The default IP address is 0.0.0.0.

Log Settings

This setting provides you with the option to delete the User settings and Log files after uninstallation of eScan from the computer. To enable the above setting, select the checkbox. After selecting the checkbox, you can store client logs for the preferred number of days.

Client Grouping

This setting lets you manually manage domains and computers grouped under them after performing fresh installations.

Select **NetBIOS**, if you want to group clients only by hostname.

Select **DNS Domain**, if you want to group clients by hostname containing the domain name.

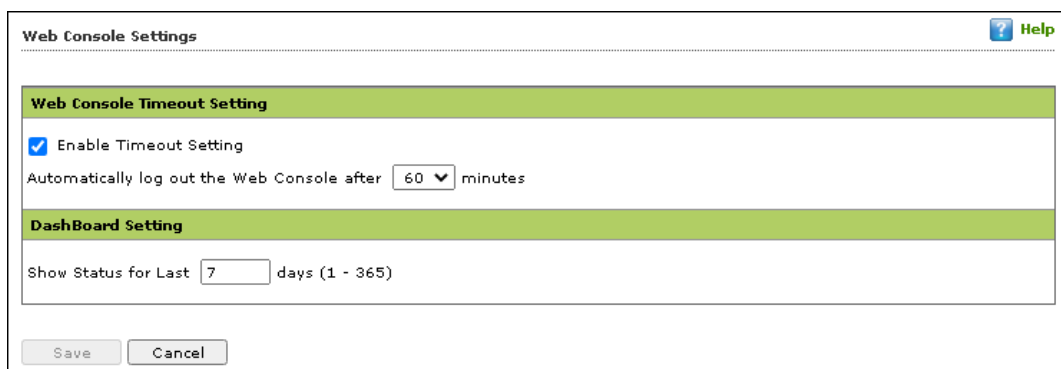
Client Connection Settings

This setting lets you modify **Thread Count** and **Query Interval** (In Seconds). To reset the values, select **Restore default values** checkbox.

After performing the necessary changes, click **Save**. The EMC Settings will be updated.

Web Console Settings

Web Console Settings submodule lets you configure web console Timeout, Dashboard, Login Page, SQL Server Connection, SQL Database compression.



The screenshot shows the 'Web Console Settings' window. It has a title bar with 'Web Console Settings' and a 'Help' icon. The window is divided into two main sections: 'Web Console Timeout Setting' and 'DashBoard Setting'. In the 'Web Console Timeout Setting' section, there is a checkbox labeled 'Enable Timeout Setting' which is checked. Below it, a text label says 'Automatically log out the Web Console after' followed by a dropdown menu showing '60' and the word 'minutes'. The 'DashBoard Setting' section has a text label 'Show Status for Last' followed by a text input field containing '7' and the text 'days (1 - 365)'. At the bottom of the window, there are two buttons: 'Save' and 'Cancel'.

Web Console Timeout Settings

To enable web console Timeout, select **Enable Timeout Setting** option.

After selecting the check box, click the drop-down and select the preferred duration.

Dashboard Setting

This setting lets you set number of days for which you wish to View the Status, Statistics and Protection Status Charts in the Dashboard. Enter the preferred number of days.

Login Page Setting

This setting lets you show or hide the download links shared for eScan Client setup, Agent setup and AV Report. To show the download links on login page, select the checkboxes of respective links.

SQL Server Connection settings

This setting lets you select an authentication mode between Microsoft Windows Authentication Mode to SQL Server Authentication Mode. Select the **SQL Server Authentication Mode** and define **Server instance** and **Host Name** along with the credentials for connecting to the database.

Server Instance

It displays the current server instance in use. To select another server instance, click **Browse**. Select an instance from the list and click **OK**.

Hostname/IP Address

It displays the Hostname or IP Address of the server instance computer.

Enter the credentials in **Username** and **Password** fields.

To check whether correct credentials are entered, click **Test Connection**.

SQL Database Purge Settings

This setting lets you define the maximum SQL database size in MB and purge data older than the specified days. To enable SQL Database Purge Settings, select **Enable Database Purge** checkbox.

Enter the preferred value in **Database Size threshold in (MB)** field.

Enter the preferred number of days in **Purge data older than specified days, if above threshold** is met field.

RMM Settings

This setting lets you configure default RMM setting for connecting to client via RMM service:

Activate View Only

By default, after taking a remote connection, you can only view the endpoint screen and are unable to perform any activity.

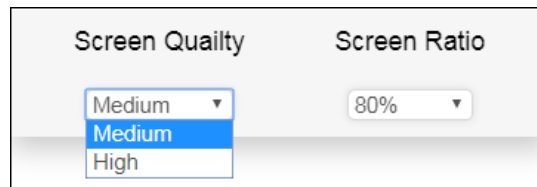
De-Activate View Only

To perform activity on an endpoint after taking remote connection, click **De-Activate View Only**.

Screen Quality Settings

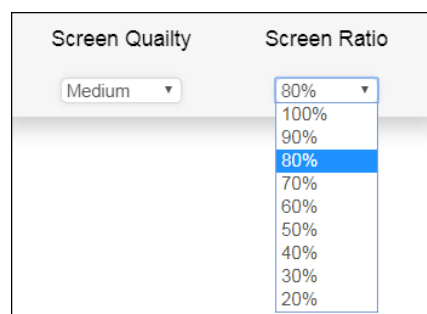
This option lets you configure the screen as per your requirements. It consists following suboptions:

- **Screen Quality** can be set to **Medium** or **High**.



Screen Quality	Screen Ratio
Medium ▼	80% ▼
Medium	
High	

- **Screen Ratio** can be set to anywhere from **20%** to **100%**.



Screen Quality	Screen Ratio
Medium ▼	80% ▼
	100%
	90%
	80%
	70%
	60%
	50%
	40%
	30%
	20%

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.

Update Settings

The Update Settings submodule keeps your virus definitions up-to-date and protects your computer from emerging species of viruses and other malicious programs. This submodule lets you configure update settings, update notifications and schedule updates according to your need.

You can configure eScan to download updates automatically either from eScan update servers or from the local network by using FTP or HTTP. You can configure following settings.

General Config

The **General Config** tab lets you configure update settings. The settings let you select the mode of update and configure proxy settings.

The screenshot shows the 'Update Settings' window with the 'General Config' tab selected. The window has a title bar with 'Update Settings' and a 'Help' button. Below the title bar are four tabs: 'General Config', 'Update Notification', 'Scheduling', and 'Update Distribution'. The 'General Config' tab is active and contains the following settings:

- Select Mode:** Two radio buttons, 'FTP' and 'HTTP'. 'HTTP' is selected.
- Proxy Settings:** A section with a checkbox 'Download via Proxy' which is unchecked.
 - HTTP:** A sub-section with fields for 'HTTP Proxy Server IP', 'Port', 'Login Name', and 'Password'.
 - FTP:** A sub-section with fields for 'FTP Proxy Server IP', 'Port', 'Login Name', and 'Password'.
 - Logon Type:** A sub-section with radio buttons for 'User@siteaddress', 'OPEN siteaddress' (selected), 'PASV Mode', and 'Socks'. There is also a dropdown menu showing '4'.

At the bottom of the window are three buttons: 'Save', 'Cancel', and 'Update'.

Select Mode

Select the mode for downloading updates. Following options are available:

- FTP
- HTTP

Proxy Settings

Proxy Settings lets you configure proxy for downloading updates.

To enable Proxy Settings, select **Download via Proxy** checkbox. You will be able to configure proxy settings depending on the mode of selection.

If you are using HTTP proxy servers, enter the HTTP proxy server IP address, port number and HTTP proxy server's authentication credentials.

If you are using FTP proxy servers, along with HTTP settings mentioned above you will have to enter FTP proxy server IP address, Port number, FTP proxy server's authentication credentials and Logon enter.

After filling the necessary data, click **Save > Update**. The General Config tab will be saved and updated.

Update Notification

The **Update Notification** tab lets you configure email address and SMTP settings for email notifications about database update.

Update Settings

General Config | **Update Notification** | Scheduling | Update Distribution

☐ Update Notification

Sender:

Recipient:

SMTP Server: SMTP Port:

☐ Use SMTP Authentication

User name:

Password:

Test

Save Cancel Update

Update Notification

To receive email notifications from eScan about virus signature database update, select this option.

Sender

Enter an email ID for sender.

Recipient

Enter the notification recipient's email ID.

SMTP Server and Port

Enter the SMTP server's IP address and Port number in the respective fields.

Use SMTP Authentication

If the SMTP server requires authentication, select this checkbox and enter the login credentials in the **Username** and **Password** fields.

After filling the necessary data, click **Save > Update**. The Update Notification will be saved and updated.

Scheduling

The Scheduling tab lets you schedule updates with Automatic or Schedule Download mode.

The screenshot shows the 'Update Settings' dialog box with the 'Scheduling' tab selected. The dialog has four tabs: 'General Config', 'Update Notification', 'Scheduling', and 'Update Distribution'. The 'Scheduling' tab is active, showing two main sections: 'Automatic Download' and 'Schedule Download'. In the 'Automatic Download' section, the 'Query Interval' is set to 15 minutes. In the 'Schedule Download' section, the 'Daily' option is selected, and the time is set to 12:02 PM. There are also checkboxes for 'Weekly' and 'Monthly' scheduling. At the bottom of the dialog are 'Save', 'Cancel', and 'Update' buttons.

Automatic Download

The eScan Scheduler sends a query to the update server at set intervals and downloads the latest updates if available. To set an interval, click the **Query Interval** drop-down and select a preferred duration.

Schedule Download

The eScan Scheduler lets you set a schedule the download for daily, weekly, or monthly basis at a specified time. The scheduled query will be sent to the update server as per your preferences.

After filling the necessary data, click **Save > Update**. The Scheduling tab will be saved and updated.

Update Distribution

The Update Distribution tab allows the admin to enable and disable the sharing of eScan Virus signature to be distributed to air-gapped/isolated network.

The screenshot shows the 'Update Settings' dialog box with the 'Update Distribution' tab selected. The 'Setting' section has two radio buttons: 'Enable Share' (unselected) and 'Disable Share' (selected). Below this, there are sections for 'Anti-spam/product Updates' and 'AntiVirus Updates'. The 'AntiVirus Updates' section includes a '32 bit share path' field, a checked checkbox for 'Enable 64 bit update (Required only if 64 bit Linux and MAC system are in network)', and a '64 bit share path' field. A red note at the bottom states: '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)'. At the bottom are 'Save' and 'Cancel' buttons.

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.



- Click **Settings**. Update Settings window appears.

Update Settings

General Config | After Update | Scheduling

Select Mode: ☐ FTP ☐ HTTP ☒ Network

Proxy Settings

☒ Download via Proxy

HTTP

HTTP Proxy Server IP: Port:

Login Name: Password:

FTP

FTP Proxy Server IP: Port:

Login Name: Password:

Logon Type

☐ User@siteaddress

☒ OPEN siteaddress

☐ PASV Mode

☐ Socks

Network Source UNC Path:

Default OK Cancel Apply

- Select **Network** option and set the **Source UNC Path** as **\\ServerName\esupd** or **\\ServerIP\esupd**.

E.g.: \\192.0.2.0\esupd

After setting UNC path for the air-gapped network, the update will be available automatically to the Isolated/Air-gapped network.

Auto-Grouping

The Auto grouping submodule consists following subsections:

- Auto Add Client setting
- Client(s) list excluded from Auto adding under Managed Group(s)
- Group and Client selection criteria for Auto adding under Managed Group(s)

Auto Grouping
Refresh
Help

Auto Add Client setting

☒ Auto adding client(s) under Managed Group(s)

Client(s) list excluded from Auto adding under Managed Group(s)

Add

Remove

e.g.: Host Name
Host Name with wildcard
IP Address
IP Address Range

Group and Client selection criteria for Auto adding under Managed Group(s)

Group Name

Add

Remove

Browse

Up

Down

e.g.: group1
group1\subgroup...

Client Criteria

Add

Remove

Run Now

e.g.: Host Name
Host Name with wildcard
IP Address
IP Address Range

Save

Cancel

Auto Add Client setting

Selecting the checkbox **Auto adding client(s) under Managed Group(s)** enables automatic adding computers under Managed group(s) after manual installation of eScan client.

Client(s) list excluded from Auto adding under Managed Group(s)

Adding a client in this list ensures that it does not auto add itself again after you remove it from the Managed computer(s).

Group and Client selection criteria for Auto adding under Managed Group(s)

This section lets you define/create groups with client criteria for auto adding under managed group(s). You can add a list of clients under a particular group name here and then add it under the exclusion list if required.

Excluding clients from auto adding under Managed Group(s)

To exclude clients from auto adding under managed group(s), follow the steps given below:

1. Enter either the host name, host name with wildcard, IP address or IP address range.
2. Click **Add**. The computer will be displayed in the list below.

Removing clients from the excluded list

1. Select the computer you want to remove.
2. Click **Remove**. The computer will be removed from the list.

Group and Client selection criteria for Auto adding under Managed Group(s)

This feature can be used to automate the process of adding computers/clients under a particular group. This process is manually done under unmanaged computers.

Defining a group and client selection criteria for auto adding under managed computer(s)

To define group and client selection criteria for auto adding under managed groups(s), follow the steps given below:

Group and Client selection criteria for Auto adding under Managed Group(s)

Group Name

Group Name input field

Buttons: Add, Remove, Browse, Up, Down

e.g.: group1
group1\subgroup...

Client Criteria

Client Criteria input field

Buttons: Add, Remove, Run Now

e.g.: Host Name
Host Name with wildcard
IP Address
IP Address Range

1. Under the Group Name, enter the group's name and click **Add**.

OR

Click **Browse** and select the group from the existing list.

NOTE To browse through the list of groups, click **Up** or **Down**.

2. Select the group for which you want to define the criteria.
3. Under the Client Criteria, enter either Hostname, Hostname with wildcard, IP address or IP address range and click **Add**. The clients displayed in the list will be added under the selected group.
4. Click **Save**. The client will be saved under that group.
5. To apply the settings for the newly added client, click **Run Now**.

Two-Factor Authentication (2FA)

The system login password is Single-Factor Authentication which is considered unsecure as it may put your organization's data at high risk of compromise. The Two-Factor Authentication, also more commonly known as 2FA, adds an extra layer of protection to your eScan web console login.

The 2FA feature mandates you to enter a Time-based One-Time Password (TOTP) after entering eScan credentials. So, even if somebody knows your eScan credentials, the 2FA feature secures data against unauthorized logins. Only administrator can enable/disable the 2FA feature. It can also be enabled for added users as well.

To use 2FA login feature, you need to install the Authenticator app for Android devices from [Play Store](#) or for iOS devices from [App Store](#) on your smart device. The Authenticator app needs camera access for scanning a QR code, so ensure you get an appropriate approval to use device camera in your organization. If a COD or BYOD policy restricts you from using device camera in your organization, enter the Account Key in the Authenticator app.



NOTE

Ensure that the smart device's date and time matches with the system's date and time or else TOTP's generated by app won't get validated.

IMPORTANT

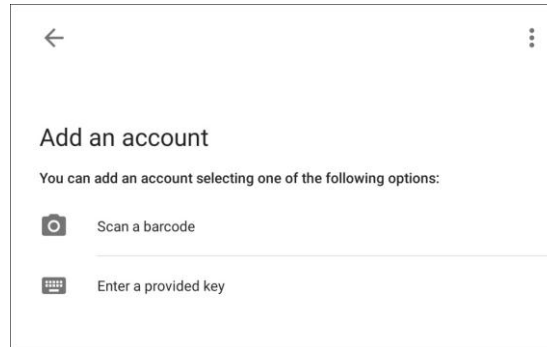
We recommend that you save/store the **Account Key** in offline storage or a paperback copy, in case you lose the account access.

Enabling 2FA login

To enable 2FA login,

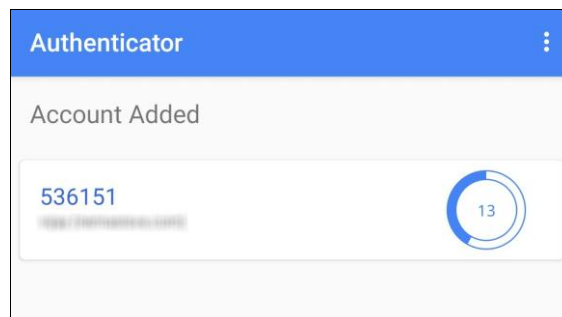
1. Go to **Settings > Two-Factor Authentication**.
2. Open the Authenticator app.

After basic configuration following screen appears on smart device.

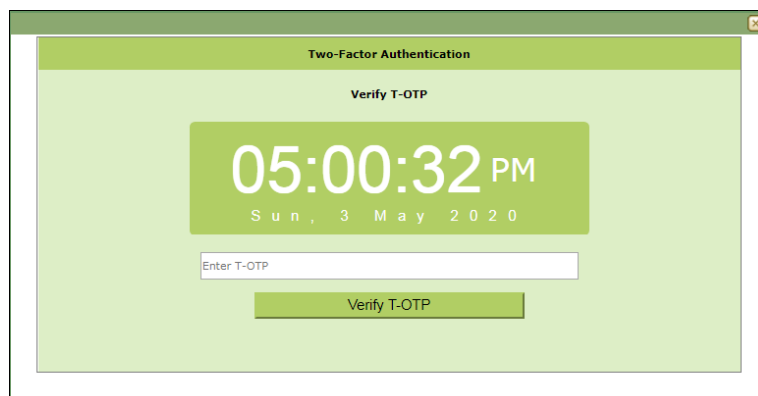


3. Select a preferred option. If you tapped **Scan a barcode**, scan the onscreen QR code via your smart device. If you tapped **Enter a provided key**, enter the Account Key and then tap **ADD**.



After scanning the Account QR code or entering Account Key the eScan server account gets added to the Authenticator app. The app then starts displaying a Time-based One-Time Password (TOTP) that is valid for 30 seconds.

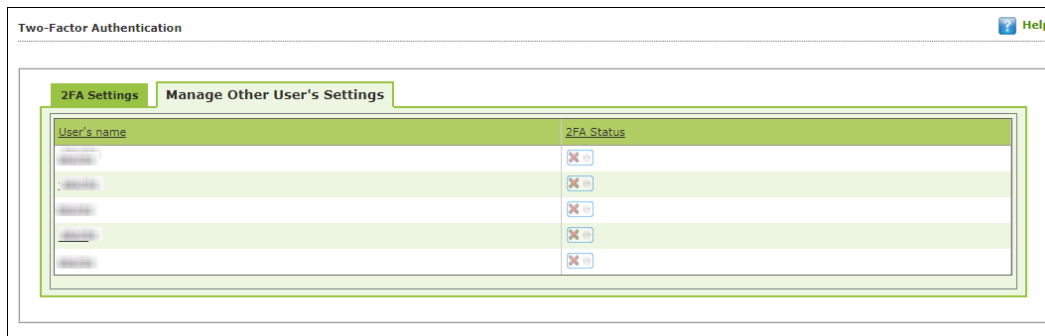


4. Click **Enable Two-Factor Authentication**.
Verify TOTP window appears.



5. Enter the TOTP displayed on smart device and then click **Verify TOTP**.
The 2FA login feature gets enabled.
6. To apply the login feature for users, click **Manage Other User Settings** tab.
The tab displays list of added users and whether 2FA status is enabled or disabled.

-  - 2FA Disabled
-  - 2FA Enabled

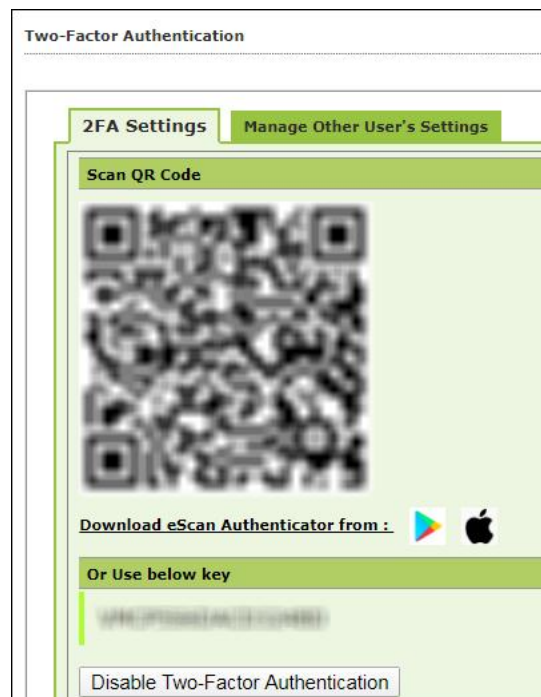


7. To enable 2FA login for an added user, click the button to check icon.
The 2FA login for added users gets enabled. After enabling the 2FA login for users, whenever they log in to eScan web console Verify TOTP window appears.

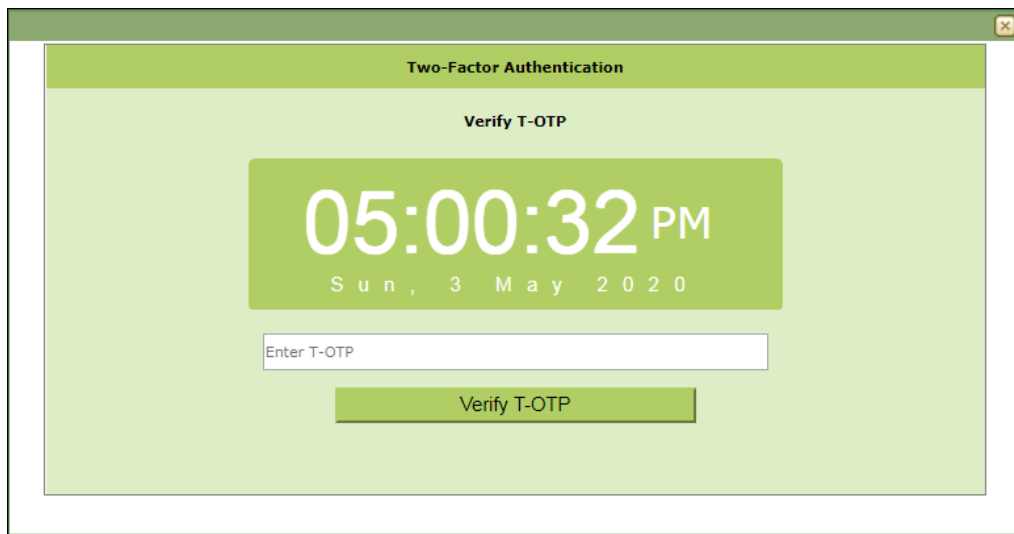
Disabling 2FA login

To disable 2FA login,

1. Go to **Settings > Two Factor Authentication**.
2. Click **Disable Two-Factor Authentication**.



Verify TOTP window appears.



3. Enter the TOTP and then click **Verify TOTP**.
The 2FA feature gets disabled.

NOTE	After disabling the 2FA feature and enabling it again, the 2FA login status will be reinstated for added users.
-------------	---

Administration

The Administration module lets you create User Accounts and allocate them Admin rights for using eScan Management Console. In a large organization, installing eScan client on all computers may consume lot of time and efforts. With this option, you can allocate rights to the other employees and allow them to install eScan Client, implement Policies and Tasks.

The Administration module consists following submodules:

- User Accounts
- User Roles
- Export & Import
- Customize Setup

User Accounts

For a large organization, installing eScan Client and monitoring activities may become a difficult task. With User Accounts submodule, you can create new user accounts and assign Administrator role to added users and reduce the workload. This submodule displays a list of users and their details like Domain, Role, Session Log and Status.

User Accounts					
Create New Account Delete		1 - 1 of 1 page 1 of 1		Rows per page: 100	
User name	Full Name	Domain	Role	Session Log	Status
root	Administrator account created during installation		Administrator	View	
Create New Account Delete		1 - 1 of 1 page 1 of 1		Rows per page: 100	

Create New Account

To create a User Account,

1. In the User Accounts screen, click **Create New Account**.
Create User form appears.

Create User

User Accounts > Create User

Account Type and Information

User name*:

Full Name*:

Password*:

Confirm Password*:

Email Address*:

For Example: user@yourcompany.com

Account Role

Role*: Administrator

Save

Cancel

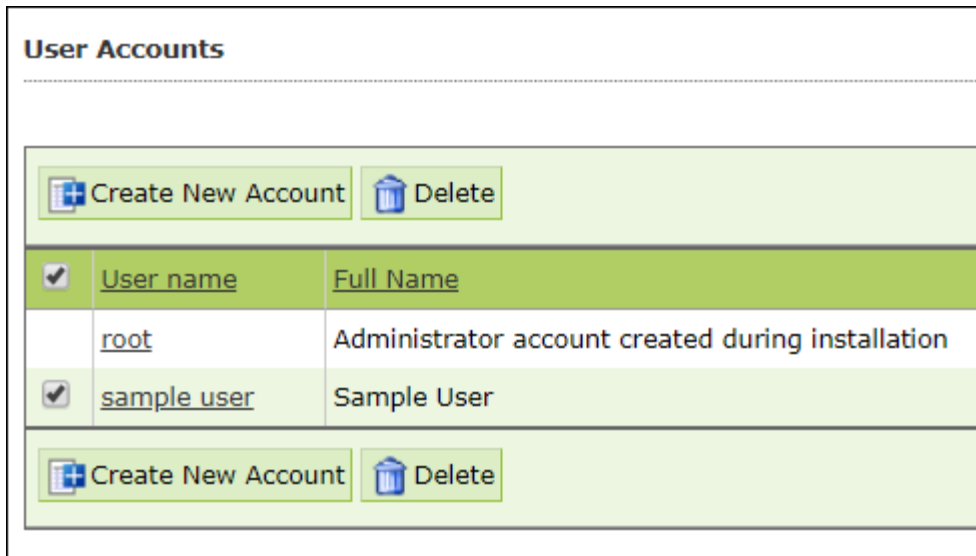
(*) Mandatory Fields

2. After filling all the details, click **Save**.
The user will be added to the User Accounts list.

Delete a User Account

To delete a user account

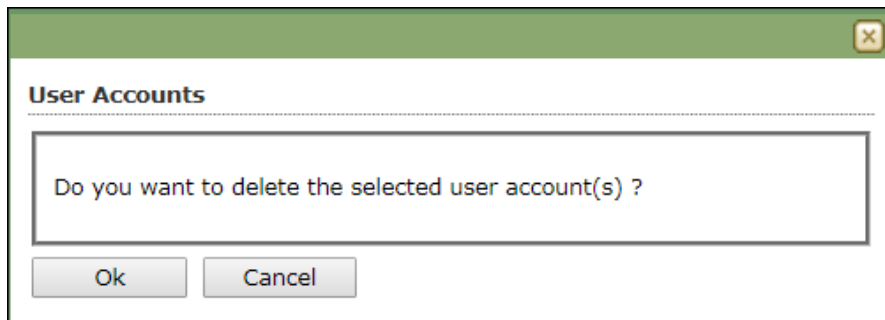
1. In the User Accounts screen, select the user you want to delete.



User Accounts

<input checked="" type="checkbox"/>	User name	Full Name
<input type="checkbox"/>	root	Administrator account created during installation
<input checked="" type="checkbox"/>	sample user	Sample User

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.

The screenshot shows the 'User Roles' management interface. At the top, there are buttons for 'New Role', 'Properties', and 'Delete'. Below these is a table with two columns: 'Role Name' and 'Description'. The table contains one entry: 'Administrator'.

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.

The screenshot shows the 'New Role' form. It has a breadcrumb 'User Roles > New Role'. Under the 'Role Details' section, there are three fields: 'New Role Name : *' (required), 'Description :', and 'Select Group :'. The 'Select Group' dropdown is open, showing a list of groups with 'Managed Computers' selected. At the bottom, there is an 'Ok' button.

2. Enter name and description for the role.
3. Click **Managed Computers** and select the specific group to assign the role.
The added role will be able to manage and monitor only the selected group's activities.
4. Click **OK**.

Permissions section appears displaying Main Tree Menu and Client Tree Menu tabs. The Main Tree Menu consists of Navigation Panel Access permissions while the Client Tree Menu consists of selected groups on which permissions the user is allowed to take further.

Permissions		
Main Tree Menu	Client Tree Menu	
Menu	View	Configure
Dashboard	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Managed Computers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Report Templates	<input type="checkbox"/>	<input type="checkbox"/>
Report Scheduler	<input type="checkbox"/>	<input type="checkbox"/>
Events & Computers	<input type="checkbox"/>	<input type="checkbox"/>
Asset Management	<input type="checkbox"/>	<input type="checkbox"/>
User Activity	<input type="checkbox"/>	<input type="checkbox"/>
Print Activity	<input type="checkbox"/>	<input type="checkbox"/>
Session Activity Report	<input type="checkbox"/>	<input type="checkbox"/>
File Activity Report	<input type="checkbox"/>	<input type="checkbox"/>
Notifications	<input type="checkbox"/>	<input type="checkbox"/>
Event Alert	<input type="checkbox"/>	<input type="checkbox"/>
Unlicense Move Alert	<input type="checkbox"/>	<input type="checkbox"/>
Settings	<input type="checkbox"/>	<input type="checkbox"/>
Web Console Settings	<input type="checkbox"/>	<input type="checkbox"/>

5. Select the check boxes that will allow the role to view/configure the module.
6. After selecting the necessary check boxes, click **Save**.
The role will be added to the User Roles list.

View Role Properties

To view the properties of a role

1. In the User Roles screen, select a role.
2. This enables **Properties** and **Delete** buttons.

User Roles		
<div> New Role Properties Delete </div>		
Role Name	Description	
Administrator		
<input checked="" type="checkbox"/> Monitor	For viewing activities	

3. Click **Properties**.

Properties screen appears. It lets you modify role description, permissions for accessing and configuring modules and assign the role to other groups by clicking **Select Group Tree**.

Properties Help

User Roles > Properties

Role Details

New Role Name :*

Description :

Select Group :

Permissions

Main Tree Menu Client Tree Menu

Menu	View	Configure
DashBoard	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Managed Computers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Report Templates	<input type="checkbox"/>	<input type="checkbox"/>
Report Scheduler	<input type="checkbox"/>	<input type="checkbox"/>
Events & Computers	<input type="checkbox"/>	<input type="checkbox"/>
Asset Management	<input type="checkbox"/>	<input type="checkbox"/>
User Activity	<input type="checkbox"/>	<input type="checkbox"/>
Print Activity	<input type="checkbox"/>	<input type="checkbox"/>
Session Activity Report	<input type="checkbox"/>	<input type="checkbox"/>
File Activity Report	<input type="checkbox"/>	<input type="checkbox"/>
Notifications	<input type="checkbox"/>	<input type="checkbox"/>
Event Alert	<input type="checkbox"/>	<input type="checkbox"/>
Unlicense Move Alert	<input type="checkbox"/>	<input type="checkbox"/>
Settings	<input type="checkbox"/>	<input type="checkbox"/>
Web Console Settings	<input type="checkbox"/>	<input type="checkbox"/>
Excluded Clients	<input type="checkbox"/>	<input type="checkbox"/>
Administration	<input type="checkbox"/>	<input type="checkbox"/>
User Accounts	<input type="checkbox"/>	<input type="checkbox"/>
User Roles	<input type="checkbox"/>	<input type="checkbox"/>
License	<input type="checkbox"/>	<input type="checkbox"/>
Policy Templates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

4. To modify client configuration permissions, click **Client Tree Menu**.

Client Tree Menu

Define the Actions that the created role can configure for the allocated group. The menu has Action List, Client Action List, Select Policy Template, Policy Criteria, and Group Tasks.

User Roles > Properties

Role Details

Role Name : *

Description :

Select Group :

Permissions

Main Tree Menu Client Tree Menu

Managed Computers

[Managed Computers/Escan]

Menu	Configure
Action List	<input type="checkbox"/>
New Sub Group	<input checked="" type="checkbox"/>
Remove Group	<input checked="" type="checkbox"/>
Create Client Setup	<input checked="" type="checkbox"/>
Properties	<input checked="" type="checkbox"/>
Client Action List	<input type="checkbox"/>
Move to Group	<input checked="" type="checkbox"/>
Remove from Group	<input checked="" type="checkbox"/>
Manage Add-On License	<input checked="" type="checkbox"/>
Export	<input checked="" type="checkbox"/>
Show Installed Softwares	<input checked="" type="checkbox"/>
Create OTP	<input checked="" type="checkbox"/>
Properties	<input checked="" type="checkbox"/>
Anti-Theft Options	<input checked="" type="checkbox"/>
Disable Anti-Theft	<input checked="" type="checkbox"/>
Select Policy Template	<input checked="" type="checkbox"/>

- To let the role configure these actions, under the Configure column select the check boxes of corresponding actions.
- Click **Save**.
The Role Properties will be updated accordingly.

Delete a User Role

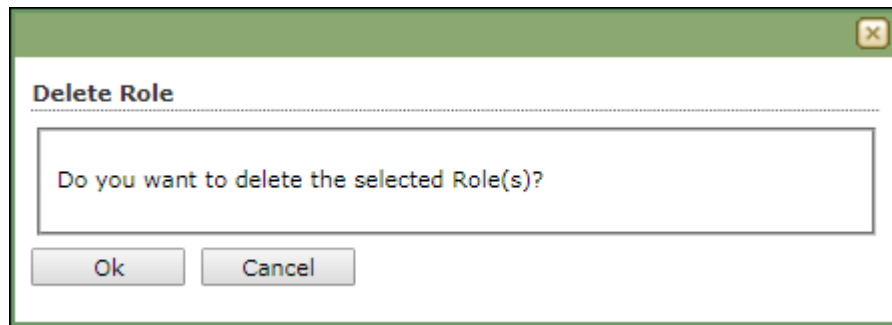
To delete a user role

- In the User Roles screen, select the user role you want to delete.

User Roles

Role Name	Description
Administrator	
<input checked="" type="checkbox"/> Monitor	For viewing activities

- Click **Delete**.
A delete confirmation prompt appears.



3. Click **OK**.
The User Role will be deleted.

Export & Import

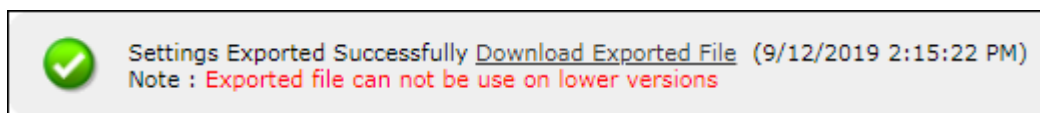
The Export & Import submodule lets you to take a backup of your eScan server settings, in case you want to replace the existing eScan server. You can export the Settings, Policies and the Database from existing server to a local drive and import it to the new server.

Export Settings

This tab lets you export the eScan Server Settings, Policies, and Database. To export the eScan Server settings, follow the steps given below:

1. In the Export Import Settings screen, click **Export Settings** tab.

2. To backup Settings and Policies and Database, select both the checkboxes. The backup file will be exported to the path shown in Export File Path field. To change the file path, click **Change Path**. Enter the file path and click **Add**.
3. Click **Export**. The backup file will be exported to the destination path. A success message appears at the top displaying date, time and a download link for the exported file.



Import Settings

This tab lets you import the eScan Server Settings, Policies, and Database. To import the eScan Server settings, follow the steps given below:

1. In the Export Import Settings screen, click **Import Settings** tab.

Export Import Settings

Export Settings | **Import Settings** | Scheduling

File Name No file chosen

☒ WMC Settings and Policies

☐ Database

[View Exported Files](#)

1. Select file to import (EservConf_[YYYYMMDDhhmm]_[SCHD].zip)
 2. Select required settings
 3. Click on "Import" button to import the saved settings

2. Click **Choose File**.
The Import Settings tab lets you import only Settings and Policies or Database.
3. To import Settings and Policies and Database, select both the checkboxes.
4. Click **Import**.
The backup file will be imported. A success message is displayed after complete import.

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.

To create a Schedule for export, follow the steps given below:

1. Select **Enable Export Scheduler** checkbox.
2. Select the checkboxes whether to back up both Settings and Policies and Database.
3. Schedule the backup for a **Daily**, **Weekly** (Select a day) or **Monthly** (Select a date) basis.
4. For the **At** field, click the drop-down and select a time for backing up data.

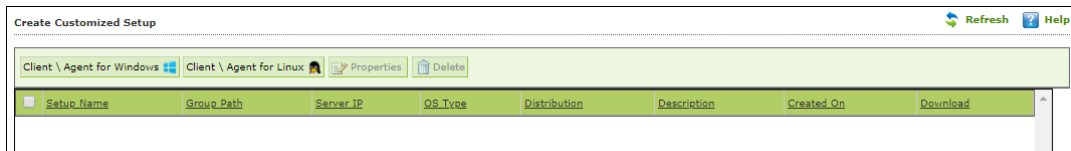
If you want to receive email notifications about the procedure, select Enable Notifications Settings checkbox and fill in the necessary details. If the SMTP server requires authentication, select the Use SMTP Authentication checkbox and enter the credentials. To check if the SMTP settings are correct, click **Test**. A test email will be sent to recipient email ID.

To configure additional settings for backup file, select the Enable Optional Settings, and make the necessary changes. To restore the changes made, click **Default**.

5. After performing all the necessary steps, click **Save**.
The export schedule will be saved.

Customize Setup

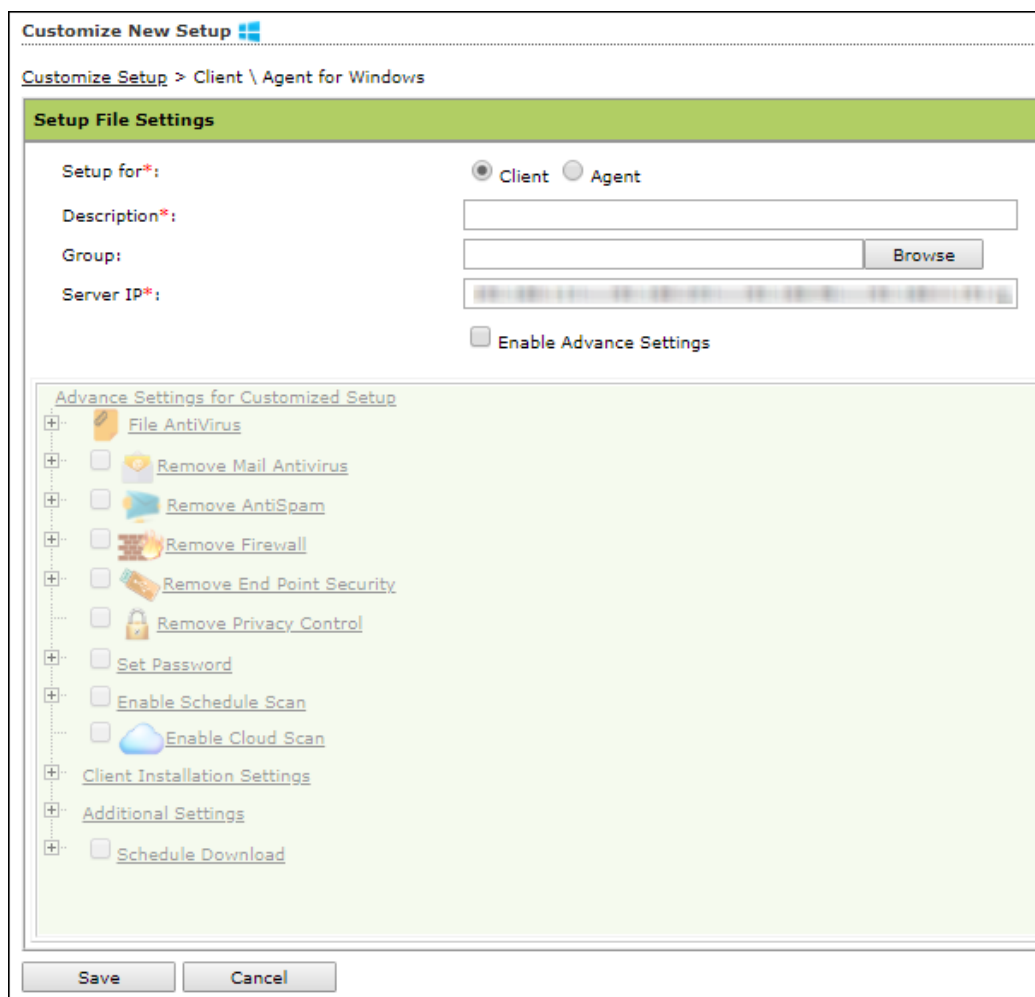
This submodule lets you create a customized setup for a Client or an Agent with fewer modules and deploy it to various locations. This can be very useful, if there are locations to which a server is unable to push the setup or locations that are unable to connect to the server directly. The custom setup can be downloaded as a file and sent to different locations.



Creating a customized setup for Windows

To create a customized setup for Windows, follow the steps given below:

1. In Create Customized Setup screen, click **Client/Agent for Windows**.
Customize New Setup screen appears.



2. Select whether the setup file is being created for **Client** or **Agent**.
3. Enter description for the setup file.
4. Click **Browse** and select a group for which this setup is being created.
5. Enter eScan Server IP address.
6. If you want to provide advanced settings with the setup, select the **Enable Advance Settings** checkbox. Doing so enables the bottom field. Select the setting checkboxes you want to provide.
7. Click **Save**.
The customized setup for Windows will be created.

Creating a customized setup for Linux





To create a customized setup for Linux, follow the steps given below:

1. In Create Customized Setup screen, click **Client\Agent for Linux**.
Customize New Setup screen appears.


2. Enter a description for the setup.
3. Click the drop-down select whether the setup is being created for Red Hat or Debian.
4. Source Setup file path field displays the setup file's location. If you want to change path, enter the new path in this field.
5. Click **Browse** and select a group for which this setup is being created.
6. Enter eScan Server IP address.
7. Click **Save**.
The customized setup for Linux will be created.

Editing Setup Properties (only Windows)

The properties can be edited for only customized Windows setup. To edit the customized Windows setup's properties, follow the steps given below:

Client \ Agent for Windows  Client \ Agent for Linux  Properties  Delete 			
<input type="checkbox"/>	Setup Name	Group Path	Server IP
<input type="checkbox"/>	Managed Computers_20190913_144040721.rpm	Managed Computers	192.168.1.100:8080
<input checked="" type="checkbox"/>	Setup_20190913_144233504.exe	Managed Computers	192.168.1.100:8080

1. In the Create Customized Setup screen, select the Windows setup you want to edit.
2. Click **Properties**.
Edit Customized Setup screen appears.

Edit Customized Setup 

Customize Setup > Client \ Agent for Windows

Setup File Settings

Setup for*: Client Agent

Description*: Sample

Group: Managed Computers Browse

Server IP*: 192.168.1.100:8080

☐ Enable Advance Settings

Advance Settings for Customized Setup

File AntiVirus

☐ Remove Mail Antivirus

☐ Remove AntiSpam

☐ Remove Firewall

☐ Remove End Point Security

☐ Remove Privacy Control

☐ Set Password

☐ Enable Schedule Scan

☐ Enable Cloud Scan

Client Installation Settings

Additional Settings

☐ Schedule Download

Save

Cancel

3. Make the necessary changes and then click **Save**. The setup will be updated.

Deleting a Setup

To delete a setup, follow the steps given below:

<div> Client \ Agent for Windows Client \ Agent for Linux Properties Delete </div>			
<input type="checkbox"/>	Setup Name	Group Path	Server IP
<input type="checkbox"/>	Managed Computers_20190913_144040721.rpm	Managed Computers	
<input checked="" type="checkbox"/>	Setup_20190913_144233504.exe	Managed Computers	

1. In the Create Customized Setup screen, select the setup you want to delete.
2. Click **Delete**.

The setup will be deleted.

License

The License module lets you manage user licenses. You can add, activate, and view the total number of licenses available for deployment, previously deployed, and licenses remaining with their corresponding values. The module also lets you move the licensed computers to non-licensed computers and vice versa. Here you can also view the number of add-on license along with the name of it. For example, as you can see here there are 15 add-on licenses for eBackup feature. The add-on license is available for eBackup, 2FA, and DLP features.

License

Refresh Help

Register Information

License Key(30 char)	Activation Code(50 char)	Registration Status	Contract Period Ends on	No. of Users	Add On License
-----	Activate Now	Activate before 01-Jun-2020	-	10	---
-----	-----	Activated	20-Apr-2021	200	EBackup+ RMM+ DLP+ 2FA
-----	-----	Activated	13-May-2021	200	---

To Add License [Click Here](#)

License

License In Use

132

License Remaining

268

Total License Size

400

Manage License

Adding and Activating a License

To add and activate a license

1. In the License screen, click the **Click Here** link.

To Add License [Click Here](#)

Add License Key dialog box appears.

Add 30 Character License Key.

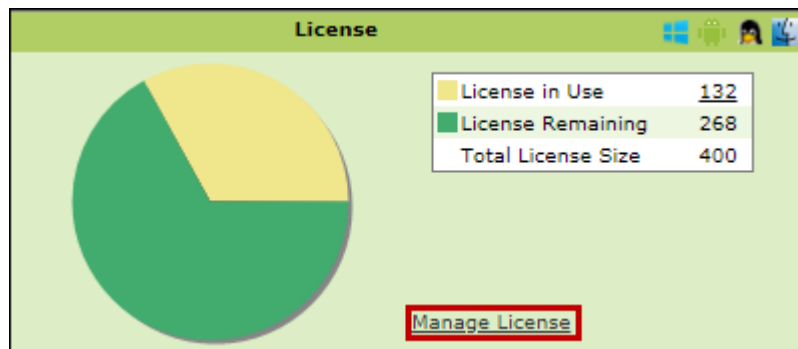
OK Cancel

2. Enter the license key and then click **OK**.
The license key will be added and displayed in the **Register Information** table.

Moving Licensed Computers to Non-Licensed Computers

To move licensed computers to non-licensed computers,

1. In the License statistics box, click **Manage License**.



Manage License window appears.

Manage License ? Help

Licensed Computers / Devices (132) Filter License: All ▼ Move to Non-License

<input type="checkbox"/>	Machine Name	Group
<input type="checkbox"/>	WIN-7-100	Managed - Computers - All - Apps
<input type="checkbox"/>	WIN-7-100	Managed - Computers - All - Apps
<input type="checkbox"/>	WIN-7-100	Managed - Computers - All - Apps
<input type="checkbox"/>	WIN-7-100	Managed - Computers - All - Apps
<input type="checkbox"/>	WIN-7-100	Managed - Computers - All - Apps
<input type="checkbox"/>	WIN-7-100	Managed - Computers - All - Apps
<input type="checkbox"/>	WIN-7-100	Managed - Computers - All - Apps

Non-Licensed Computers / Devices (327) Filter License: All ▼ Move to License

<input type="checkbox"/>	Machine Name	Group	Unlicense Date Time	Description
<input type="checkbox"/>	WIN-7-100	Managed - Computers - All - Apps	31/03/2018 02:08:25	
<input type="checkbox"/>	WIN-7-100	Managed - Computers - All - Apps	17/02/2018 11:10:01	
<input type="checkbox"/>	WIN-7-100	Managed - Computers - All - Apps	15/02/2018 11:50:10	

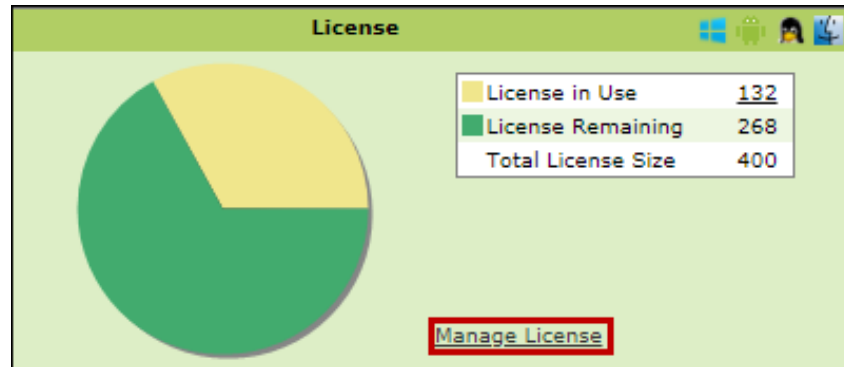
Close

2. Under the Licensed Computers section, select the computer(s) that you want to move to Non-Licensed Computers section.
3. Click **Move to Non-License**.
4. The selected computer(s) will be moved to Non-Licensed computers section.

Moving Non-Licensed Computers to Licensed Computers

To move licensed computers to non-licensed computers, follow the steps given below:

1. In the License statistics box, click **Manage License**.



Manage License window appears.

Manage License Help

Licensed Computers (385) Move to Non-License

<input type="checkbox"/>	Machine Name	Group
<input type="checkbox"/>	WIN-10-10-10-10-10-10-10-10	Managed Computers
<input type="checkbox"/>	WIN-10-10-10-10-10-10-10-10	Managed Computers
<input type="checkbox"/>	WIN-10-10-10-10-10-10-10-10	Managed Computers
<input type="checkbox"/>	WIN-10-10-10-10-10-10-10-10	Managed Computers
<input type="checkbox"/>	WIN-10-10-10-10-10-10-10-10	Managed Computers
<input type="checkbox"/>	WIN-10-10-10-10-10-10-10-10	Managed Computers

Non-Licensed Computers (2) Move to License

<input type="checkbox"/>	Machine Name	Group	Unlicense Date Time	Description
<input type="checkbox"/>	WIN-10-10-10-10-10-10-10-10	Managed Computers	13/09/2019 17:13:16	
<input type="checkbox"/>	WIN-10-10-10-10-10-10-10-10	Managed Computers	13/09/2019 17:13:16	

2. Under the Non-Licensed Computers section, select the computer(s) that you want to move to Licensed Computers section.
3. Click **Move to License**.
4. The selected computer(s) will be moved to Licensed Computers section.

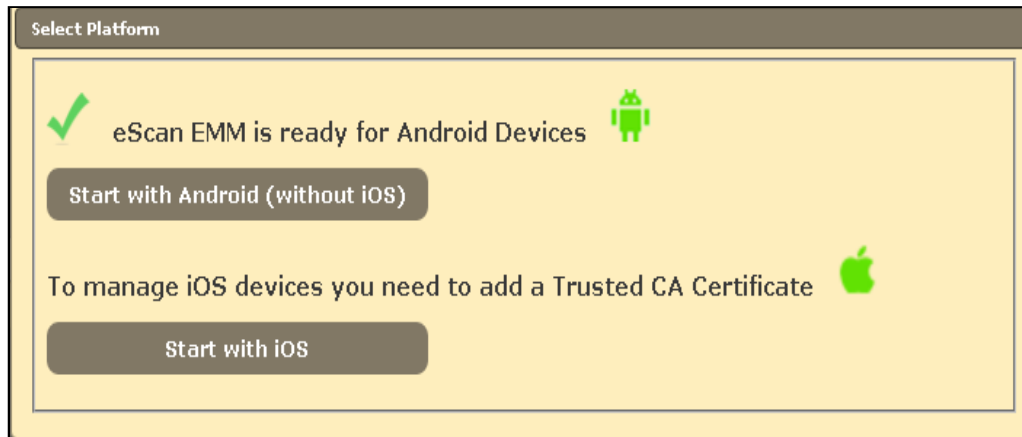
eScan Mobility Management

eScan Mobility Management solution is specifically designed for your smartphones and tablets. The application helps you secure and protect your devices against viruses, malwares, Trojans, and safeguards your confidential data. It also lets you block access to other applications and websites ensuring complete device protection. By using eScan Mobility Management Solution you can manage and secure Mobile as well as Smartphones.

eScan Mobility Management lets you monitor, secure and manage all of your devices remotely. By using this application you can control and monitor all security settings, gain real-time visibility of security status into mobile devices accessing your corporate network, and administer consistent policies across all devices.

Getting Started

Click **eScan Mobility Management** in the Navigation Panel. Select Platform prompt appears.



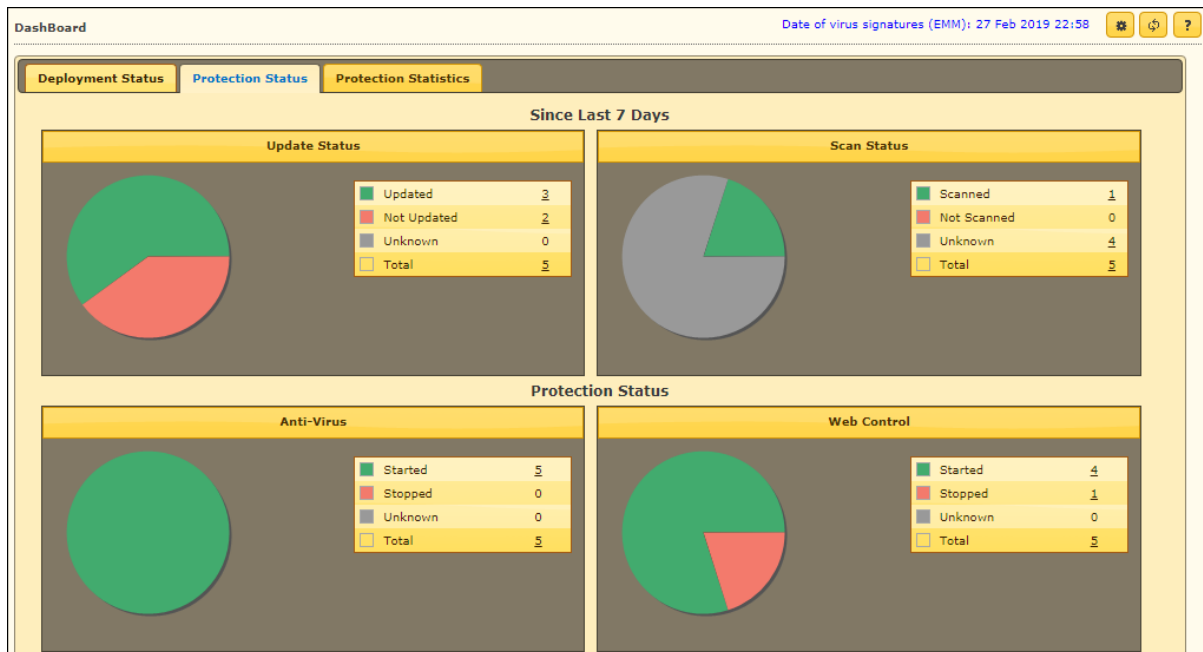
Clicking **Start with iOS** takes you to the **Settings** module > **Certificate Management** tab. To learn more about it, [click here](#).

Clicking **Start with Android (without iOS)** displays the **eScan Mobility Management Console**.

If you clicked **Start with Android**, go to **Settings** module > **Email Notification Settings** tab. These settings should be configured at start as they help administrator receive notifications. Learn more about **Email Notification Settings** by clicking [here](#).

Dashboard

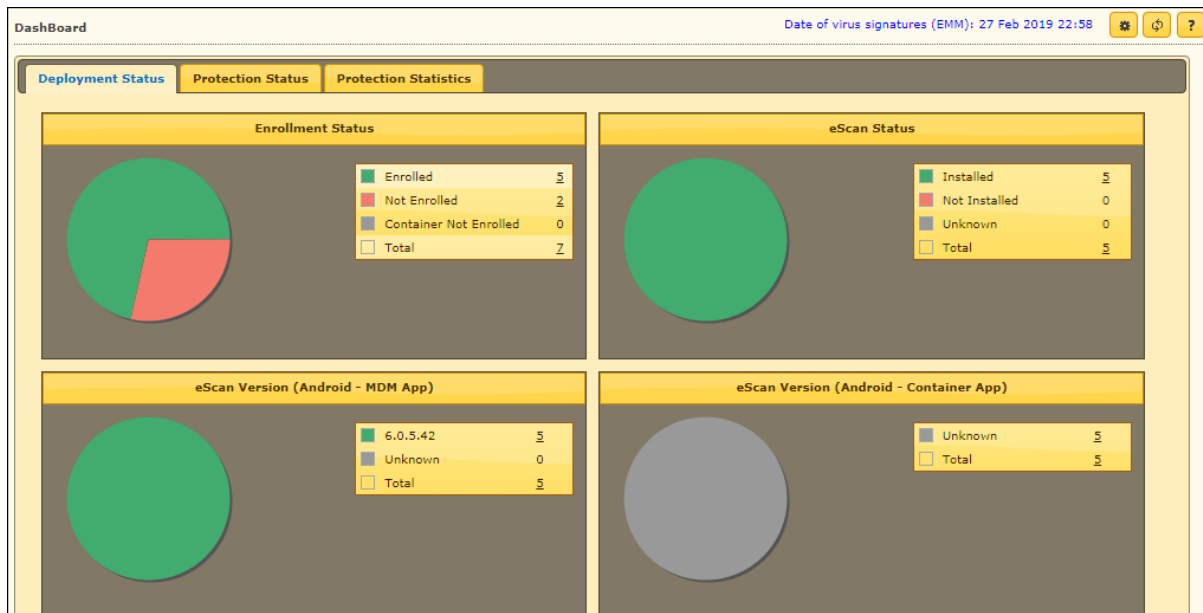
The Dashboard displays eScan MDM application's real-time Deployment Status, Protection Status and Protection Statistics for managed devices.



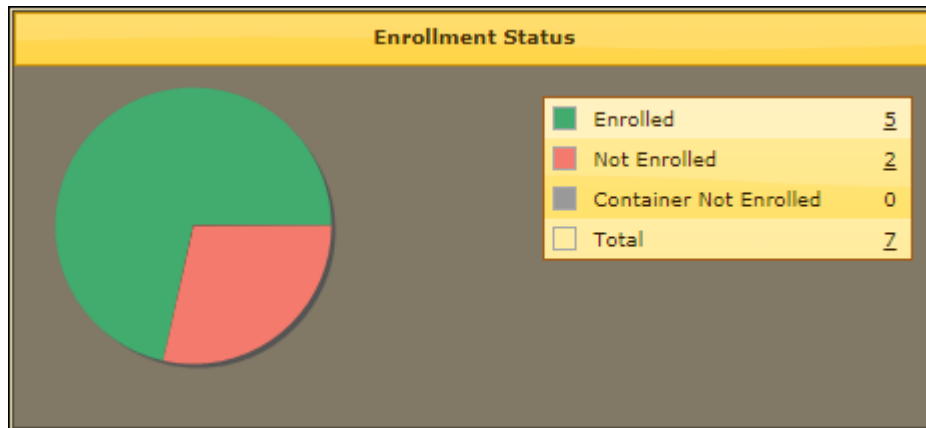
Deployment Status

This tab displays detailed pie chart view and statistics of the following –

- Enrollment Status
- eScan Status
- eScan Version (Android - MDM App)
- eScan Version (Android - Container App)
- eScan Version (iOS - MDM App)
- Android Version
- iOS Version
- Device Sync Status (Successful)
- Device Compliance
- Kiosk Status



Enrollment Status



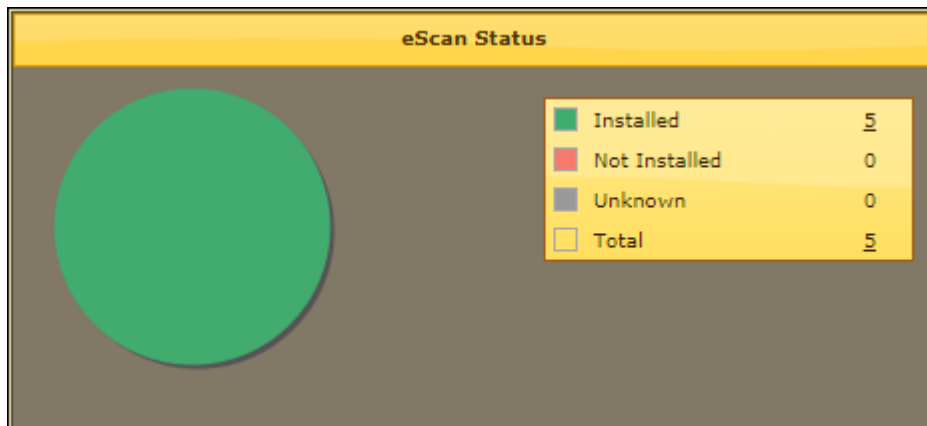
Enrolled – It displays the number of devices that are enrolled.

Not Enrolled - It displays the number of devices that are not enrolled.

Container Not Enrolled – It displays the number of devices on which Container application is not enrolled.

Total – It displays the total number of devices.

eScan Status



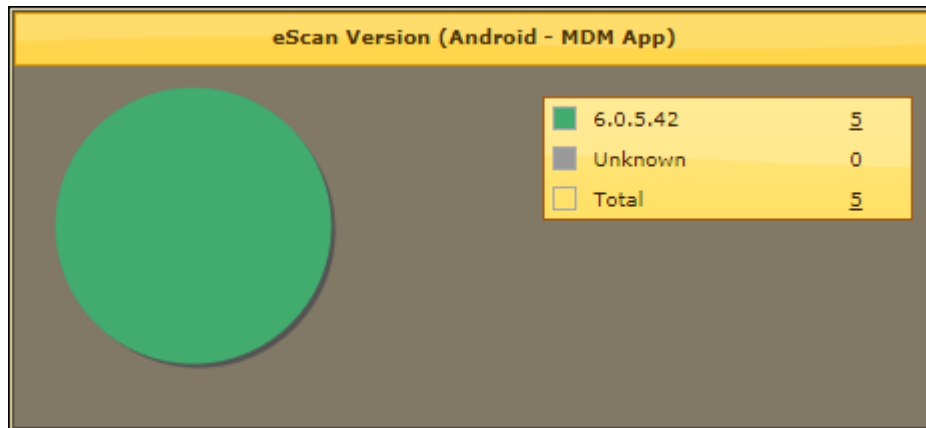
Installed – It displays the number of devices on which eScan MDM application is installed.

Not Installed – It displays the number of devices on which eScan MDM application is not installed.

Unknown – It displays the number of devices on which the eScan MDM application installation status is unknown.

Total – It displays the total number of devices.

eScan Version (Android - MDM App)

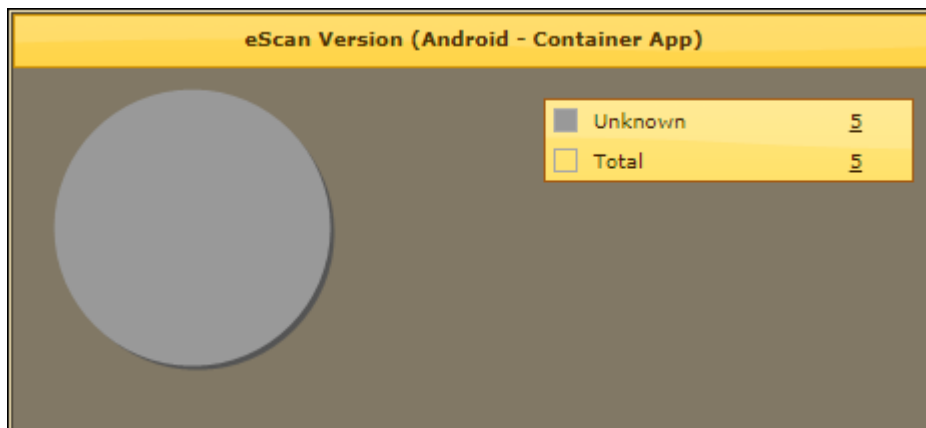


Version Numbers – It displays the Android MDM application's version number installed on devices.

Unknown – It displays the number of devices on which the Android MDM application's version number is unknown.

Total – It displays the total number of devices.

eScan Version (Android - Container App)

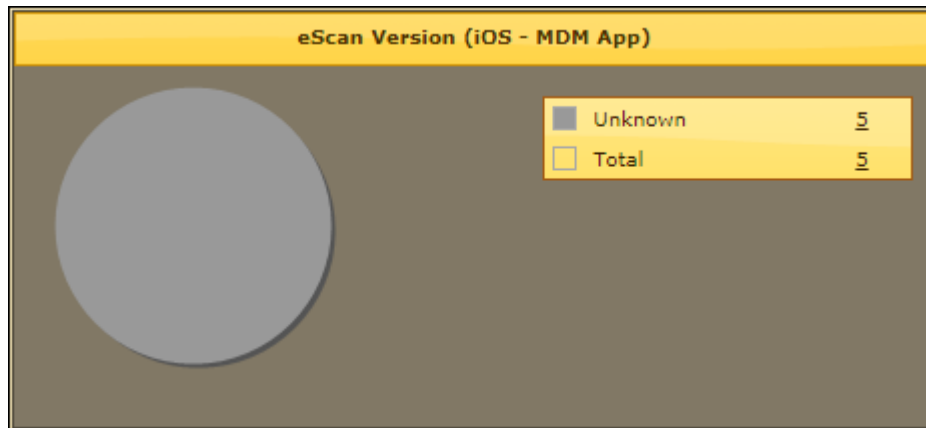


Version Numbers – It displays the Container application's version number installed on devices.

Unknown – It displays the number of devices on which the Container application's version number is unknown.

Total – It displays the total number of devices.

eScan Version (iOS - MDM App)

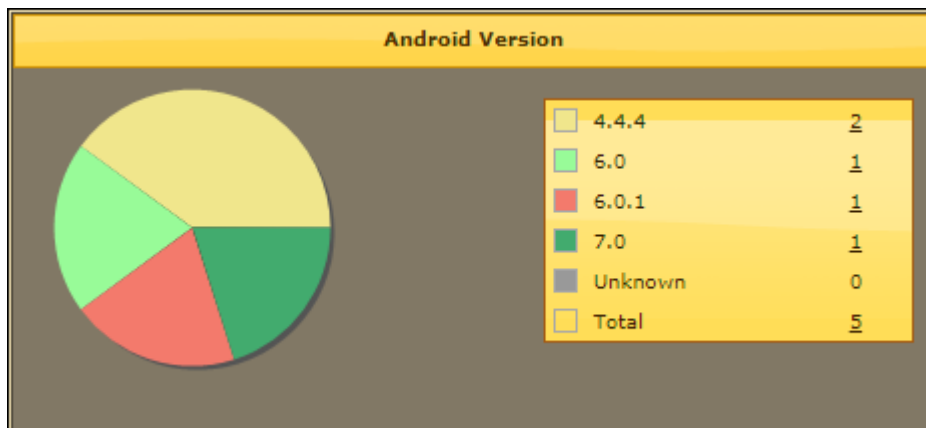


Version Numbers – It displays the iOS MDM application's version number installed on devices.

Unknown – It displays the number of devices on which the iOS MDM application's version number is unknown.

Total – It displays the total number of devices.

Android Version

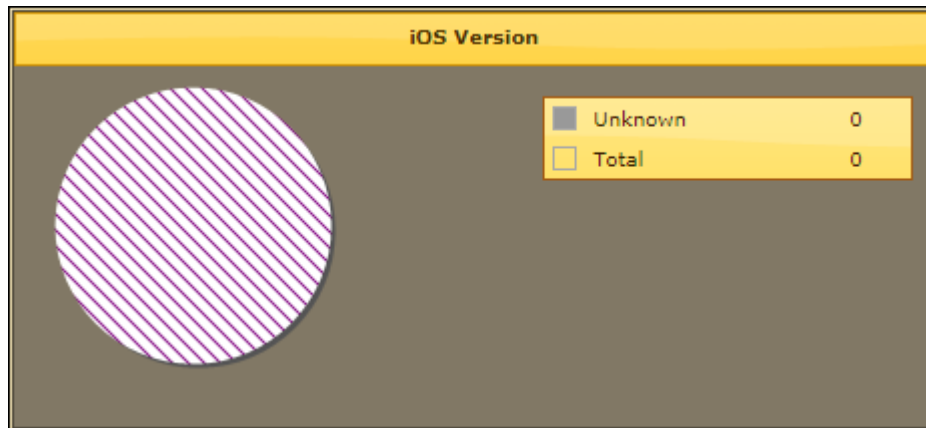


Version Numbers – It displays the Android version numbers and the number of devices which are running it.

Unknown – It displays the number of devices on which the Android version is unknown.

Total – It displays the total number of devices.

iOS Version

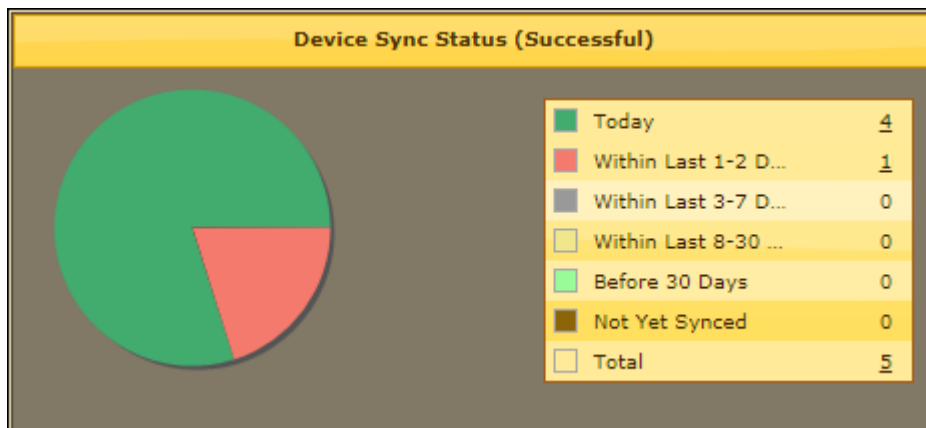


Version Numbers – It displays the iOS version numbers and the number of devices which are running it.

Unknown – It displays the number of devices on which the iOS version is unknown.

Total – It displays the total number of devices.

Device Sync Status (Successful)

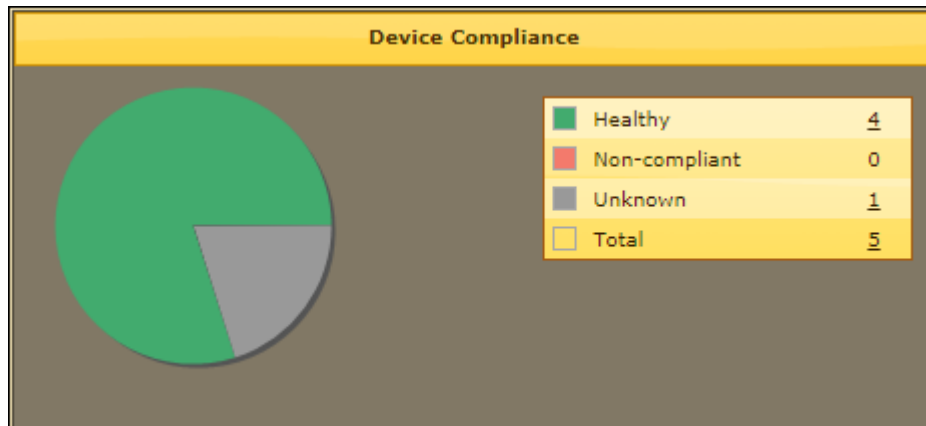


It displays the last sync status of the managed device with the server. You can view the statistics of the devices that are synced with the eScan server for Today, Within Last 1-2 Days, Within Last 3-7 Days, Within Last 8-30 Days, Before 30 Days.

Not Yet Synced – It displays the number of devices that are not yet synced with the eScan server.

Total – It displays the total number of devices.

Device Compliance



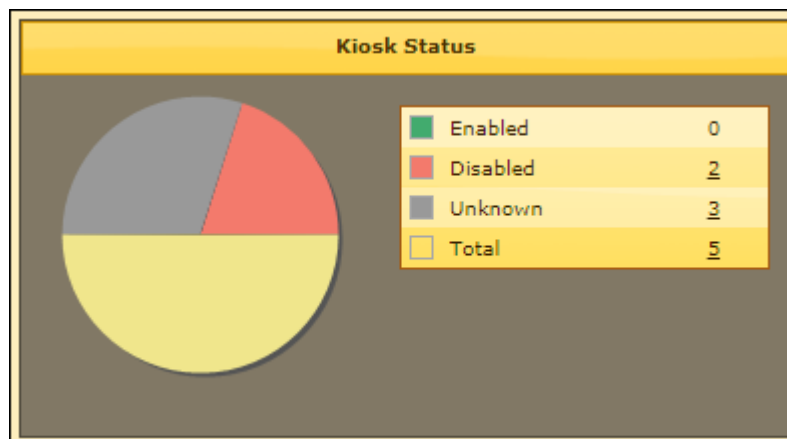
Healthy – It displays the number of devices that meet the compliances.

Non-compliant – It displays the number of devices that do not meet the compliances.

Unknown – It displays the number of devices whose compliance status is unknown.

Total – It displays the total number of devices.

Kiosk Status



Enabled – It displays the number of devices on which the kiosk is enabled.

Disabled – It displays the number of devices on which the kiosk is disabled.

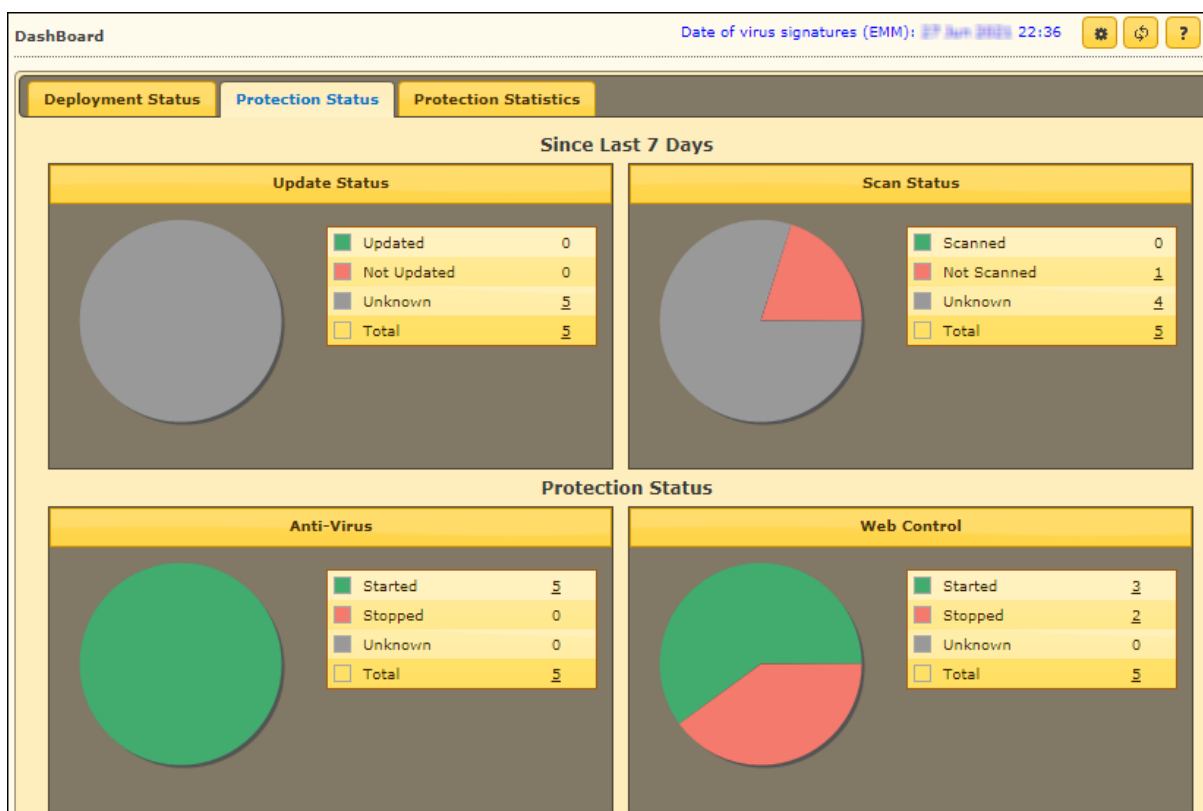
Unknown – It displays the number of devices on which the kiosk status is unknown.

Total – It displays the number of devices.

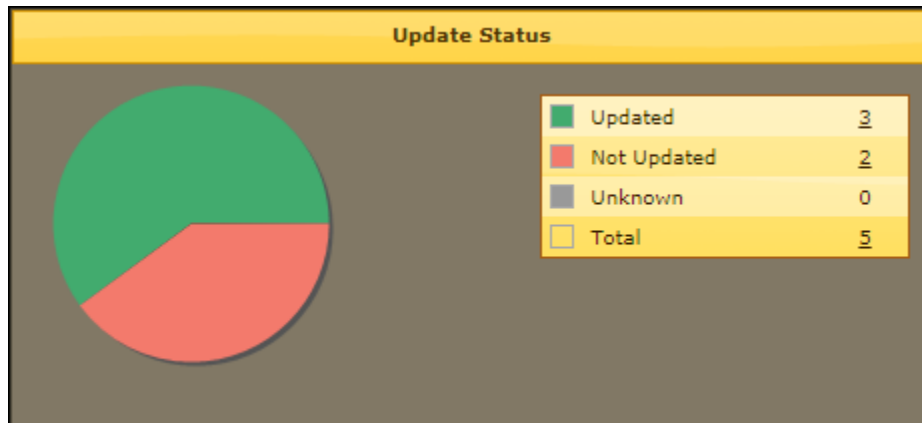
Protection Status

This tab displays detailed pie chart view and statistics of the following –

- Update Status
- Scan Status
- Anti-Virus
- Web Control
- Application Control
- Call & SMS Filter
- Firewall Status



Update Status



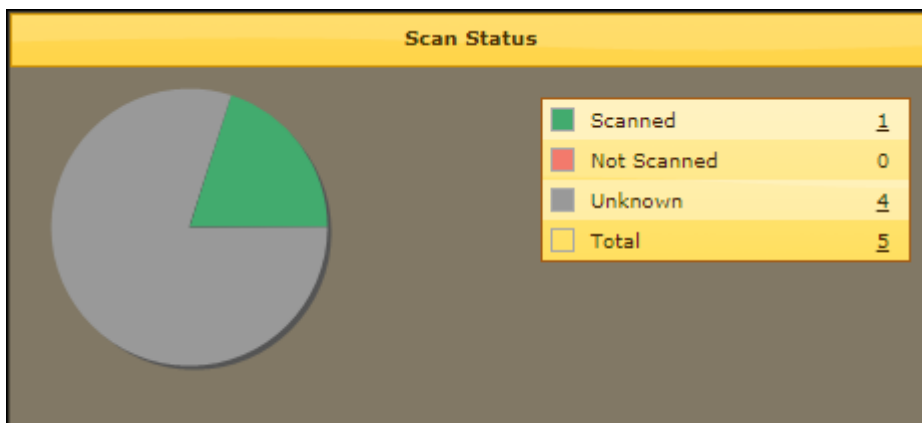
Updated – It displays the number of devices on which the Anti-Virus signatures are updated.

Not Updated – It displays the number of devices on which the Anti-Virus signatures are not updated.

Unknown – It displays the number of devices on which the Anti-Virus signatures update status is unknown.

Total – It displays the number of devices.

Scan Status



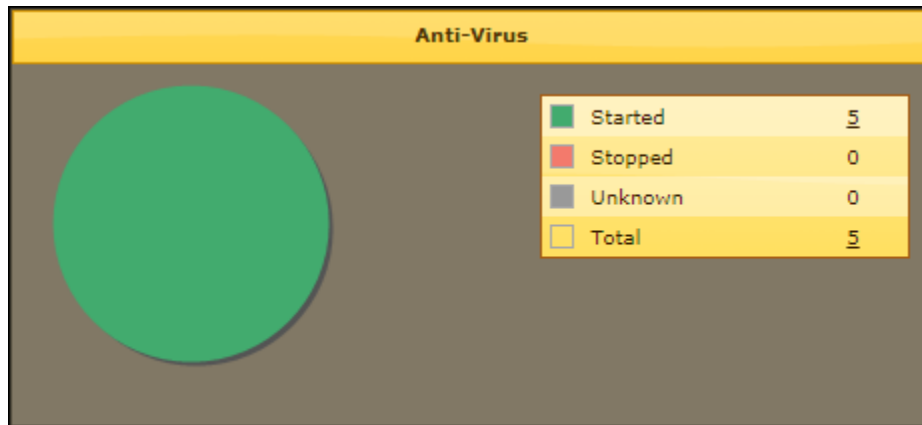
Scanned – It displays the number of devices which are scanned.

Not Scanned – It displays the number of devices which are not scanned.

Unknown – It displays the number of devices on which the scan status is unknown.

Total – It displays the total number of devices.

Anti-Virus



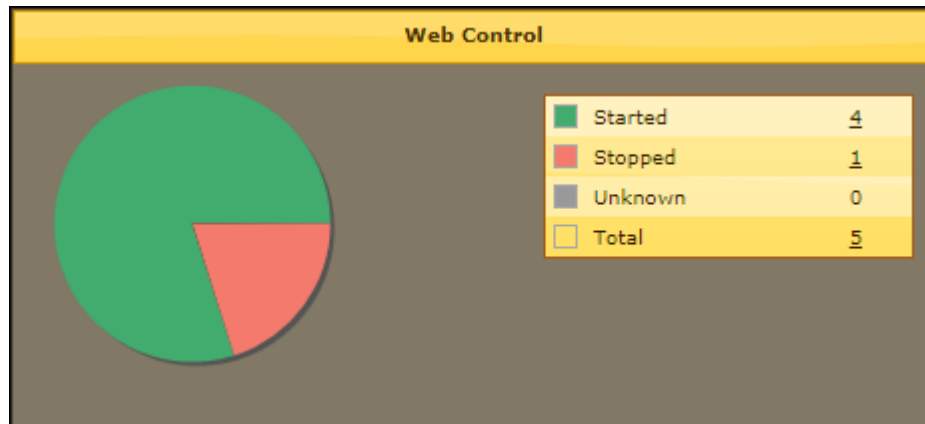
Started – It displays the number of devices on which the Anti-Virus module is started.

Stopped – It displays the number of devices on which the Anti-Virus module is stopped.

Unknown – It displays the number of devices on which the Anti-Virus module status is unknown.

Total – It displays the total number of devices.

Web Control



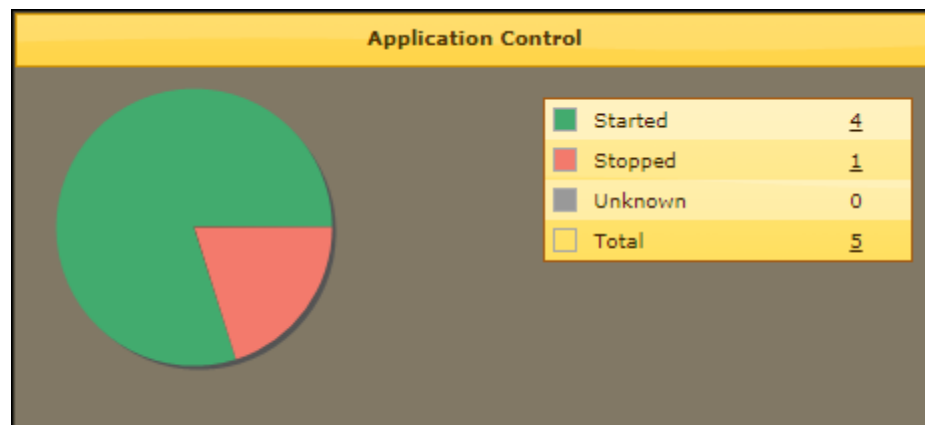
Started – It displays the number of devices on which the Web Control module is started.

Stopped – It displays the number of devices on which the Web Control module is stopped.

Unknown – It displays the number of devices on which the Web Control module status is unknown.

Total – It displays the total number of devices.

Application Control



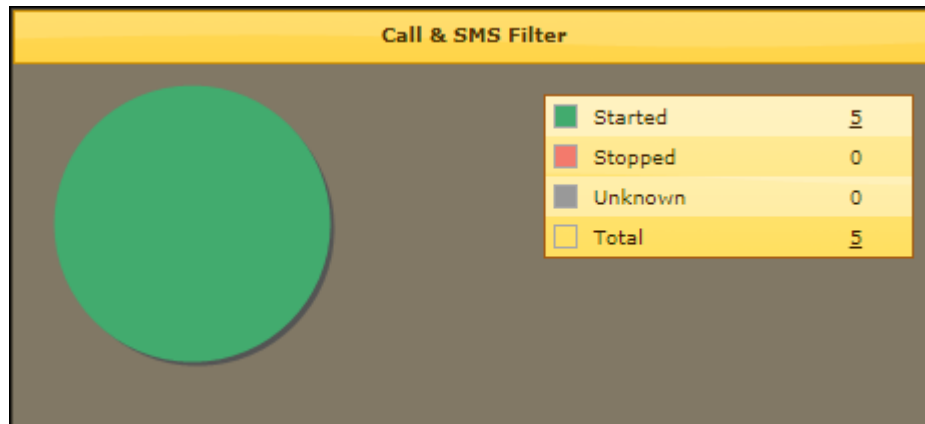
Started – It displays the number of devices on which the Application Control module is started.

Stopped – It displays the number of devices on which the Application Control module is stopped.

Unknown – It displays the number of devices on which the Application Control module status is unknown.

Total – It displays the total number of devices.

Call and SMS Filter



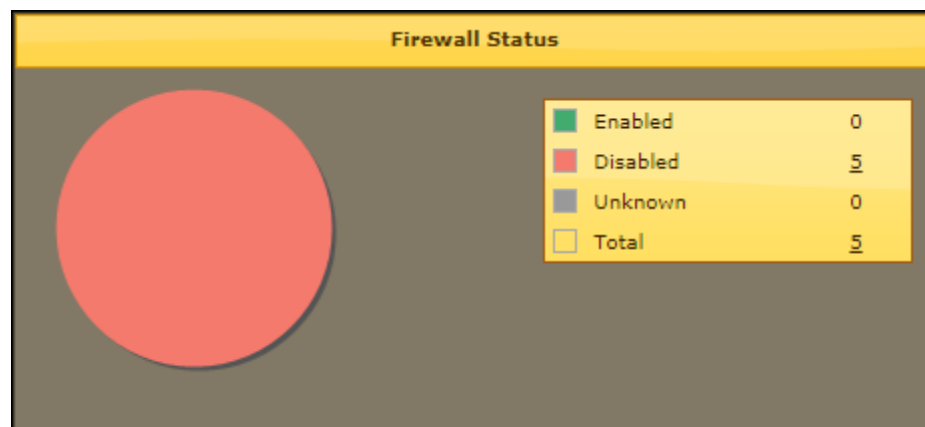
Started – It displays the number of devices on which the Call and SMS filter is started.

Stopped – It displays the number of devices on which the Call and SMS filter is stopped.

Unknown – It displays the number of devices on which the Call and SMS filter status is unknown.

Total – It displays the total number of devices.

Firewall Status



Enabled – It displays the number of devices on which the firewall is enabled.

Disabled – It displays the number of devices on which the firewall is disabled.

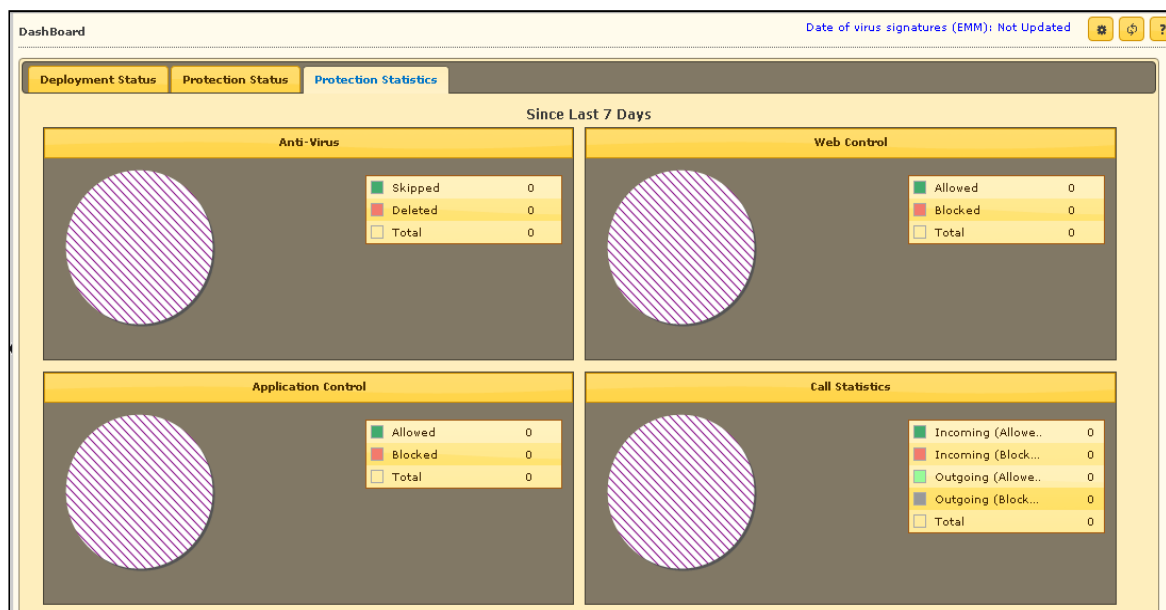
Unknown – It displays the number of devices on which the firewall status is unknown.

Total – It displays the number of devices.

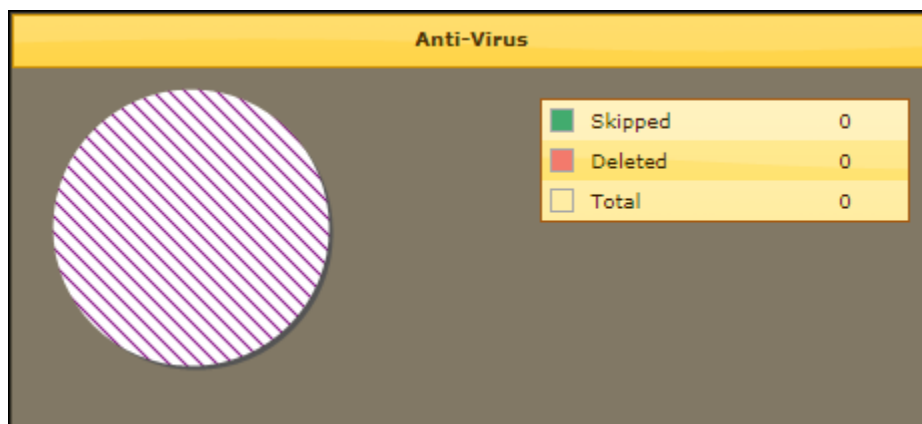
Protection Statistics

This tab displays pie chart view of detailed eScan module activity on devices. You can view details of each device by clicking the numerical.

- Anti-Virus
- Web Control
- Application Control
- Call Statistics
- SMS Statistics



Anti-Virus

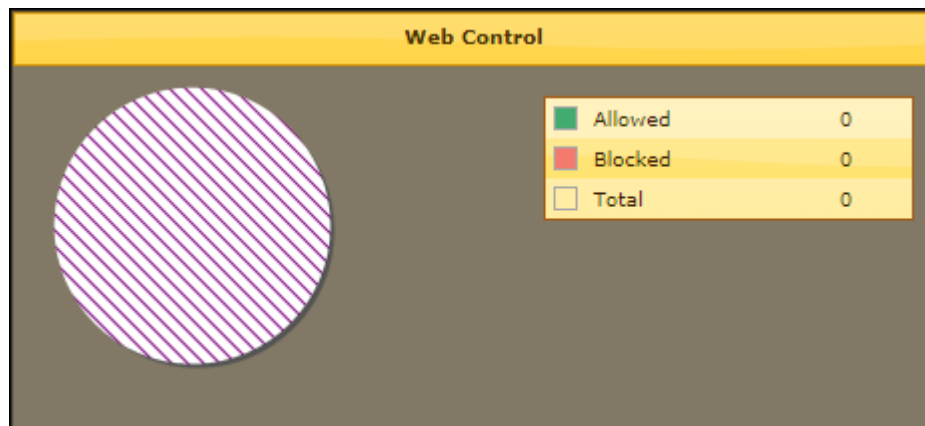


Skipped – It displays the number of files skipped during a scan on a device.

Deleted – It displays the number of files deleted during a scan on a device.

Total – It displays the total number of files.

Web Control

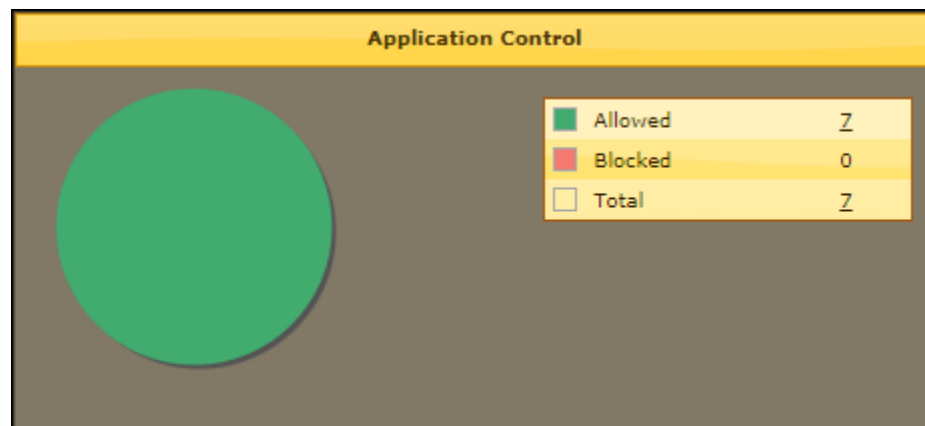


Allowed – It displays the number of websites allowed on a device.

Blocked – It displays the number of websites blocked on a device.

Total – It displays the total number of websites.

Application Control

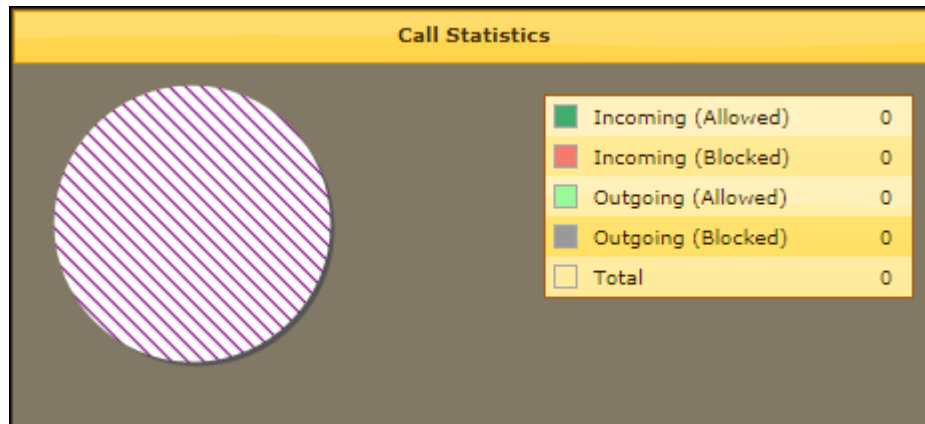


Allowed – It displays the number of applications allowed on a device.

Blocked – It displays the number of applications blocked on a device.

Total – It displays the total number of applications.

Call Statistics



Incoming (Allowed) – It displays the number of incoming calls allowed on a device.

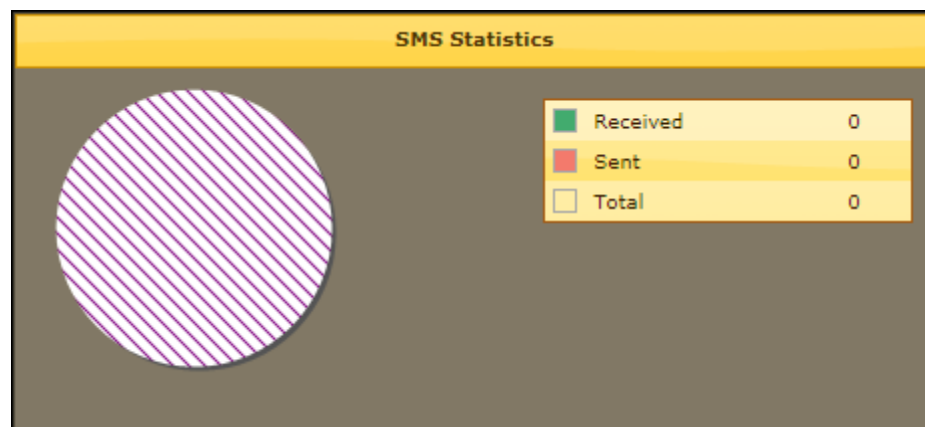
Incoming (Blocked) – It displays the number of incoming calls blocked on a device.

Outgoing (Allowed) – It displays the number of outgoing calls allowed from a device.

Outgoing (Blocked) – It displays the number of outgoing calls blocked from a device.

Total – It displays the total number of calls.

SMS Statistics



Received – It displays the number of messages received on a device.

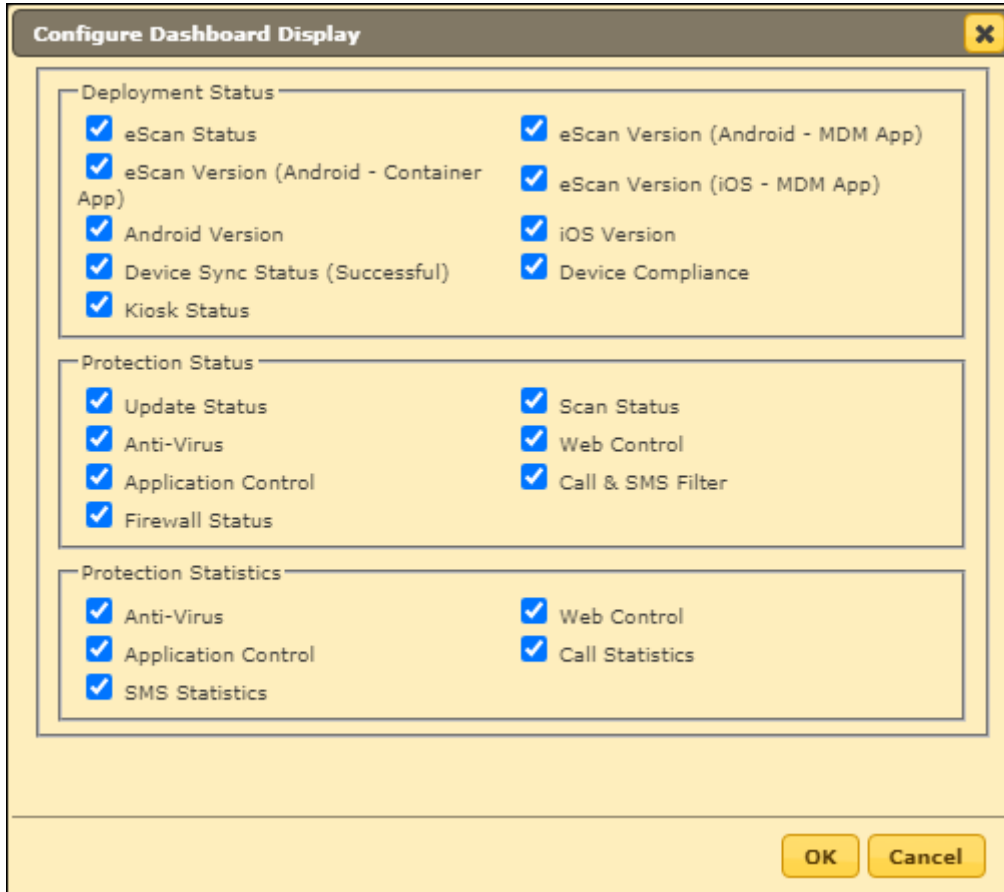
Sent - It displays the number of messages sent from a device.

Total – It displays the total number of messages.

Settings

The Settings let you configure the modules to be displayed see in all tabs.

1. Click settings icon .
Configure Dashboard Display window appears.



The image shows a 'Configure Dashboard Display' dialog box with a title bar containing a close button. The dialog is divided into three sections: 'Deployment Status', 'Protection Status', and 'Protection Statistics'. Each section contains a list of modules with checkboxes, all of which are currently checked. At the bottom right, there are 'OK' and 'Cancel' buttons.

Deployment Status	
<input checked="" type="checkbox"/> eScan Status	<input checked="" type="checkbox"/> eScan Version (Android - MDM App)
<input checked="" type="checkbox"/> eScan Version (Android - Container App)	<input checked="" type="checkbox"/> eScan Version (iOS - MDM App)
<input checked="" type="checkbox"/> Android Version	<input checked="" type="checkbox"/> iOS Version
<input checked="" type="checkbox"/> Device Sync Status (Successful)	<input checked="" type="checkbox"/> Device Compliance
<input checked="" type="checkbox"/> Kiosk Status	

Protection Status	
<input checked="" type="checkbox"/> Update Status	<input checked="" type="checkbox"/> Scan Status
<input checked="" type="checkbox"/> Anti-Virus	<input checked="" type="checkbox"/> Web Control
<input checked="" type="checkbox"/> Application Control	<input checked="" type="checkbox"/> Call & SMS Filter
<input checked="" type="checkbox"/> Firewall Status	

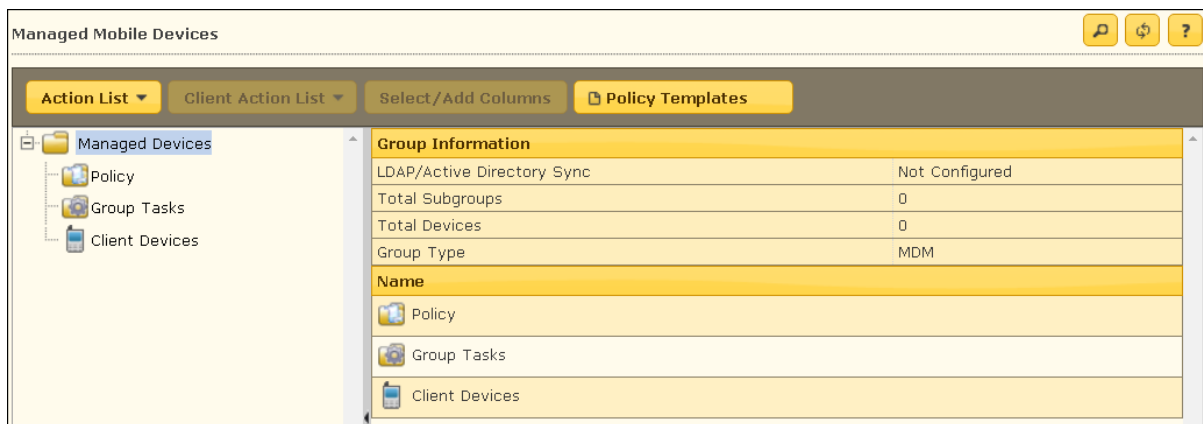
Protection Statistics	
<input checked="" type="checkbox"/> Anti-Virus	<input checked="" type="checkbox"/> Web Control
<input checked="" type="checkbox"/> Application Control	<input checked="" type="checkbox"/> Call Statistics
<input checked="" type="checkbox"/> SMS Statistics	

2. Select the module(s) to be displayed see in the tabs and then click **OK**.

Managed Mobile Devices

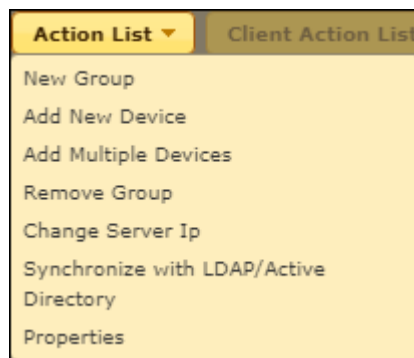
The Managed Mobile Devices module lets you take action related to a group and specific device(s). There are following buttons in this module:

- Action List
- Client Action List
- Select/Add Columns
- Policy Templates



Action List

This drop-down lets you take an action for a group.



Options	Description
New Group	This option lets you create a new group for categorizing/adding devices.
Add New Device	This option lets you add new devices to the selected groups.

Add Multiple Devices	This option lets you import (*.txt) file with device and user details in the following format for adding multiple devices at once. Mobile no.1,Username1,Email ID1 for example: 9012345678,ABCD,abcd@xyz.com Note: Do not put space before or after comma in the above format.
Remove Group	This option lets you remove a group from the Managed Devices.
Change Server IP	This option lets you change the server IP address on the managed device. The new server IP can be allotted to a particular group or list of devices.
Synchronize with LDAP/Active Directory	This option lets you synchronize the managed devices with the source active Directory Organization unit, the minimum sync interval is five minutes and you can also exclude ADS source files that are not required.
Properties	This option lets you view properties of the group such as Name, Parent Group, Group Type.

Group Type

MDM

In case the containerization benefits are not required, select the group type as MDM. The policies are applied to the Personal profile of the devices in the MDM group type. Web-blocking, Application Control etc. policies can be applied to the devices without creating a work profile (Container).

COD

In case the device belongs to a company and is given to an employee for company work/task purposes, select the group type as COD (Company Owned Device). As company is the device owner, the device will always be policy restricted irrespective of the Geo/Wi-Fi location. Containerization and its benefits are available for COD group type.

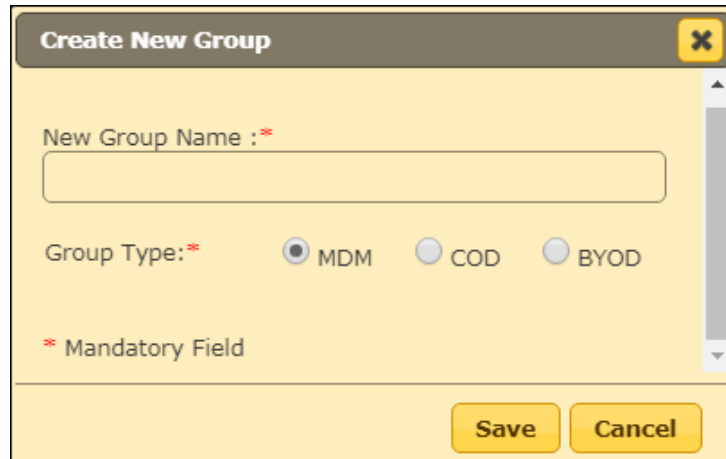
BYOD

In case the users are allowed to bring their own devices to company for work/task purposes, select the group type as BYOD (Bring Your Own Device). In this group type, policies will be applied within the Geo/Wi-Fi location. The restrictions as per the policy will be applied only if the device is in Geo/Wi-Fi location. If the device is out of the Geo/Wi-Fi location, the device will be free of restrictions. Containerization and its benefits are available for BYOD group type.

For differentiation between applications required to be installed, enrollment procedures and policies for the respective group type, [click here](#).

Creating a New Group

1. Select a group to which the group is to be added.
2. Click **Action List > New Group**.
Create New Group window appears.



The 'Create New Group' dialog box is shown. It has a title bar with a close button (X). The main area contains a text field labeled 'New Group Name : *'. Below this is a section for 'Group Type : *' with three radio buttons: 'MDM' (selected), 'COD', and 'BYOD'. At the bottom left, there is a note '* Mandatory Field'. At the bottom right, there are two buttons: 'Save' and 'Cancel'.

3. Enter a name.
4. Select a preferred group type.
5. Click **Save**. A new group will be created.

Adding a New Device

After a group is created, you will be required to add devices to the respective groups for managing and securing them efficiently. To add a device, follow the steps given below:

1. Select a group.
2. Click **Action List > Add New Device**.
Add New Device window appears.

3. Enter the mandatory details.
4. Select the appropriate OS type.
5. Click **Add**.

An enrollment email with a link to download and install eScan Device Management (client) will be sent to the specified email address.

Note	The mobile number required here is only for indicative purposes and it need not be an actual mobile number.
-------------	---

Adding Multiple Devices

By using Add Multiple Devices option, you can add multiple devices to a group by importing details from a .csv or .txt file in the following format – Mobile no.1, Username1, Email-id1

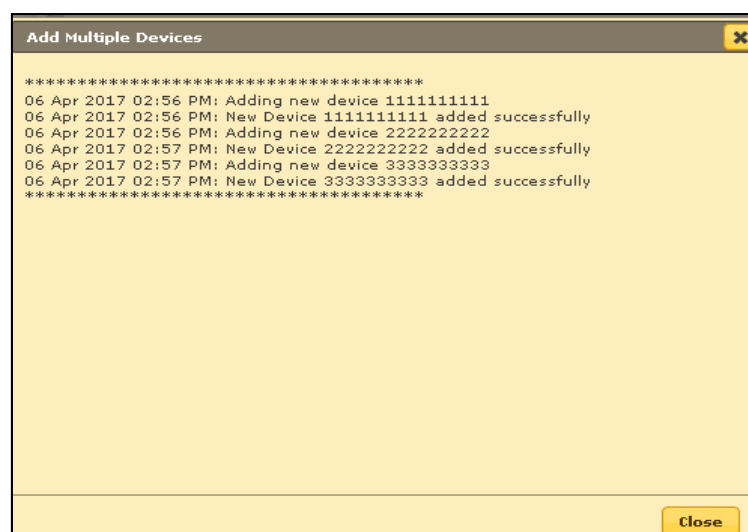
To add multiple devices, follow the steps given below:

1. Select a group.
2. Click **Action list > Add Multiple Devices**.
Add Multiple Devices window appears.



3. Click **Browse** and select the .txt and .csv file consisting required details.
4. Click **OK**. All devices from the .txt and .csv file will be added to the group. After the successful addition, the following window will be displayed.

Note	Ensure there is no space before or after comma in the above format. Use a line break to separate each device's information.
-------------	--



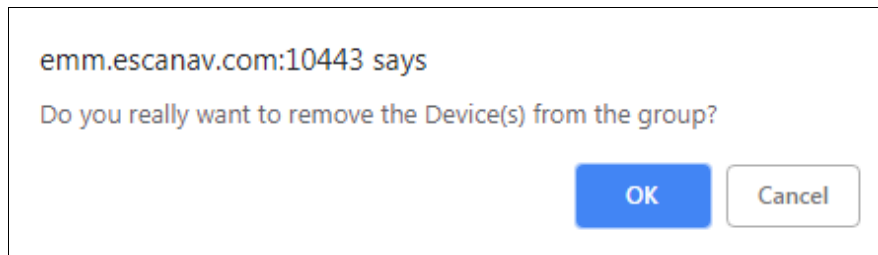
Removing a group

To remove a group, follow the steps given below:

Group Removal is allowed only for empty groups. (Group(s) that contains no devices)

1. Select a group.
2. Click **Action List > Remove Group**.

A confirmation prompt appears.



3. Click **OK**.
The group will be removed.

Changing Server IP address

1. Select a group.
2. Click **Action List > Change Server IP**.
Change Server IP Address window appears. The IP Address field displays the current IP address of a group.

3. Select the **Change To** check box and enter the new server IP address.
4. In the **Apply To** section, select whether IP address change is for **Groups** or **List of Devices**.
5. Select the group or devices in below section. After you are done making changes, click **Apply**.
6. After a group's or device's IP address is changed, a success message appears.

Synchronizing with Active Directory

To synchronize a group with Active Directory, follow the steps given below:

1. Select a group and then click **Action List > Synchronize with LDAP/Active Directory**.
Synchronize with LDAP/Active Directory window appears.

Synchronize with LDAP/Active Directory

Synchronize with LDAP/Active Directory

Target Groups : **Browse**

Source LDAP/Active Directory Organisation Unit : **Browse**

Synchronization interval : Minutes (Minimum 5 Minutes)

Exclude From LDAP/Active Directory Sync

☐ Excluded LDAP/Active Directory Sources

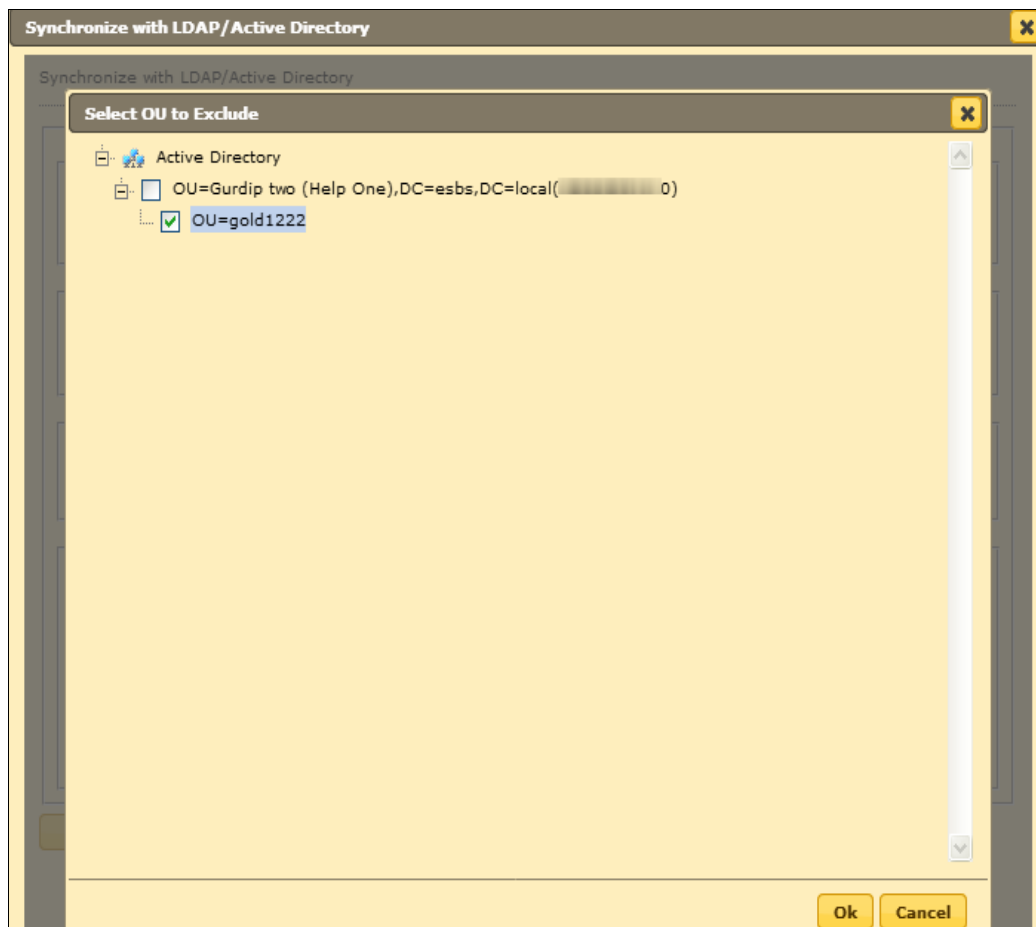
Exclude

Delete

Ok **Close**

2. If you want to change the target group for synchronization, click **Browse** and select a group or subgroup. (Skip this step if you don't want to change the group).

3. Select the Source LDAP/Active Directory Organization Unit by clicking **Browse**. It takes you to **LDAP/Active Directory**; selection will depend upon which OU you want to synchronize. After selecting OU, click **OK**.



4. Set the Synchronization Interval as per your requirement.

Synchronize with LDAP/Active Directory

Synchronize with LDAP/Active Directory

Target Groups :

Source LDAP/Active Directory Organisation Unit :

Synchronization interval :
 Minutes (Minimum 5 Minutes)

Exclude From LDAP/Active Directory Sync

☒ **Excluded LDAP/Active Directory Sources**

☒ OU=gold1222,OU=Gurdip two (Help One),DC=esbs,DC=local

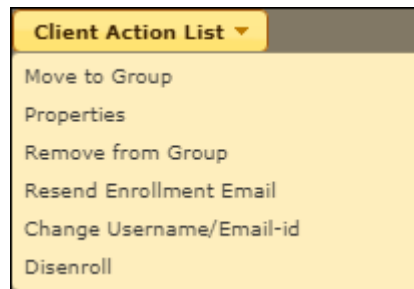
5. Click **OK**.

To exclude group(s) from AD sync

1. Check **Excluded LDAP/Active Directory Sources**. Click **Exclude**.
Select OU to Exclude pop-up appears.
2. Select the group you want to exclude and then click **OK**.

Client Action List

This drop-down lets you take action for the devices added in the console.



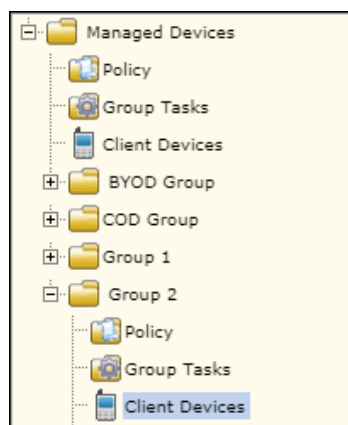
Select a device or devices and take the action of your preference.

Moving Devices from one group to the other group

After adding devices in a group, you can move a device or devices from one group to other as per your requirement.

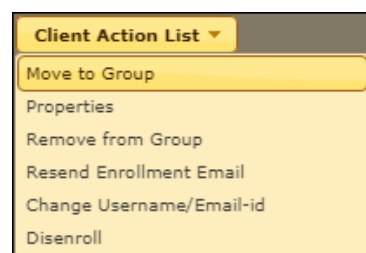
To move device(s) from one group to other, follow the steps given below:

1. Select the group in which the device(s) is already added and then click **Client Devices**.



2. Select the device you want to move to another group and then click **Client Action List > Move to Group**.

<input type="checkbox"/>	Mobile Number	User's name	QR Code
<input checked="" type="checkbox"/>	12345	user 1	View
<input type="checkbox"/>	78945	user 2	View
<input type="checkbox"/>	56123	user 3	View



3. Select Group window appears.



4. Select the group to which you wish to move the device(s) and then click **OK**.

Note	You can create a New Group by clicking New Group and move the device(s) to that group.
-------------	---

Checking a Device's Properties

The Properties option lets you check a device's general properties, anti-virus settings, protection status and miscellaneous properties.

1. Select a device.
2. Click **Client Action List > Properties**.

The Properties window for the selected device appears.

Properties(55555)

General

Mobile Number	55555
User's name	
Mac Number	
Email Id	
Enrollment Date	13 Feb 2019 01:13 PM

AV Setting

eScan Install	Installed
eScan Version	6.0.5.41
Last Connection	11 Feb 2019 11:00 PM
Last Update	24 Mar 2017 10:36 AM
Last Scanned	-

Protection

Anti-Virus	Enabled
Web Control	Enabled
Application Control	Enabled
Call & SMS Filter	Enabled

Miscellaneous

Battery Status	<div><div></div></div> 15%
WiFi Strength	<div><div></div></div> 77%
SIM Signal Strength	<div><div></div></div> 80%

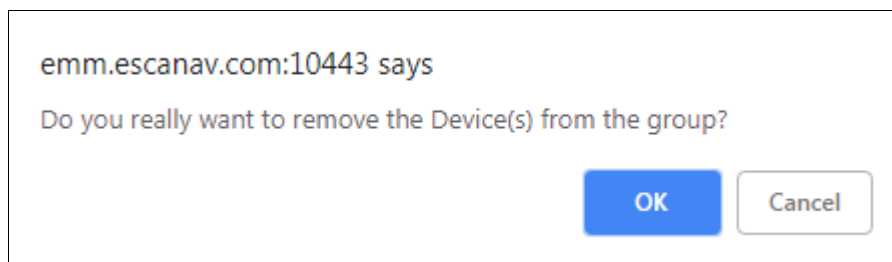
Close

Removing a device from group

The Remove from Group option lets you remove any device from a group.

1. Select a device.
2. Click **Client Action List** > **Remove from Group**.

A confirmation prompt appears.



3. Click **OK**.
- The device will be removed from the group.

NOTE

If a device is removed, all details related to that device are also deleted from the database.

Resending Enrollment Email

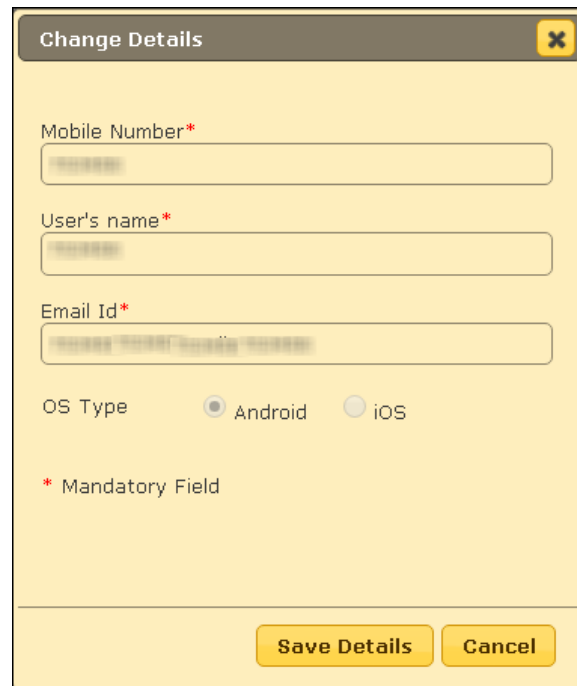
The Resend Enrollment Email option lets you resend the enrollment email to the user who didn't receive it at the time of adding the device.

1. Select the specific device.
 2. Click **Client Action List** > **Resend Enrollment Email**.
- A new enrollment email will be sent to the user.

Changing a User's Name/Email ID

The Change Username/Email ID option lets you change the name/email ID of a user.

1. Select the specific device.
2. Click **Client Action List > Change Username/Email ID**.
Change Details window appears.



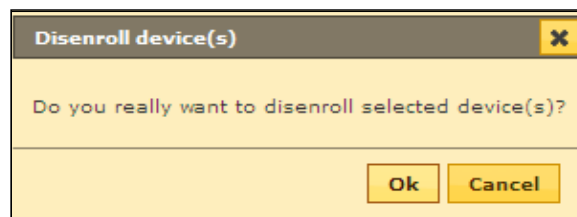
The 'Change Details' dialog box is a yellow window with a title bar containing the text 'Change Details' and a close button (X). It contains three text input fields: 'Mobile Number*' (with a masked number '1234567890'), 'User's name*' (with a masked name 'XXXXXXXXXX'), and 'Email Id*' (with a masked email 'XXXXXXXXXX@XXXXXX.XX'). Below these fields are two radio buttons for 'OS Type': 'Android' (selected) and 'iOS'. At the bottom left, there is a red asterisk followed by the text '* Mandatory Field'. At the bottom right, there are two buttons: 'Save Details' and 'Cancel'.

3. Make the required changes and then click **Save Details**.
The User details will be updated.

Disenrolling a device

The Disenroll option lets you disenroll a device.

1. Select a device.
2. Click **Client Action List > Disenroll**.
A confirmation prompt appears.



The 'Disenroll device(s)' dialog box is a yellow window with a title bar containing the text 'Disenroll device(s)' and a close button (X). It contains a single line of text: 'Do you really want to disenroll selected device(s)?'. At the bottom right, there are two buttons: 'Ok' and 'Cancel'.

3. Click **OK**.
The selected device will be disenrolled.

Select/Add Columns

You can customize the view regarding the details of devices, according to the requirement.

Select/Add Customized Columns

☐ Select All

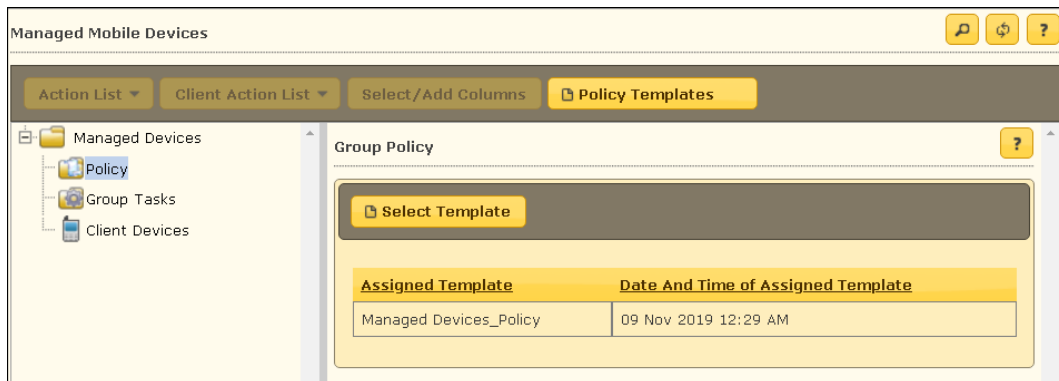
<input checked="" type="checkbox"/> Mobile Number	<input checked="" type="checkbox"/> Anti-Virus
<input checked="" type="checkbox"/> User's name	<input checked="" type="checkbox"/> Web Control
<input type="checkbox"/> <input type="text"/>	<input checked="" type="checkbox"/> Network Block Status
<input type="checkbox"/> <input type="text"/>	<input checked="" type="checkbox"/> Application Control
<input type="checkbox"/> <input type="text"/>	<input checked="" type="checkbox"/> Call & SMS Filter
<input type="checkbox"/> <input type="text"/>	<input checked="" type="checkbox"/> Last Connection
<input checked="" type="checkbox"/> QR Code	<input checked="" type="checkbox"/> Last Update
<input checked="" type="checkbox"/> Device Added Date	<input checked="" type="checkbox"/> Last Scanned
<input checked="" type="checkbox"/> Enrollment Status	<input checked="" type="checkbox"/> Update Server
<input checked="" type="checkbox"/> Enrollment Date	<input checked="" type="checkbox"/> Client OS
<input checked="" type="checkbox"/> Mac Number	<input checked="" type="checkbox"/> Policy Applied Date
<input checked="" type="checkbox"/> Email Id	<input checked="" type="checkbox"/> GPS Status
<input checked="" type="checkbox"/> Kiosk Status	<input checked="" type="checkbox"/> eScan Status
<input checked="" type="checkbox"/> Battery Status	<input checked="" type="checkbox"/> eScan Version
<input checked="" type="checkbox"/> WiFi Strength	<input checked="" type="checkbox"/> Container Version
<input checked="" type="checkbox"/> SIM Signal Strength	

To configure this, select the device and click **Select/Add Columns** option. You can select and configure the required columns accordingly.

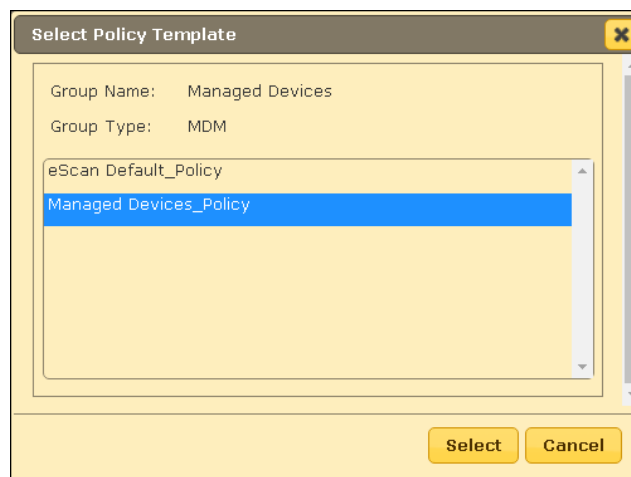
Policy

Steps for Defining Policies for the Group

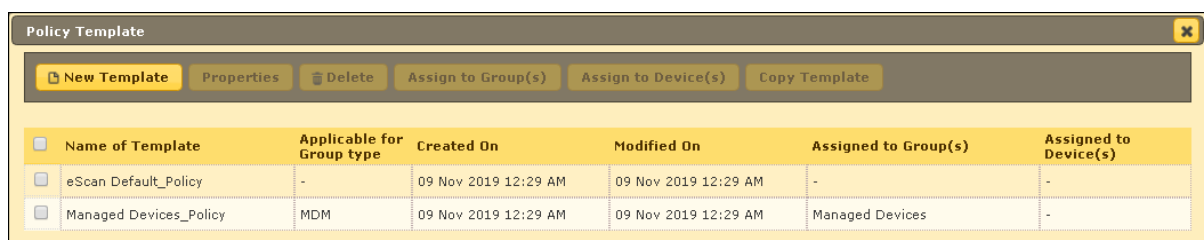
To define policies for a group, select a group and under the group, click Policy. Group Policy pane appears on the right side.



Clicking **Select Template** displays a list of available templates.



Clicking Policy Templates displays Policy Template screen and lets you create, copy, and assign template to specific group or devices.

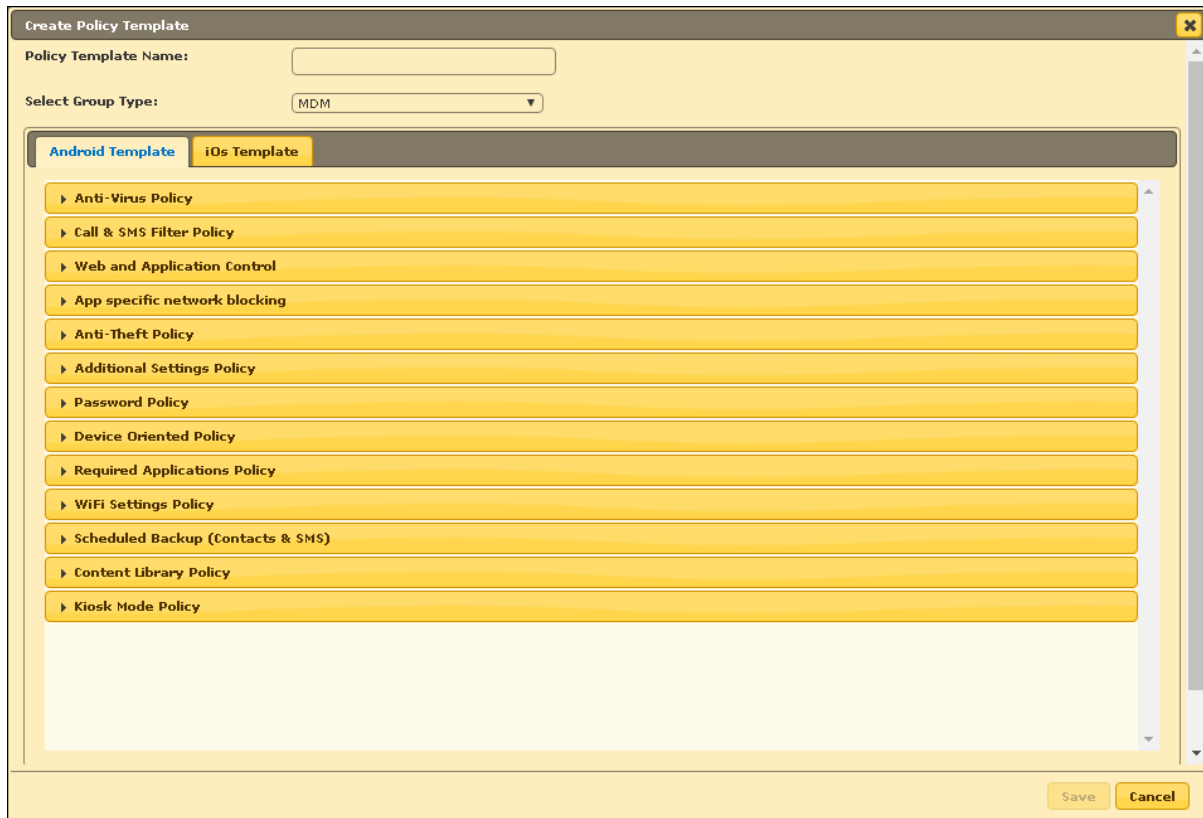


Creating New Template

To create a new template, follow the steps given below:

1. Click **New Template**.

Create Policy Template window appears.

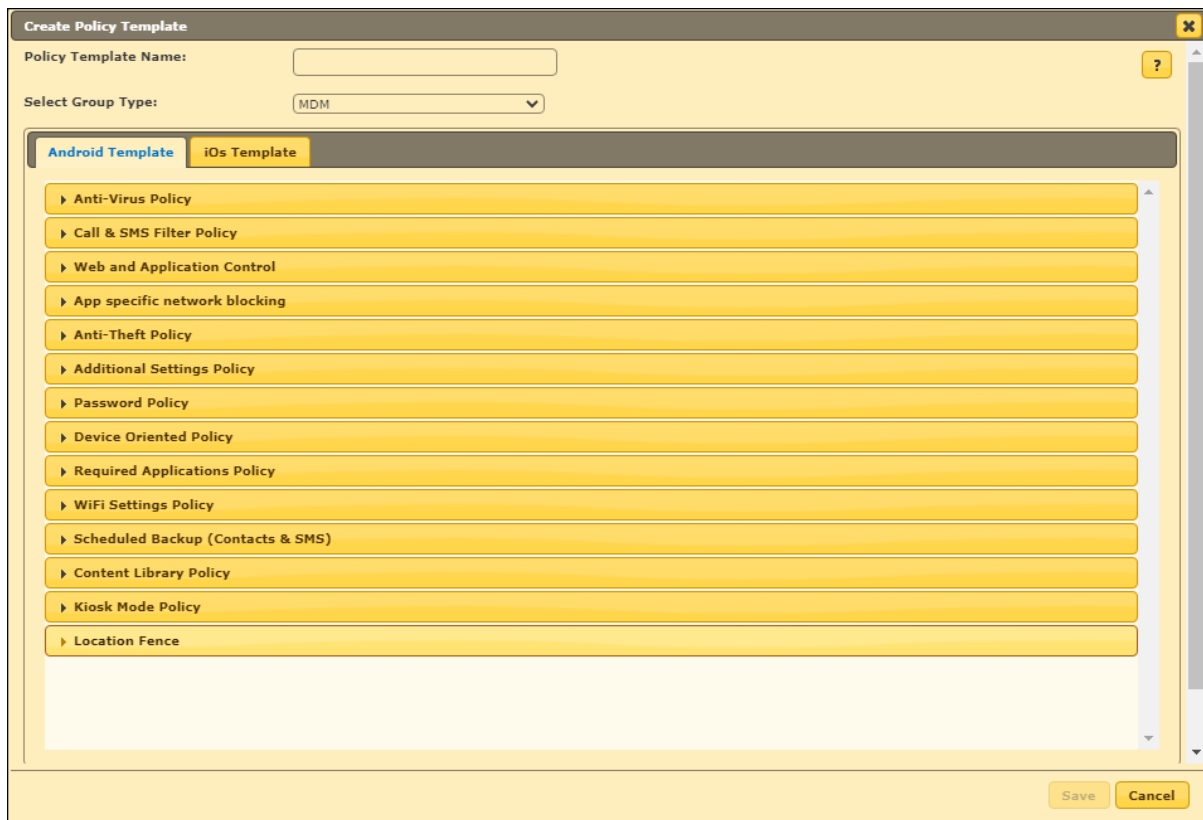


The screenshot shows the 'Create Policy Template' window. It has a title bar with a close button. Below the title bar, there is a 'Policy Template Name:' label followed by a text input field. Below that is a 'Select Group Type:' label followed by a dropdown menu showing 'MDM'. There are two tabs: 'Android Template' (selected) and 'iOS Template'. Below the tabs is a list of policy categories, each with a right-pointing arrow icon: Anti-Virus Policy, Call & SMS Filter Policy, Web and Application Control, App specific network blocking, Anti-Theft Policy, Additional Settings Policy, Password Policy, Device Oriented Policy, Required Applications Policy, WiFi Settings Policy, Scheduled Backup (Contacts & SMS), Content Library Policy, and Kiosk Mode Policy. At the bottom right, there are 'Save' and 'Cancel' buttons.

2. Enter a name for template.
3. Select appropriate group type.

The Create Policy Template lets you create template for both Android and iOS devices discussed below.

Android Template



Create Policy Template

Policy Template Name:

Select Group Type:

Android Template | iOS Template

- ▶ Anti-Virus Policy
- ▶ Call & SMS Filter Policy
- ▶ Web and Application Control
- ▶ App specific network blocking
- ▶ Anti-Theft Policy
- ▶ Additional Settings Policy
- ▶ Password Policy
- ▶ Device Oriented Policy
- ▶ Required Applications Policy
- ▶ Wi-Fi Settings Policy
- ▶ Scheduled Backup (Contacts & SMS)
- ▶ Content Library Policy
- ▶ Kiosk Mode Policy
- ▶ Location Fence

Save Cancel

The Android Template consists following policies:

- Anti-Virus Policy
- Call & SMS Filter Policy
- Web and Application Control
- App specific network blocking
- Anti-Theft Policy
- Additional Settings Policy
- Password Policy
- Device Oriented Policy
- Required Applications Policy
- Wi-Fi Settings Policy
- Scheduled Backup (Contacts & SMS)
- Content Library Policy
- Kiosk Mode Policy
- Location Fence

Anti-Virus Policy

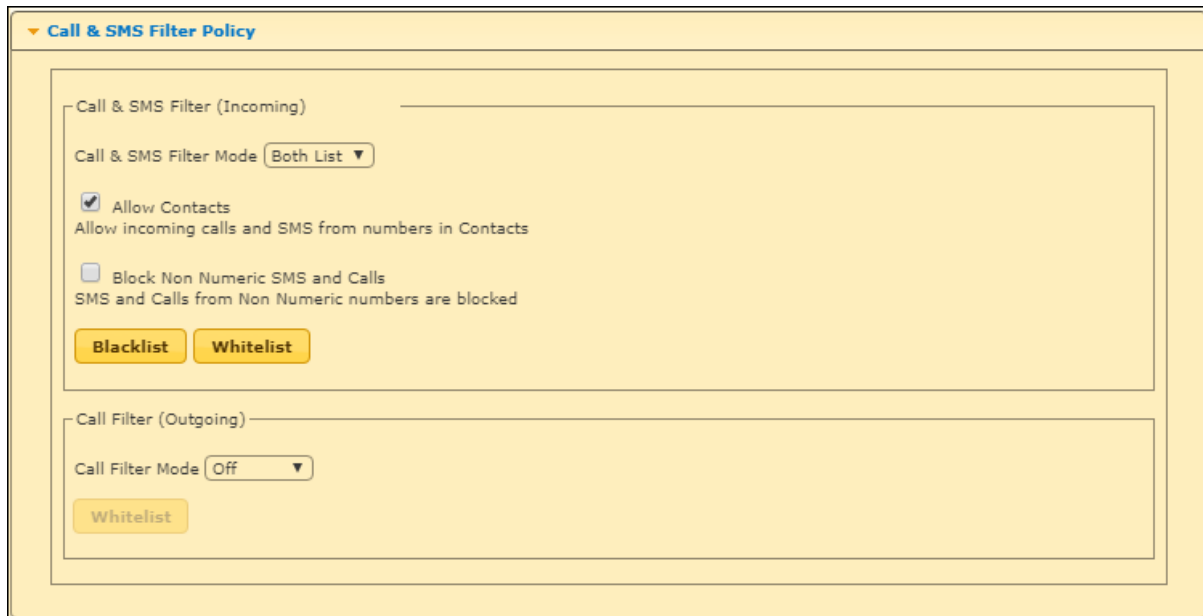
Anti-Virus Policy lets you scan the device, schedule a scan and update the virus signature database as per your requirement.

Options	Description
Scan Settings	Using the options present under the Anti-Virus Policy, the administrator can define settings for enabling or disabling virus protection on devices along with settings for file types to be scanned on managed devices.
Protection Scanning for files on installation is enabled	Select Enabled or Disabled to enable or disable protection on managed devices in the group.
Scan Type	Select the Scan Type as All Files or Executable only files on managed devices in the group.
Automatic Scan	Use options present under the Anti-Virus Policy to scan devices on startup or schedule the scan as per requirement.
Startup Scan	Select from drop-down to enable or disable scanning on device startup, as per your requirement.
Schedule Scan	Select a schedule to scan managed devices. You can conduct a weekly or daily scan as required or even disable the scan schedules.

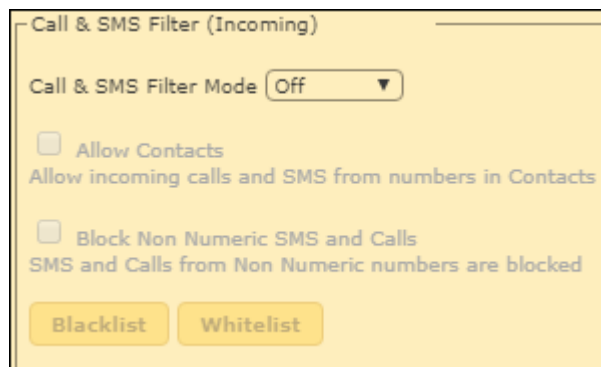
Scan Day	Select a particular day of the week to scan the managed devices present in the group. This check box will be activated only if you select weekly scan.
Select Scan Time	Set time for scanning the managed devices in the group.
Schedule Update Settings	Define settings for updating eScan on managed devices.
Schedule Update	Define a schedule to update virus signature database on a daily or weekly basis or disable the update schedule.
Update Day	Select a particular day of the week to update the managed devices present in the group. This check box will be activated only if you select weekly update.
Update Time	Set time for the devices to take virus signature database update from the server. It will be helpful in saving network congestion where large numbers of devices are added in the MDM Server.
Update from Internet server	Select this check box to update the virus signature database from the Internet server.
Update only if Wi-Fi is available	Select this check box to update virus signature database only if the Wi-Fi connection is available.

Call & SMS Filter Policy

The Call & SMS Filter Policy lets you set filter for incoming calls, text messages and outgoing calls on managed devices.

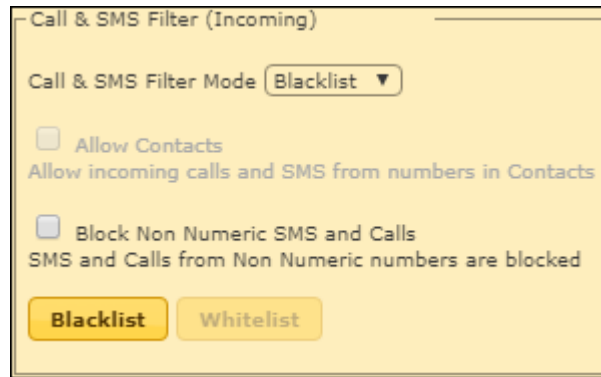


Call and SMS filter Mode set to Off



If the Call and SMS filter mode is set to Off, all calls and text messages will be allowed.

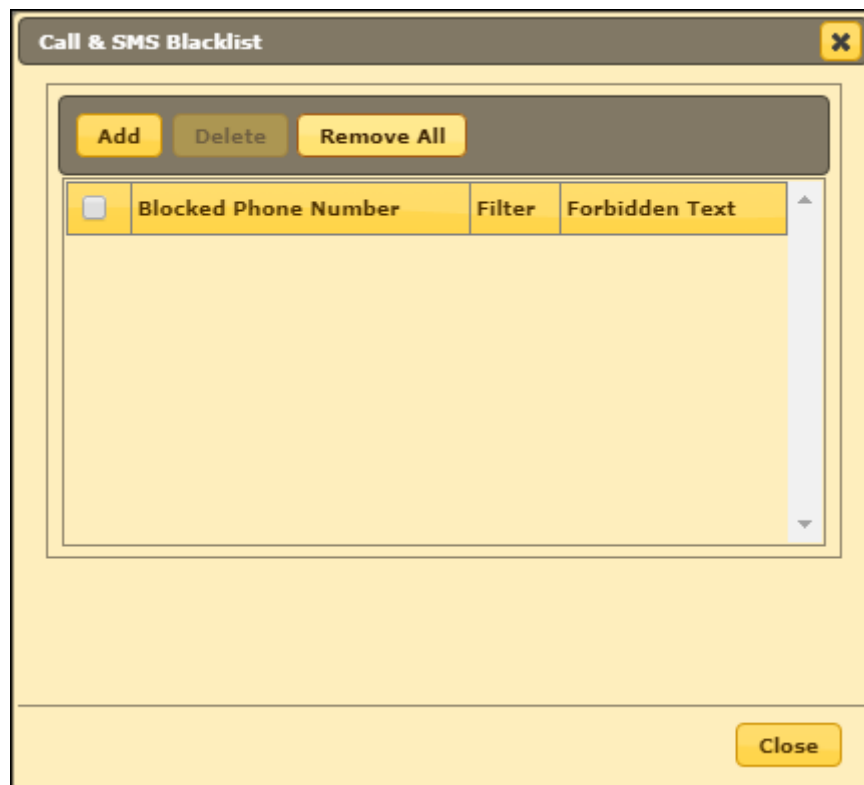
Call and SMS filter mode set to Blacklist



Select Block Non-Numeric SMS and Calls check box to block SMS and calls from non-numeric numbers.

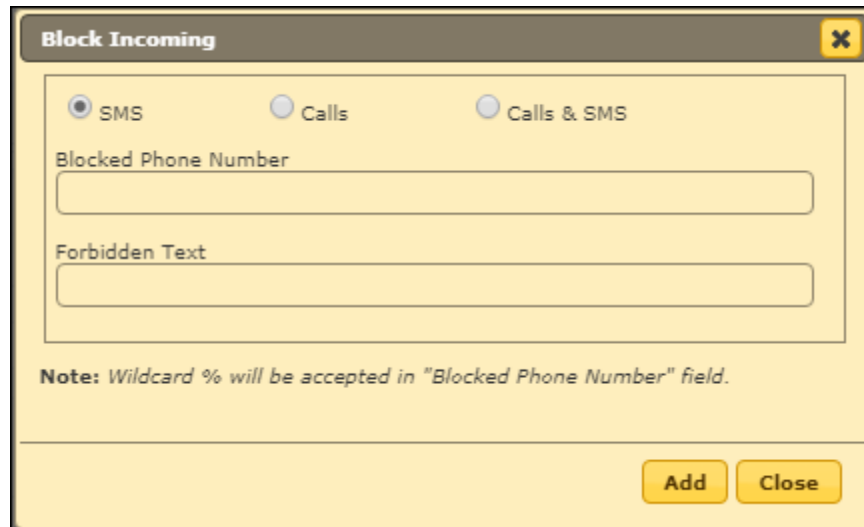
To block incoming calls from known numbers and SMS consisting specific keywords, click **Blacklist**.

Call and SMS Blacklist window appears.



Click **Add**.

Block Incoming window appears.



Block Incoming [X]

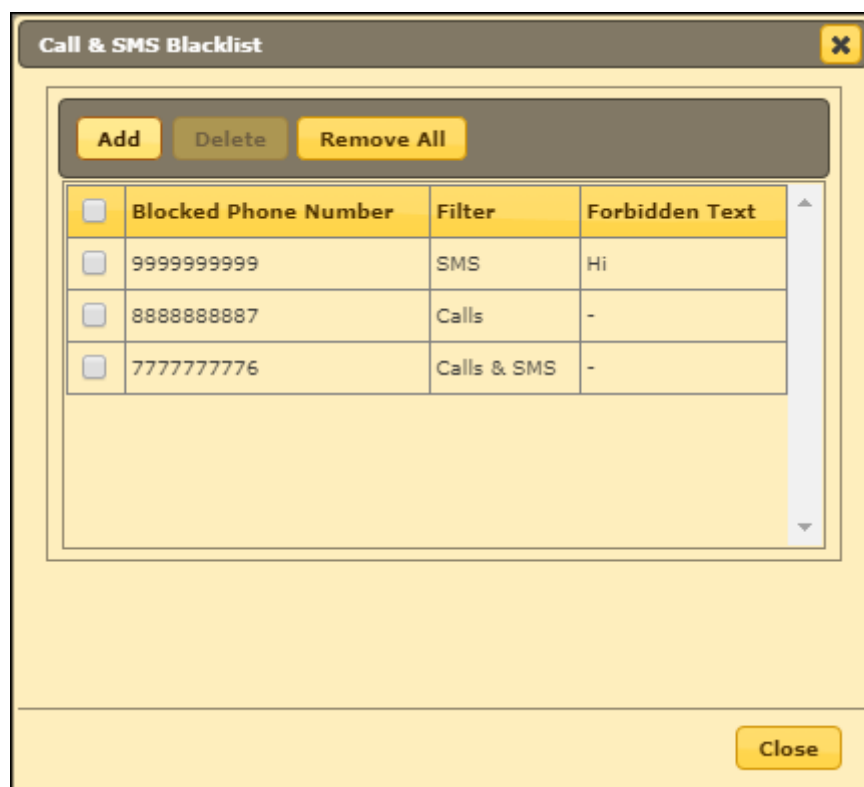
☒ SMS
 ☐ Calls
 ☐ Calls & SMS

Blocked Phone Number

Forbidden Text

Note: Wildcard % will be accepted in "Blocked Phone Number" field.

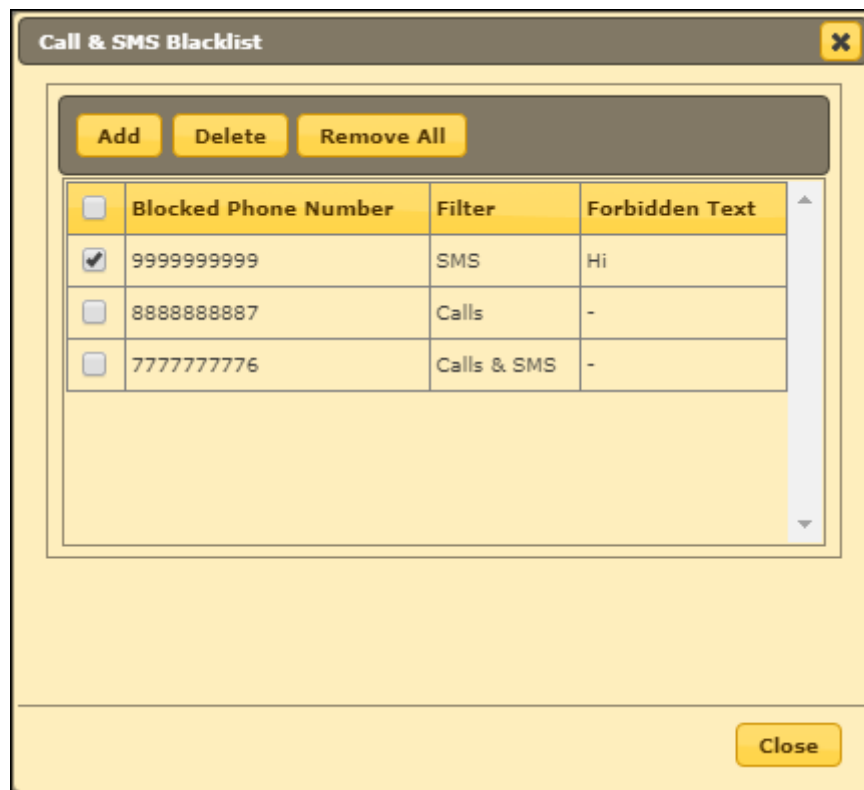
Select whether to block **SMS**, **Calls** or both **Calls & SMS**. Enter the Blocked Phone Number and Forbidden Text in the fields and then click **Add**.



Call & SMS Blacklist [X]

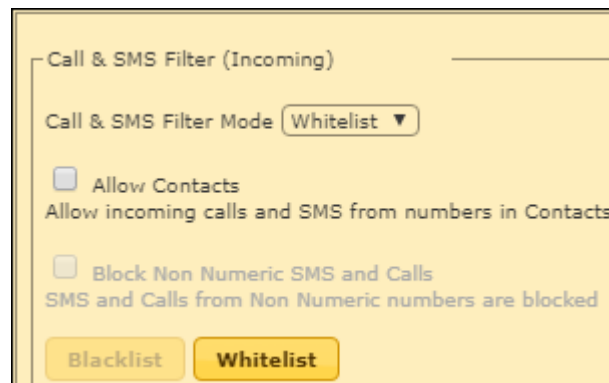
<input type="checkbox"/>	Blocked Phone Number	Filter	Forbidden Text
<input type="checkbox"/>	9999999999	SMS	Hi
<input type="checkbox"/>	8888888887	Calls	-
<input type="checkbox"/>	7777777776	Calls & SMS	-

To delete a specific number from the Blacklist, select the number and click **Delete**.



The selected number will be deleted.

Call and SMS filter mode set to Whitelist



Check **Allow Contacts** check box and then click **Whitelist**.

Call and SMS Whitelist window appears.

Call & SMS Whitelist

Add

Delete

Remove All

<input type="checkbox"/>	Allowed Phone Number	Filter	Allowed Text

Close

Click **Add**.

Allow Incoming window appears.

Allow Incoming

☒ SMS

☐ Calls

☐ Calls & SMS

Allowed Phone Number

Allowed Text

Note: Wildcard % will be accepted in "Allowed Phone Number" field.

Add

Close

Select whether to allow **SMS**, **Calls** or both **Calls & SMS**. Enter the Allowed Phone Number and Forbidden Text in the fields and then click **Add**.

Call & SMS Whitelist

Add **Delete** **Remove All**

<input type="checkbox"/>	Allowed Phone Number	Filter	Allowed Text
<input type="checkbox"/>	9999999999	SMS	Hello
<input type="checkbox"/>	8888888888	Calls & SMS	-
<input type="checkbox"/>	7777777777	Calls	-

Close

To delete a specific number from whitelist, select the number and click **Delete**.

Call & SMS Whitelist

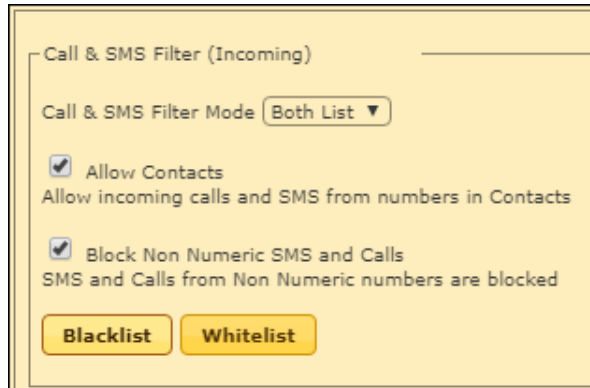
Add **Delete** **Remove All**

<input type="checkbox"/>	Allowed Phone Number	Filter	Allowed Text
<input type="checkbox"/>	9999999999	SMS	Hello
<input checked="" type="checkbox"/>	8888888888	Calls & SMS	-
<input type="checkbox"/>	7777777777	Calls	-

Close

The number will be deleted. To remove all numbers in a single-click, click **Remove All**.

Call and SMS filter mode set to Both List



Call & SMS Filter (Incoming)

Call & SMS Filter Mode **Both List** ▼

☒ Allow Contacts
Allow incoming calls and SMS from numbers in Contacts

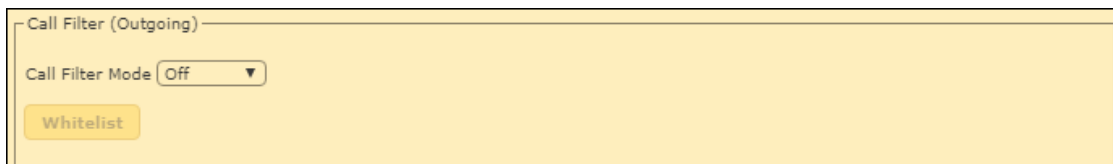
☒ Block Non Numeric SMS and Calls
SMS and Calls from Non Numeric numbers are blocked

Blacklist **Whitelist**

Check Allow Contacts and Block Non-Numeric SMS and Calls and you will be able to access both Blacklist's and Whitelist's features.

Call Filter (Outgoing) Mode set to Off

If Call Filter Mode is set to Off, all outgoing calls will be allowed.



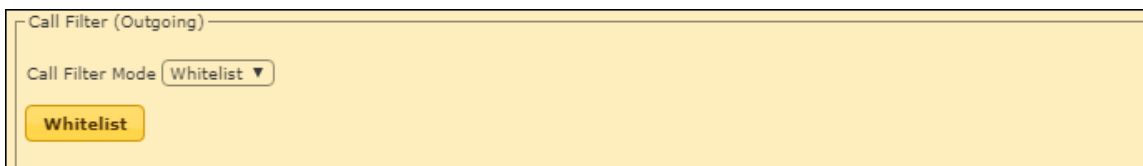
Call Filter (Outgoing)

Call Filter Mode **Off** ▼

Whitelist

Call Filter (Outgoing) Mode set to Whitelist

If Call Filter Mode is set to Whitelist, a user can make outgoing calls only to whitelisted numbers.

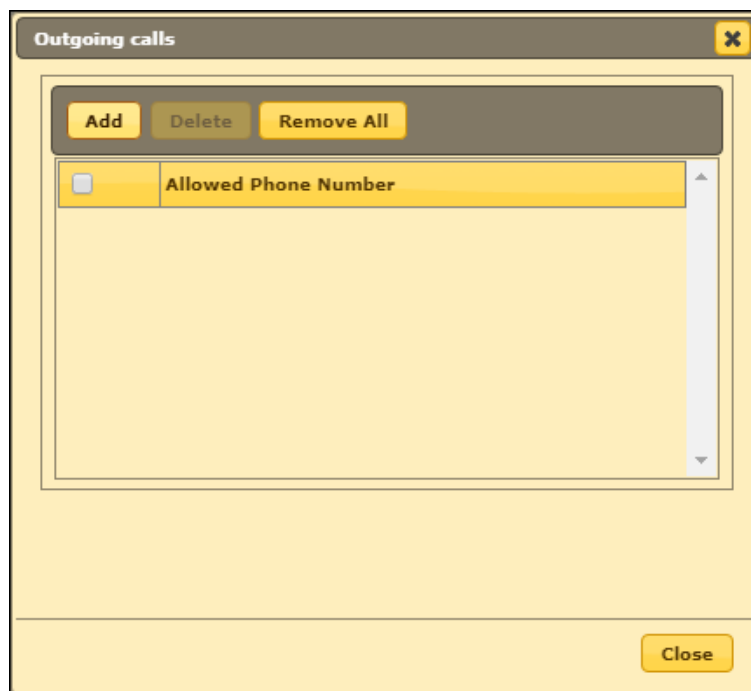


Call Filter (Outgoing)

Call Filter Mode **Whitelist** ▼

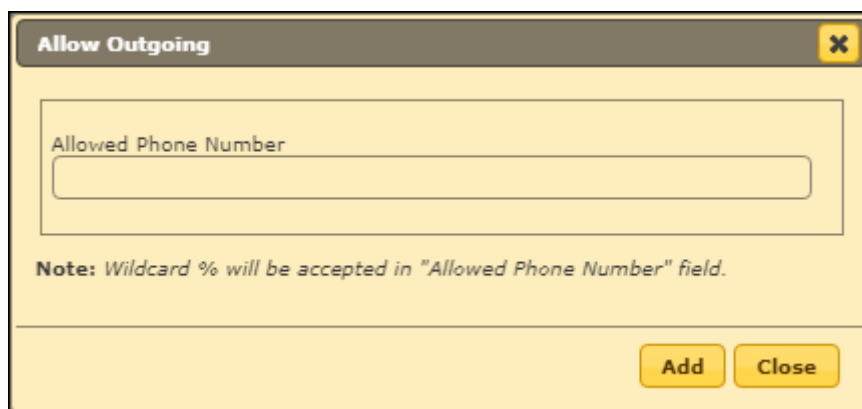
Whitelist

Click **Whitelist**. Outgoing calls window appears.



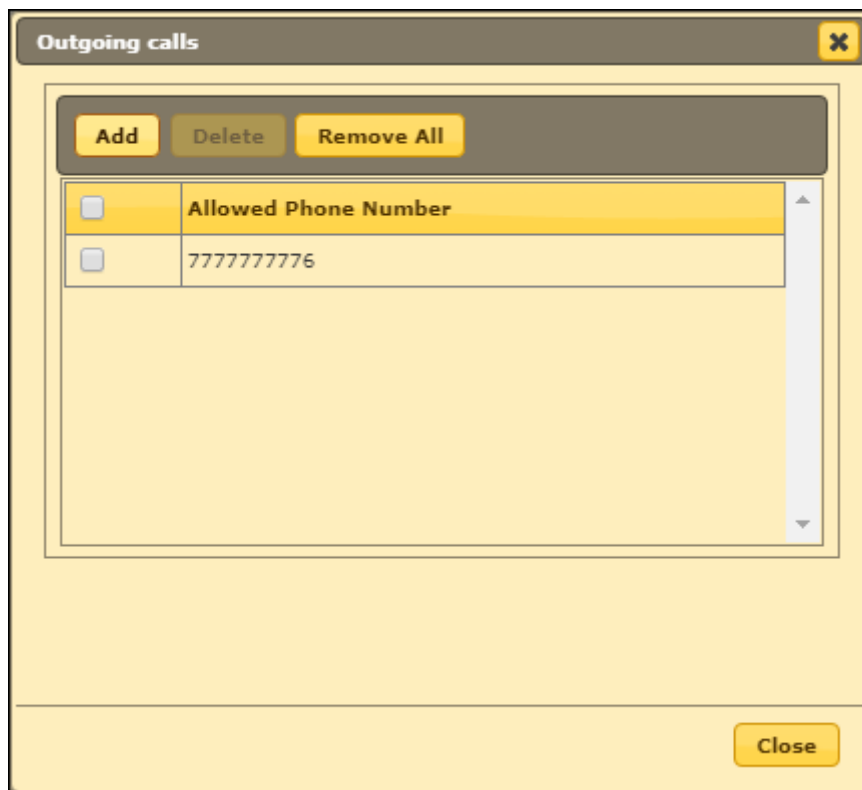
Click **Add**.

Allow outgoing window appears.

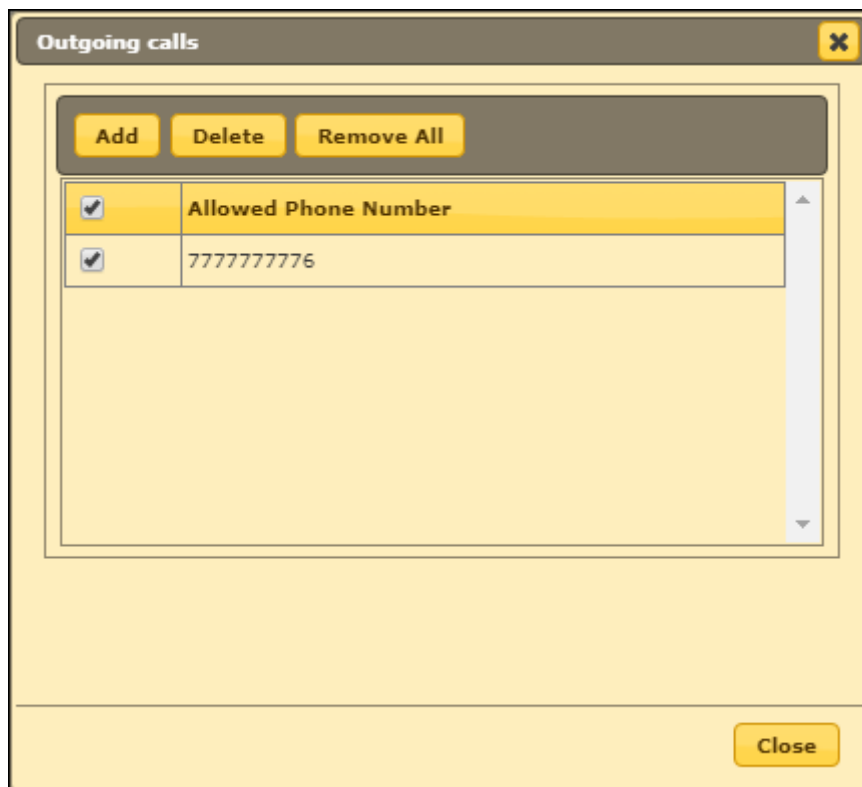


Enter the phone number and then click **Add**.

The number will be added to the Whitelist.



To delete a specific number, select a number and then click **Delete**.



The number will be deleted.

Web and Application Control

Web and Application Control policy lets you allow and block applications and websites on managed devices.

Web and Application Control

Control Mode: Both

Allow / Block Application List

Allow / Block Website categories

Filter Categories

Category Name	Allow	Block
Select All	<input type="checkbox"/>	<input type="checkbox"/>
Advertisements and Popups	<input checked="" type="radio"/>	<input type="radio"/>
Alcohol and Tobacco	<input type="radio"/>	<input checked="" type="radio"/>
Anonymizers	<input type="radio"/>	<input checked="" type="radio"/>
Arts	<input checked="" type="radio"/>	<input type="radio"/>

Allow List Block List

Control Mode

Allow or Block **Applications/Website** or **Both** or **Off** based on your requirement and Policies.

Control mode set to Off

If the Control Mode is set to **Off**, you cannot allow/block websites or applications.

Web and Application Control

Control Mode: Off

Control mode set to Website

Setting the Control Mode to Website lets you allow and block website categories.

Web and Application Control

Control Mode: Website

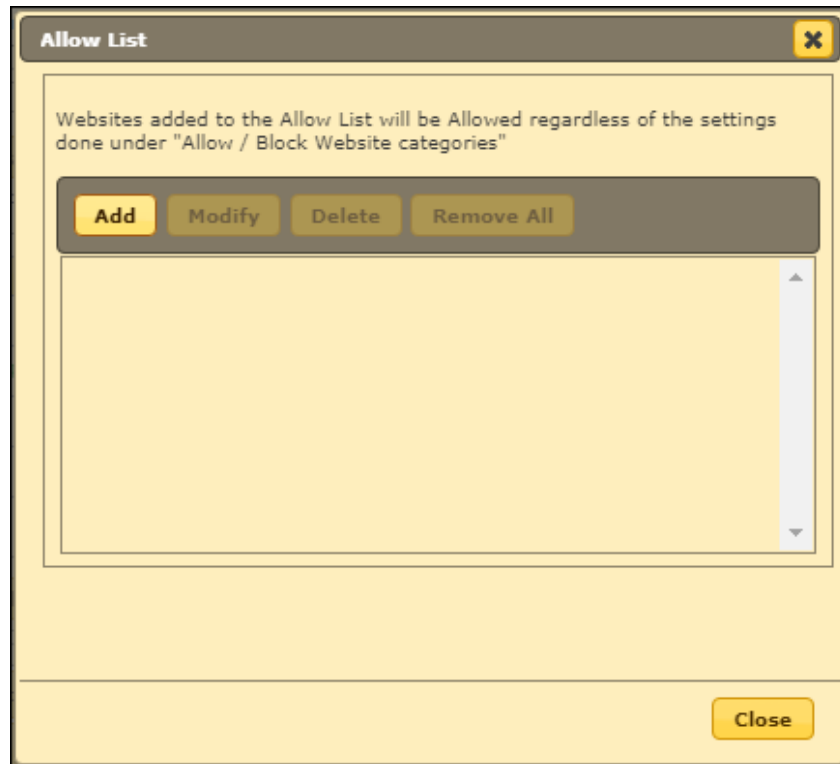
Allow / Block Website categories

Filter Categories

Category Name	Allow	Block
Select All	<input type="checkbox"/>	<input type="checkbox"/>
Advertisements and Popups	<input checked="" type="radio"/>	<input type="radio"/>
Alcohol and Tobacco	<input type="radio"/>	<input checked="" type="radio"/>
Anonymizers	<input type="radio"/>	<input checked="" type="radio"/>
Arts	<input checked="" type="radio"/>	<input type="radio"/>

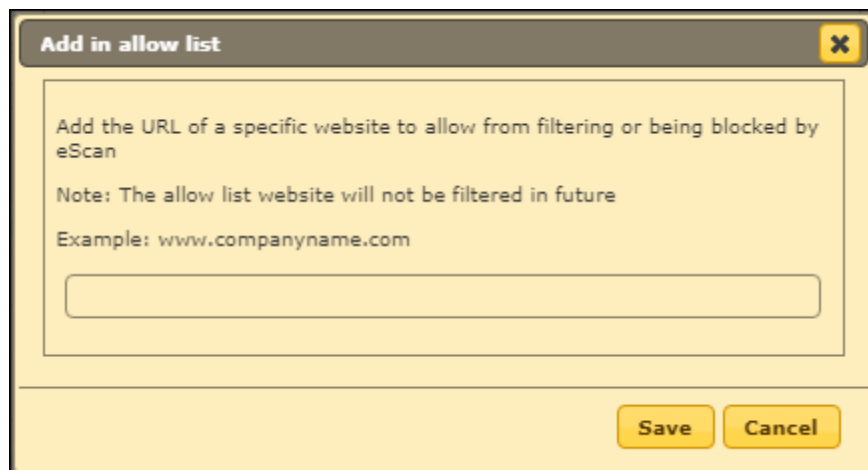
Allow List Block List

Allow List: Websites added to this list can be accessed in browser. You can modify, delete and also remove the list of websites.



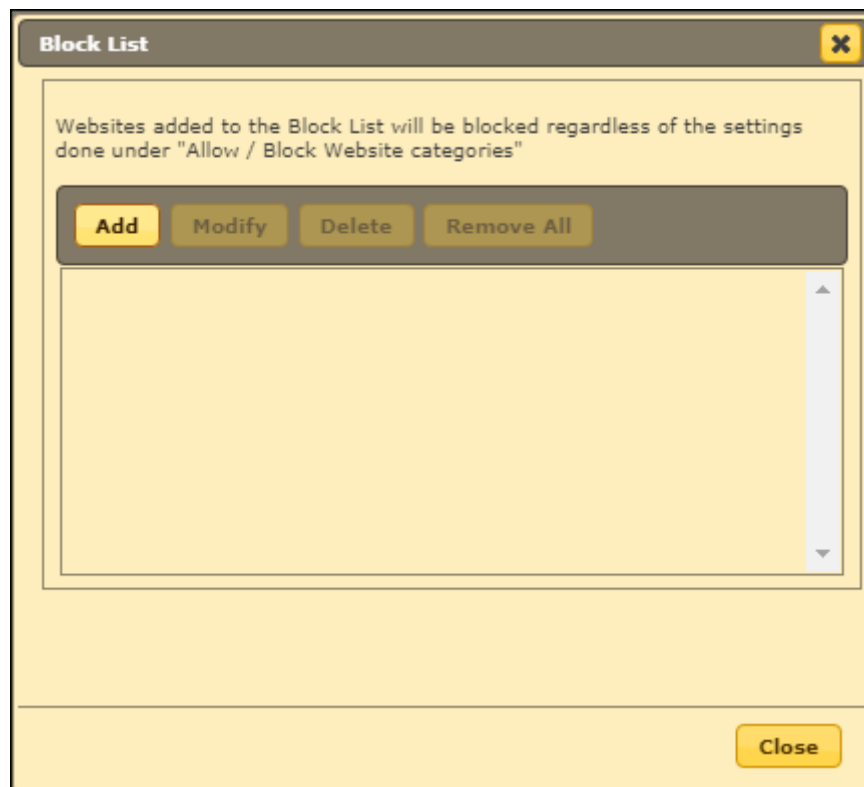
Click **Add**.

Add in allow list window appears.



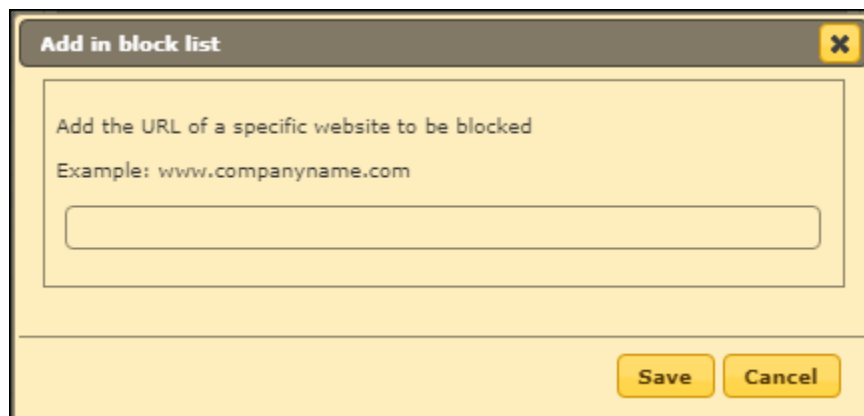
Enter the URL in the field and then click **Save**.

Block List: Websites added to this list will be blocked in browser. You can modify, delete and remove the list of websites from the Block List.



Click **Add**.

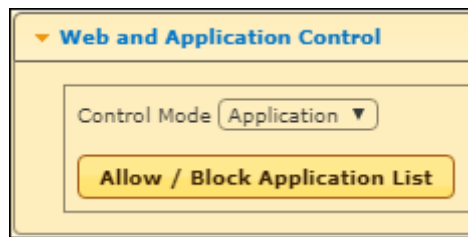
Add in block list window appears.



Enter the URL and then click **Save**.

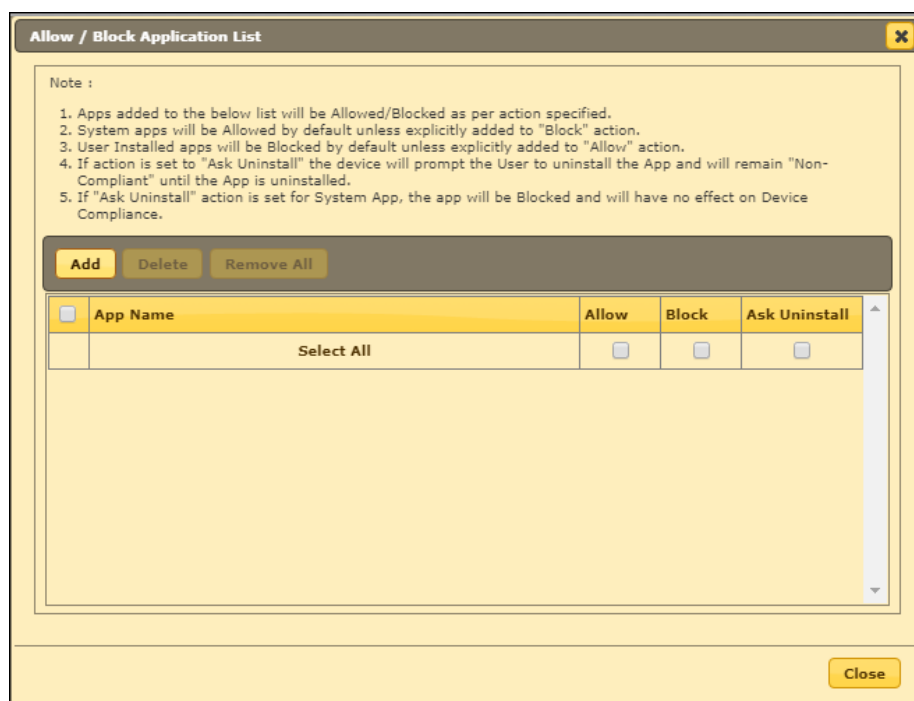
Control mode set to Application

Setting the Control Mode to **Application** lets you allow or block an application.



Click **Allow/Block Application List**.

Allow/Block Application List window appears.



Click **Add**.

Application List

1. Applications added to this list will be allowed/blocked as per the specified action.
2. System applications will be allowed by default unless explicitly added to "**Block**" section.
3. User installed applications will be blocked by default unless explicitly added to "**Allow**" section.
4. If the action is set to "**Ask Uninstall**" the device will prompt the user to uninstall the application and will remain "**Non-Compliant**" until the application is uninstalled.
5. If "**Ask Uninstall**" action is set for the system applications, the applications will be blocked and will have no effect on the device compliance.

Allow/Block Application window appears.

Allow / Block Application

Available applications

[All](#)
[A](#)
[B](#)
[C](#)
[D](#)
[E](#)
[F](#)
[G](#)
[H](#)
[I](#)
[J](#)
[K](#)
[L](#)
[M](#)
[N](#)
[O](#)
[P](#)
[Q](#)
[R](#)
[S](#)
[T](#)
[U](#)
[V](#)
[W](#)
[X](#)
[Y](#)
[Z](#)
<#>

<input type="checkbox"/>	Application Name	Allow	Block	Ask Uninstall
<input type="checkbox"/>	Select All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note: If Application is NOT in the "Available Applications" list, you can add the package name with the "Enter Package Name" option.

Enter Package Name:

Allow Add

Save Close

Enter the application's package name in the field. Select whether to **Allow**, **Block** or **Ask to Uninstall** the specific application and then click **Add** > **Save**.

Note If Application is NOT in the "Available Applications" list you can add the package name with the "Enter Package Name" option.

Control mode set to Both

Setting the Control Mode to Both lets you allow/block website categories and applications.

Web and Application Control

Control Mode: Both

Allow / Block Application List

Allow / Block Website categories

Filter Categories

Category Name	Allow	Block
Select All	<input type="checkbox"/>	<input type="checkbox"/>
Advertisements and Popups	<input checked="" type="radio"/>	<input type="radio"/>
Alcohol and Tobacco	<input type="radio"/>	<input checked="" type="radio"/>
Anonymizers	<input type="radio"/>	<input checked="" type="radio"/>
Arts	<input checked="" type="radio"/>	<input type="radio"/>

Allow List Block List

App Specific Network Blocking

The App Specific Network Blocking Policy lets you block a particular application from accessing the Internet.

▼ App specific network blocking

Enter Package Name: Add

Delete Remove All

<input type="checkbox"/>	Package Name
--------------------------	--------------

In the **Enter Package Name** field, type the application's package name and then click **Add**.

The package will be added and displayed in **Package Name** section below.

After a package is added, the respective application will be unable to access the Internet.

Note VPN permission is needed for this functionality to work.

To delete a package from the list, select the specific package and then click **Delete**.

To remove all packages, click **Remove All**.

▼ App specific network blocking

Enter Package Name: Add

Delete Remove All

<input type="checkbox"/>	Package Name
<input checked="" type="checkbox"/>	com.android.chrome
<input type="checkbox"/>	com.android.firefox
<input type="checkbox"/>	com.android.opera

Anti-Theft Policy

Anti-Theft Policy lets you keep track of a device's location history, block a device and send alert about SIM card change.

Anti-Theft Policy

☒ Enable Anti-Theft

Location History

☐ Enable Location History Interval 30 Mins ▼

Capture location details - Time based [Configure](#)

Note : Location coordinates will be captured by the device(s) only during the selected time slots.

☐ Show GPS alert block screen

Note : "Screen Overlay" permission is required for displaying the GPS alert screen on the device.

Uninstall Protection

☒ Block Device

☐ Ask "Admin Access Password" (Do not block device)

Anti-Theft WIPE Settings

☒ Delete all configured email accounts

☐ Delete specific domain account

Enter domain names:

Note: Add domain name in comma seperated format
eg. yourcompany.com, gmail.com, yahoo.com

Sim watch settings

☐ Send SMS notification on SIM card change

To Mobile No.:

☐ Send Email notification on SIM card change

☒ Administrator Email Id:
techeav@gmail.com

☐ Custom Email Id:

Options	Description
Enable Anti-Theft	By default, this check box is selected.
Enable Location History	Select this check box to track the location history. NOTE: Location coordinates will be captured by the device only during the selected time slots.
Interval in Mins	Track the location history at a defined interval. You can set the interval using Interval field.
Show GPS alert block screen	Select this checkbox to show the GPS alert and lock the screen. NOTE: Screen Overlay permission should be enabled on the device in order to work.
Block Device	Select this check box to block the device before uninstallation of eScan application.
Ask "Admin Access Password" (Do not block	Select this option if you don't want the device to be blocked if a user tries to uninstall the MDM application. The application will

device)	ask the user to enter the Admin Access Password.
Delete all configured email accounts	Select this check box to delete all email accounts configured on the managed device.
Delete specific domain account	Select this check box to delete email accounts of specific domain. After selecting this check box, enter the domain name in Enter domain names field.
Send SMS notification on SIM card change	Select this check box to receive a text message informing about SIM card change. The text message will be sent to the number added by you. Add the desired number in To Mobile No.
Send Email notification on SIM card change	Select this check box to receive an email informing about SIM card change. The notification email will be sent to the administrator's email ID or the custom email ID that the administrator has specified.

Additional Settings Policy

☒ Show Notification

Notifications will be shown

☒ Sound

Sound notifications for application events

☐ Write Logs

Write user actions to the eScan Log File

Sync Settings

☒ Sync at Device Reboot

Sync Everytime When Device Reboots

Sync Frequency

60 Mins

Policy Data Collection Frequency

Use this option to enable or disable the above options on selected managed devices.

Options	Description
Show Notification	Selecting this check box will display all notifications on devices.
Sound	Selecting this check box will play notification sound for eScan MDM application events.
Write Logs	Selecting this check box will enable MDM application to write logs of user actions on the eScan log file.
Sync at Device Reboot	Selecting this check box will sync the device with the eScan server after it reboots.
Sync Frequency	You can set the Sync Frequency in minutes and let the device sync with the eScan server.

Password Policy

Password Policy lets you define Administrator Access Password that allows an authorized user to configure settings of eScan Module on respective Managed devices.

Enter the password in **Admin Access Password** field.

Note The password should be numeric and minimum of four digits are required.

Device Oriented Policy

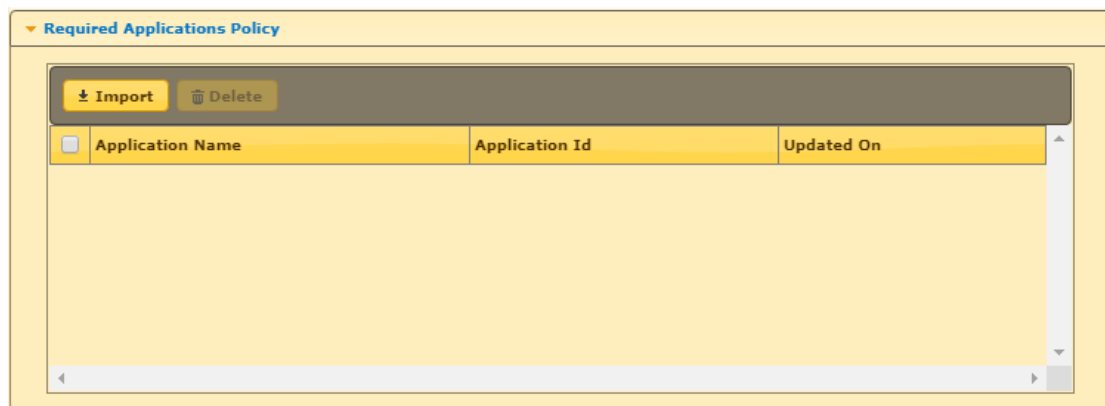
Device Oriented Policy lets you enable GPS and disable Camera, Bluetooth, and USB Connectivity on a device.

Options	Description
Enable GPS (For devices with Android version below 4.0)	Select this check box to enable GPS.
Disable Device Settings	Select this checkbox to block the access to Android Settings. NOTE: This option to work, Web And Application Control Mode should be set to Both/Application .
Disable Camera (For device with Android version 4.0 and Above)	Select this check box to disable the camera.

Disable Bluetooth & Bluetooth Discovery	Select this check box to disable the Bluetooth and Bluetooth discoveries.
Disable USB Connectivity (For devices with Android version below 4.0)	Select this check box to disable USB Connectivity.
Send Call Details to server, including Call/SMS filter events	Select this check box if you want device(s) to send their Call/SMS details to the server.
Set Device Block	This option allows to set the Days and Hours to block the device.

Required Applications Policy

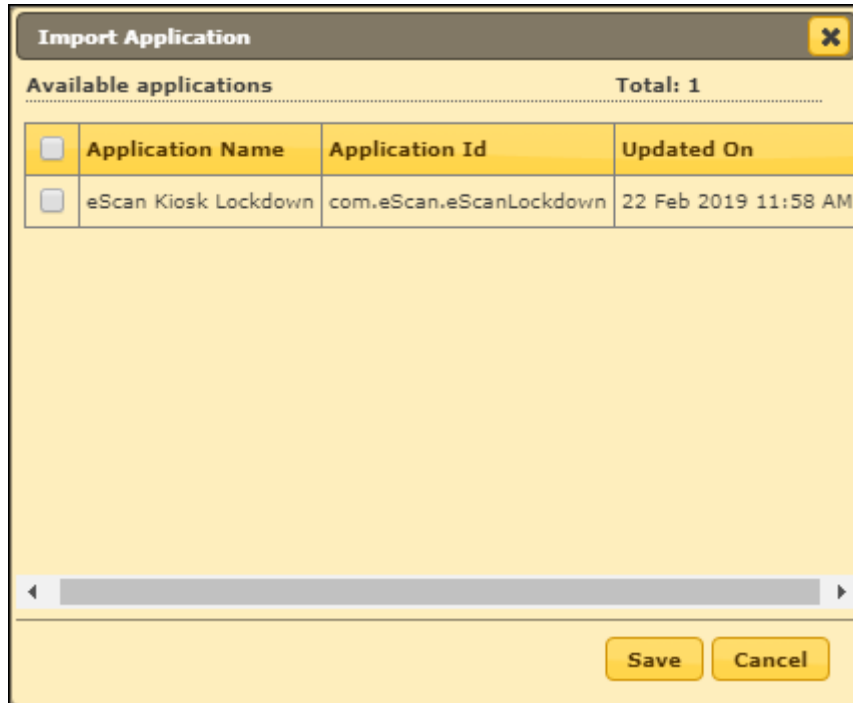
The Required Applications Policy lets you import applications from the App Store module for installation on devices in the group through policy deployment.



Importing an application

1. Click **Import**.

Import Application window appears.

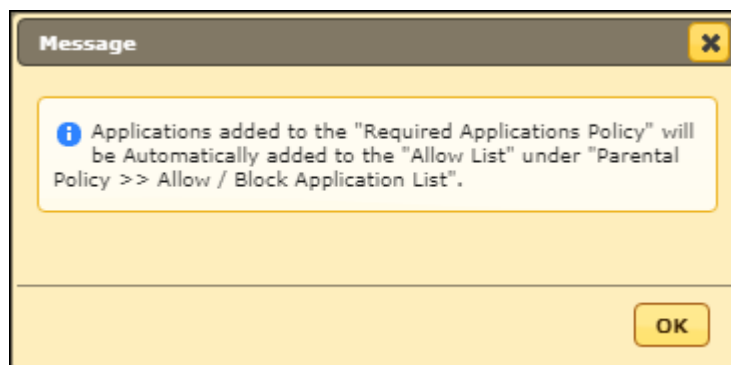


2. Select the application(s).

3. Click **Save**.

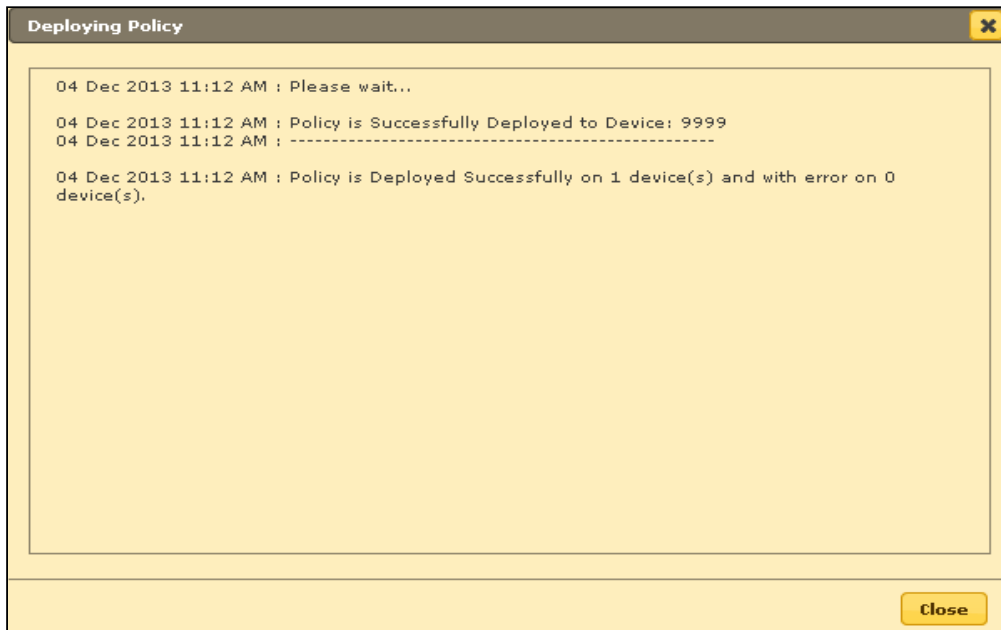
The selected application will be imported.

A pop-up message appears displaying Applications added to the "Required Applications Policy" will be automatically added to the "Allow List" under "Parental Policy >> Allow/Block Application List".



Click **Deploy**.

The policy will be deployed on the device instantly if the device is connected to the Internet. The following prompt appears after the successful policy deployment.



Note

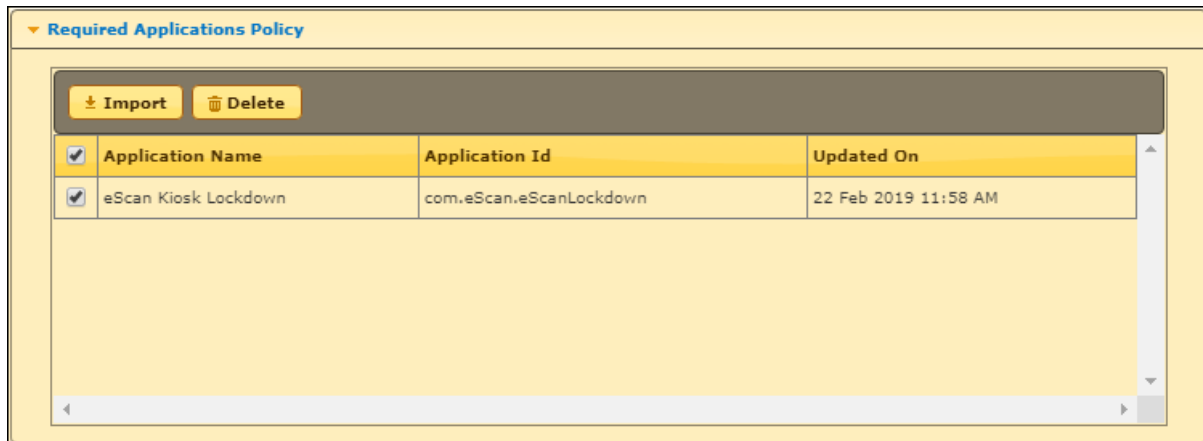
If the device is not connected to Internet, the policy changes will be applied on the next sync with the server. By default, the device(s) sync with the server every 60 minutes.

If an application is deployed via the Required Application Policy, the device(s) in the group receive a notification to install the application. The user will be provided with the option to start the installation process and install the application. If the device user cancels the installation, it will alert the user about application installation on the next sync with the server.

If the deployed application with the same version number already exists on device, the device user won't receive notification.

Deleting an application from “Required Applications Policy”

To delete an application, select the application and then click **Delete**.



The selected application will be deleted.

Wi-Fi Settings Policy

The Wi-Fi Settings policy lets you define the settings for your Wi-Fi connections. You can disable WLAN/Wi-Fi or restrict the usage of Wi-Fi by allowing the device to connect only to the listed Wi-Fi networks. The device can be automatically locked or raise a sound alarm if it is not connected to any of the listed Wi-Fi connections.

Enable Wi-Fi Restrictions (For devices with Android version below 6.0)

Select this checkbox to allow device to connect ONLY to the listed WiFi network name (SSIDs). This option is available only for devices with Android version below 6.0.

Adding a Wi-Fi SSID

1. Select the check box Enable Wi-Fi Restrictions and then click **Add**.
Add window appears.

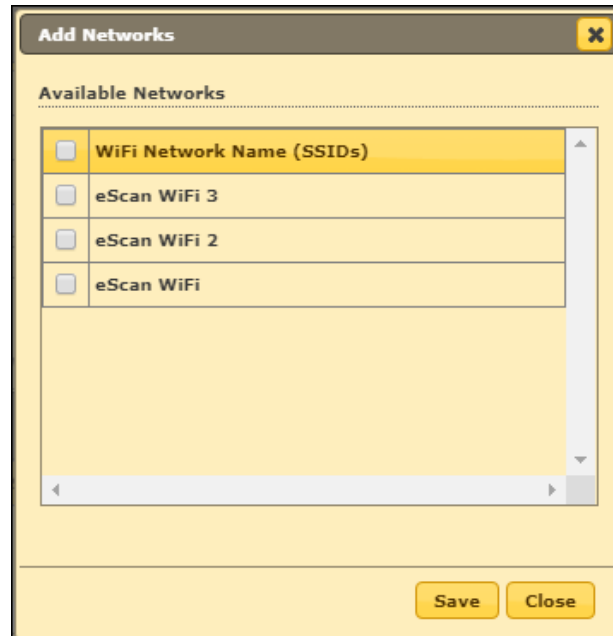
2. Enter the Wi-Fi network name (SSID) in the field and then click **Add**.
The Wi-Fi network will be added to the console.

The devices will be allowed to connect only to the added Wi-Fi network SSID.

Locking/Sounding alarm on a device

1. Select the check boxes **Lock Device** or **Sound Alarm** as per your requirement and then click **Add**.

Add Networks window appears.

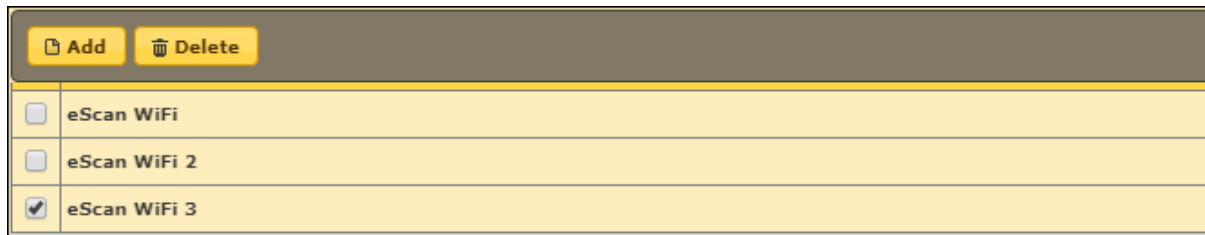


2. Select the Wi-Fi networks you want the device to always be connected to and then click **Save**.

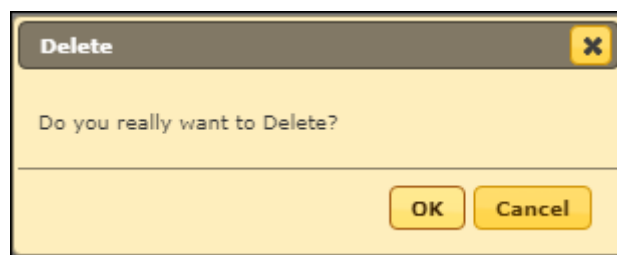
If the devices are not connected/disconnected from the added Wi-Fi network SSID, they will be locked or raise a loud alarm as per the policy configuration.

Deleting a Wi-Fi network SSID

1. Select a Wi-Fi network SSID and then click **Delete**.



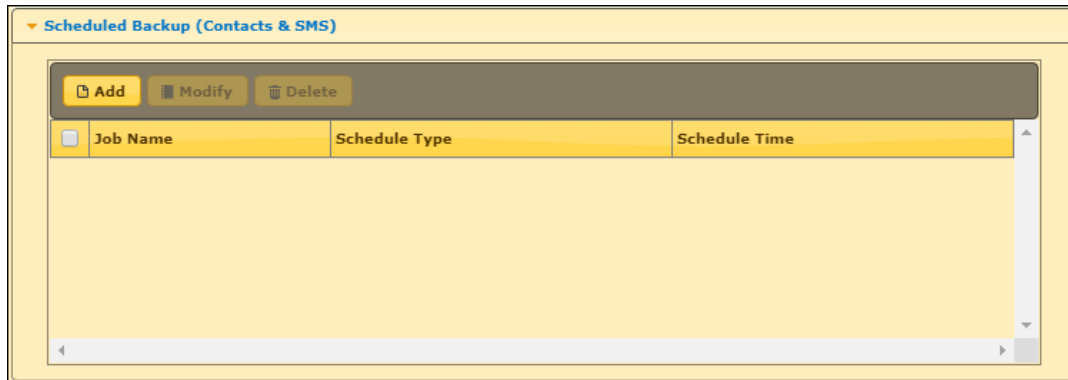
A confirmation prompt appears.



2. Click **OK**.
The Wi-Fi network SSID will be deleted.

Scheduled Backup (Contacts & SMS)

The Schedule Backup policy lets you take a backup of all the contacts and text messages on a device as per your requirements. The backup of contacts and text messages can be saved in two different folders. The backup can be scheduled for daily/weekly basis.



Creating a schedule

1. Click **Add**.
Add new job window appears.

Add new job

Job Name:

Job Settings

Select Backup

☐ SMS

☐ Contacts

Job Scheduler Settings

2. Enter a job name.
3. In **Job Settings**, select the preferred backup(s).
4. In **Job Scheduler Settings**, select whether you want to take a backup daily or weekly.
5. Set the specific time at which you want to take the backup and then click **Save**.

Add new job

Job Name:

► **Job Settings**

▼ **Job Scheduler Settings**

☐ Daily
☒ Weekly
☐ Disable Schedule

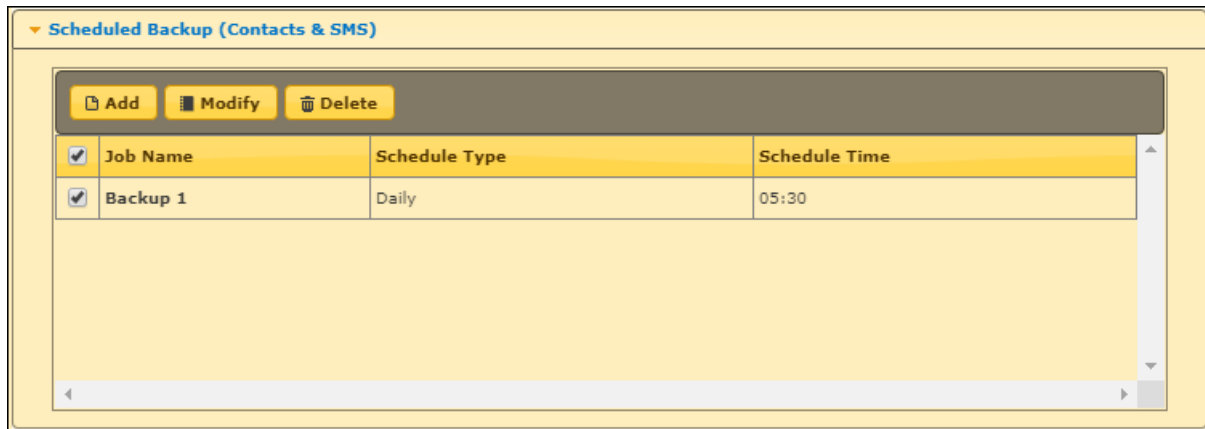
☐ Mon ☐ Tue ☐ Wed ☐ Thu
☐ Fri ☐ Sat ☐ Sun

At: 05:30

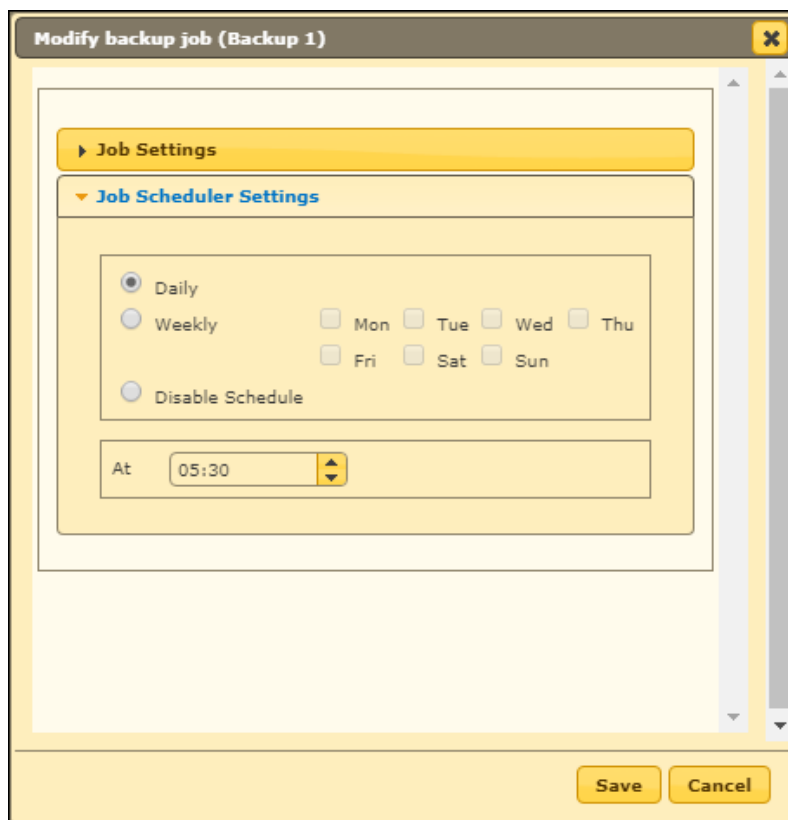
Save Cancel

Modifying a schedule

1. To modify a schedule, select the specific schedule and then click **Modify**.



Modify backup job window appears.



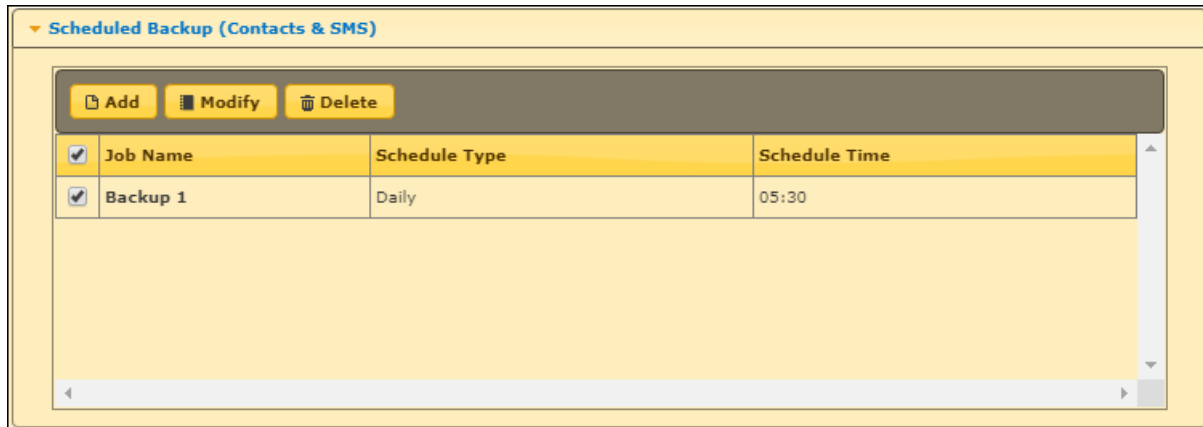
2. Make the required changes and then click **Save**.
The schedule will be modified.

As an Administrator, you can even disable a scheduled backup by selecting the option **Disable schedule** > **Save**.

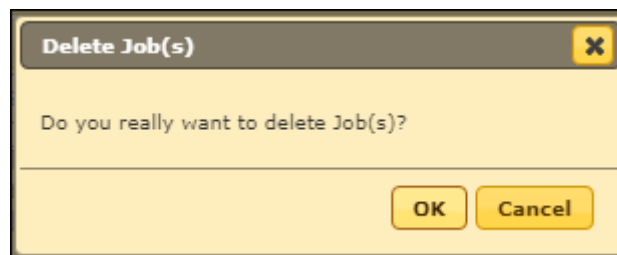
Deleting a schedule

To delete a schedule, follow the steps given below:

1. Select a schedule and then click **Delete**.



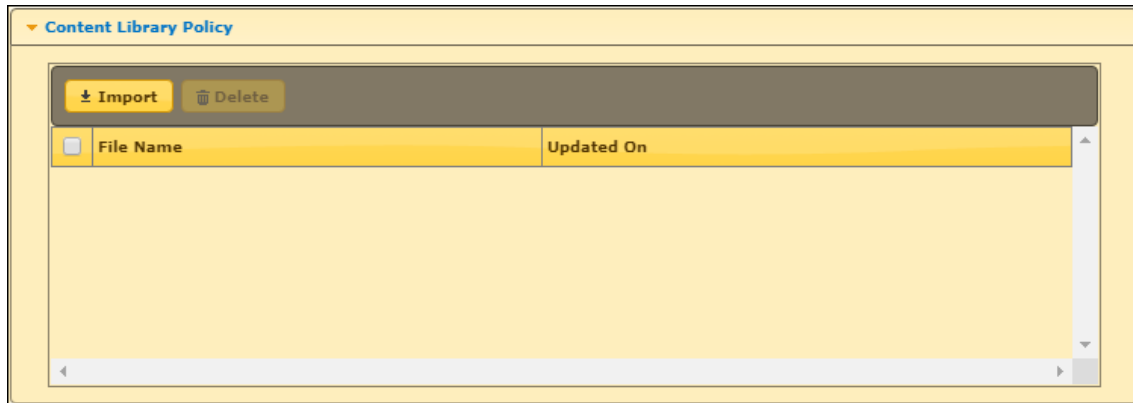
A confirmation prompt appears.



2. Click **OK**.
The schedule will be deleted.

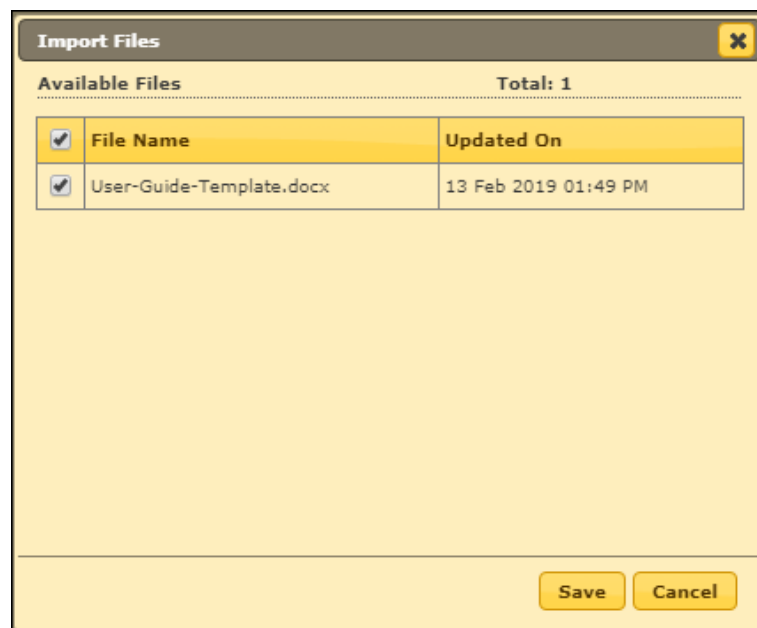
Content Library Policy

Content Library policy lets you deploy documents to the users' devices. The documents can be imported from the Content Library module and deployed to the users. To learn more about Content Library, [click here](#).

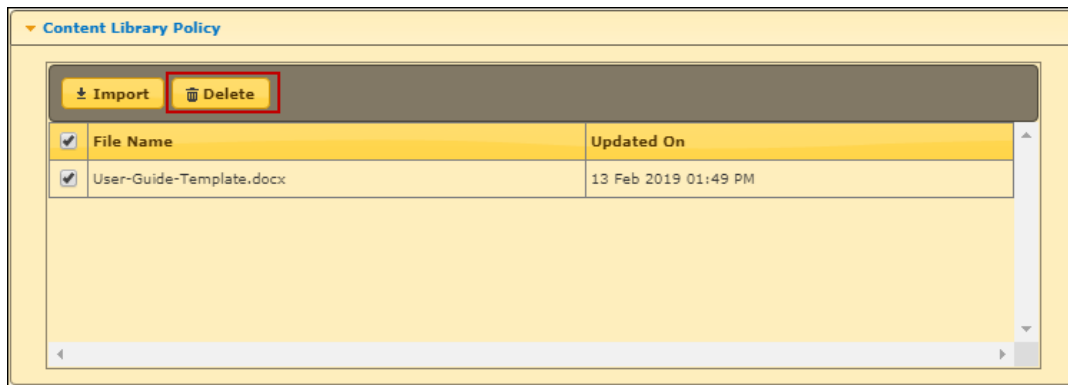


Import a file

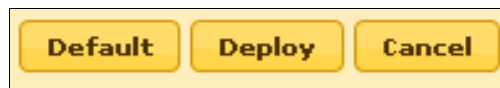
To import a file from Content Library, click **Import**. Select the file and then click **Save**.



To delete a file, select the specific file and then click **Delete**.



Default, Deploy, or Cancel



Description - You can select eScan **Default** settings or **Deploy** the setting defined by you for implementing/deploying on specific groups.

Kiosk Mode Policy

To configure Kiosk Mode Policy, select **Enable Kiosk Mode** check box.

Application(s) to be added to Kiosk section allows an application to be accessed in Kiosk mode.

Use Single App Mode

Select this checkbox to use the app in the single mode. The Kiosk Mode Policy lets you run a device in Single App Mode wherein the device will run only one app even if multiple apps are installed. The device user will be unable exit the application or perform other device activities.

It also provides another option wherein the dropdown menu displays a list of installed applications. Select an application and then click **Add**. The application will be added. To delete the added application(s) from Kiosk mode, select the application(s) and then click **Delete**. The application will be deleted.

Force user to install all apps as required by Kiosk policy

Select this check to install the apps added in the list before entering the Kiosk mode.

NOTE	Unchecking Force user to install all apps as required by Kiosk policy option will allow user to enter Kiosk mode even if any of the app is not installed.
-------------	--

Whitelist for apps

This section lets you to whitelist the apps.

Whitelist for apps

Enter Package Name:

+ Add

Note:

1. Package names added to the list will be allowed if launched from within any other apps added to kiosk mode.

2. These apps will not be visible in Kiosk mode.

Delete

☐

Package Name

☐ Allow all non-launchable system apps
(All non-launchable system apps will be allowed if launched from within any other app added to Kiosk mode)

Add

Enter the name of the app/package and click **Add** to whitelist the particular app.

Allow all non-launchable system apps

Select this check box if you want to allow the non-launchable system apps to launch from within any other app added to Kiosk mode.

NOTE	All non-launchable system apps will be allowed if launched from within any other app added to Kiosk mode.
-------------	---

Hardware Key Control

☐ Disable Power button

☐ Disable Volume buttons

Allow User to Turn ON/OFF

☒ WiFi

Check "WiFi Settings Policy" if this option is inactive.

☒ Bluetooth

Check "Device Oriented Policy" if this option is inactive.

☒ Volume

☒ Brightness

NOTE: Unchecking will not display Control to the user.

☐ Allow Wi-Fi setting

☐ Allow device setting

Hardware Key Control

Kiosk mode also lets you disable a device's hardware keys.

Disable Power button – Selecting this check box disables a device's Power button.

Disable Volume buttons – Selecting this check box disables a device's Volume buttons.

Allow User to Turn ON/OFF

Wi-Fi – Selecting this check box allows a user to turn device's Wi-Fi ON/OFF through Kiosk application.

Bluetooth – Selecting this check box allows a user to turn device's Bluetooth ON/OFF through Kiosk application.

Volume – Selecting this check box allows a user to increase/decrease the device's volume through Kiosk application.

Brightness – Selecting this check box allows a user to increase/decrease the device's brightness through Kiosk application.

Note	Unchecking options won't display Control to the user on the Kiosk application.
-------------	--

Allow Wi-Fi setting

Selecting this check box allows user to access and configure the Wi-Fi settings in the Kiosk mode.

Allow device setting

Selecting this check box allows user to access and configure the device settings in the Kiosk mode.

Location Fencing

The Location Fencing feature allows to define an address on the map and set the radius around that address. If the device is in that region, then the policy set by the administrator will be active on the device. To learn more about location fencing, [click here](#).

Import Geo Fencing location(s)

☐ Geo Fencing

<input type="checkbox"/>	Custom Address	Latitude	Longitude	Radius(m)
<input type="checkbox"/>				

☒ Block device when outside of the set fence
(If unchecked, only events will be sent to the server, device will not be blocked)

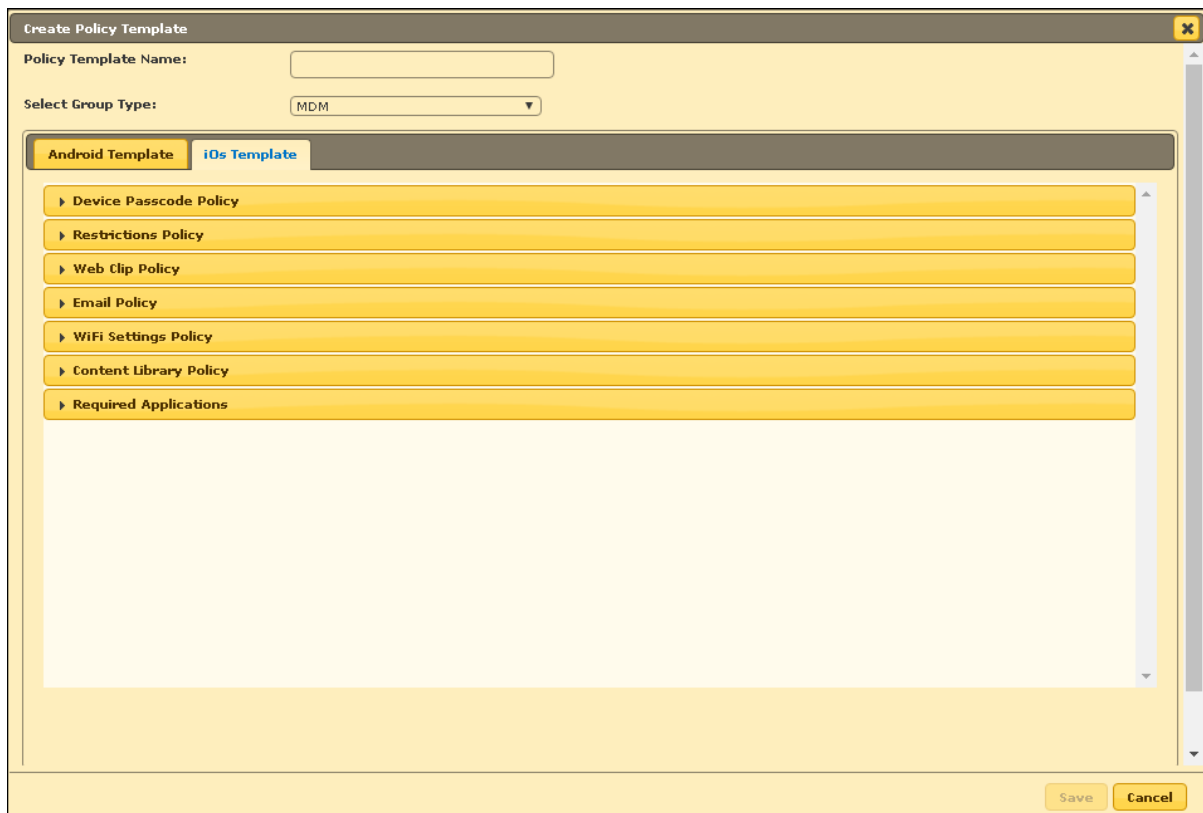
To configure Location Fencing policy, enable **Geo Fencing** option. After enabling this option, you can import the fencing locations. Click **Import** option to select and import the custom location.

Block device when outside of the set fence

Select this check box to block the device when it is outside the set fencing location.

NOTE	If Block device when outside of the set fence is unchecked then device will not be blocked but only events will be sent to the server.
-------------	---

iOS Template



Create Policy Template

Policy Template Name:

Select Group Type:

Android Template iOS Template

- ▶ Device Passcode Policy
- ▶ Restrictions Policy
- ▶ Web Clip Policy
- ▶ Email Policy
- ▶ WiFi Settings Policy
- ▶ Content Library Policy
- ▶ Required Applications

Save Cancel

The iOS Template consists following policies:

- Device Passcode Policy
- Restrictions Policy
- Web Clip Policy
- Email Policy
- Wi-Fi Settings Policy
- Content Library Policy
- Required Applications

Device Passcode Policy

The Device Passcode Policy lets you configure the passcode, auto-lock duration, device lock grace period and data wipe in case of maximum passcode fail attempts.

Select the **Enable** check box to enable all the fields in this section.

You can set the Device passcode policy for the device using this policy.

Allow Simple Value: Set this option to **Yes** if the passcode should be simple value. For example, 1234 or 0000

Require Alphanumeric Value: Set this option to **Yes** if the passcode should be alphanumeric. For example, abc123 or 123abc

Minimum Passcode Length: This option lets you set the minimum passcode length. The numeric value can be set between 1 and 16.

Minimum Number of Special characters: This option lets you set the count of special characters required to construct a passcode. The count for special characters in passcode can be set between 1 and 4.

Maximum Passcode Age (days 1-730, or blank): This option lets you set the maximum number of days from 1 to 730 before the password expires and asks the user to set a new one.

Allowed idle time, before Auto-Lock: This option lets you set time for a device (in minutes), before it gets auto-locked.

Number of Passcodes to be maintained in the history (1-50, or blank): This option lets you set the number of passcodes to be maintained in the history.

Grace Period for Device Lock: Grace period is a time duration that ensures the device stays locked until the next passcode entry. This option lets you set the grace period for a device from 1 Minute to 4 Hours.

Maximum Number of Failed Attempts (Before all data is erased): This option lets you set the maximum number of failed attempts allowed for unlocking a device before all data on the device is erased.

Restrictions Policy

The Restrictions Policy lets you apply restrictions on a device.

- Device Functionality
- Application
- Safari Settings
- iCloud
- Security and Privacy
- Content Ratings
- Ratings by Region

Device Functionality

Device Functionality	
Allow Installing Apps	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow Use of Camera	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow FaceTime	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow Screen Captur	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow Automatic Sync While Roaming	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow Siri	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow Siri while device locked	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow usage of Touch ID to unlock device (iOS 7 and above)	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow Passbook while device locked (iOS 6 and above)	<input checked="" type="radio"/> Yes <input type="radio"/> No
Show Control Center in lock screen (iOS 7 and above)	<input checked="" type="radio"/> Yes <input type="radio"/> No
Show Notification Center in lock screen (iOS 7 and above)	<input checked="" type="radio"/> Yes <input type="radio"/> No
Show Today view in lock screen (iOS 7 and above)	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow Voice Dialing	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow In App Purchase	<input checked="" type="radio"/> Yes <input type="radio"/> No
Force User to enter iTunes Store password	<input type="radio"/> Yes <input checked="" type="radio"/> No
Allow Multiplayer Gaming	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow Adding Game Center Friends	<input checked="" type="radio"/> Yes <input type="radio"/> No

Allow Installing Apps: Set this option to **Yes** to allow users to install applications.

Allow Use of Camera: Set this option to **Yes** to allow users to access device's camera.

Allow FaceTime: Set this option to **Yes** to allow users to access FaceTime.

Allow Screen Capture: Set this option to **Yes** to allow users to take a screenshot or record their screen.

Allow Siri: Set this option to **Yes** to allow users to use Siri.

Allow Siri while the device is locked: Set this option to **Yes** to allow users to use Siri while the device is locked.

Allow usage of Touch ID to unlock device (iOS 7 and above): Set this option to **Yes** to allow users to unlock their devices with Touch ID.

Allow Apple Wallet while the device is locked (iOS 6 and above): Set this option to **Yes** to allow use of Apple Wallet while the device is locked. Learn more about Apple Wallet by clicking [here](#).

Show Control Center in lock screen (iOS 7 and above): Set this option to **Yes** to allow users to access Control Center in the lock screen. Learn more about Control Center by clicking [here](#).

Show Notification Center in lock screen (iOS 7 and above): Notification Center is a feature in iOS that provides an overview of application notifications. Set this option to **Yes** to allow users to view Notification Center in lock screen.

Show Today view in lock screen (iOS 7 and above): Set this option to **Yes** to allow users to view Today View in lock screen.

Allow Voice Dialing: Set this option to **Yes** to allow users to call their contacts via voice.

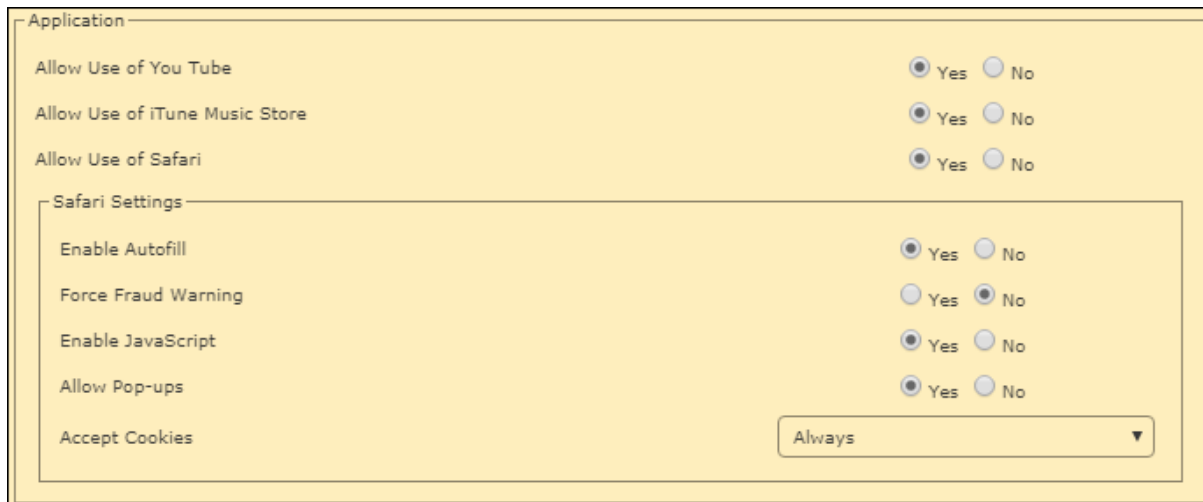
Allow In-App Purchase: Set this option to **Yes** to allow users to make in-app purchases.

Force User to enter iTunes Store password: Set this option to **Yes** to force a user to enter their iTunes Store password.

Allow Multiplayer Gaming: Set this option to **Yes** to allow a user to play a multiplayer game on their device.

Allow Adding Game Center Friends: Set this option to **Yes** to allow a user to add Game Center friends.

Application



Allow Use of YouTube: Set this option to **Yes** to allow users to access YouTube.

Allow Use of iTunes Music Store: Set this option to **Yes** allow users to access iTunes Music Store.

Allow Use of Safari: Set this option to **Yes** to allow users to access Safari.

Safari Settings

Enable Autofill: Set this option to **Yes** if you want Safari to remember the information users entered in the web forms.

Force Fraud Warning: Set this option to **Yes** if you want Safari to prevent the user from visiting websites identified as being fraudulent or compromised.

Enable JavaScript: Set this option to **Yes** if you want Safari to accept all JavaScript on websites.

Allow Pop-ups: Set this option to **Yes** if you want Safari to allow all pop-ups on a website.

Accept Cookies: Select the appropriate option for Safari to accept cookies.

- Always
- From Visited Sites
- Never

iCloud

Setting	Yes	No
Allow Backup	<input checked="" type="radio"/>	<input type="radio"/>
Allow Document Sync	<input checked="" type="radio"/>	<input type="radio"/>
Allow Photo Stream	<input checked="" type="radio"/>	<input type="radio"/>
Allow Shared Stream (iOS 6 and above)	<input checked="" type="radio"/>	<input type="radio"/>

Allow Backup: Set this option to **Yes** to allow backup of device data to iCloud.

Allow Document Sync: Set this option to **Yes** to allow Document Sync on a device.

Allow Photo Stream: Set this option to **Yes** to allow Photo Stream on a device.

Allow Shared Stream (iOS 6 and above): Set this option to **Yes** to allow Shared Stream on a device.

Security and Privacy

Setting	Yes	No
Allow Diagnostic Data to be sent to Apple (iOS 6 and above)	<input checked="" type="radio"/>	<input type="radio"/>
Allow User to accept untrusted TLS Certificates	<input checked="" type="radio"/>	<input type="radio"/>
Allow automatic updates to certificate trust settings (iOS 7 and above)	<input checked="" type="radio"/>	<input type="radio"/>
Force Encrypted Backups	<input type="radio"/>	<input checked="" type="radio"/>
Force limited ad tracking (iOS 7 and above)	<input type="radio"/>	<input checked="" type="radio"/>
Allow documents from managed apps in unmanaged apps (iOS 7 and above)	<input checked="" type="radio"/>	<input type="radio"/>
Allow documents from unmanaged apps in managed apps (iOS 7 and above)	<input checked="" type="radio"/>	<input type="radio"/>

Allow Diagnostic Data to be sent to Apple (iOS 6 and above): Set this option to **Yes** to allow a device's diagnostic data to be sent to Apple servers.

Allow User to accept untrusted TLS Certificates: Set this option to **Yes** to allow user to accept untrusted TLS Certificates.

Allow automatic updates to certificate trust settings (iOS 7 and above): Set this option to **Yes** to allow automatic updates to certificate trust settings.

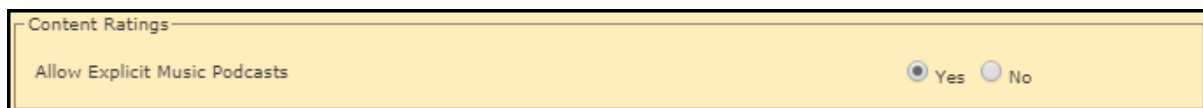
Force Encrypted Backups: Set this option to **Yes** to force a device to take encrypted backups.

Force limited ad tracking (iOS 7 and above): Set this option to **Yes** to stop receiving targeted advertisements on a device. This feature does not block ads. The device user may still receive random ads.

Allow documents from managed apps in unmanaged apps (iOS 7 and above): Set this option to **Yes** to allow documents from managed applications to open in unmanaged applications.

Allow documents from unmanaged apps in managed apps (iOS 7 and above): Set this option to **Yes** to allow documents from unmanaged applications to open in managed applications.

Content Ratings

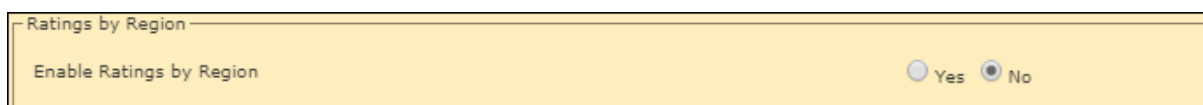


Content Ratings

Allow Explicit Music Podcasts ☒ Yes ☐ No

Allow Explicit Music Podcasts: Set this option to **Yes** to allow explicit music podcasts to be played on a device.

Ratings by Region



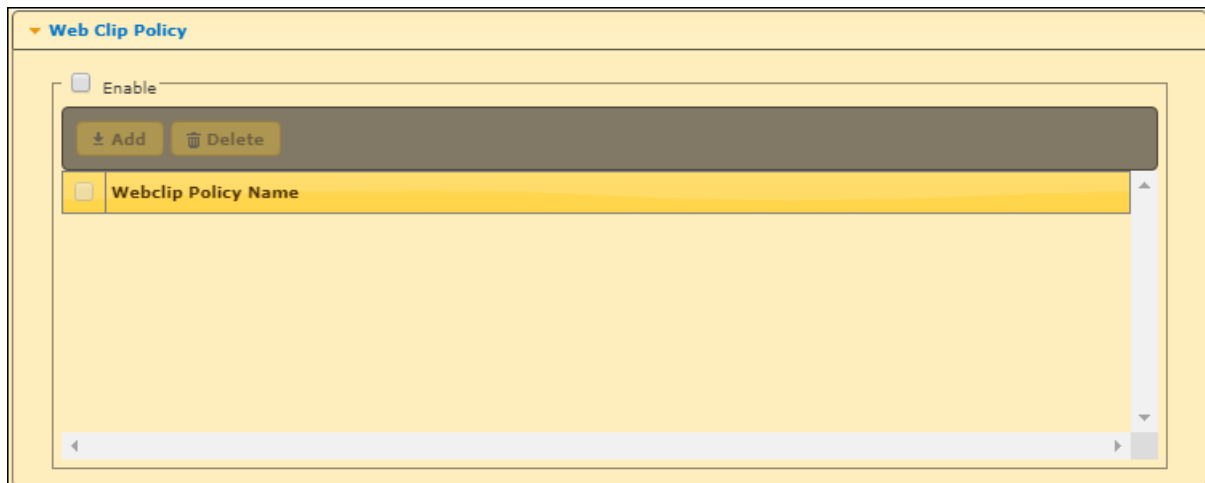
Ratings by Region

Enable Ratings by Region ☐ Yes ☒ No

Enable Ratings by Region: Set this option to **Yes** to enable content ratings by region.

WebClip Policy

The WebClip policy lets you get important websites on a device's home screen to let users access it quickly.



Adding a WebClip

Check **Enable** and then click **Add**.
WebClip Policy window appears.

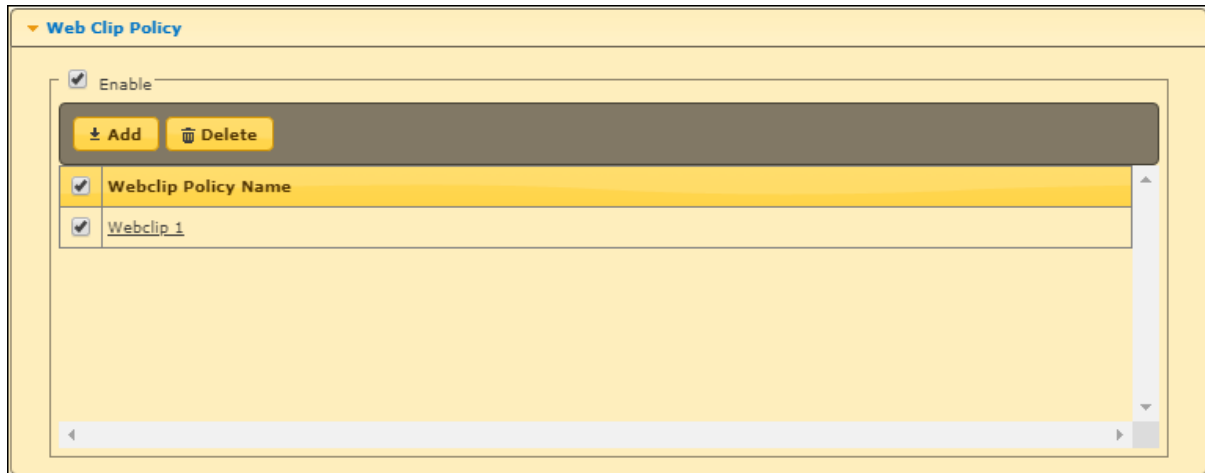
WebClip Label: Enter a name for the WebClip.

URL to be Linked: Enter the website URL.

Removal of WebClip: Set the WebClip status as either **Enable** or **Disable**. If enabled, the user can remove the WebClip from the device.

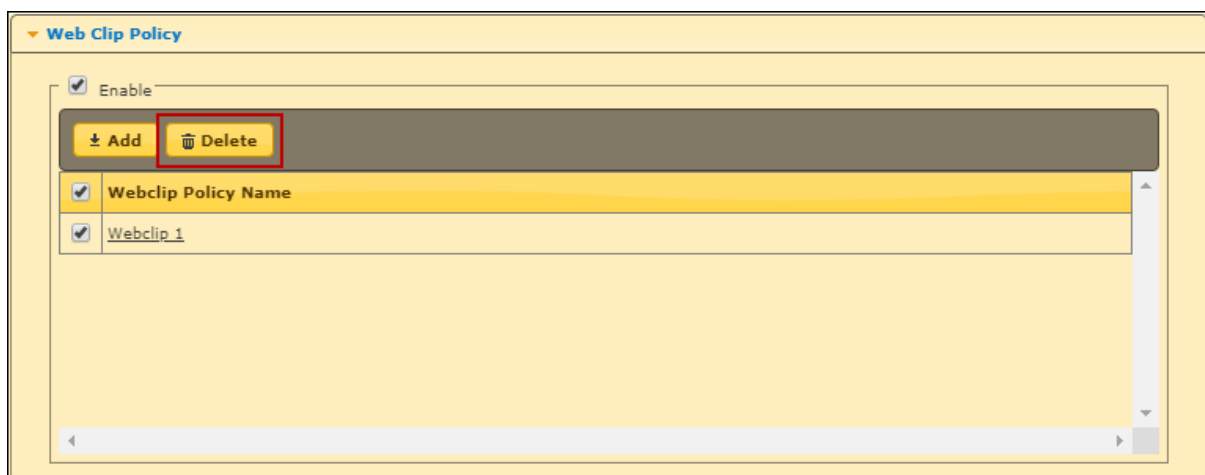
Allow Full Screen: Select **Yes** to allow full screen and **No** to disable full screen.

After entering all the details, click **Save**. The new web clip policy will be added.



Deleting a WebClip

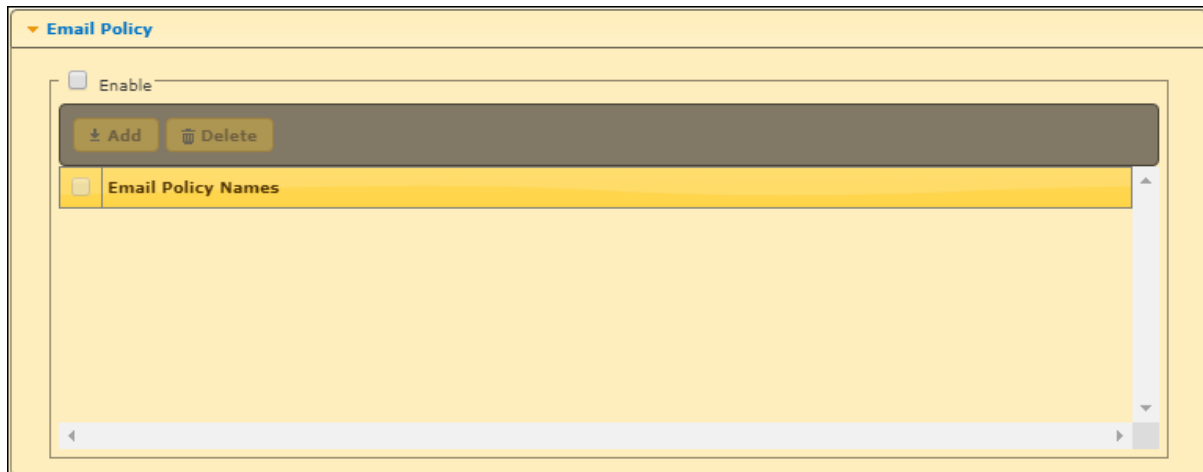
Select a WebClip and then click **Delete**.



The WebClip will be deleted.

Email Policy

The Email Policy lets you set up an email account for the managed devices and define the settings for incoming and outgoing emails.



Check **Enable** and then click **Add**.

Email Policy window appears.

Email Policy

Account Name *

Account Type

IMAP

Path Prefix

User Display Name

Note : "%username%" or "%email%" will fetch the appropriate Username/Email mapped to the device

Email Address

Note : "%email%" will fetch the appropriate Email Address mapped to the device

Allow Move

☒ Yes
☐ No

Disable recent mail address sync (iOS 6 and above)

☐ Yes
☒ No

Save

Cancel

Account Name: Enter an account name.

Account Type: Set the Account Type as **IMAP** or **POP**.

Choose POP if...

- You need constant access to your email, regardless of the Internet availability.
- You have limited server storage.

Choose IMAP if...

- You have a reliable and active Internet connection.
- You want to receive a quick overview of new emails on the server.
- Your local storage space is limited.

Path Prefix: In some cases, it is possible that you will not see the **Sent, Trash, Drafts,** and **Junk** folders. Typically, these folders are in your INBOX and you'll have to set a prefix path for it to work correctly.

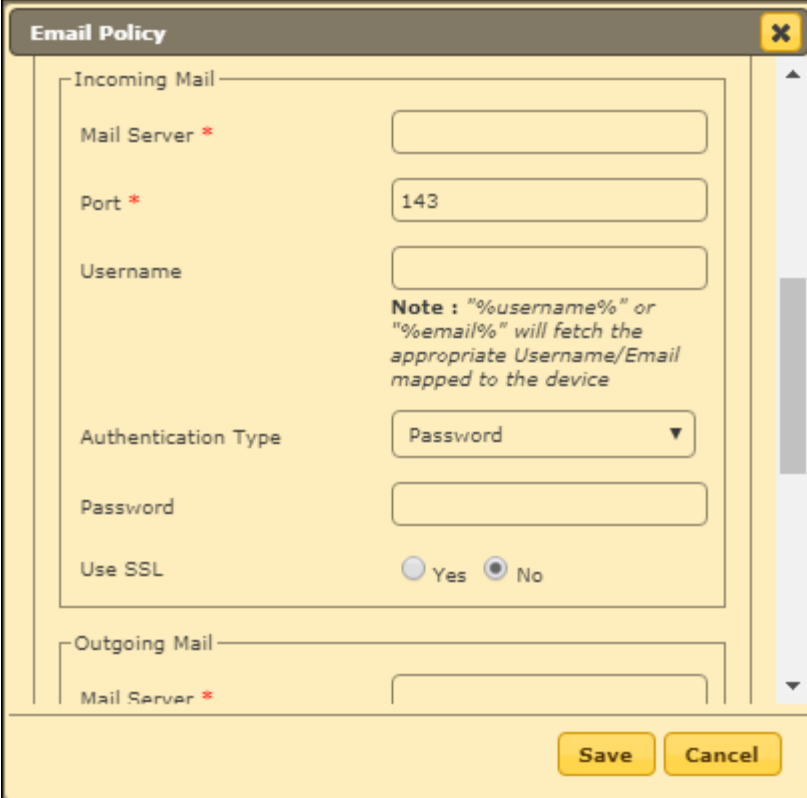
User Display Name: Type in the prefix "*%username%*" or "*%email%*". It will fetch the appropriate Username/Email mapped to the device.

Email Address: Typing in the prefix "*%email%*" will fetch the appropriate email ID mapped to the device.

Allow Move: Select the **Yes** option to Allow Move. Selecting **No** will prevent email data from being opened in other applications.

Disable recent mail address sync (iOS 6 and above): Selecting **Yes** will remove the mailbox from Recent addresses syncing.

Incoming Mail



The image shows a screenshot of the 'Email Policy' configuration window. It has a title bar with a close button (X). The window is divided into two main sections: 'Incoming Mail' and 'Outgoing Mail'. The 'Incoming Mail' section contains the following fields and controls:

- Mail Server ***: A text input field.
- Port ***: A text input field containing the value '143'.
- Username**: A text input field.
- Note**: A text block stating: "Note : \"%username%\" or \"%email%\" will fetch the appropriate Username/Email mapped to the device".
- Authentication Type**: A dropdown menu currently showing 'Password'.
- Password**: A text input field.
- Use SSL**: Two radio buttons, 'Yes' and 'No', with 'No' selected.

The 'Outgoing Mail' section is partially visible at the bottom, showing a 'Mail Server *' field. At the bottom right of the window are 'Save' and 'Cancel' buttons.

Mail Server: Enter the hostname for Incoming Mail Server in this field.

Port: Designates the incoming mail server port number. If no port number is specified, the default port for a given protocol is used.

Username: Add the **prefixes** `"%username%"` or `"%email%"`. It will fetch the appropriate Username/Email mapped to the device.

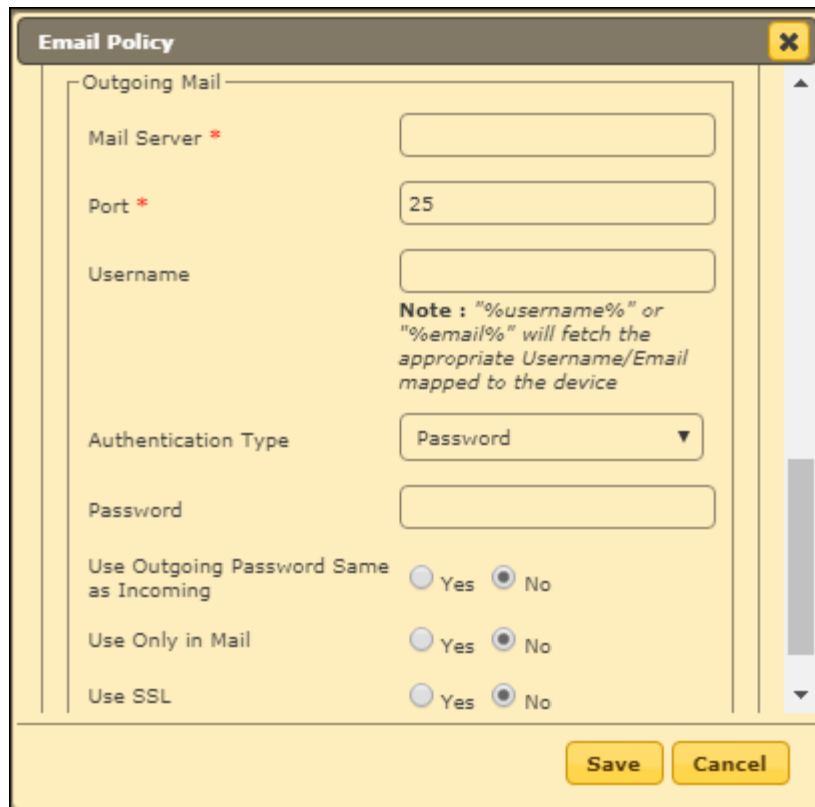
Authentication Type: Select the appropriate authentication type from the following options:

- None
- Password
- MD5 Challenge Service-Response
- NTLM
- HTTP MD5 Digest

Password: Set a password for incoming emails.

Use SSL: Designates whether or not the incoming mail server uses SSL certificate. Select **Yes** to allow the mail server to use SSL.

Outgoing Mail



The screenshot shows the 'Email Policy' window with the 'Outgoing Mail' tab selected. The window contains the following fields and options:

- Mail Server ***: A text input field.
- Port ***: A text input field containing the value '25'.
- Username**: A text input field.
- Note**: A text block stating: "Note : \"%username%\" or \"%email%\" will fetch the appropriate Username/Email mapped to the device".
- Authentication Type**: A dropdown menu currently showing 'Password'.
- Password**: A text input field.
- Use Outgoing Password Same as Incoming**: Radio buttons for 'Yes' and 'No', with 'No' selected.
- Use Only in Mail**: Radio buttons for 'Yes' and 'No', with 'No' selected.
- Use SSL**: Radio buttons for 'Yes' and 'No', with 'No' selected.
- Buttons**: 'Save' and 'Cancel' buttons at the bottom right.

Mail Server: Enter the hostname for outgoing mail server.

Port: Enter the outgoing mail server port number.

Username: Add the **prefixes** "*%username%*" or "*%email%*". It will fetch the appropriate Username/Email mapped to the device.

Authentication Type: Select the appropriate authentication type from the drop-down. Following authentication types are available:

- None
- Password
- MD5 Challenge Service-Response
- NTLM
- HTTP MD5 Digest

Password: Set a password for outgoing emails.

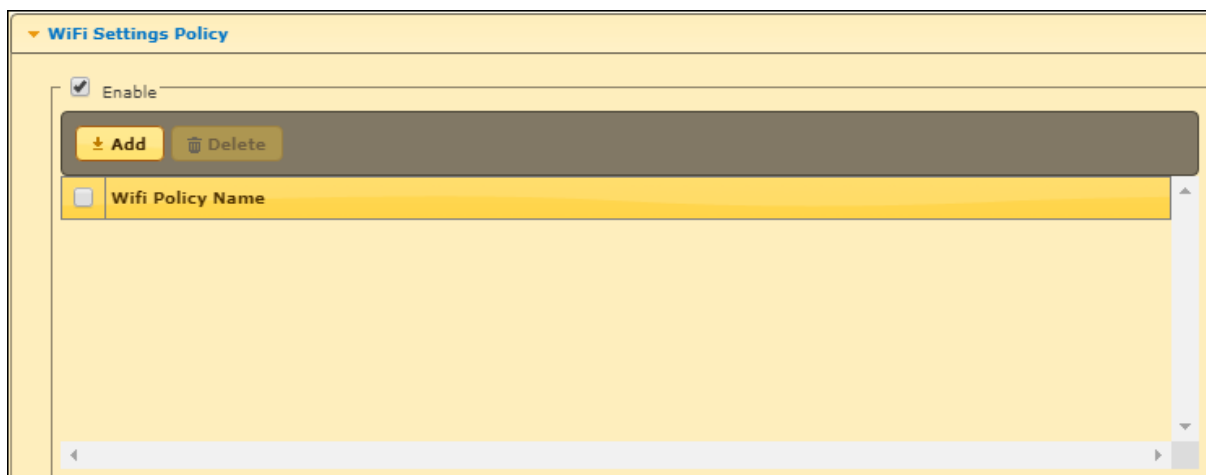
Use Outgoing Password Same as Incoming: If you want to use the same password set for the incoming email server, select **Yes**.

Use Only in Mail: Prohibits sending messages from other applications, such as Safari or Photos. If yes, configured account cannot be selected as default mail account on the device.

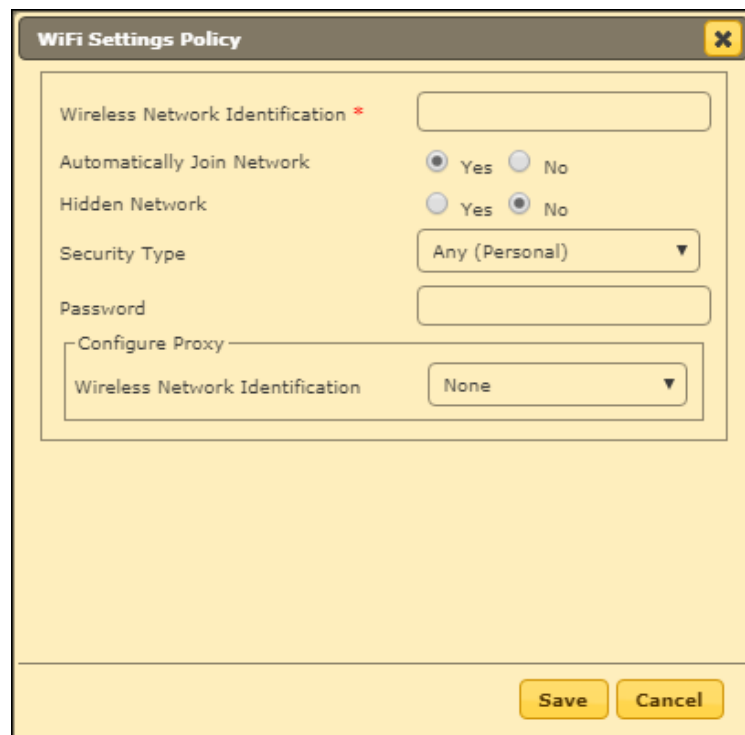
Use SSL: Determines whether or not the outgoing mail server uses SSL certificate.

Wi-Fi Settings Policy

The Wi-Fi Settings Policy lets you manage how a user connects their devices to a Wi-Fi network.



Check **Enable** and then click **Add**. Wi-Fi Settings Policy window appears.



Wireless Network Identification: Enter a name for the Wireless Network Identification.

Automatically Join Network: Set this option to **Yes** to automatically join a Wi-Fi network.

Hidden Network: Select this option to **Yes** to add a hidden network.

Security Type: Select a Security type for Wi-Fi network from the following options:

- None
- WEP
- WPA/WPA2
- Any(Personal)
- WEP Enterprise
- WPA/WPA2 Enterprise
- Any (Enterprise)

Password: Enter the password to connect to the Wi-Fi network.

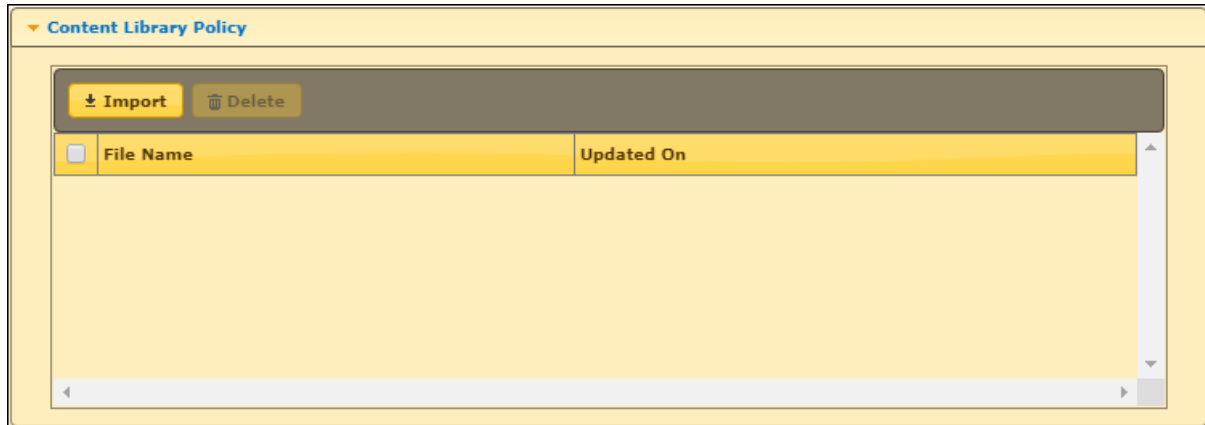
Configure Proxy: Configure a proxy for Wi-Fi settings by selecting a Wireless Network Identification.

- None
- Manual
- Automatic

After entering the appropriate details, click **Save**.

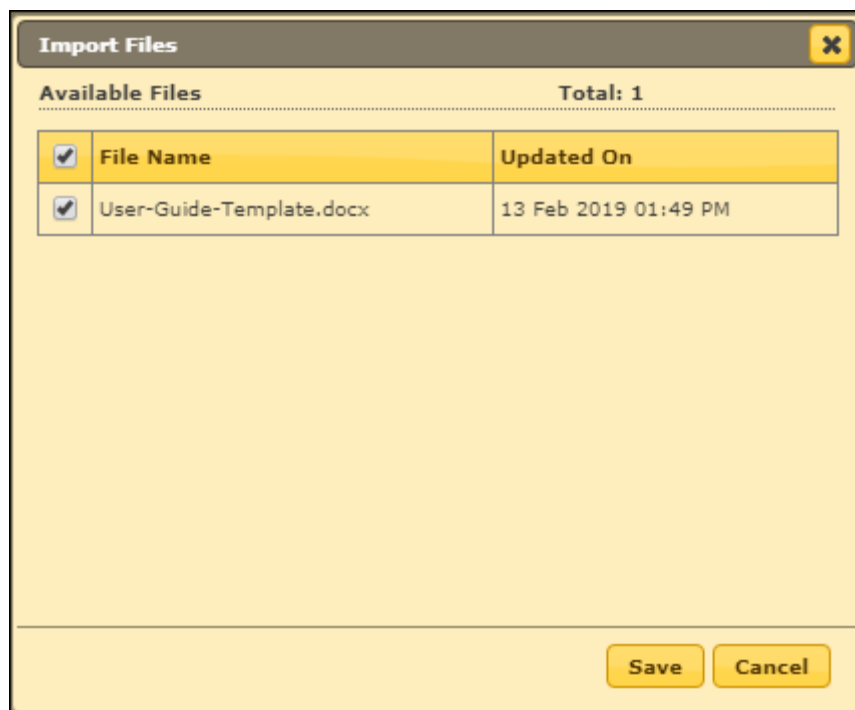
Content Library Policy

The Content Library policy lets you share documents with the users. The documents can be imported from the Content Library module and deployed to multiple users at the same time. To learn more about Content Library, [click here](#).



Importing a file

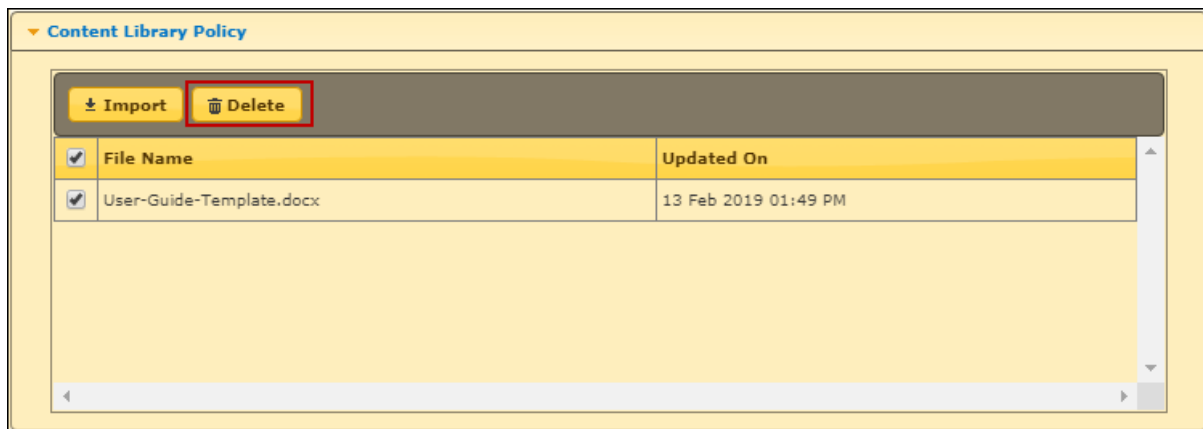
1. Check **Enable** and then click **Import**.
Import Files window appears.



2. Select a file and then click **Save**.

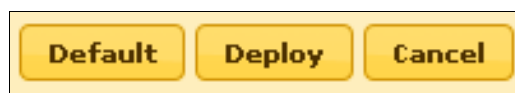
Deleting a file

Select a file and then click **Delete**.



The file will be deleted.

Default, Deploy or Cancel



You can select eScan **Default** settings or **Deploy** the setting defined by you for implementing/deploying on selected managed devices.

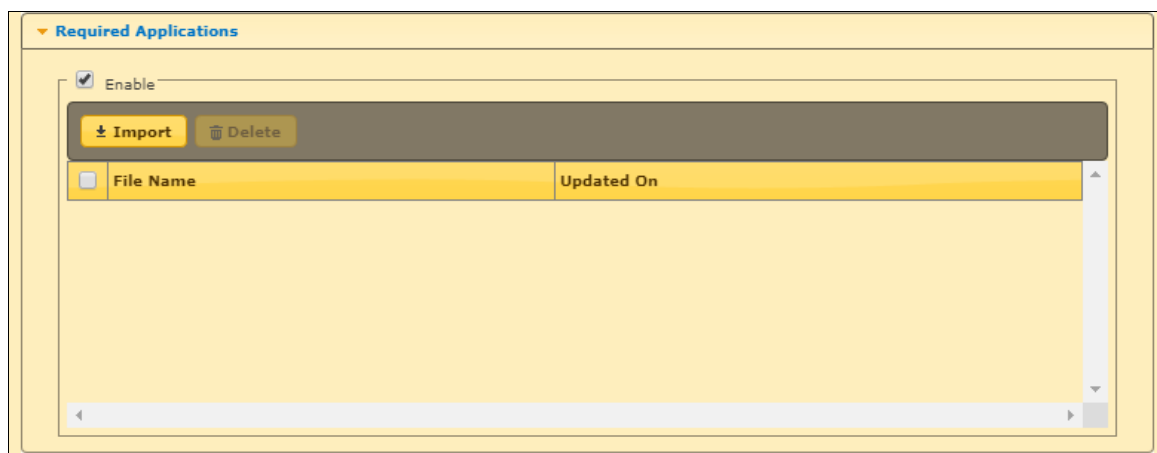
Required Applications Policy

The Required Applications policy lets you import applications from the App Store module for installation on managed devices in the group through policy deployment.

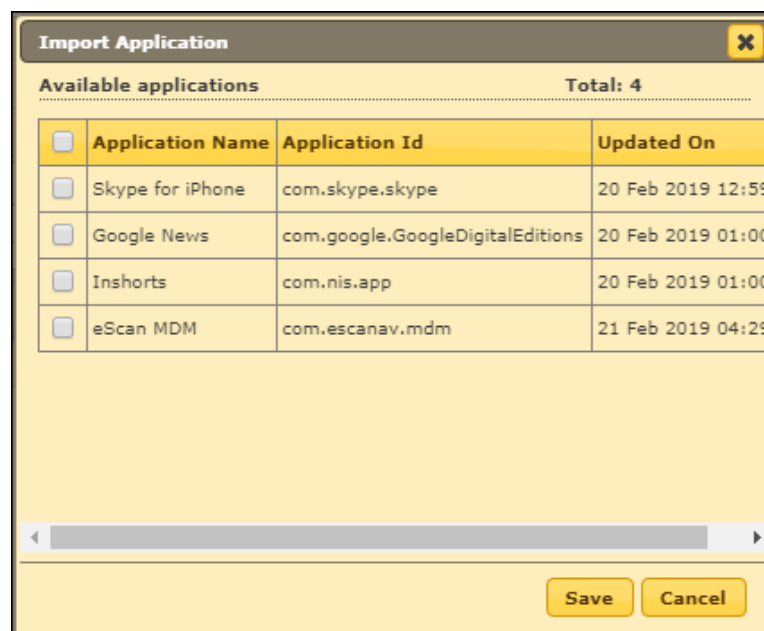
Importing an application

To import applications from the App Store, follow the steps given below:

1. Select **Enable** check box and then click **Import**.



Import Application window appears.



2. Select the application(s) to be installed on users' devices and then click **Save**.
3. The application(s) will be imported.

Deleting an application

Select an application and then click **Delete**.

▼ Required Applications

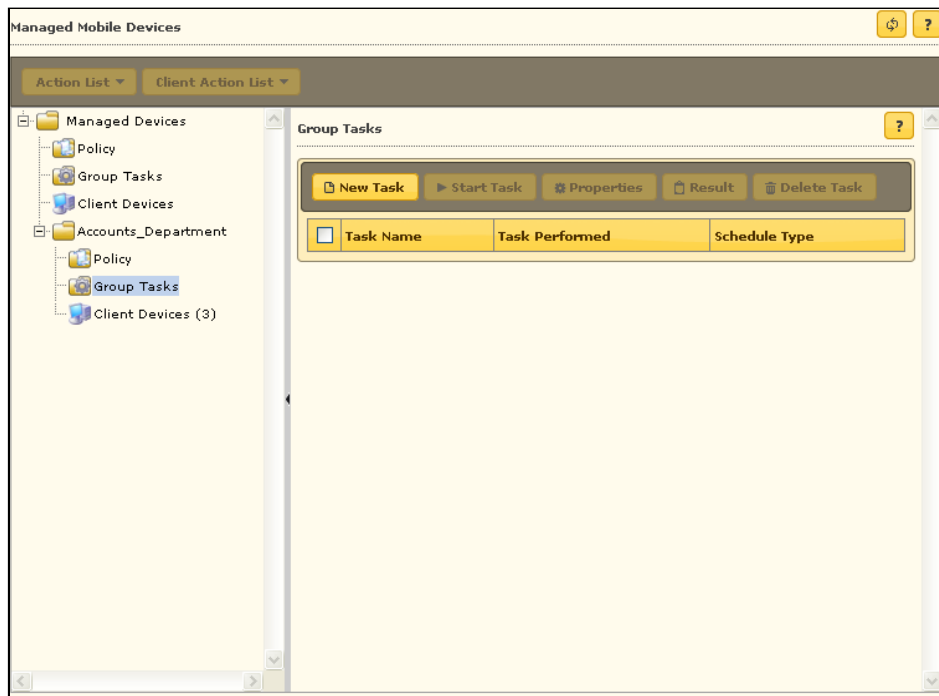
☒ Enable

<input type="checkbox"/>	File Name	Updated On
<input type="checkbox"/>	Skype for iPhone	20 Feb 2019 12:59 PM
<input type="checkbox"/>	Google News	20 Feb 2019 01:00 PM
<input checked="" type="checkbox"/>	Inshorts	20 Feb 2019 01:00 PM
<input type="checkbox"/>	eScan MDM	21 Feb 2019 04:29 PM

The selected application will be deleted.

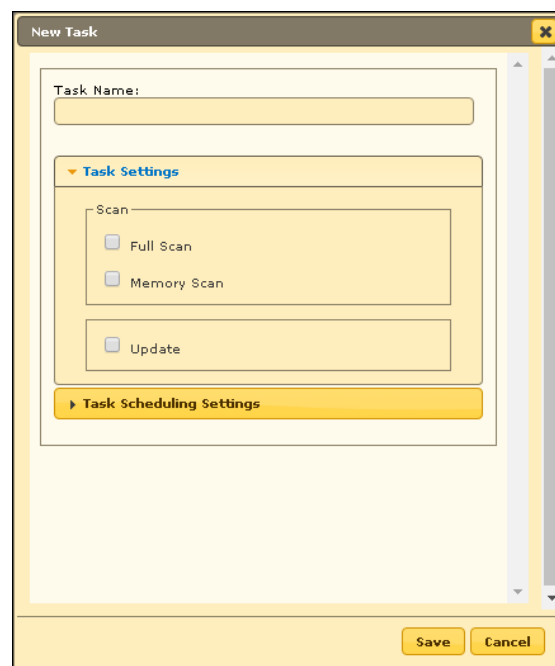
Group Tasks

The Group Tasks option lets you create and schedule tasks for the devices in a group.

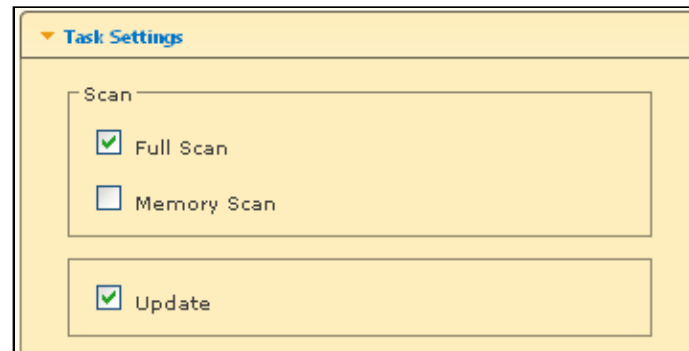


Creating a New Group Task

1. Select a group and then click **Group Tasks > New Task**.
The New Task window appears.



2. Enter a task name.
3. In **Task Settings**, select the scan type to be run on a device. By checking Update, you can also let the application update its virus signature database.



Task Settings

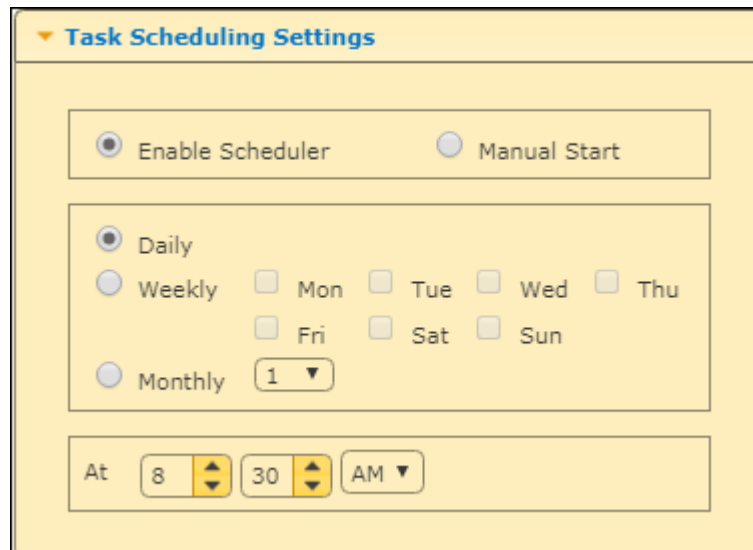
Scan

☒ Full Scan

☐ Memory Scan

☒ Update

4. In **Task Scheduling Settings**, schedule the created task by selecting the appropriate options.



Task Scheduling Settings

☒ Enable Scheduler ☐ Manual Start

☒ Daily

☐ Weekly ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

☐ Monthly 1 ▼

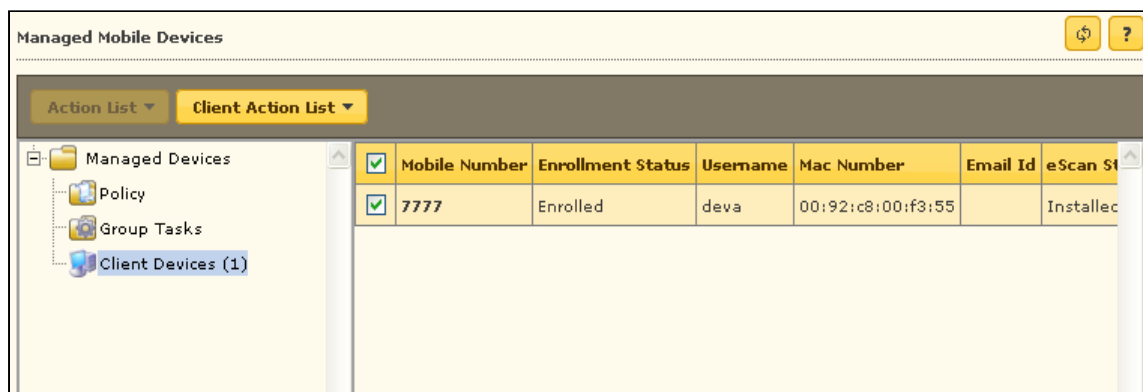
At 8 30 AM ▼

5. Click **Save**.
The task will be created instantly.

Selecting a task enables following options –

Options	Description
Start Task	Click Start Task to run the selected task for the specific group.
Properties	Click Properties to view properties and change settings of the selected task.
Results	Click Results to view detailed results of the selected task.
Delete Task	Click Delete Task to delete the selected task from the list of tasks.

Viewing Managed Client Devices



Installation and Enrollment of Android Device for MDM Group

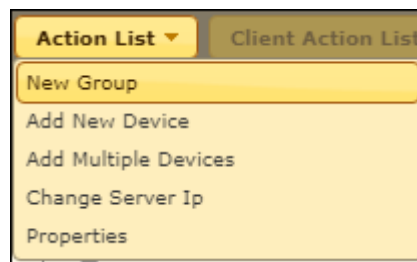
The enrollment procedure for an Android device consists of two main steps:

- Adding a device to the console
- Enrolling the added device

Adding a device to the console

To add a device to the console, perform the following steps:

1. Click **Managed Mobile Devices > Action List > New Group**.



2. Enter a name for the group; select the group type as **MDM** and then click **Save**.

 A screenshot of a 'Create New Group' dialog box. The dialog has a title bar with 'Create New Group' and a close button (X). Inside, there is a text input field labeled 'New Group Name : *'. Below this, there is a 'Group Type : *' section with three radio buttons: 'MDM' (selected), 'COD', and 'BYOD'. At the bottom left, there is a note '* Mandatory Field'. At the bottom right, there are two buttons: 'Save' and 'Cancel'.

3. Select the group.
4. Click **Action List > Add New Device**.

Add New Device window appears.

Add New Device [Group Name: Test Group] [Group Type: MDM]

Mobile Number*

User's name*

Email Id*

OS Type ☒ Android ☐ iOS

* Mandatory Field


QR Code: eScan Enterprise Security

Buttons: Add, Add More, Close


5. Enter the mandatory details, select the appropriate OS Type and then click **Add**.
6. The device will be added to the MDM group as shown in the following screen.

Managed Mobile Devices

Action List Client Action List Total Devices: 1

	Mobile Number	Enrollment Status	Enrollment Date	User's name	Mac Number	Email Id	eScan Status	eScan
<input type="checkbox"/> 	54545454	Not Enrolled	-	karishma	-		Not Installed	-

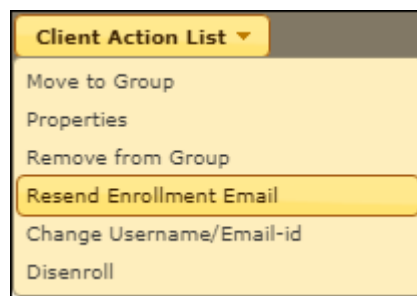
Left Panel: Managed Devices, Policy, Group Tasks, Client Devices, Group_MDM, Policy, Group Tasks, Client Devices (1)

After adding a device to the group, you will see  icon next to the check box. This icon indicates that the added device is not enrolled.

Enrolling the added device

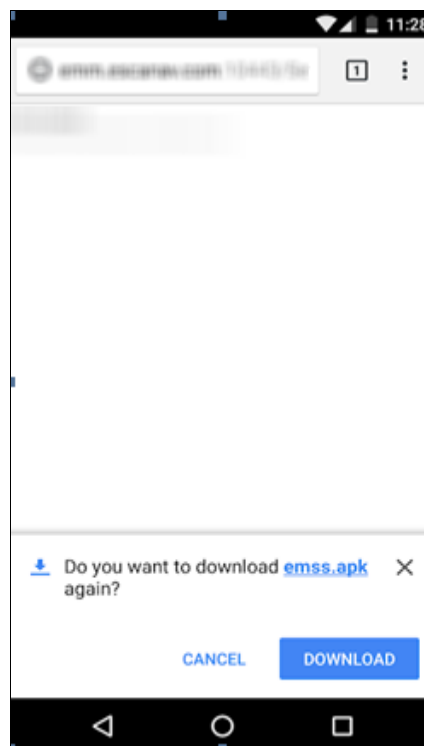
After a device is added to the console, an enrollment email is sent to the specified email ID. This email contains enrollment details and steps to download the MDM application. It also contains the QR code which directly fetches the enrollment details by scanning it from the device.

In case a user did not receive the enrollment email at the time of adding the device, you can resend it. Select the specific device and then click **Client Action List > Resend Enrollment Email**.

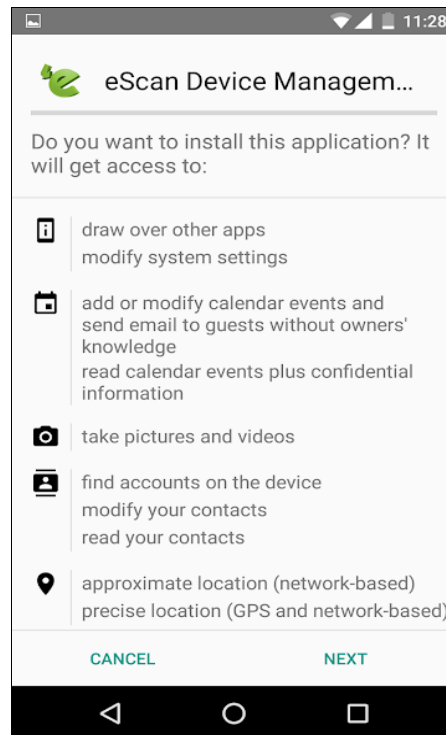


After receiving the enrollment email, the user should perform the following steps:

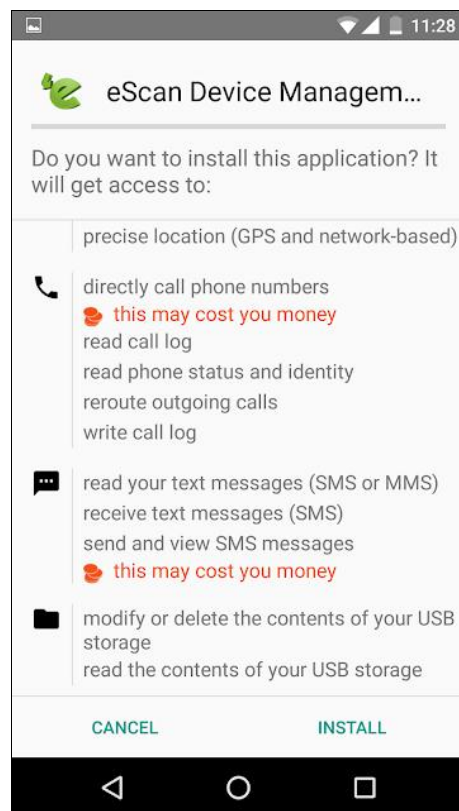
1. Tap the shared URL in the email. A prompt appears asking you to download the eScan MDM application. Tap **DOWNLOAD**.



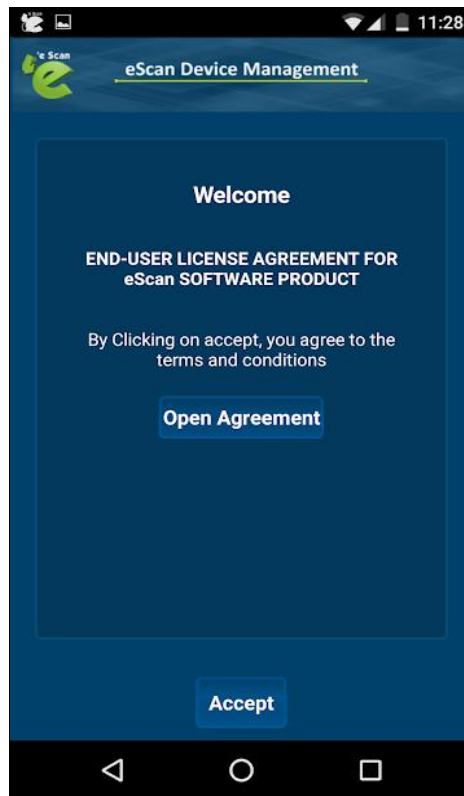
2. Tap the downloaded file and read thoroughly about the permissions asked by the application. To proceed, tap **NEXT**.



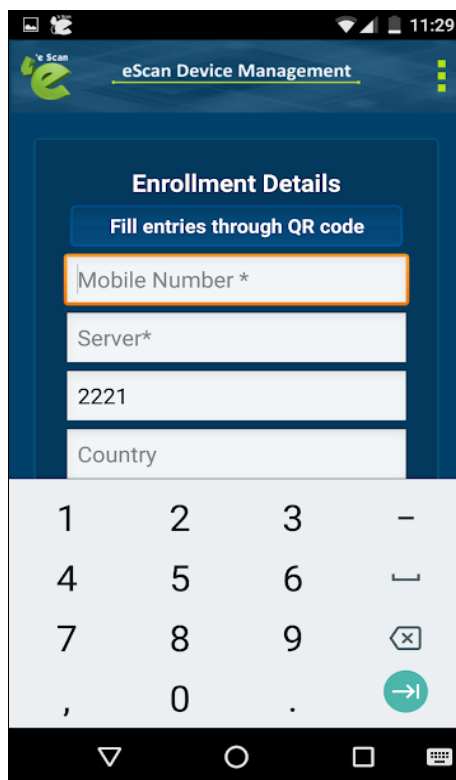
3. After reading the application's access permissions, tap **INSTALL**.



Welcome screen appears.



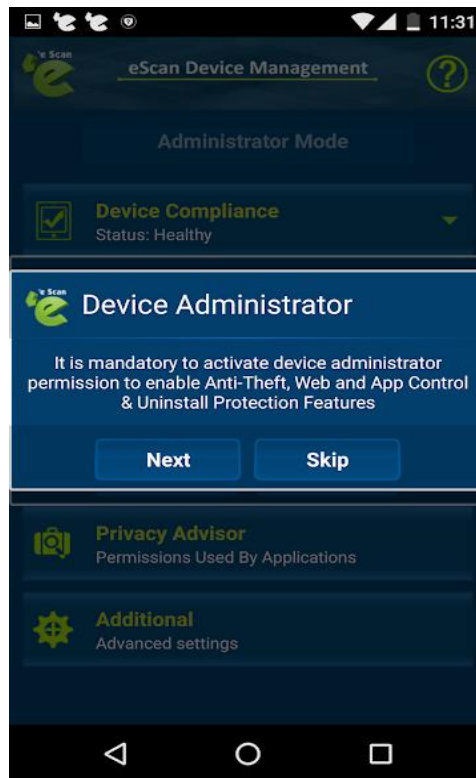
4. Tap **Open Agreement** and read the agreement completely.
5. After reading the agreement, tap **Accept**. Enrollment Details form appears.



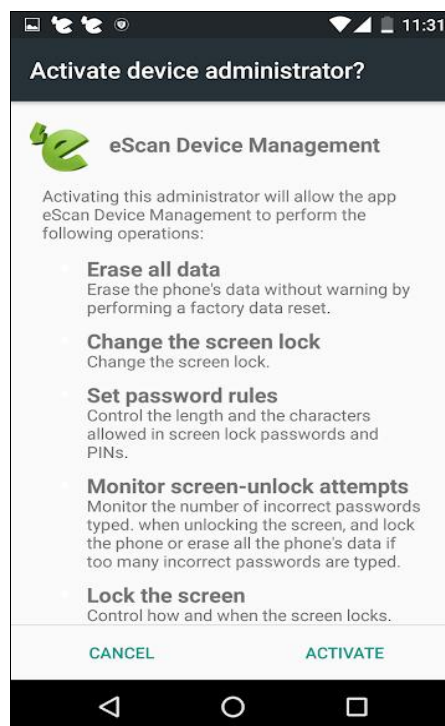
6. Enter the enrollment details mentioned in the email. To fetch the details automatically by scanning QR code, tap **Fill entries through QR Code**. Doing so allows application to access device's camera. Match up the on-screen square with the QR code and hold device steady till the application scans it. After the details are filled, tap **Enroll Device**.

7. Device Enrollment begins. Wait till the device gets enrolled.

Device Administrator prompt appears.

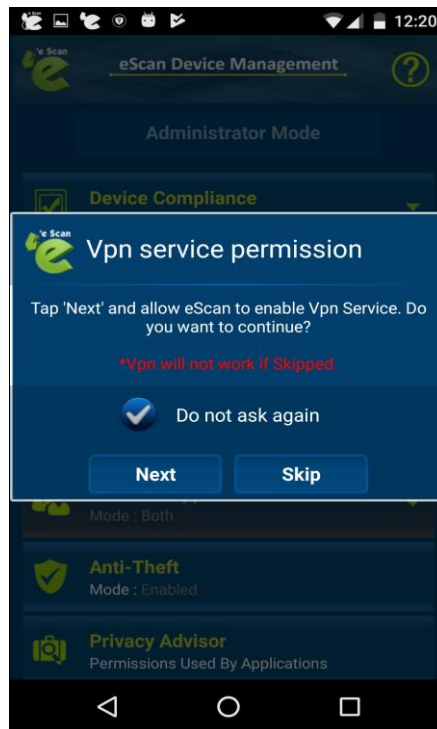


8. It is recommended that you tap **Next**.
Activate Device Administrator prompt appears.



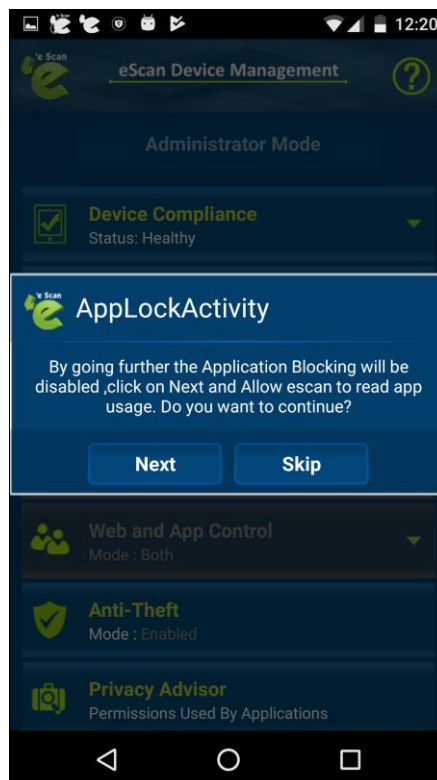
9. Read about the permissions completely and then tap **ACTIVATE**.

VPN Service Permission dialog box appears.

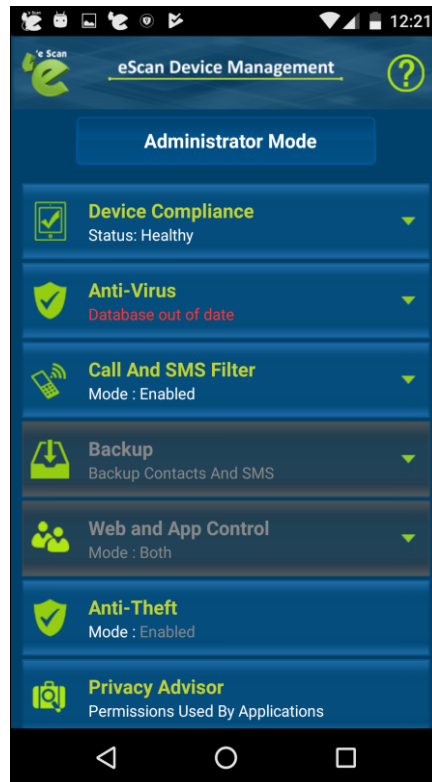


10. It is recommended that you tap **Next** as VPN won't work if you tap **Skip**. This permission is required for the proper functioning of the "App Specific Network Blocking" feature.

App Lock Activity prompt appears.



11. It is recommended that you tap **Next**.
The application enrollment is completed after this step.



Installation and Enrollment of Android Device for COD and BYOD Group

The enrollment procedure for Android devices for COD and BYOD Group

The enrollment procedure for an Android device consists of two main steps:

1. Adding a device to the console
2. Enrolling the added device

Adding a device to the console

To add a device in the eScan Mobility Management (EMM) console, perform the following steps:


1. Click **Managed Mobile Devices > Action List > New Group**.
2. Enter a name for the group and select the group Type as COD to create COD group or BYOD to create BYOD Group.

COD Group Creation

BYOD Group Creation

3. Select a group.
4. Click **Action List > Add New Device**.
Add New Device screen appears.
5. Enter the required details, select the appropriate OS Type and then click **Add**.

The device will be added to the console in the COD or BYOD group.

You can see the device being added in the console. Notice the icon  in the **Mobile Number** column; this indicates that the device is not enrolled.

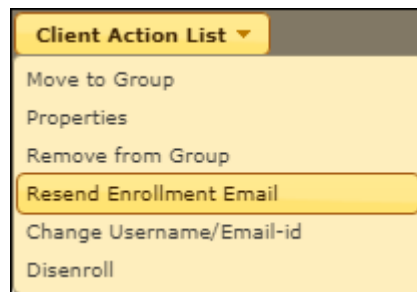
Enrolling the added device

After a device is added to the console, an email containing the enrollment procedure will be sent to the specified email ID. This email contains enrollment details and steps to download MDM application. In addition to this, it also contains the QR code which will directly fetch the enrollment details by scanning it from the device.

In case a user didn't receive the enrollment email at the time of adding the device, you can resend the email by using Resend Enrollment Email option.

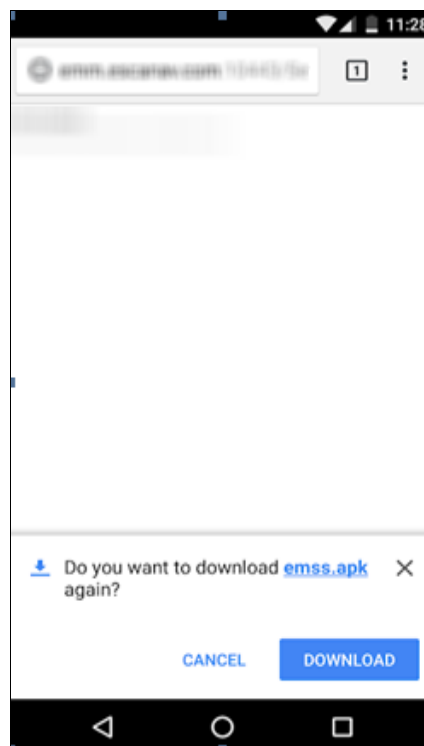
Resend Enrollment email for Device in COD/BYOD Group

Select the specific device and then click **Client Action List** > **Resend Enrollment Email**.

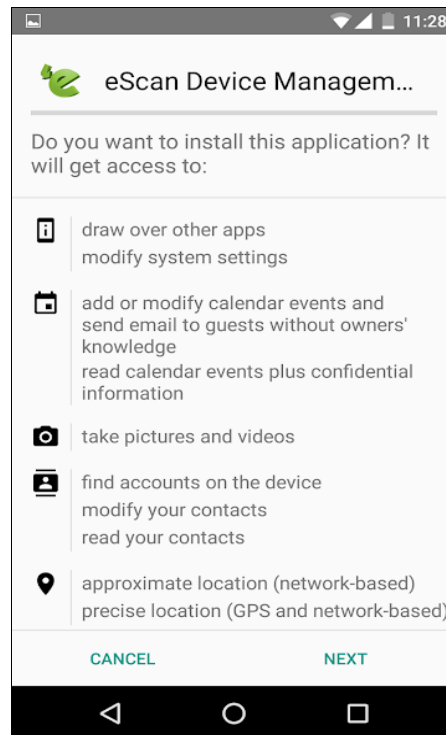


After receiving the enrollment email, the user should perform the following steps:

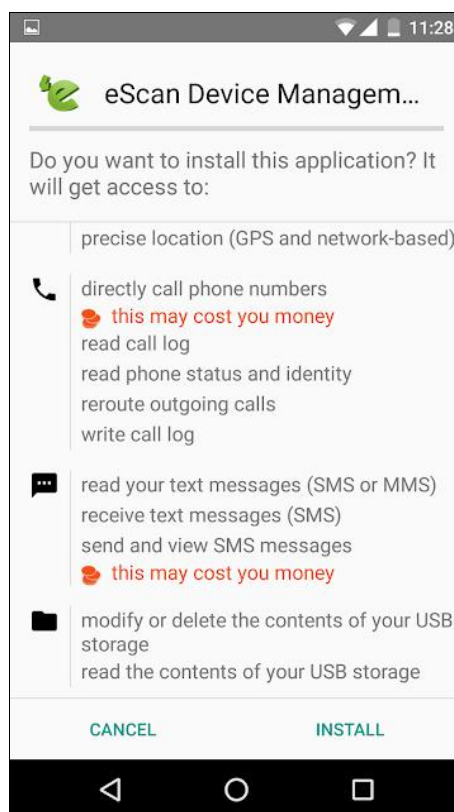
1. Tap the shared URL in the email. A prompt appears asking you to download the eScan MDM application. Tap **DOWNLOAD**.



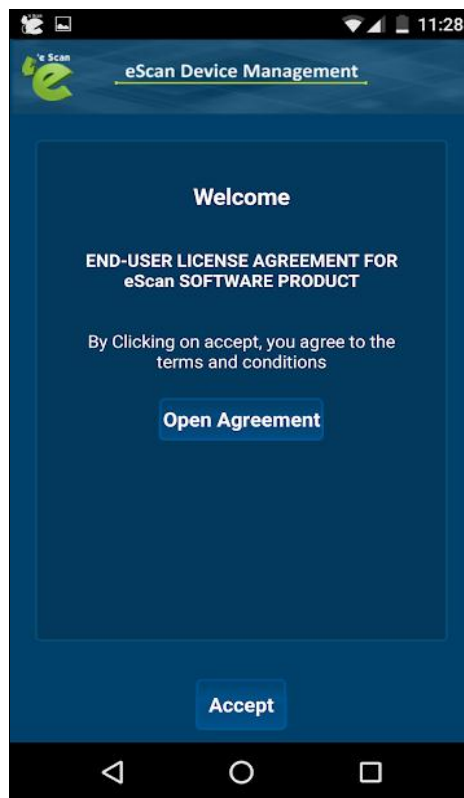
2. Tap the downloaded file and read thoroughly about the permissions asked by the application. Tap **NEXT** to proceed.



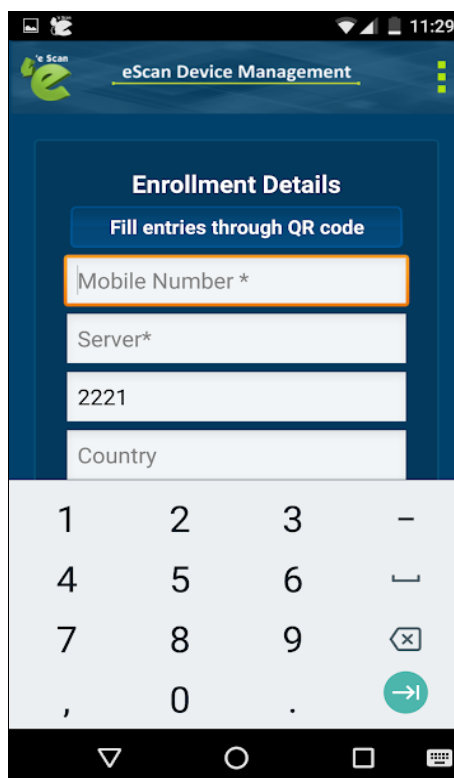
3. The application will get access to your call logs, text messages and USB storage. Tap **INSTALL**.



Welcome screen appears.



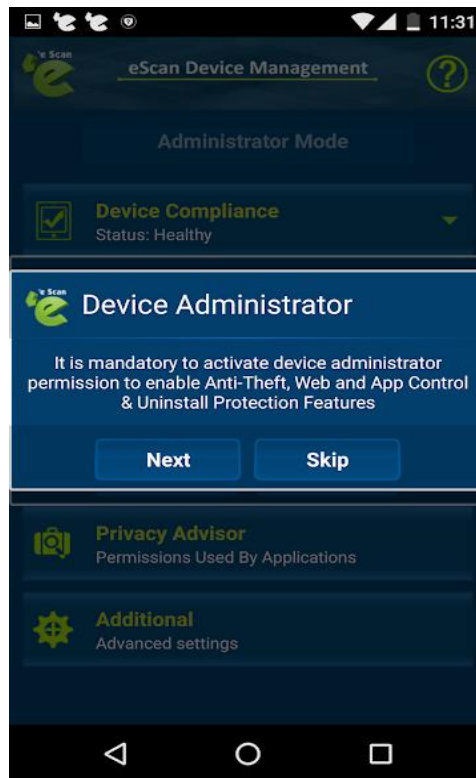
4. Tap **Open Agreement** and read the agreement completely.
5. After reading the agreement completely, tap **Accept**.
Enrollment Details form appears.



6. Enter the details mentioned in the enrollment email or scan the QR code to fetch the details automatically by tapping **Fill entries through QR Code**. Doing so will turn on your device's camera. Match up the on-screen square with the QR code and hold your device steady till the application scans it. The details will be automatically filled. After the details are filled, tap **Enroll Device**.

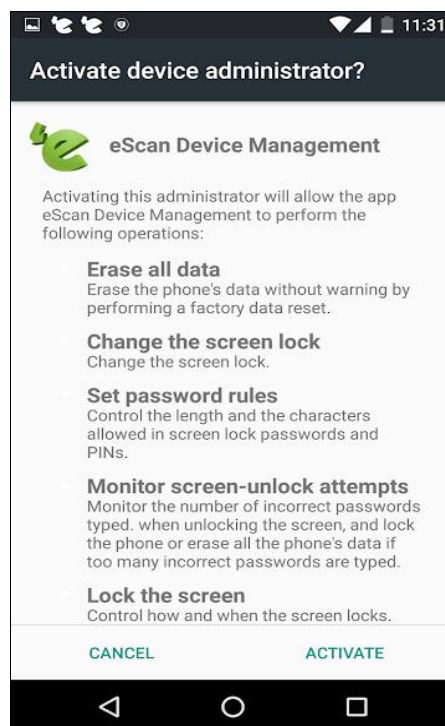
Device Enrollment begins. Wait till the device gets enrolled.

Device Administrator prompt appears.



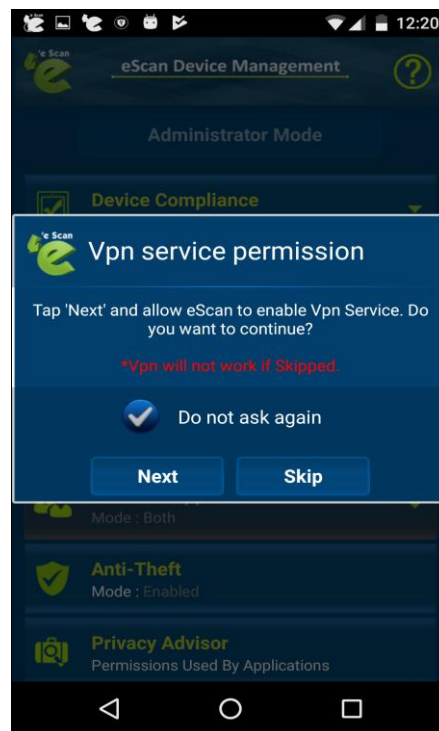
7. It is recommended that you tap **Next**.

Activate Device Administrator prompt appears.



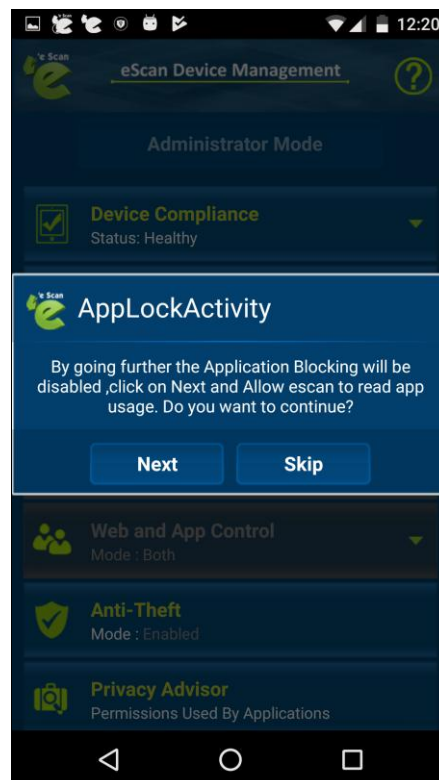
8. Read about the permissions asked by the application completely and then tap **ACTIVATE**.

VPN Service Permission dialog box appears.

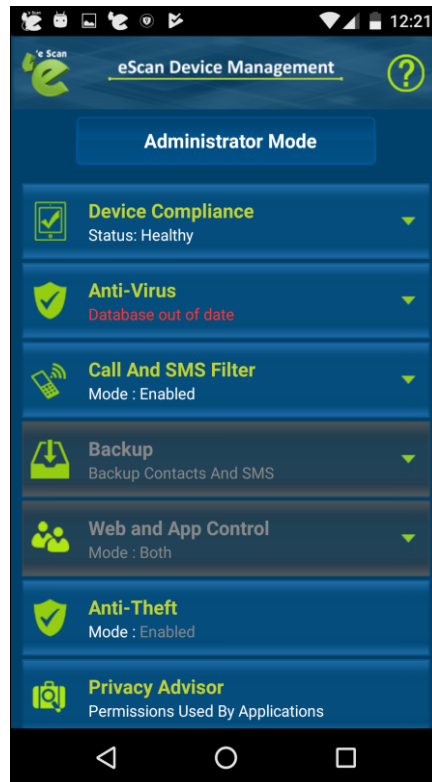


9. It is recommended that you tap **Next** as VPN won't work if you tap **Skip**. This permission is required for the proper functioning of the "App Specific Network Blocking" feature.

App Lock Activity prompt appears.



10. It is recommended that you tap **Next**.
The application enrollment is completed after this step.



After the MDM application is installed, install the Container Application.

Differences between COD and BYOD group

Enterprises empower their employees by allowing the use of mobile devices under Company Owned Devices (COD) policy or by implementing Bring Your Own Device (BYOD) policy for work operations. This enhances employee productivity and allows seamless business operations. It allows organizations to have a comprehensive approach in safeguarding critical applications and enterprise data accessed or residing in mobile devices. It ensures that corporate data is secured from data loss, malware or unauthorized access.

After the MDM application is successfully installed on a device, the administrator can see the device details in the management console. Policy deployment on the managed devices will be carried out under the MDM Category.

Container deployment will provide you with a medium to allow users to use their device for office work within the defined perimeter under BYOD through geo-fencing policy deployment.

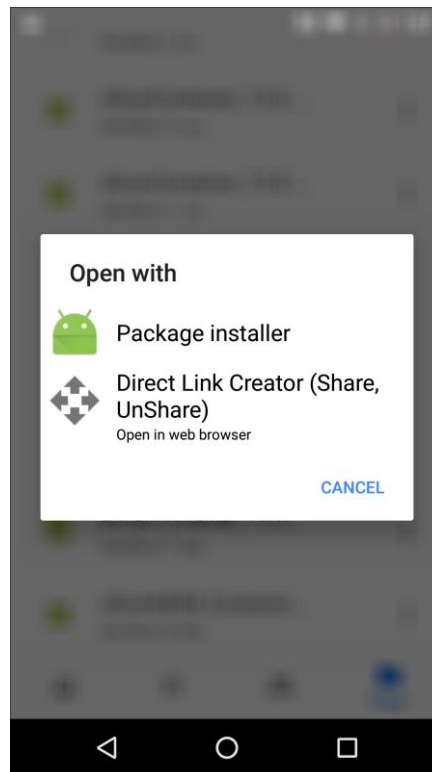
In case the device is provided by the enterprise, you can enroll the device as COD (Company Owned Device) where the security policies for the container will be applicable irrespective of the device location.

Note	<p>By default, whenever an administrator adds mobile device(s), it will be added in the MDM group.</p> <p>The Container application can be accessed only after the eScan MDM application is installed and enrolled on the managed device.</p>
-------------	---

Installing eScan Container app

To install eScan Container app, follow the steps given below:

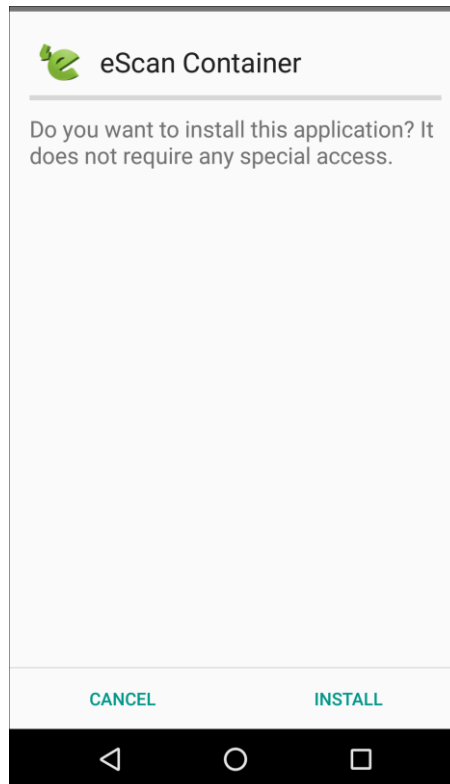
1. Instruct the user to tap the installation notification. Tapping this notification will initiate the download of eScan container application. Tap the downloaded **.apk** file. Following screen appears.



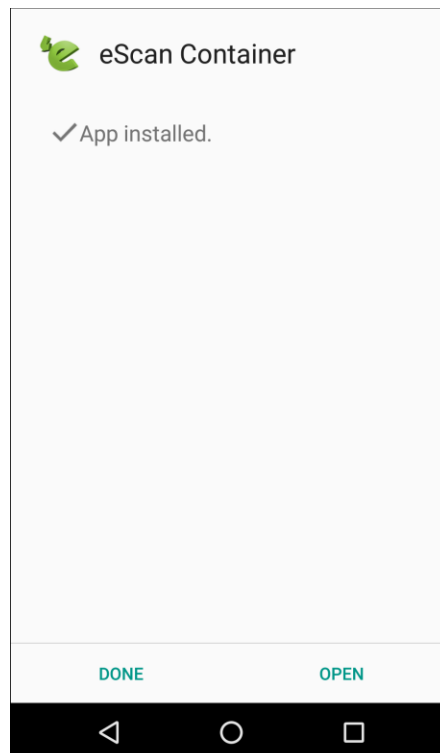
2. Tap **Package Installer**.

Note	It is recommended that a user tap Install and initiate the installation of the Container application.
-------------	---

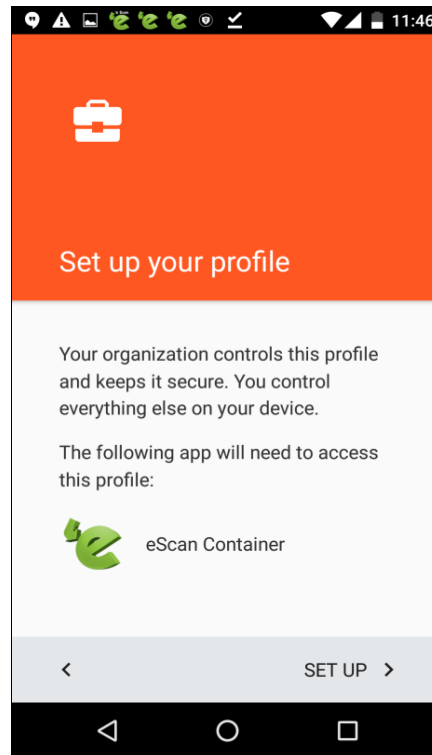
After tapping **INSTALL**, an installation prompt appears.



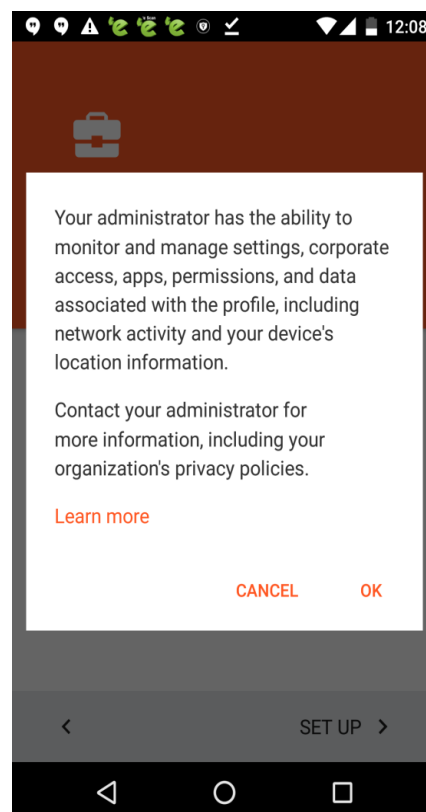
3. Tap **INSTALL**. The Container application will be successfully installed on the user's device.
4. Following screen appears after successful installation. Tap **OPEN**.



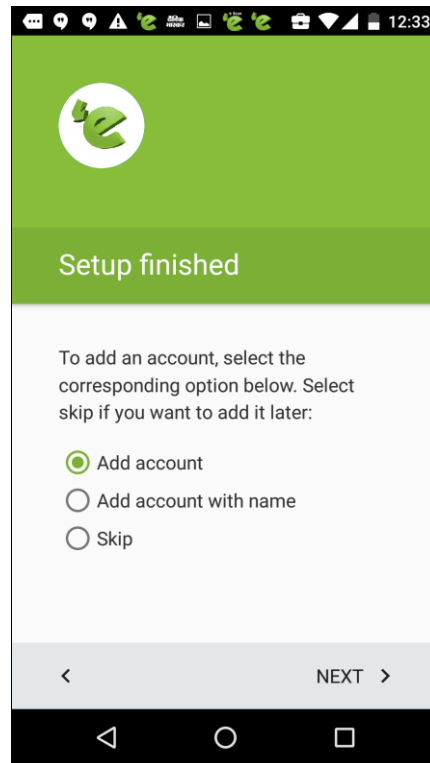
5. Launch the Container application. The application asks you to set up your profile. Tap **SET UP >**.



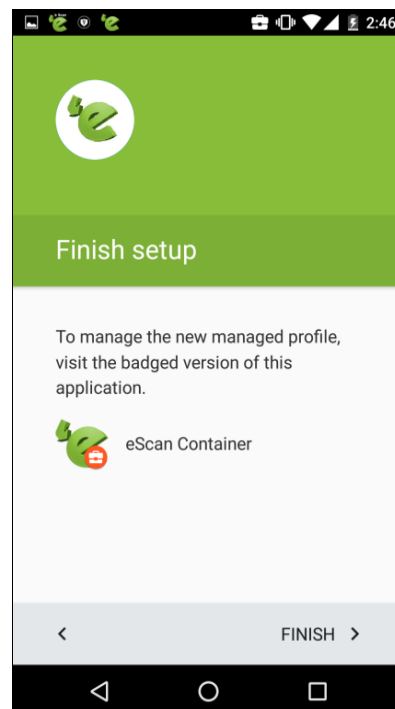
6. A message informing about device information access to administrator is displayed. Tap **OK** to proceed.




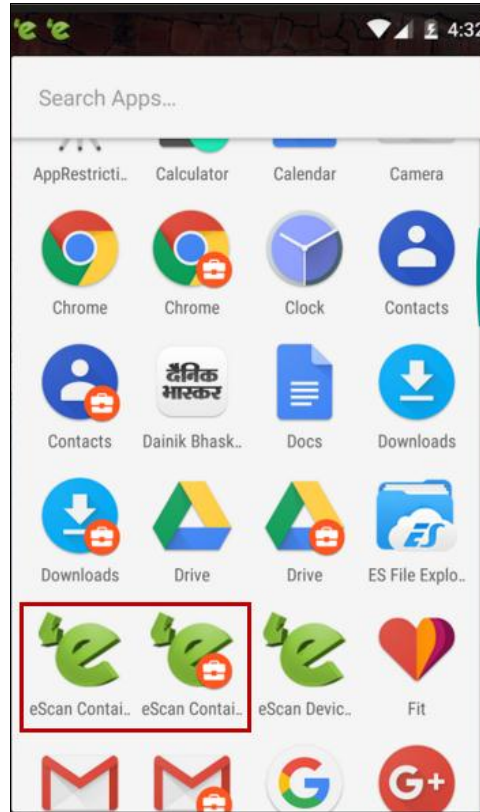
7. To create a work profile, select one of the following three options.
 - **Add Account:** Enter your Gmail account details and tap **ACCEPT**.
 - **Add account with name:** Enter your Gmail account details and name.
 - **Skip:** Select this option to skip entering your login details.
8. After selecting an option, tap **NEXT** >.



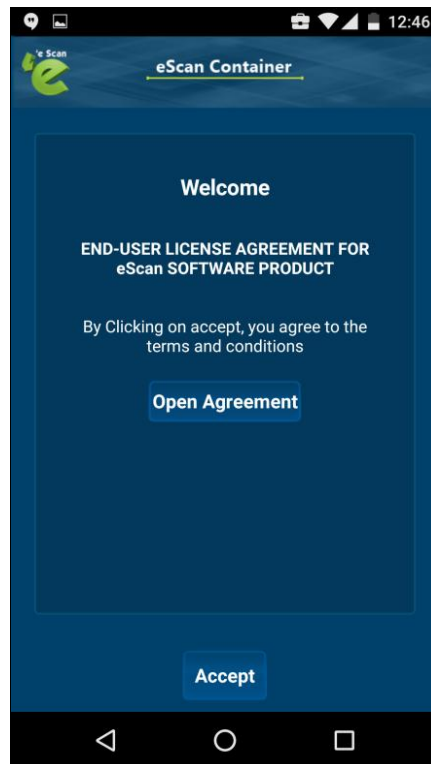
9. Finish setup screen appears, tap **FINISH** >.



10. Launch eScan Container and then tap **ACCEPT**.
11. After the Container app is successfully installed, there will be two eScan containers displayed on the device as follows. Uninstall the eScan Container without the  icon.

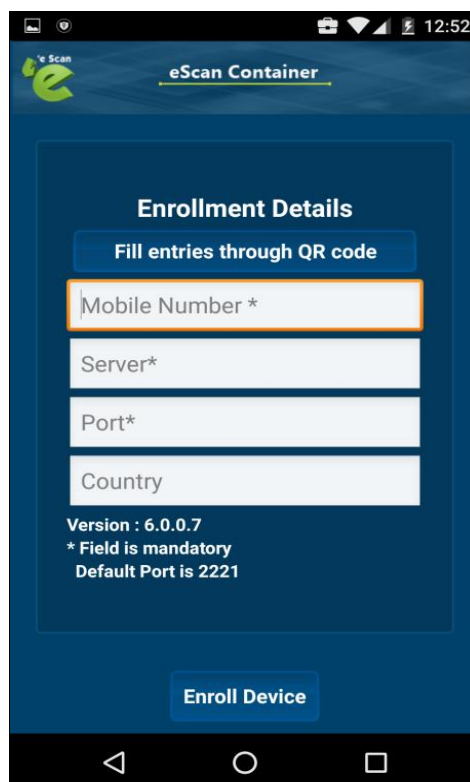


12. Launch eScan Container. Following screen will be displayed.



Enrollment Process for container

Tap **Accept** to proceed with the enrollment process, the following screen will be displayed.



A user can fill up the enrollment details using any of the following procedures:


- Filling enrollment details manually
- Filling enrollment details by scanning QR code

Filling enrollment details manually

1. Open eScan Container app. Enrollment Details form appears.
2. Fill in the required details from the enrollment email.
3. After filling all the details, tap **Enroll container**. The device will be enrolled instantly and a Device Administrator pop-up message appears.
4. Tap **Next** to activate device administrator permission to enable Anti-theft, Parental Control and Uninstall Protection features on the device. You will be forwarded to the information window for activating Device Administrator.
5. Tap **Activate** for activating Device Administrator.

Filling enrollment details by scanning QR Code

1. Open the enrollment email containing QR code on your tablet/computer.
2. Open the eScan Container app. Enrollment Details form appears.
3. Tap **Fill entries through QR Code**. Doing so will turn on your device's camera.
4. Match up the on-screen square with the QR code and hold your device steady till the application scans it. After the successful scan, the enrollment details will be automatically filled.
5. Tap **Enroll Device**.

All the container applications will display a briefcase icon .

Note	The application(s) added to the container by default will vary from device to device.
-------------	---

The administrator can deploy applications and content through **App Store** and **Content Library** modules. The user will be able to access only selected applications and content that the administrator has deployed based on the geo-fencing. The administrator can add applications under the App Store and then deploy the application to the managed device via the Required Applications policy.

The user will receive the following notification:

"Install following app- your administrator requested you to install the following application – (Application name)

Tap **OK** to install the application. Go to the **App Store** under application option on the device, the deployed application will be displayed, click download and install. Tap **Download** to install the app.

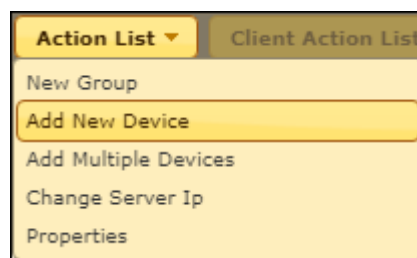
Installation and Enrollment of iOS Device

The enrollment procedure for an iOS device consists of two main steps:

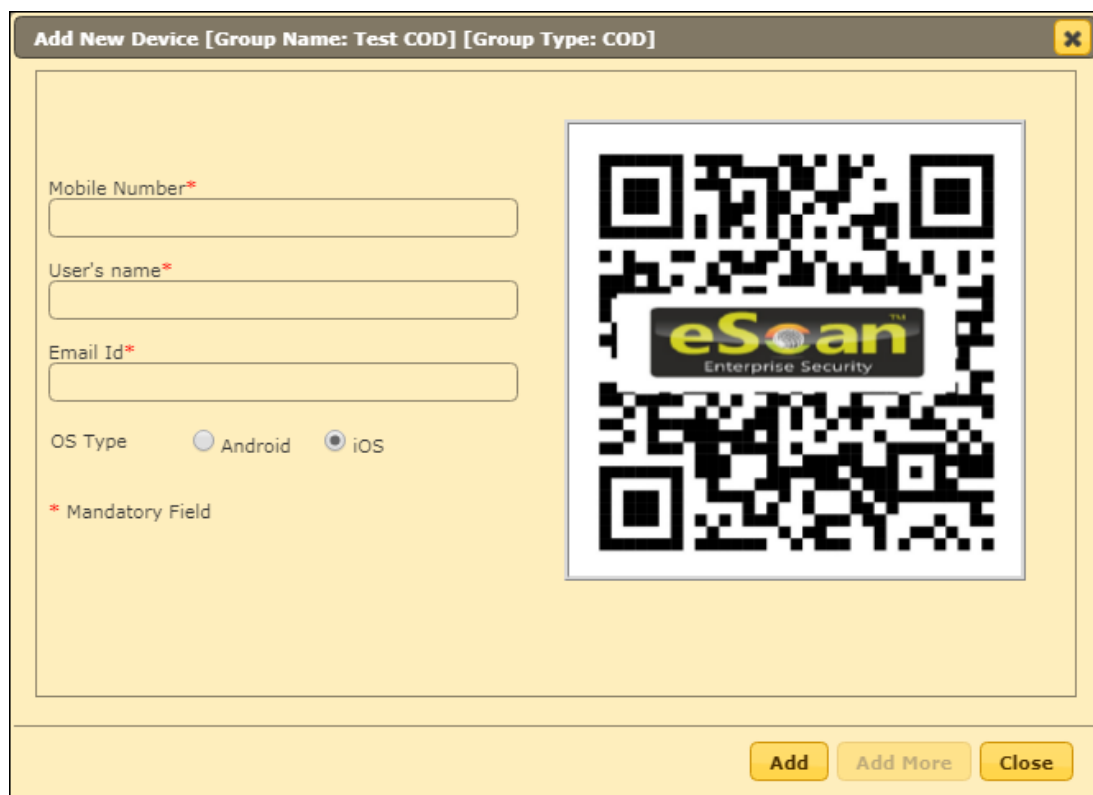
1. Adding a device to the console
2. Enrolling the added device

Adding a device to the console

1. Click **Managed Mobile Devices > Action List > Add New Device**.



Add New Device window appears.

A screenshot of the 'Add New Device' window in the eScan console. The window title is 'Add New Device [Group Name: Test COD] [Group Type: COD]'. It contains several input fields: 'Mobile Number*' (with an asterisk indicating it's mandatory), 'User's name*', and 'Email Id*'. Below these is the 'OS Type' section with radio buttons for 'Android' and 'iOS' (which is selected). A legend at the bottom left states '* Mandatory Field'. On the right side of the window is a large QR code with the eScan logo in the center. At the bottom right, there are three buttons: 'Add', 'Add More', and 'Close'.

2. Enter the details, select the OS Type as **iOS** and then click **Add**.

- After clicking **Add**, the device will be added to the console as shown in the following screen.

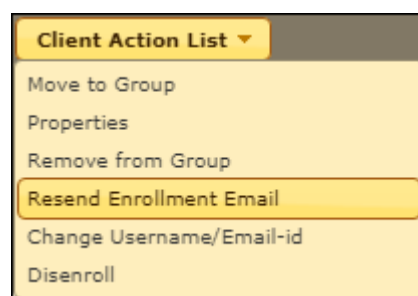
Mobile Number	Enrollment Status	Enrollment Date	User's name	Mac Number	Email Id
009198	Enrolled	08 May 2018 03:19 PM		30:82:11:11:11:11	
009198	Enrolled	05 May 2018 06:48 PM		7C:11:11:11:11:11	
0091	Not Enrolled	-	User 1	-	

- Notice the icon  in the **Mobile Number** column; it denotes that the device is not enrolled.

Enrolling the added device

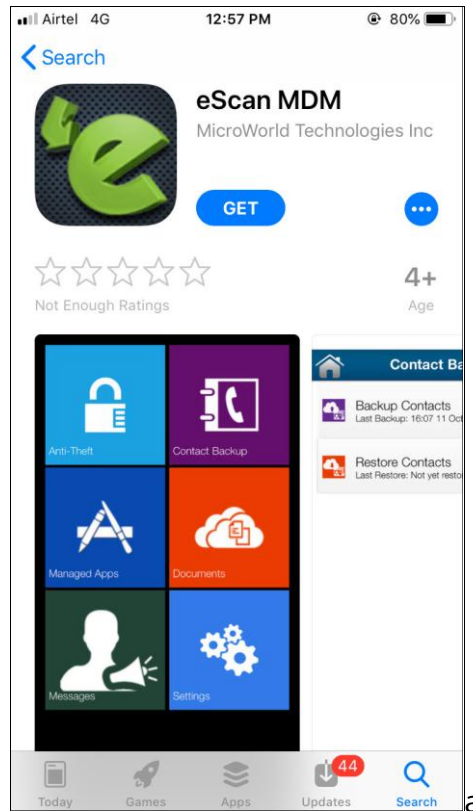
After a device is added to the console, an email containing the enrollment procedure will be sent to the specified email ID. This email will contain steps to download MDM application and details such as Mobile No, Server, and Port. In addition to this, it will also contain the QR code that will fetch the above mentioned details by scanning it from the device. In case a user didn't receive the enrollment email at the time of adding the device, you can resend the enrollment email.

Select the specific device and then click **Client Action List > Resend Enrollment Email**.



After you've received the enrollment email, perform the following steps:

1. Download and install the **eScan MDM** application from the App Store.

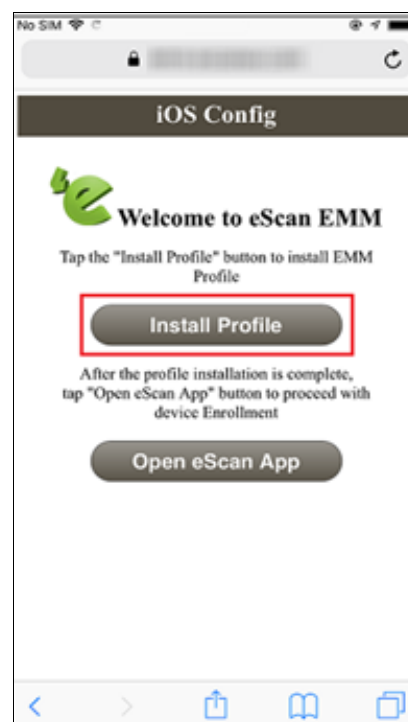


2. Read the eScan Agreement completely and then tap **Accept**.



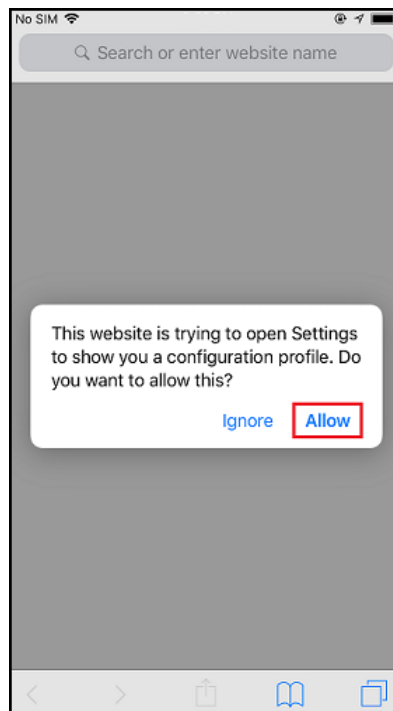
3. Launch the eScan MDM application and enter the details mentioned in the enrollment email, or fill in the details automatically via QR code by tapping **Read QR Code**. Doing so will turn on your device's camera. Match up the on-screen square with the QR code and hold your device steady till the application scans it. After the successful scan, the details will be automatically filled.

4. After the enrollment details are filled, tap **Enroll Device**. iOS Config screen appears.



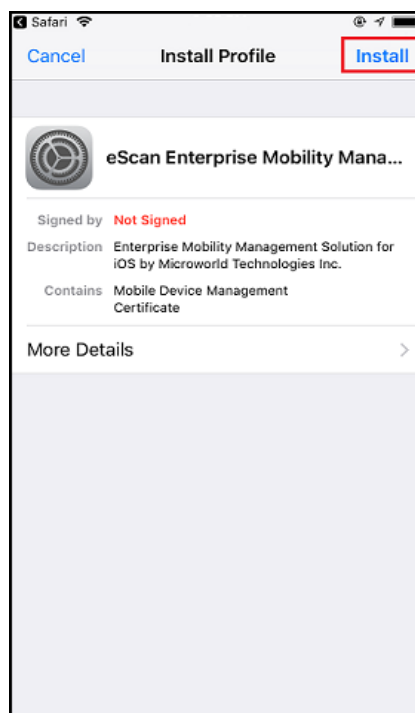
5. Tap **Install Profile**.

The application attempts to access your device's Settings. The following dialog box appears asking confirmation.



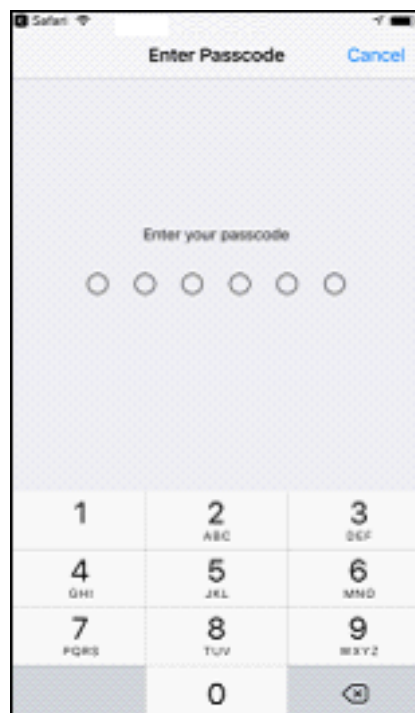
6. Tap **Allow**.

Install Profile settings appear.

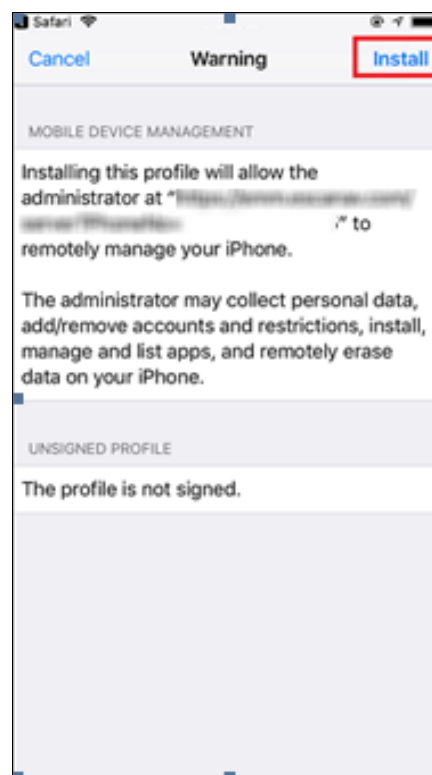


7. Tap **Install**.

Enter Passcode screen appears.

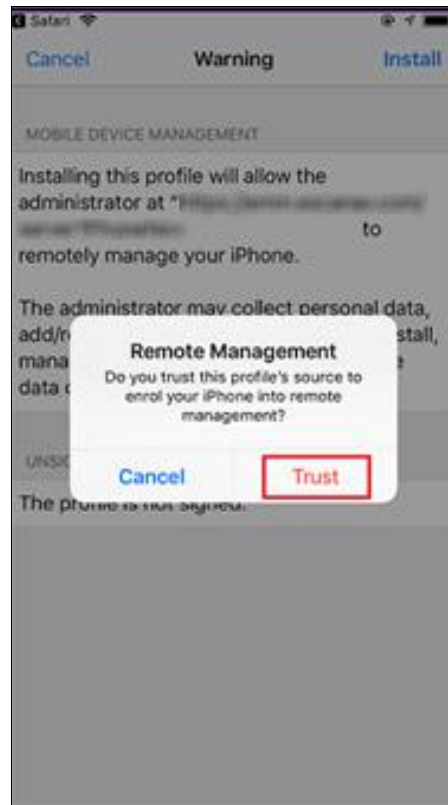


8. Enter the device's passcode to proceed with the installation.
After entering the passcode, Warning message appears stating that the administrator will be able to remotely manage your device.

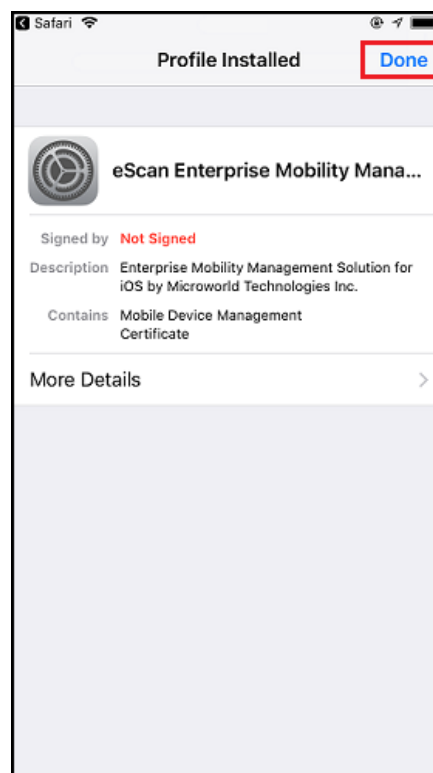


9. To proceed with the installation, tap Install.

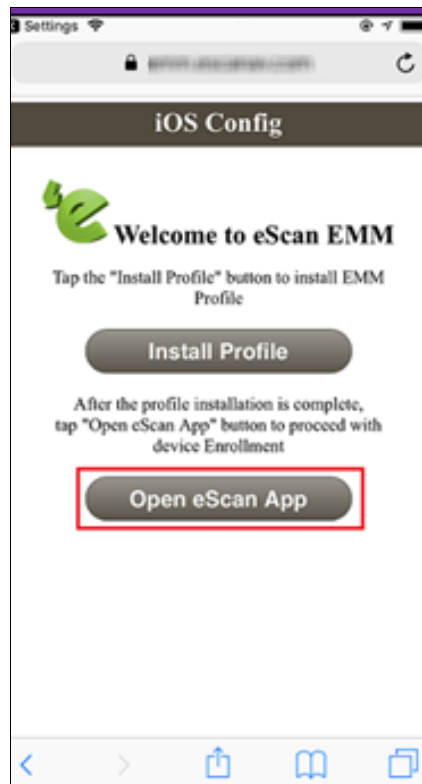
A pop-up message appears asking confirmation for remote management of your device.



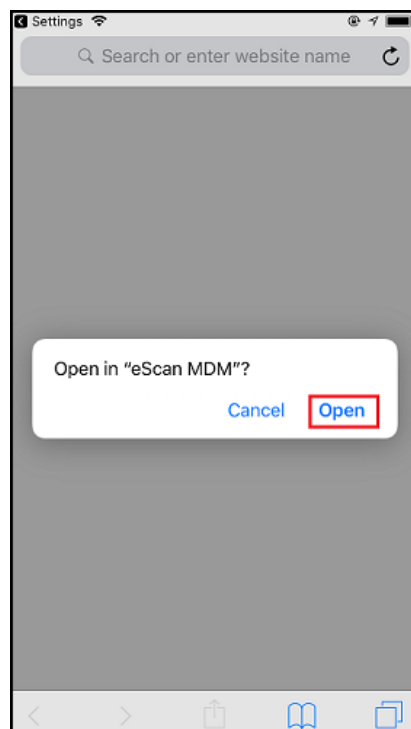
10. Tap **Trust**. The MDM profile will be installed on your device. To exit the installation process, tap **Done**.



The iOS Config screen appears.

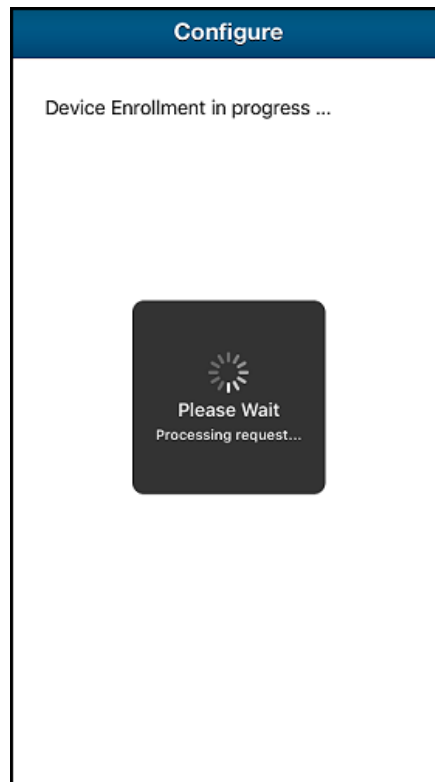


11. Tap **Open eScan App**.
A pop-up appears.



12. Tap **Open**.

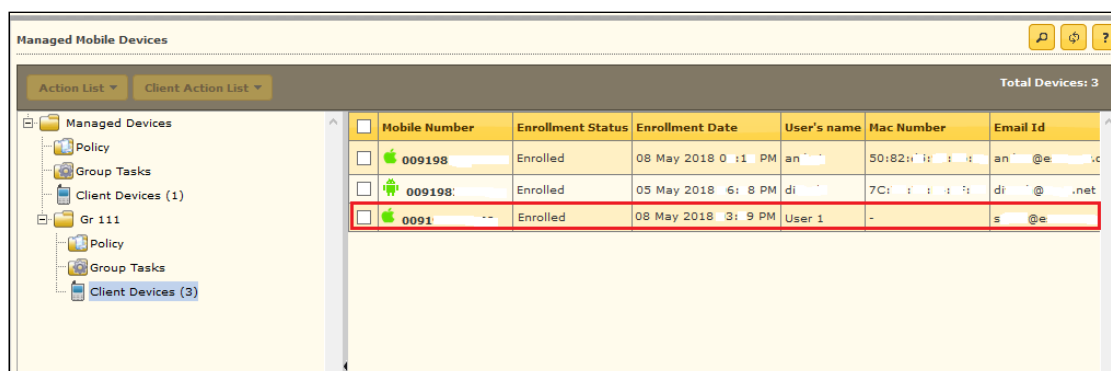
Configure screen appears stating that the Device Enrollment is in progress.



After the device enrollment is complete, following screen appears.



In the **eScan Mobility Management (EMM)** console, you can see the icon change to green from red and the enrollment status change to **Enrolled** from **Not Enrolled**.



Policy comparison of MDM, COD and BYOD Group Types

Policies for MDM	Policies for COD	Policies for BYOD
Anti-Virus Policy	Anti-Virus Policy	Anti-Virus Policy
Call & SMS Filter Policy	Call & SMS Filter Policy	Call & SMS Filter Policy
Web and Application Control	Web and Application Control	Web and Application Control
App Specific Network Blocking	App Specific Network Blocking	App Specific Network Blocking
Anti-Theft Policy	Anti-Theft Policy	Anti-Theft Policy
Additional Settings Policy	Additional Settings Policy	Additional Settings Policy
Password Policy	Password Policy	Password Policy
Device Oriented Policy	Device Oriented Policy	Device Oriented Policy
Required Applications Policy	Required Applications Policy	Required Applications Policy
Wi-Fi Settings Policy	Wi-Fi Settings Policy	Wi-Fi Settings Policy
Scheduled Backup (Contacts & SMS)	Scheduled Backup (Contacts & SMS)	Scheduled Backup (Contacts & SMS)
Content Library Policy	Content Library Policy	Content Library Policy
	Restriction Policy	Restriction Policy
		Location Fence

Note	Policies sporting icon are applicable for container version of the application for BYOD and COD groups.
	Policies sporting icon are also applicable for MDM group.
	Policies not representing any icons are applicable for the container version as well as MDM version for BYOD and COD group types.

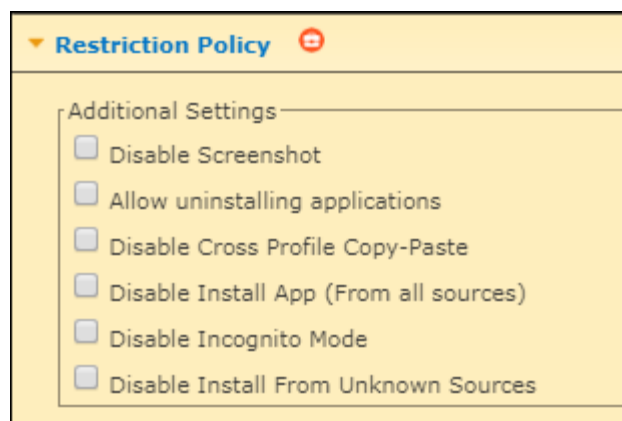
For detailed policy description for following policies, refer [Policies section under Managed Mobile Device](#).

- Anti-Virus Policy
- Call & SMS Filter Policy
- Web and Application Control
- App specific network blocking
- Anti-Theft Policy
- Additional Settings Policy
- Password Policy
- Device Oriented Policy
- Required Applications Policy
- Wi-Fi Settings Policy
- Scheduled Backup (Contacts & SMS)
- Content Library Policy

For more on **Additional Features** Policy for COD and **Location Fence** Policy for BYOD group refer below.

Restriction Policy

The Restriction Policy lets you apply certain restrictions on a device that prevents the device user from getting access to few device features.



Disable Screenshot - Select this check box to disable a device from taking a screenshot.

Allow uninstalling applications - Select this check box to allow a user to uninstall applications.

Disable Cross Profile Copy-Paste - Select this check box to disable cross profile copy-paste on a device.

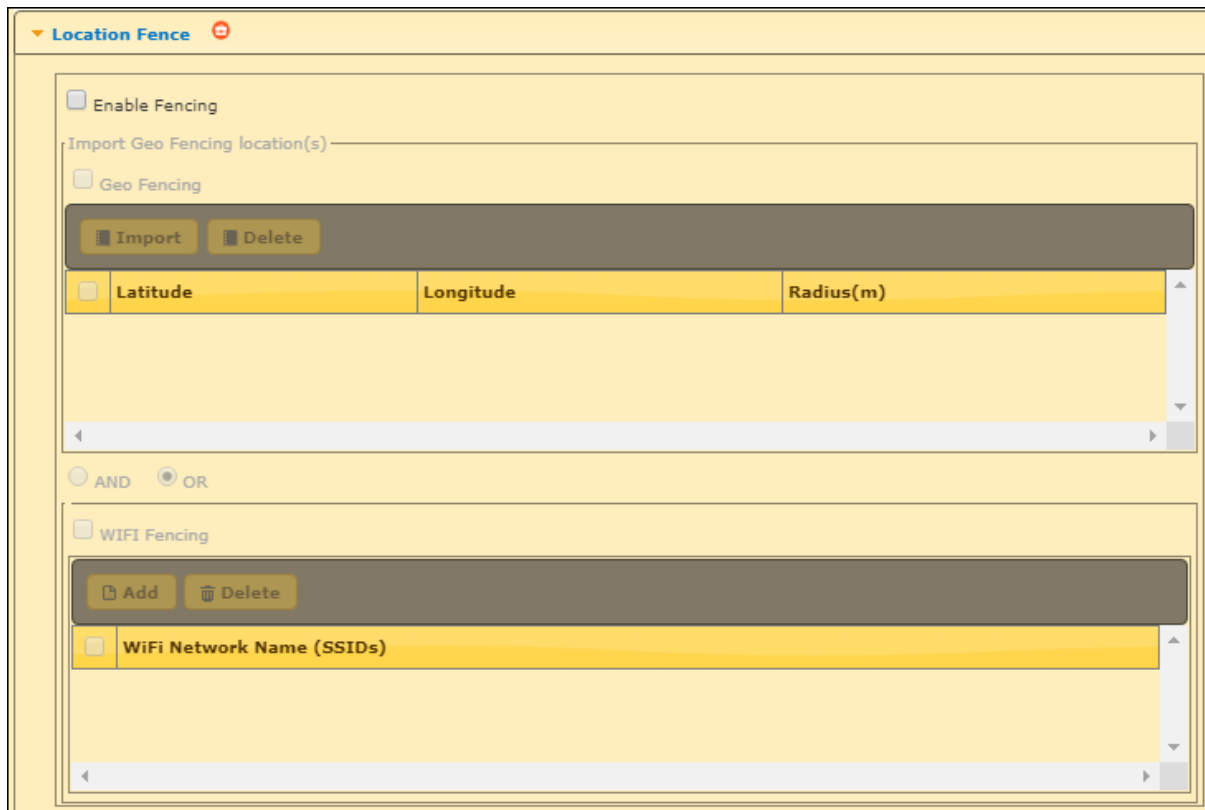
Disable Install App (From all sources) - Select this check box to disable application installations from all sources on a device.

Disable Incognito Mode - Select this check box to disable web browsing in incognito mode on a device.

Disable Install From Unknown Sources - Select this check box to disable application installation from unknown sources on a device.

Location Fence

Under Location Fence policy, restrictions as per the policy will be applied only if the device is in the Geo/Wi-Fi location. If the device is out of the Geo/Wi-Fi location, there will be no restrictions on the device.



Location Fence ⓘ

☐ Enable Fencing

Import Geo Fencing location(s) _____

☐ Geo Fencing

Import Delete

Latitude	Longitude	Radius(m)

AND OR

☐ WIFI Fencing

Add Delete

WiFi Network Name (SSIDs) _____

To use Location Fence feature, check **Enable Fencing** check box.

Select the appropriate type of fencing you want to use for devices.

To use **Geo Fencing**, it is necessary that a default location must be set first. To learn more about fencing location, [click here](#).

Geo fencing: To enable Geo Fencing, check this check box.

1. Click **Import**.

Fencing Location(s) window appears.

Fencing Location(s)

Select Geo Fencing Locations(s)

<input type="checkbox"/>	Custom Address	Latitude	Longitude	Radius(m)	Address
<input type="checkbox"/>	Mumbai Office	19.12000	72.87357	200	80, Rd Number 15, Marol MIDC Industry Estate, Andheri East, Mumbai, Maharashtra 400069, India

Save

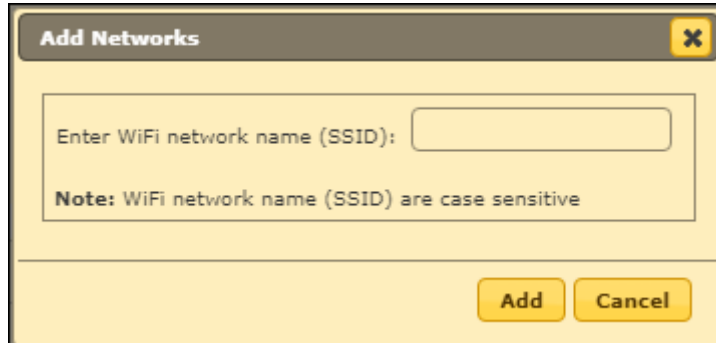
Cancel

2. Select location to import location details and then click **Save**.

Wi-Fi Fencing: To enable Wi-Fi Fencing, check Wi-Fi Fencing check box.

1. Click **Add**.

Add Networks window appears.

A screenshot of a software dialog box titled "Add Networks". The dialog has a yellow background and a dark grey title bar with a close button (X) in the top right corner. Inside the dialog, there is a text input field preceded by the label "Enter WiFi network name (SSID):". Below the input field, a note states "Note: WiFi network name (SSID) are case sensitive". At the bottom right of the dialog, there are two buttons: "Add" and "Cancel".

2. Enter Wi-Fi network name (SSID) and then click **Add**.

Select AND/OR option as per requirement.

In case you want to Import Geo Fencing location(s) and add Wi-Fi Fencing at the same time.

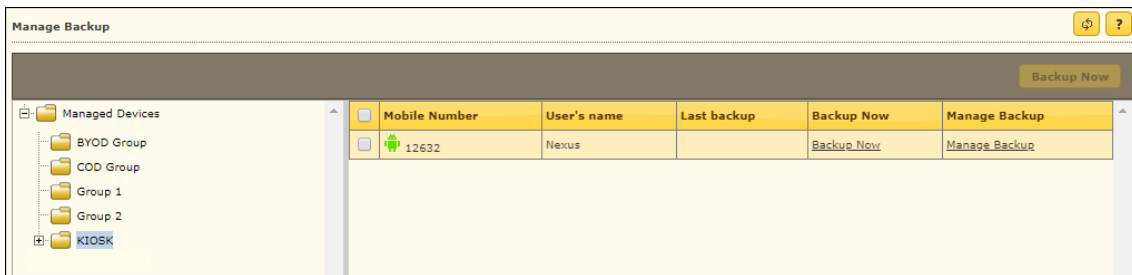
Select the **AND** option otherwise select the **OR** option.

Manage Backup

Manage Backup module lets you take a backup of SMS and Contacts saved on the managed devices to the server and restore it on the device whenever required.

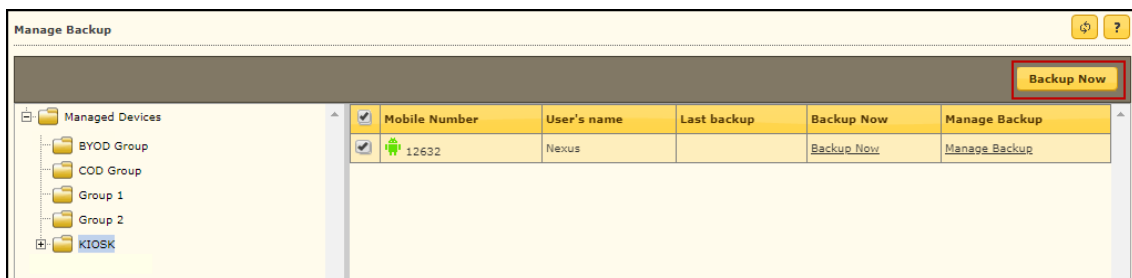
Clicking a group displays all the devices it contains and their details such as **Mobile Number**, **User's Name**, **Last Backup**, **Backup Now** and **Manage Backup**.

Clicking on a device shows information about its last **SMS Backup**, **Contacts Backup** and **Device Status**.

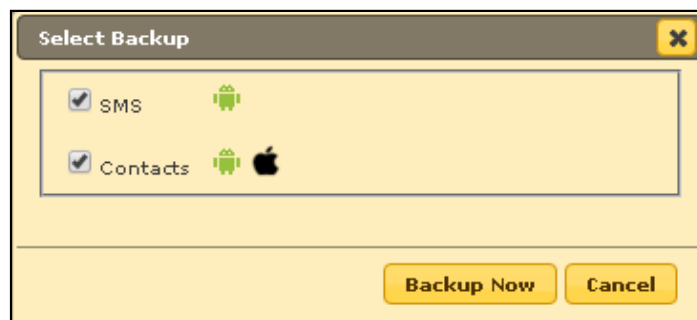


Taking a backup from devices to the server

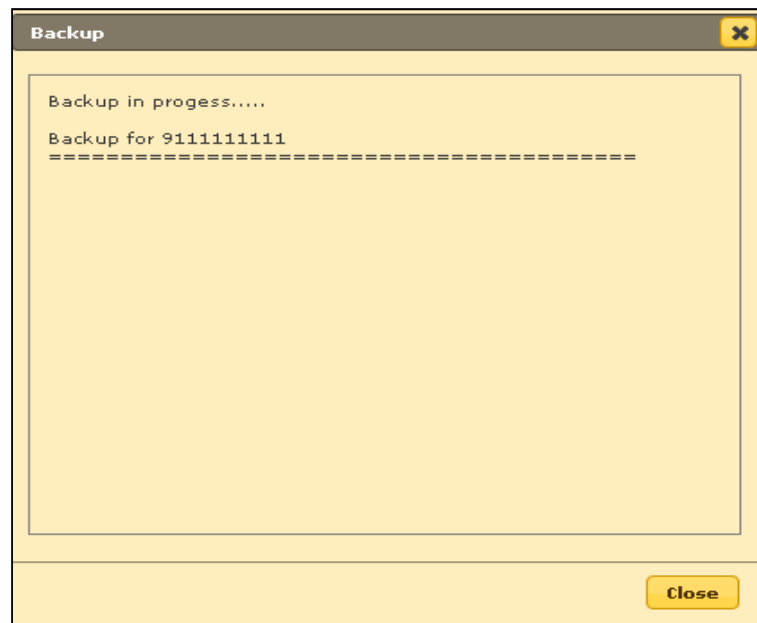
1. Click **Manage Backup** and select the specific group or devices of you wish to take a backup to the MDM server. Selecting a device will enable **Backup Now** option.



2. Select the desired backup and then click **Backup Now**.

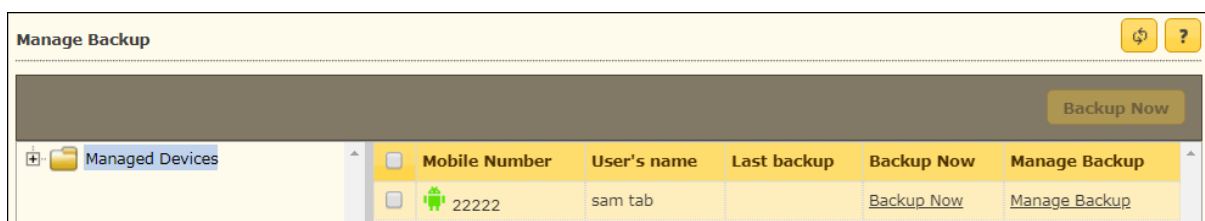


Backup window appears displaying the progress.

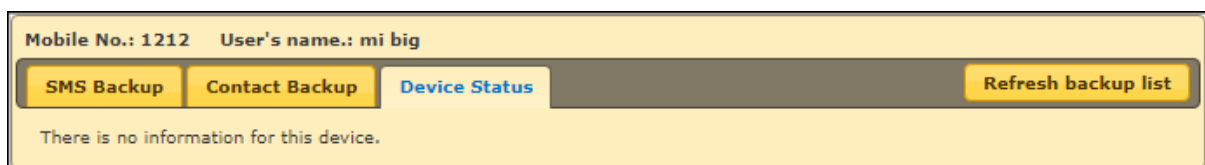


The report displays following fields.

Mobile Number, User's name, Last backup, Backup Now, Manage Backup.



Manage Backup: Clicking Manage Backup link displays following screen.



It displays the **SMS Backup**, **Contact Backup**, **Device Status** and **Refresh backup list**.

SMS Backup: It displays the SMS backup status for the selected device.

Contact Backup: It displays the contact backup status for the selected device.

Device Status: It displays the following fields.

Date-Time and Description

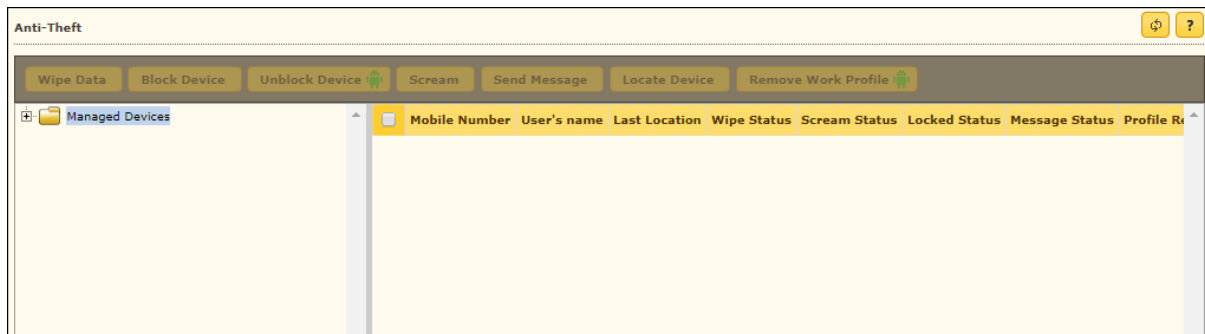
Date-Time displays the date and time when the Contacts and SMS backup was requested by the server.

Description displays whether the Contacts or SMS backup was requested from the server.

Clicking **Refresh backup list** refreshes the backup list.

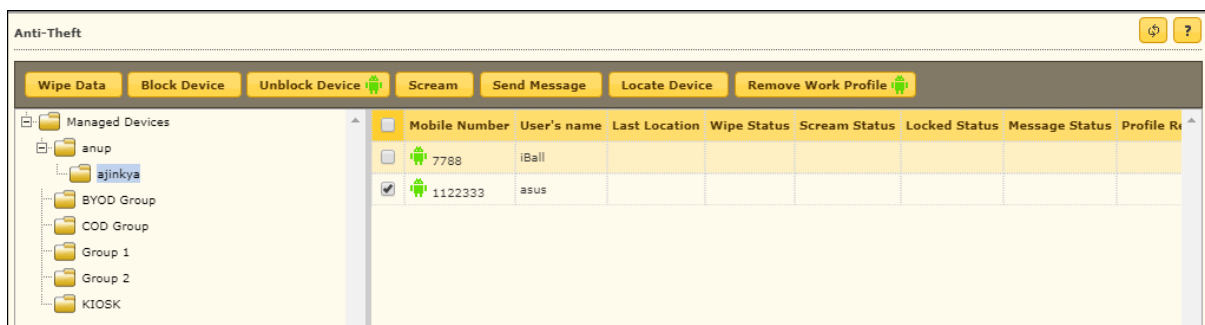
Anti-Theft

The Anti-Theft module lets you remotely locate and lock a device. This module also lets you wipe data available on a device.



Selecting an added device enables following tabs:

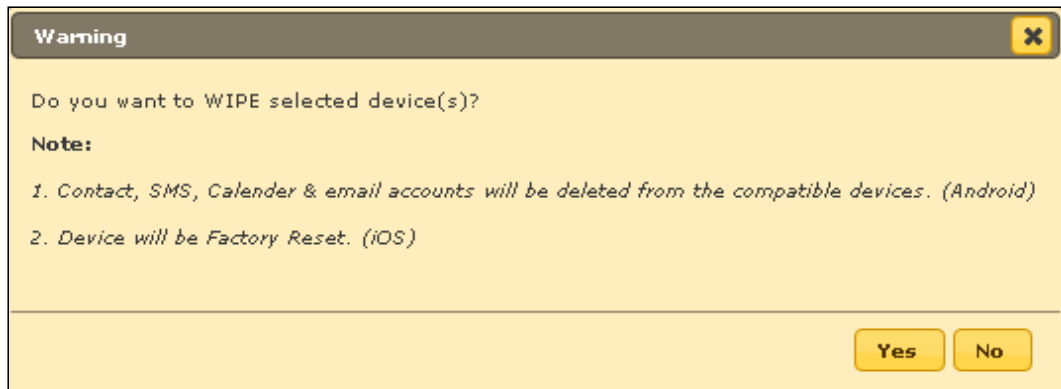
- Wipe Data
- Block Device
- Unblock Device (Android)
- Scream
- Send Message
- Locate Device
- Remove Work Profile (Android)



Wipe Data

With this option you can delete data from the device if it gets lost or stolen. To wipe the data, select the specific device and then click **Wipe Data**.

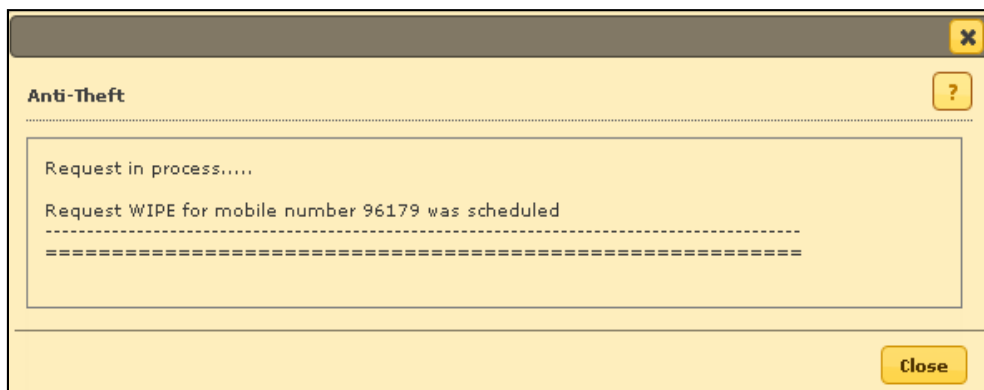
A confirmation message appears.



Wipe Data option will delete Contacts, SMS, Calendar & email accounts from an **Android device** whereas, an **iOS device** will be factory reset.

Click **Yes** to confirm data wipe on a device.

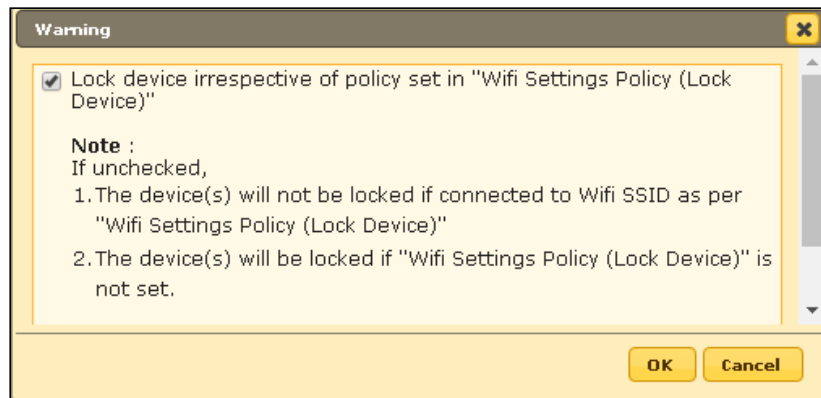
A window appears displaying the request in progress.



Block Device

This option lets you block a device. To block a device that has been lost or stolen, select the device from the list of managed devices and then click **Block Device**.

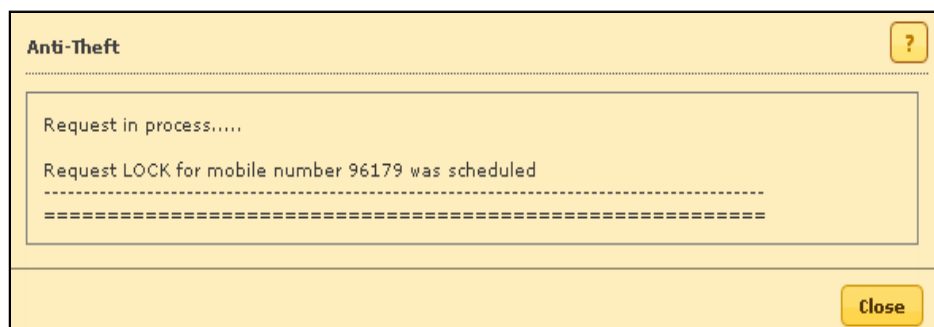
Warning window appears.



This option can be used for both iOS and Android devices.

Click **OK**.

Anti-Theft window appears displaying the request in process.



After the device is blocked, the device user will need the Admin Access Password to unlock the device.

Unlock Device

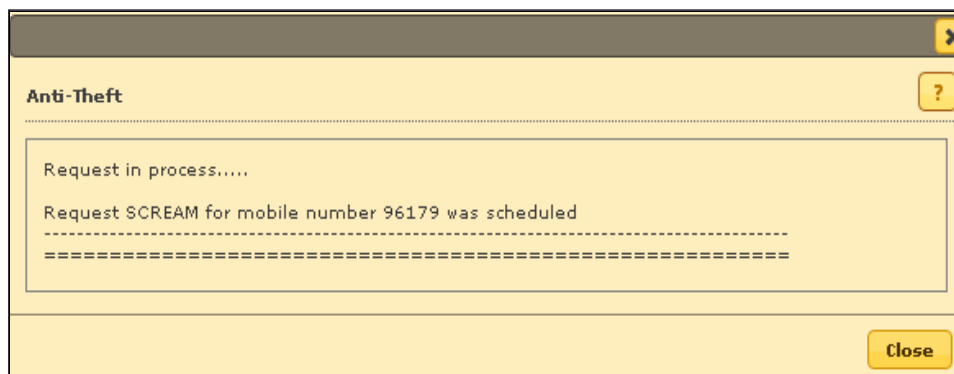
This option lets you unblock a device. To unblock a device, select the device from the list of managed devices and then click **Unlock Device**. Following window appears after clicking **Unlock Device**.

This feature works only for Android devices.



Scream

The Scream lets you raise a loud alarm on a device helping the user locate their device if it is in the vicinity. To raise a loud alarm on a device, select the specific device and then click **Scream**. Following window will be displayed on screen. This option can be used for both iOS and Android devices.

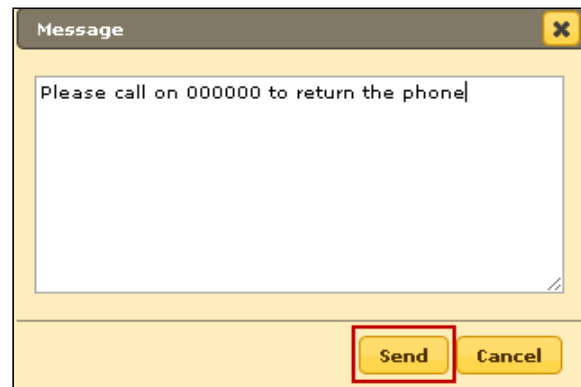


Send Message

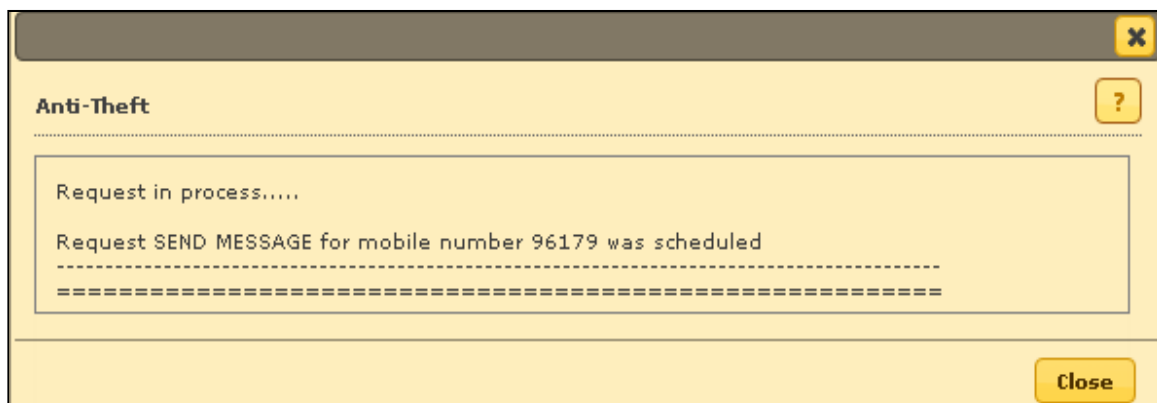
The Send Message lets you send a message to the device. This option can be used for both iOS and Android devices.

To send a message (notification message) select the specific device and then click **Send Message**.

Message window appears.



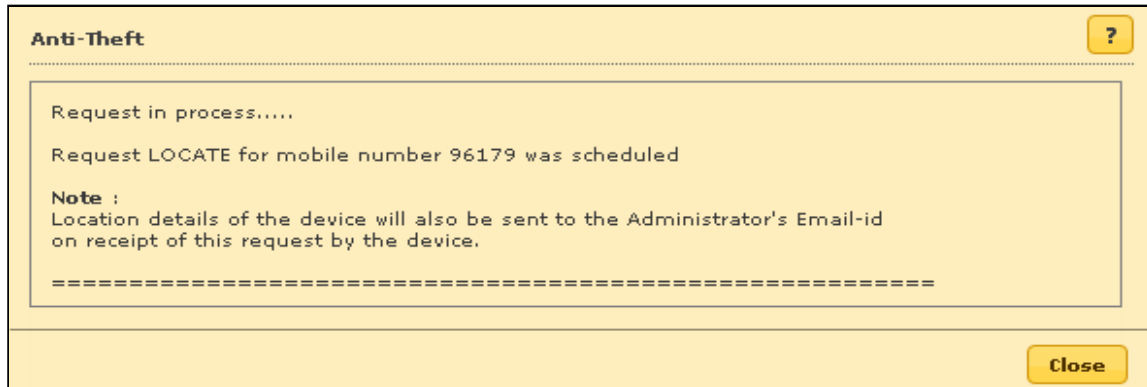
Type the message in the field and then click **Send**.



Locate Device

The Locate Device option lets you locate a device by using the wireless network or a device's GPS. eScan server displays the device's location on Google Maps. This option can be used for both iOS and Android devices.

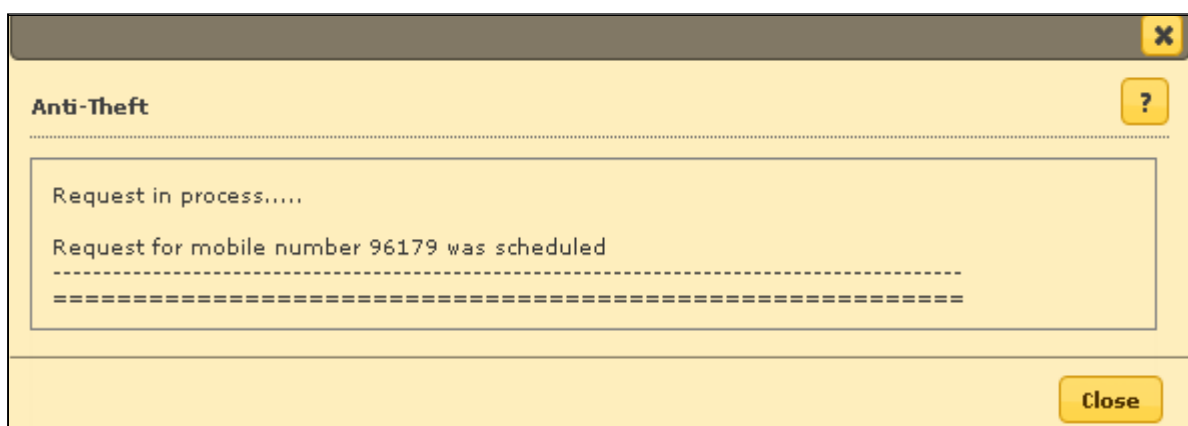
To locate a device, select the specific device and click **Locate Device**. Anti-Theft window appears displaying process.



Remove work Profile

The Remove Work Profile lets you remove the container work profile from a device.

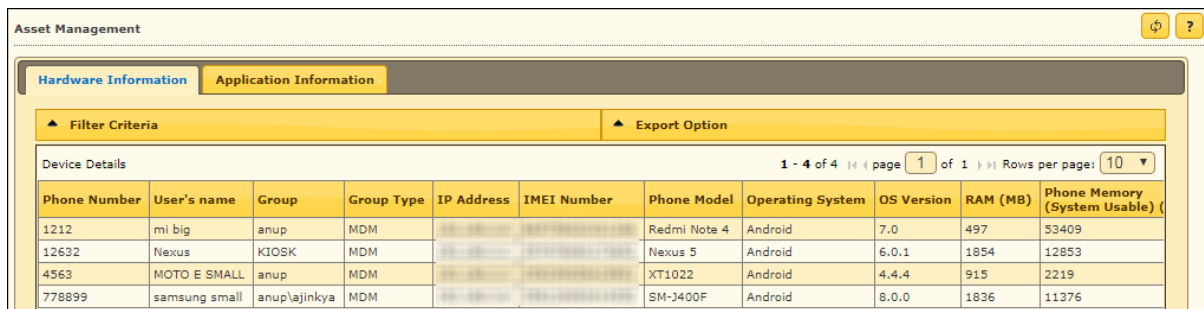
To remove container work profile from a device, select the specific device and then click **Remove Work Profile**. Following window appears after removing the work profile from a device. This feature is available for only Android devices.



Asset Management

The Asset Management module displays detailed description of all the hardware configuration and applications installed on the managed devices.

Asset Management – Hardware Information



Asset Management

Hardware Information Application Information

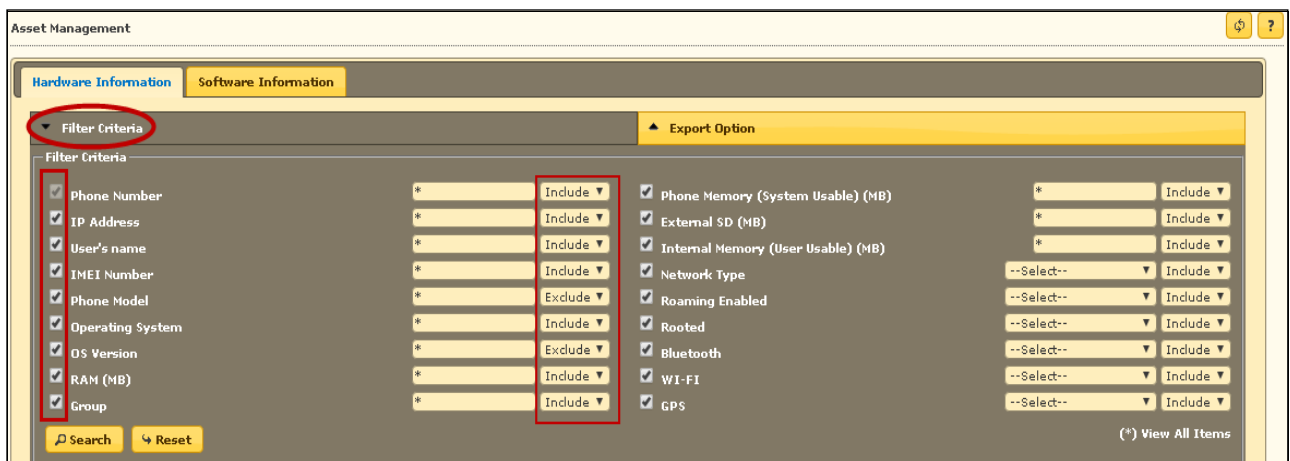
Filter Criteria Export Option

1 - 4 of 4 page 1 of 1 Rows per page: 10

Phone Number	User's name	Group	Group Type	IP Address	IMEI Number	Phone Model	Operating System	OS Version	RAM (MB)	Phone Memory (System Usable)
1212	mi big	anup	MDM			Redmi Note 4	Android	7.0	497	53409
12632	Nexus	KIOSK	MDM			Nexus 5	Android	6.0.1	1854	12853
4563	MOTO E SMALL	anup	MDM			XT1022	Android	4.4.4	915	2219
778899	samsung small	anup/lajinkya	MDM			SM-J400F	Android	8.0.0	1836	11376

Viewing Hardware information

1. Click **Asset Management** and then click **Hardware Information** to view all the hardware related information and all the information captured by the eScan Server can be filtered.
2. To filter the hardware information, click **Filter Criteria** drop-down.



Asset Management

Hardware Information Software Information

Filter Criteria Export Option

Filter Criteria

<input checked="" type="checkbox"/> Phone Number	*	Include	<input checked="" type="checkbox"/> Phone Memory (System Usable) (MB)	*	Include
<input checked="" type="checkbox"/> IP Address	*	Include	<input checked="" type="checkbox"/> External SD (MB)	*	Include
<input checked="" type="checkbox"/> User's name	*	Include	<input checked="" type="checkbox"/> Internal Memory (User Usable) (MB)	*	Include
<input checked="" type="checkbox"/> IMEI Number	*	Include	<input type="text" value="--Select--"/>		Include
<input checked="" type="checkbox"/> Phone Model	*	Exclude	<input checked="" type="checkbox"/> Network Type	--Select--	Include
<input checked="" type="checkbox"/> Operating System	*	Include	<input checked="" type="checkbox"/> Roaming Enabled	--Select--	Include
<input checked="" type="checkbox"/> OS Version	*	Exclude	<input checked="" type="checkbox"/> Rooted	--Select--	Include
<input checked="" type="checkbox"/> RAM (MB)	*	Include	<input checked="" type="checkbox"/> Bluetooth	--Select--	Include
<input checked="" type="checkbox"/> Group	*	Include	<input checked="" type="checkbox"/> WI-FI	--Select--	Include
			<input checked="" type="checkbox"/> GPS	--Select--	Include

Search Reset (*) View All Items

3. Select the check box next to each criterion and select include/exclude to include/exclude that particular criterion in the filtered report.

Following Hardware information is captured from Managed Devices –

Options	Description
Phone Number	Displays the mobile number that is assigned to the device during adding device/enrollment.
IP Address	Displays the IP address of the device.
User's name	Displays the username with which the device is registered on the MDM Server.
IMEI Number	Displays the device's IMEI number.
Phone Model	Displays the device's model details.
Operating System	Displays the device's operating system details.
OS Version	Displays the device's operating system's version.
RAM (MB)	Displays the device's RAM in MB.
Group	Displays the group to which the device belongs.
Phone Memory (System Usable) (MB)	Displays the phone memory of the device.
External SD (MB)	Displays the external SD card's storage capacity (MB) of the device.
Internal Memory (User Usable) (MB)	Displays the internal memory of the device.
Network Type	Displays the network type used by the device.
Roaming Enabled	Displays the roaming status of the device.
Rooted	Displays if the device is rooted or not.
Bluetooth	Displays if Bluetooth is available on the device or not.
Wi-Fi	Displays if Wi-Fi is available on the device or not.
GPS	Displays if GPS is available on the device or not.

Select the check box next to each criterion and select include/exclude to include or exclude that particular criterion in the filtered report.

Asset Management – Application Information

Asset Management

Hardware Information Application Information

Filter Criteria Export Option

Application Details 1 - 50 of 116 page 1 of 3 Rows per page: 50

Application Name	Device Count
Amazon Shopping	1
Android Camera	1
Android Geocode Location	1
Apps	1
Assist	1
AV Test App	1
Browser	1
Calculator	4
Calendar	4
Camera	4
CardViewExample	1
Chrome	4
Clock	4
com.kvikesh800gmail.relativlayoutjava	1
com.samsung.android.app.watchmanagerstub	1
Compass	1
Contacts	2
Contacts and dialer	1
Connectivity	2

Filtering the Application information

1. Click **Asset Management** and then click **Application Information** to view application related information. All the information captured by the eScan Server can be filtered.
2. To filter the software information, click **Filter Criteria**.

Hardware Information Application Information

Filter Criteria Export Option

Filter Criteria

Application Name Include ▼

Phone Number Include ▼

Group By

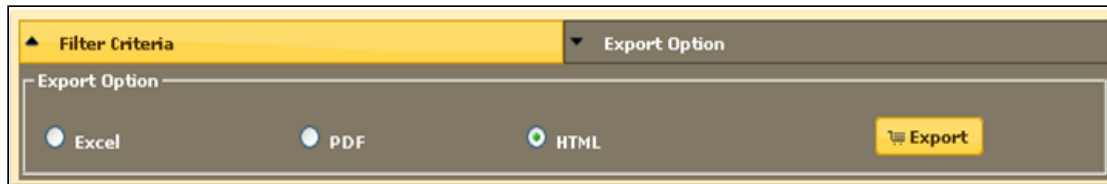
☐ Application Name

☐ Phone Number

(*) View All Items

3. Select **Include/Exclude** to include otherwise exclude that particular criterion in the filtered report. All the information captured from the devices can be filtered on the basis of the application name or the mobile number associated with the device.
4. Select the desired criteria drop-down and then click **Search**.
5. Details will be filtered in the table instantly and will be displayed in the list of software installed on managed devices as well as the device count for every installed software.

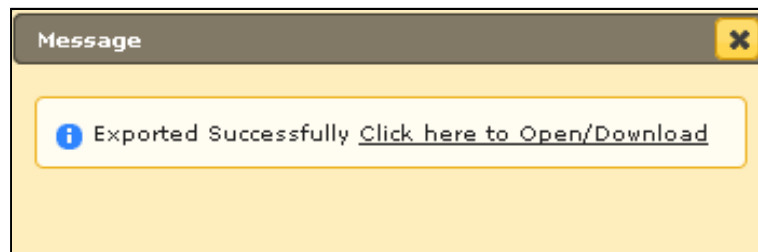
Asset Management – Export Options for the Generated Reports



You can export reports generated for the hardware as well as software inventory to **Excel**, **PDF** or **HTML** formats, as per requirement

Exporting a Report









1. Select the export option of your preference and then click **Export**.
A message appears informing about successful export.



2. Click the link in the prompt to open/download the report.

Report Templates

The Report Templates module lets you generate/edit (Customize) any pre-defined report template for any eScan module. You can also create your own customized report template as per your requirements.

Report Templates						
<div> <div>New</div> <div>Edit</div> <div>Delete</div> <div>View</div> </div>						
<input type="checkbox"/>	Template Name	Report Type	Date Filter	Sort By	Created On	Modified On
<input type="checkbox"/>	Application Control Report 	Application Control Report	This Week	Date	08 Nov 2019	08 Nov 2019
<input type="checkbox"/>	Enrollment Report  	Enrollment Report	This Year	Date	11 Nov 2019	13 Nov 2019
<input type="checkbox"/>	Inventory Report  	Inventory Report	This Week	Devices	08 Nov 2019	08 Nov 2019
<input type="checkbox"/>	Update Report 	Update Report	This Week	Date	08 Nov 2019	08 Nov 2019
<input type="checkbox"/>	Virus Report 	Virus Report	This Week	Date	08 Nov 2019	08 Nov 2019
<input type="checkbox"/>	Web Control Report 	Web Control Report	This Week	Date	08 Nov 2019	08 Nov 2019

Creating a Report Template

1. In the Report Templates screen, click **New**.
New Report Template window appears.

New Report Template

Report Template Name : *

Select Report Type

☒ Virus Report
 ☐ Update Report

☐ Web Control Report
 ☐ Inventory Report

☐ Application Control Report

Select Filter Options

Save

Cancel

2. Type a name for the new report template and select the required report type from the given options.

3. In **Select Filter Options** section, select the appropriate **Date Options** and **Sort By**, then click **Save**.

New Report Template

Template Name : * New Report Template_1

Selected Template Type

Select Filter Options

Date Options

☒ Today ☐ This Week

☐ This Month ☐ This Year

☐ Since Installed ☐ Date Range

Sort By

☒ Date ☐ Devices

☐ Websites ☐ Action Taken

Save Cancel

Editing a Report Template

1. Select a Report Template and then click **Edit**.
Edit Report Template window appears.

Edit Report Template

Template Name : * New Report Template_1

Report Details

Select Filter Options

Date Options

☐ Today ☐ This Week

☒ This Month ☐ This Year

☐ Since Installed ☐ Date Range

Sort By

☐ Date ☐ Devices




☒ Virus ☐ Action Taken

Save Cancel

- Make the required changes and then click **Save**.
The Report Template will be updated.

Deleting a Report Template

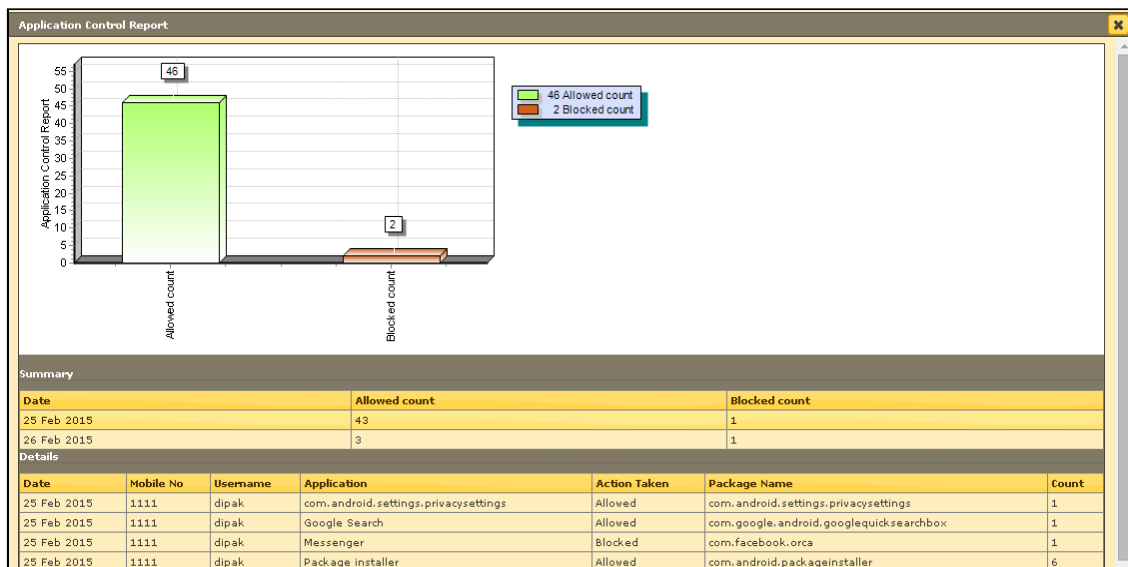
Select a Report Template and then click **Delete**.

Report Templates		
<div> New Edit Delete View </div>		
<input type="checkbox"/>	Template Name	Report Type
<input type="checkbox"/>	Application Control Report 	Application Control Report
<input type="checkbox"/>	Inventory Report  	Inventory Report
<input checked="" type="checkbox"/>	New Report Template_1 	Web Control Report
<input type="checkbox"/>	Web Control Report 	Web Control Report

The Report Template will be deleted.

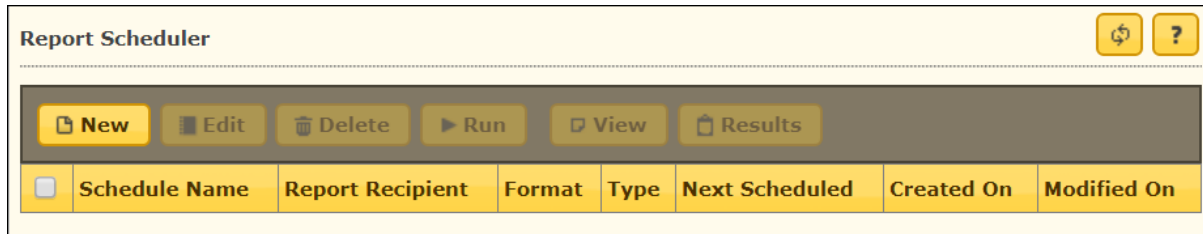
Viewing a Report

To view report details, select the specific template and then click **View**.
A window appears displaying specific details.

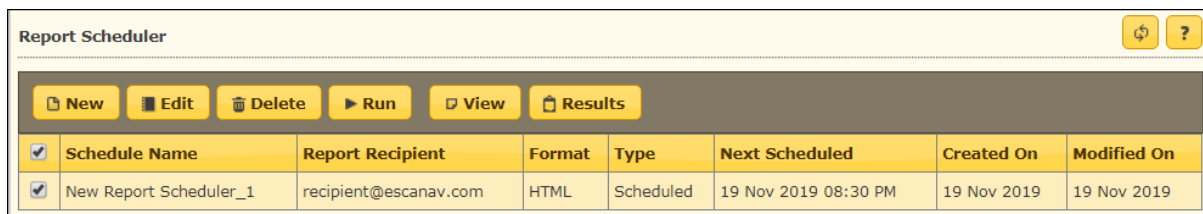


Report Scheduler

The Report Scheduler module lets you schedule a report based on the type of templates, specific group or device, file format and type of schedule.



Under Report Scheduler, following options are available. Except **New**, all other options are enabled only after selecting a template.



Options	Description
New	This option lets you create a report schedule.
Edit	This option lets you edit a report schedule.
Delete	This option lets you delete a report schedule.
Run	This option lets you run a report schedule.
View	This option lets you view a report schedule.
Results	This option lets you view the results of previously deployed report schedule.

Adding a Scheduler

After clicking **New**, New Report Scheduler window appears.

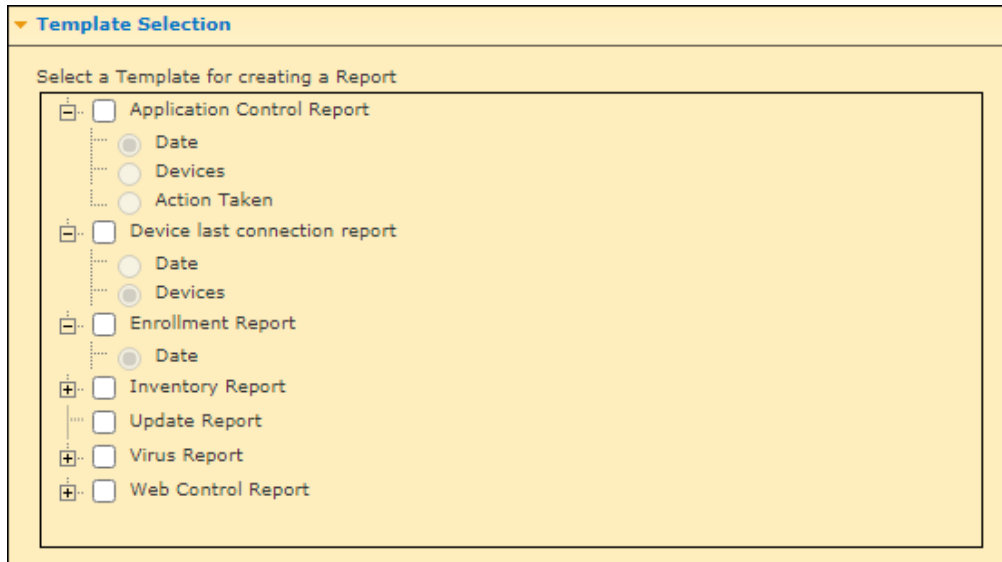
Enter a name in the New Report Scheduler field.

Below there are following sections:

- Template Selection
- Selection For Applied Groups/Clients
- Report Send Options
- Report Scheduling Settings

Template Selection

Select the appropriate template for generating a report according to your preferences of Date, Devices, and Action taken.



The screenshot shows a 'Template Selection' dialog box with a yellow background. At the top, it says 'Select a Template for creating a Report'. Below this, there is a list of templates, each with a checkbox and a sub-selection of options (Date, Devices, Action Taken) indicated by radio buttons. The templates are: Application Control Report, Device last connection report, Enrollment Report, Inventory Report, Update Report, Virus Report, and Web Control Report. The 'Application Control Report' is selected, and its sub-options are 'Date', 'Devices', and 'Action Taken'. The 'Device last connection report' is selected, and its sub-options are 'Date' and 'Devices'. The 'Enrollment Report' is selected, and its sub-option is 'Date'. The 'Inventory Report', 'Update Report', 'Virus Report', and 'Web Control Report' are not selected.

▼ Template Selection

Select a Template for creating a Report

- ☒ Application Control Report
 - ☒ Date
 - ☐ Devices
 - ☐ Action Taken
- ☒ Device last connection report
 - ☐ Date
 - ☒ Devices
- ☒ Enrollment Report
 - ☒ Date
- ☐ Inventory Report
- ☐ Update Report
- ☐ Virus Report
- ☐ Web Control Report

Under the Template Selection we have following templates:

- Application Control Report
- Device last connection report
- Enrollment Report
- Inventory Report
- Update Report
- Virus Report
- Web Control Report

Selection For Applied Groups/Clients

Select the groups for which you want to schedule the report:

- Report for Groups
- Report for a List of Devices

Select **Report for Groups/Report for a List of Devices** tab to schedule a report for the specific groups.

▼ Selection For Applied Groups/Clients

"Report for a List of Devices" will not be applicable for "Enrollment Report"

☒ Report for Groups ☐ Report for a List of Devices

☐ Select subgroups on selecting Parent group

⊕ ☐ Managed Devices

Configure the options for sending the report on email using **Report Send Options**. Select the appropriate format for sending the report on email. .xls, .html and .pdf formats are supported.

Report Send Options

▼ Report Send Options

Send Report by Email

Report Sender*: ted@ex.com

Report Recipient*: example@example.com

Add

Delete

Mail Server IP Address: smtp.gmail.com

Mail Server Port: 465

Auth. Username: ted@ex.com

Auth. Password: password

Select the Report Format

HTML page

Add the following details under the **Report Send Options** section.

Send Report by Email

- **Report Sender** – The email address set for **Email Notification Settings** will be displayed here.
- **Report Recipient** – Enter an email address for the report recipient and then click **Add**.

Select the Report Format:

Click the drop-down to select the preferred format. Following report format options are available:

- HTML Page
- Adobe PDF
- Microsoft Excel file
- CSV file

Report Scheduling Settings

Report Scheduling Settings

☒ Scheduled ☐ Manual

☒ Daily ☐ Weekly ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

☐ Monthly

☒ At

There are two options to schedule a report. The options are **Scheduled** and **Manual**.

Scheduled: Select this option to schedule a report for daily, weekly, or monthly basis.

At: This option lets you set the specific time at which you want the report.

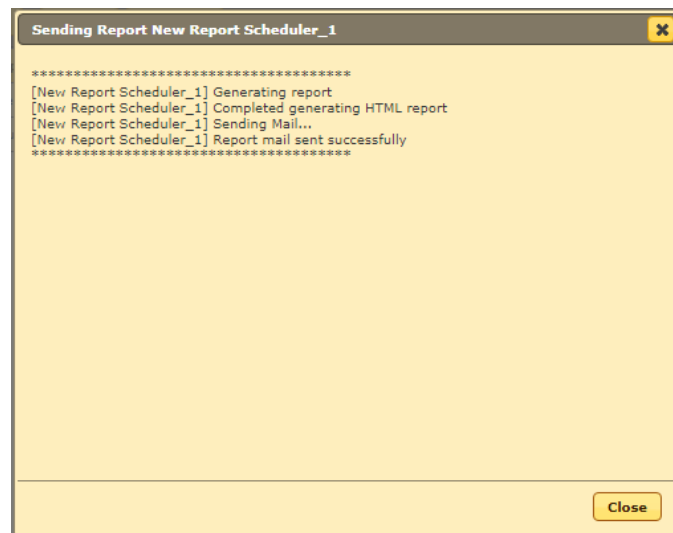
Manual - Select this option to generate a report manually at an instant.

Running a schedule

To run a schedule, select a schedule and then click **Run**.

<div> New Edit Delete Run View Results </div>							
<input checked="" type="checkbox"/>	Schedule Name	Report Recipient	Format	Type	Next Scheduled	Created On	Modified On
<input checked="" type="checkbox"/>	New Report Scheduler_1	abc@escanav.com	HTML	Scheduled	20 Feb 2019 08:30 PM	20 Feb 2019	20 Feb 2019

After clicking **Run**, the console runs the schedule, generates a report and sends it to the recipient mail address.



Editing a Schedule

Select a schedule and then click **Edit**.

Edit Report Scheduler window appears.

Make the required changes and then click **Save**.

Deleting a Schedule

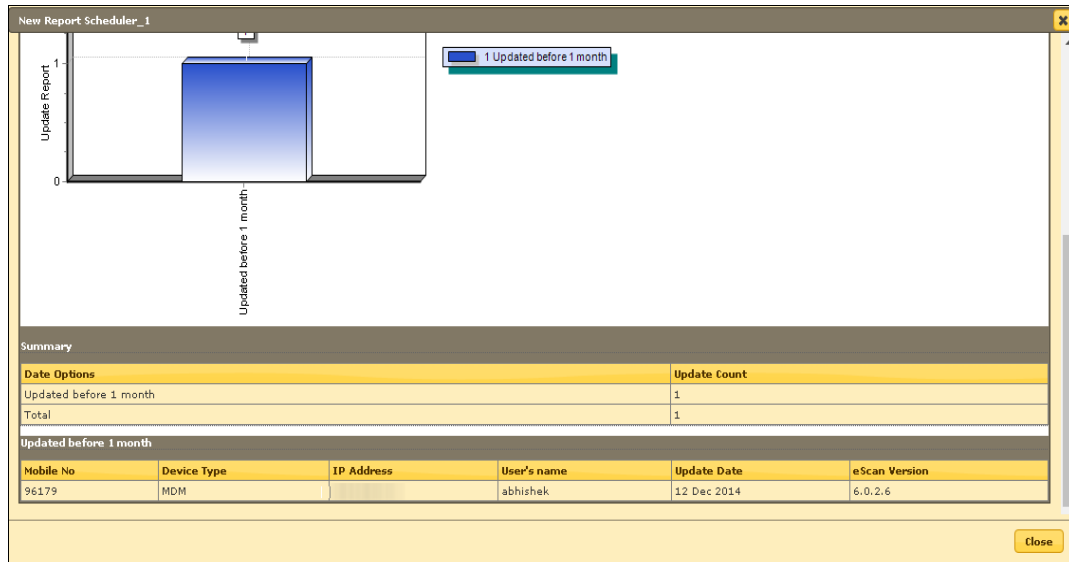
Select a schedule and then click **Delete**.

Report Scheduler							
<div> New Edit Delete Run View Results </div>							
<input checked="" type="checkbox"/>	Schedule Name	Report Recipient	Format	Type	Next Scheduled	Created On	Modified On
<input checked="" type="checkbox"/>	New Report Scheduler_1	user@domain.com	EXCEL	Scheduled	12 Feb 2019 08:30 PM	12 Feb 2019	12 Feb 2019

The selected schedule will be deleted.

Viewing the report

Select a schedule and then click **View**. A Report window appears and displays specific details.



Viewing results of a report

Select a schedule and then click **Results**. A Results window appears and displays Report results.

The screenshot shows a window titled 'New Report Scheduler_2 - Results'. It contains a table with the following data:

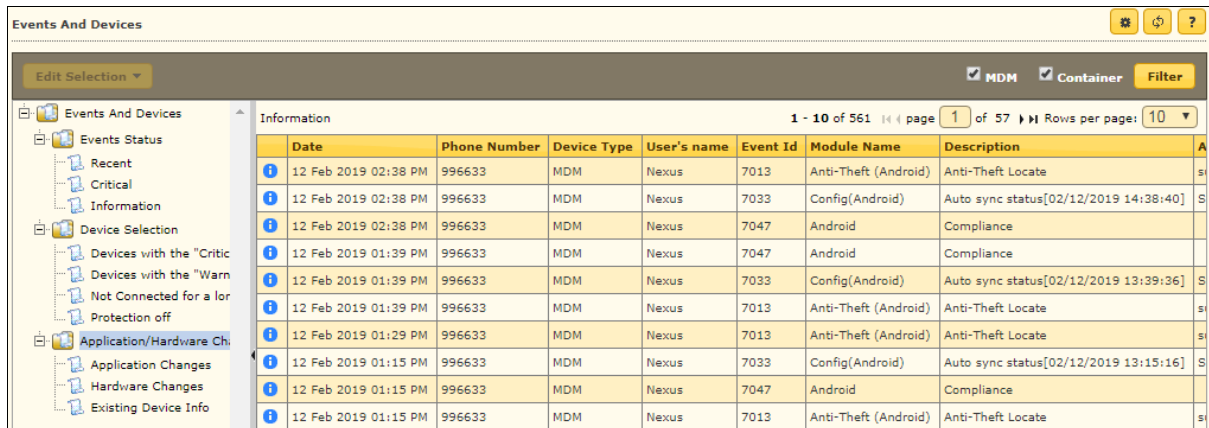
Start	Finish	Type	Status
12 Feb 2019 03:05 PM	12 Feb 2019 03:05 PM	Manual	Report mail sent successfully
12 Feb 2019 03:06 PM	12 Feb 2019 03:06 PM	Manual	Report mail sent successfully
12 Feb 2019 03:21 PM	12 Feb 2019 03:21 PM	Export	Error while exporting data

A 'Close' button is located at the bottom right of the window.

Events and Devices

Viewing Events

Events captured from the devices are categorized and displayed in this module. This will display a real-time status of security and eScan update on all the devices.



The screenshot shows the 'Events And Devices' module interface. It includes a sidebar with navigation options like 'Events Status', 'Recent', 'Critical', 'Information', 'Device Selection', and 'Application/Hardware Changes'. The main area displays a table of events with columns for Date, Phone Number, Device Type, User's name, Event Id, Module Name, and Description. The table shows various events such as 'Anti-Theft Locate', 'Config(Android)', and 'Auto sync status'.

Date	Phone Number	Device Type	User's name	Event Id	Module Name	Description
12 Feb 2019 02:38 PM	996633	MDM	Nexus	7013	Anti-Theft (Android)	Anti-Theft Locate
12 Feb 2019 02:38 PM	996633	MDM	Nexus	7033	Config(Android)	Auto sync status[02/12/2019 14:38:40]
12 Feb 2019 02:38 PM	996633	MDM	Nexus	7047	Android	Compliance
12 Feb 2019 01:39 PM	996633	MDM	Nexus	7047	Android	Compliance
12 Feb 2019 01:39 PM	996633	MDM	Nexus	7033	Config(Android)	Auto sync status[02/12/2019 13:39:36]
12 Feb 2019 01:39 PM	996633	MDM	Nexus	7013	Anti-Theft (Android)	Anti-Theft Locate
12 Feb 2019 01:29 PM	996633	MDM	Nexus	7013	Anti-Theft (Android)	Anti-Theft Locate
12 Feb 2019 01:15 PM	996633	MDM	Nexus	7033	Config(Android)	Auto sync status[02/12/2019 13:15:16]
12 Feb 2019 01:15 PM	996633	MDM	Nexus	7047	Android	Compliance
12 Feb 2019 01:15 PM	996633	MDM	Nexus	7013	Anti-Theft (Android)	Anti-Theft Locate

Event Status

Events are categorized into three types based on their severity.

Recent: It displays both critical and information events that occurred recently on devices.

Critical: It displays all critical events that occurred on devices, such as virus detection, protection disabled status etc.

Information: It displays all informative type of events, such as virus signature database update and status of the device.

Device Selection

The Device Selection tab enables you to select and save the device status settings. This module enables you to do the following activities:

Define Criteria for Filtering of Device Status on the basis of following-

- Device with the "Critical Status"
- Device with the "Warning Status"
- Database are Outdated
- Many Viruses Detected

- Not Connected for a long time
- Not Scanned for a long time
- Protection off


Application/Hardware Changes

Capture events on the basis of Application Changes, Hardware Changes or Existing Device Info.

It has following sections:

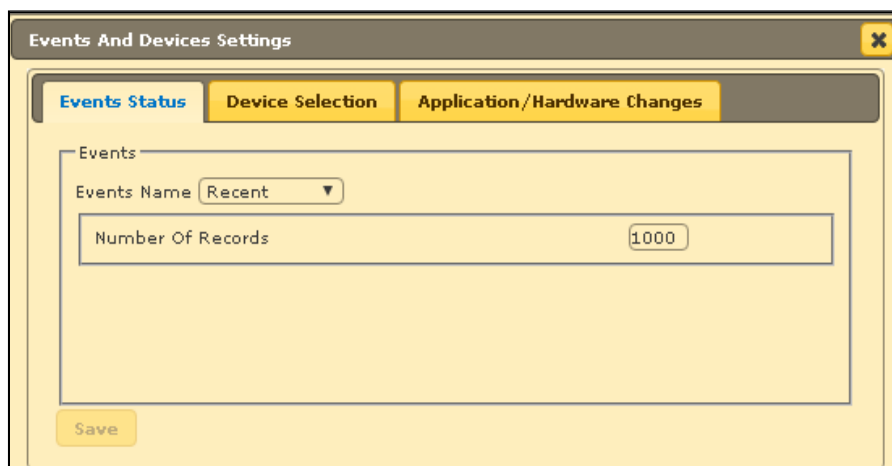
- **Application Changes:** It displays the list of managed devices on which application related changes are made. For example, installation/uninstallation of applications.
- **Hardware Changes:** It displays the list of managed devices on which hardware related changes are made.
- **Existing Device Info:** It displays the existing device's information.

Events and Devices settings

Click the **Settings** icon  present below the top right corner to define settings for Events and Devices. There are following tabs in Events and Devices Settings:

- Event Status
- Device Selection
- Application/Hardware Changes

Event Status



Select an event from the drop-down and enter the number of records you want to see.

Device Selection

The following actions can be performed by selecting this tab.

The screenshot shows the 'Events And Devices Settings' window with the 'Device Selection' tab selected. The window has three tabs: 'Events Status', 'Device Selection', and 'Application/Hardware Changes'. Under the 'Device Selection' tab, there is a 'Devices' section with a 'Device Status' drop-down menu set to 'Devices with the "Critical Status"'. Below this, there are four checked checkboxes: 'Check for Monitor Status', 'Check for Not Scanned', 'Check for Database Not Updated', and 'Check for Not Connected'. At the bottom, there are four input fields for time intervals: 'Database Not Updated from more than' (7 days), 'Device Not Scanned for more than' (7 days), 'Device Not Connected for more than' (7 days), and 'Number Of Records' (1000). A 'Save' button is located at the bottom left.

Device Status

The Device Status drop-down consists following options:

The screenshot shows the 'Device Status' drop-down menu with the following options: 'Devices with the "Critical Status"', 'Devices with the "Warning Status"', 'Database are Outdated', 'Many Viruses Detected', 'Not Connected for a long time', 'Not Scanned for a long time', and 'Protection off'. The first option, 'Devices with the "Critical Status"', is currently selected and highlighted in blue.

- Devices with the "Critical Status"
- Devices with the "Warning Status"
- Database are Outdated
- Many Viruses Detected
- Not Connected for a long time
- Not Scanned for a long time
- Protection off

Option	Description
Check for Monitor Status	Select this check box to generate events related to eScan Monitor Protection.
Check for Not Scanned	Select this check box to view the list of devices which are not scanned.
Check for Database Not Updated	Select this check box to view the list of devices on which virus signature database is not updated.
Check for Not Connected	Select this check box to view the list of devices that are not connected with the eScan server.
Database Not Updated from more than	All the devices that are not updated from more than the specified days will be added to the report.
Device Not Scanned for more than	All the devices that are not scanned for more than specified days will be added to the report.
Device Not Connected for more than	All the devices that are not connected to the eScan server for more than the specified days will be added to the report.
Number of Records	Enter the count and the number of records will be displayed.

Application/Hardware changes

The following actions can be performed using this option.

Events And Devices Settings

Events Status Device Selection **Application/Hardware Changes**

Updates

Application/Hardware Changes Application Changes ▼

Number Of Days 1 days

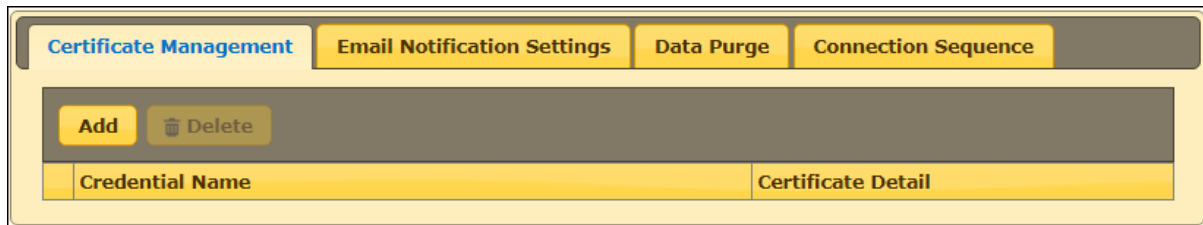
Number Of Records 1000

Save

Field	Description
Application/Hardware Changes	Select from the drop-down to generate events related to Application changes, Hardware changes, and Existing Device Info.
Number of Days	Enter the number of days, to view changes made within the specified days. For example, if you have typed 2 days, then you can view the list of devices on which any software/hardware changes have been made in the last 2 days.
Number of Records	Enter the number of records to be displayed in the list.

Settings

The Settings module lets you save server details for sending email notifications to the device users. You can also add the latest certificates required to manage iOS devices in the console via this module.



Certificate Management

The eScan EMM requires a SSL certificate to manage your iOS devices from the EMM console. This section gives you information on all the pre-requisites for managing iOS devices and how you can import the SSL certificate. It also briefs you on what the certificate is about and where you can purchase the same.

Important Note:

1. The SSL certificate is not an iOS certificate or some other certificate provided by Apple.
2. This is a normal SSL certificate that organizations use on their server for SSL communication (https). For example, when you visit [our website](#), you are on a secured connection, as an SSL certificate installed on our domain escanav.com.
3. If you own the website as 'emm.mycompany.com', you need to get an SSL certificate for the domain emm.mycompany.com. You can buy it from a Certificate Authority or generate it for free.
4. The SSL certificate thus bought from a Certificate Authority has to be renewed every year. If you have generated the SSL certificate for free it has to be renewed every 3 months.
5. In order to have a secure communication between your server and Apple's server you will have to import the SSL certificate in the console.

Importing an SSL certificate

1. Click **eScan Mobility Management (EMM)**. Select Platform prompt appears.
2. Under **To manage iOS devices** you need to add a Trusted CA Certificate. Click **Start with iOS**. It opens a new window where you can import your certificate files.
3. Search for the files in your local drive.
4. Save the files.

After saving files, a confirmation message appears.

Note	Make sure you add an authentic CA certificate and key in .crt and .key file format. A self-signed file will not be accepted.
-------------	--

To add the CA certificate if

You had selected to proceed with "**Start with Android (without iOS)**" earlier
OR

You have deleted the previous certificate, follow the steps given below:

1. On the navigation panel, click **Settings**.
2. Select **Certificate Management** tab.
3. Click **Add**.

Add Certificate window appears.

4. Click **Choose File** and select the .crt and .key files. Enter the password in Certificate Key File Password if your key file is password protected.
5. After selecting the files (and entering password) click **Save**. A confirmation message appears "**Certificate added successfully**".

Email Notification Settings

Set up an email account to receive notifications.

From (Administrator Email ID): Enter the administrator email ID.

SMTP Server: Enter the SMTP server IP address.

SMTP Port: Enter the SMTP Port number.

Auth. Username: Enter the authorized username.

Auth. Password: Enter the password.

After you are done filling the details, click **Save**.

To run a test for the configured settings, click **Test**. A test email will be sent to the entered email ID.

Data Purge

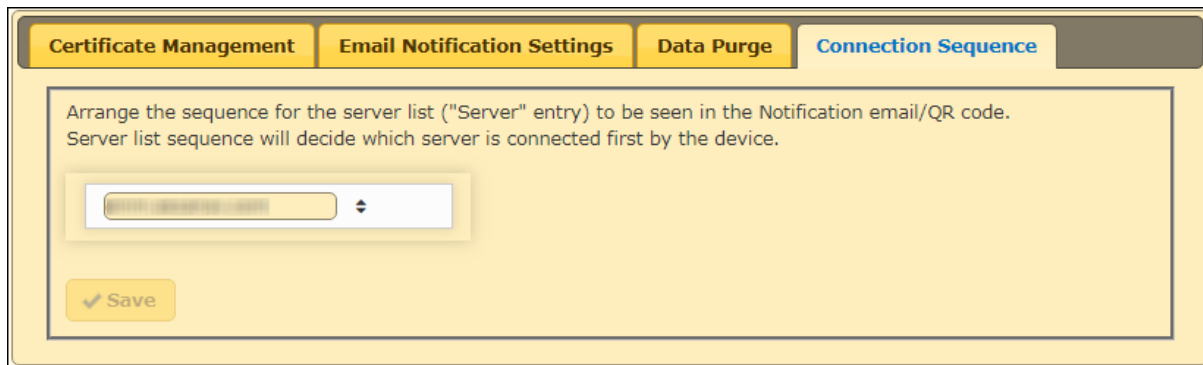
This setting lets you define the number of days for storing data in tables. The old data will be purged automatically after it reaches number of specified days. The data purge can be set for following data tables:

- Location History
- Data Usage data

- Call Logs data
- Battery Status
- Geo Fence History Data
- App Usage History data

After making the necessary changes, click **Save**. The web console Settings will be updated.

Connection Sequence

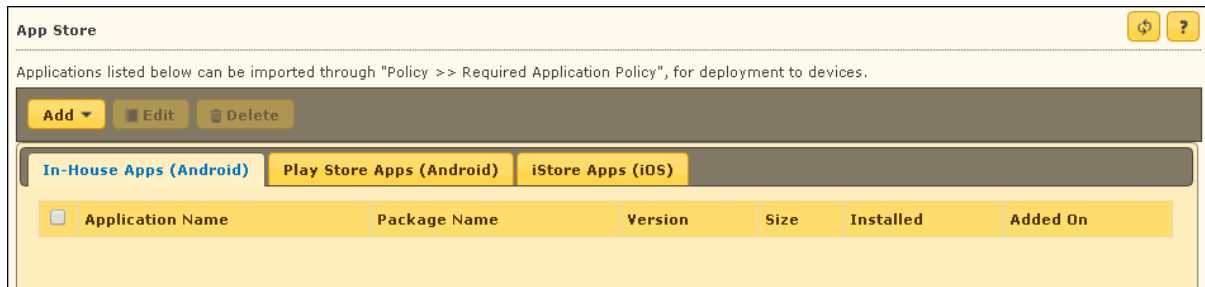


The screenshot shows a web console interface with four tabs: "Certificate Management", "Email Notification Settings", "Data Purge", and "Connection Sequence". The "Connection Sequence" tab is active. Below the tabs, there is a text box containing the instruction: "Arrange the sequence for the server list ('Server' entry) to be seen in the Notification email/QR code. Server list sequence will decide which server is connected first by the device." Below this text box is a dropdown menu with a single visible option, "Server 1", and a small upward/downward arrow icon to its right. At the bottom left of the form area is a yellow button with a checkmark icon and the text "Save".

The enrollment email and QR code consists the server list. As devices are getting enrolled, they will use these server details and connect to the servers in the same sequence. After you are done making changes, click **Save**. The Server sequence changes will be saved.

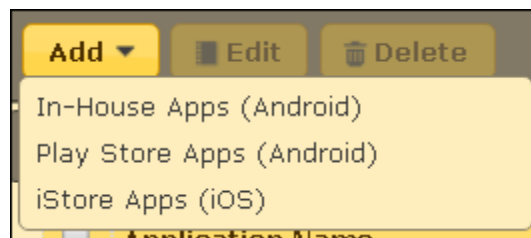
App Store

The App Store module lets you push applications on a device by policy deployment. The user will receive a notification to download and install the application. This module helps you push application(s) on multiple devices at the same time.

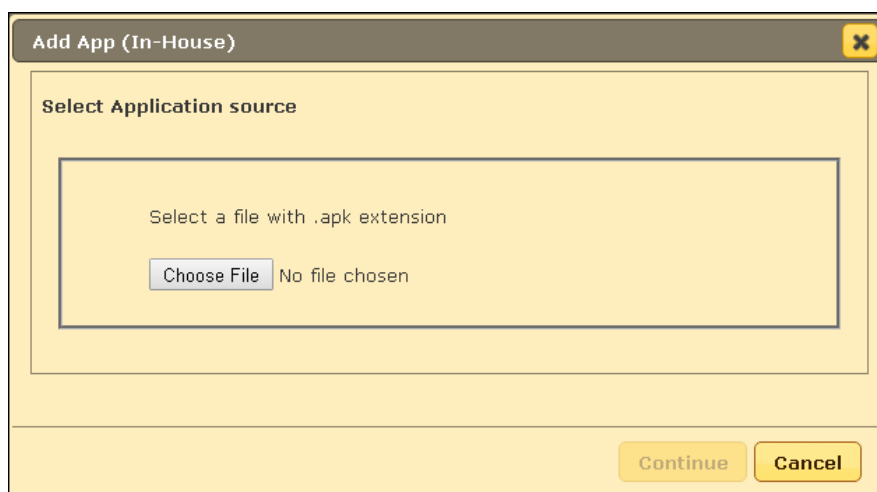


Adding an Android application with In-House Apps (Android) option

1. Click **Add > In-House Apps (Android)**.

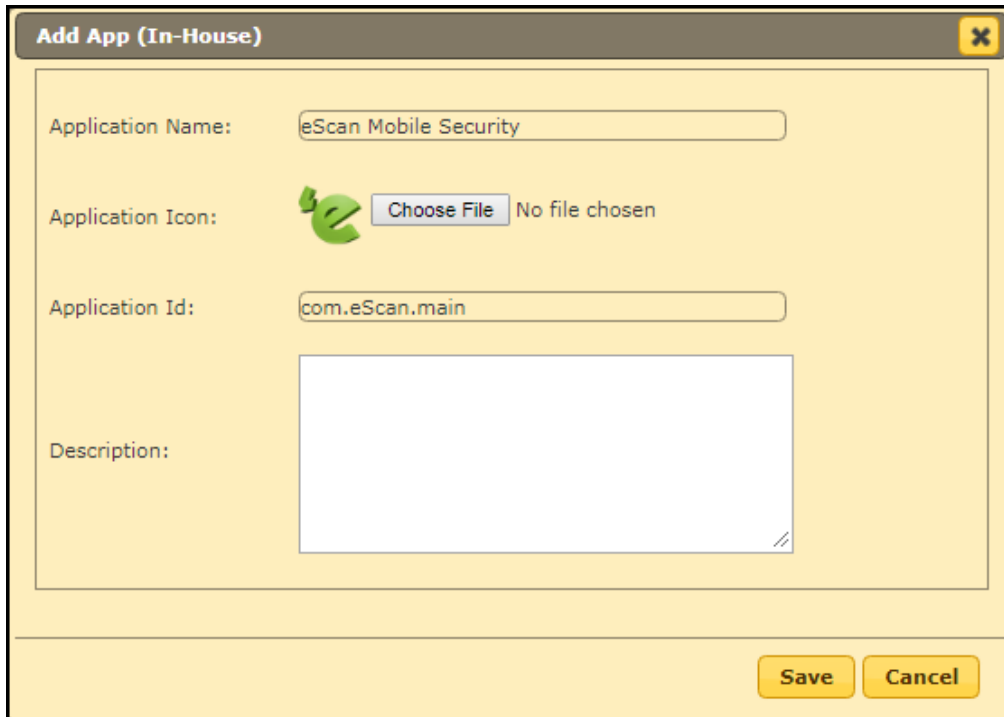


Add App (In-House) window appears.



2. Click **Choose File** and browse your computer for the **.apk** file. After selecting the file, click **Continue**.

Add Application window appears.



The image shows a dialog box titled "Add App (In-House)" with a close button (X) in the top right corner. The dialog box has a yellow background and contains the following fields and controls:

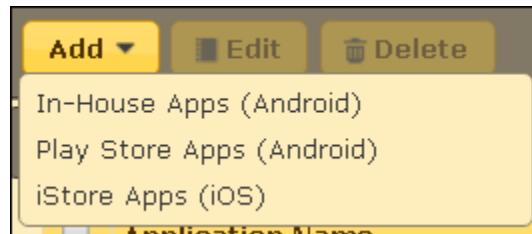
- Application Name:** A text input field containing "eScan Mobile Security".
- Application Icon:** A green icon of a stylized 'e' with a checkmark. To its right is a "Choose File" button and the text "No file chosen".
- Application Id:** A text input field containing "com.eScan.main".
- Description:** A large, empty text area for writing a description.
- Buttons:** At the bottom right, there are two buttons: "Save" and "Cancel".

3. Write a brief description about the application and then click **Save**.
The application will be added to the App Store.

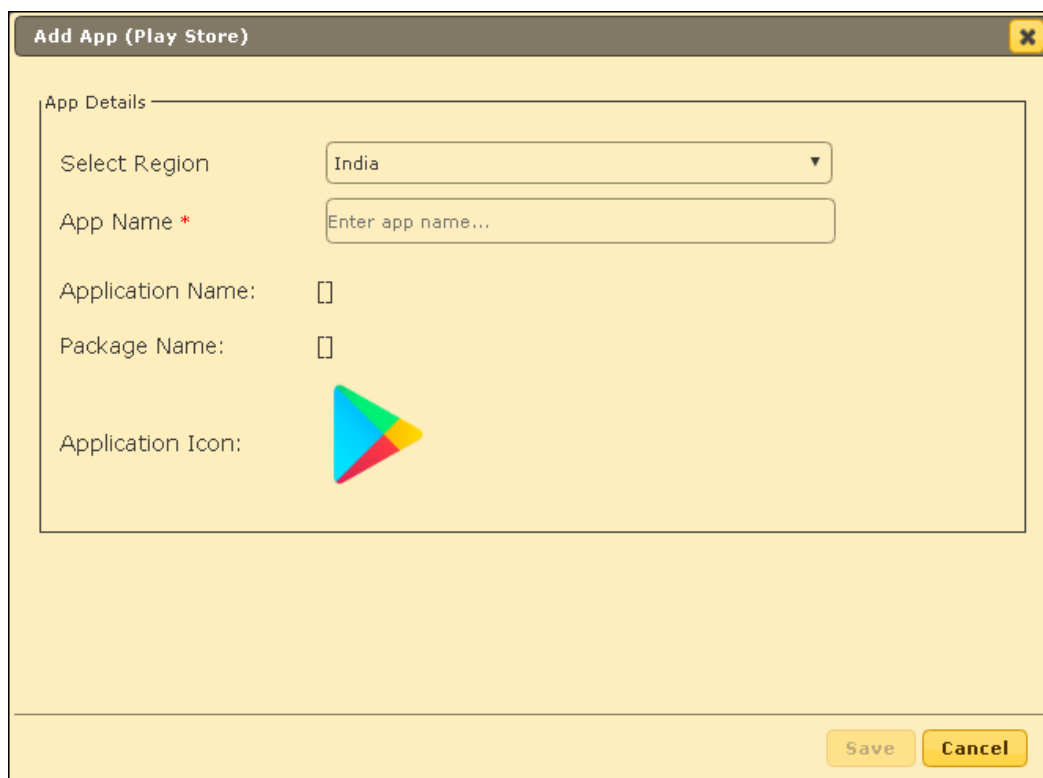
Click the numerical in the **Installed** column to view the list of devices on which the application is installed. Before the policy deployment the count will be 0. If the application with the same version number already exists on the devices, the installation count will be shown accordingly.

Adding an Android application with Play Store Apps (Android) option

1. Click **Add > Play Store Apps (Android)**.



Add App (Play Store) window appears.

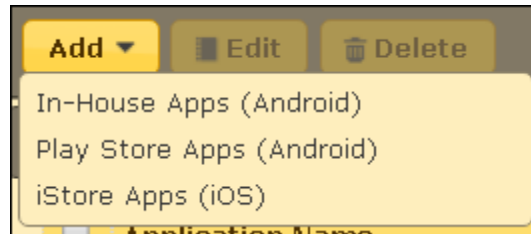


2. Select a region.
3. In the **App Name** field, enter an application name and select the appropriate application from the suggestions.
4. Click **Save**.

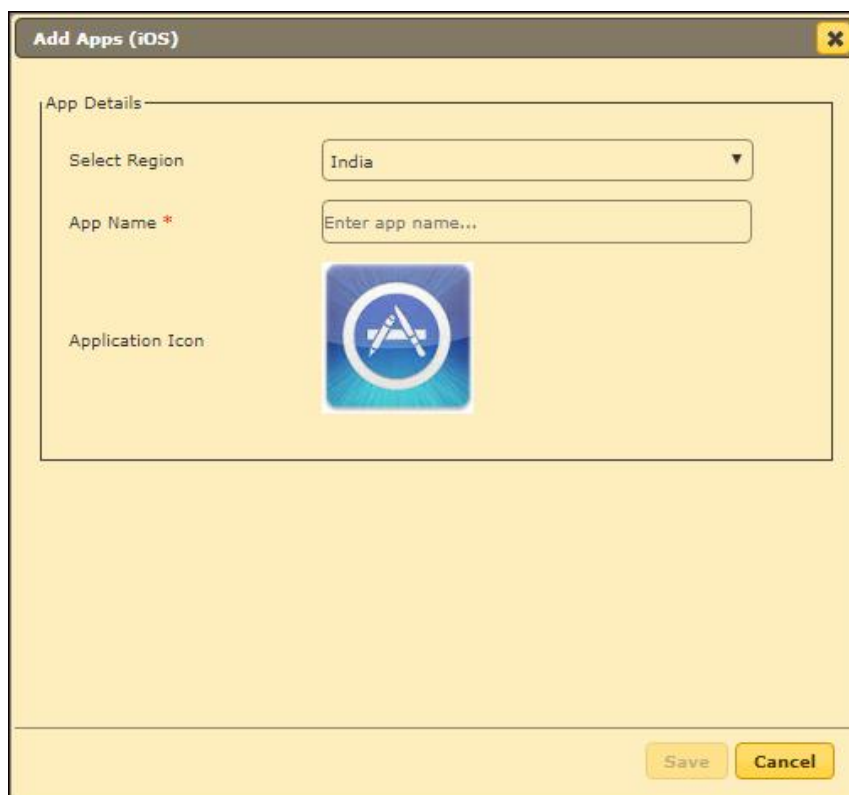
The application will be added to the App Store.

Adding an iOS application

1. Click **Add** > iStore Apps (iOS).



Add Apps (iOS) window appears.

A screenshot of a window titled 'Add Apps (iOS)'. The window has a yellow background and a close button in the top right corner. Inside the window, there is a section labeled 'App Details' which contains a 'Select Region' dropdown menu with 'India' selected, an 'App Name' text field with a red asterisk and the placeholder text 'Enter app name...', and an 'Application Icon' section showing the Apple App Store icon. At the bottom right of the window are 'Save' and 'Cancel' buttons.

2. Select a region.
3. In the **App Name** field, enter an application name and select the appropriate application from the suggestions.
4. Click **Save**.

The application will be added to the App Store.

Note	The description can be edited only for In-House Apps (Android) applications.
-------------	--

Deleting an application from the App Store

Select an application and then click **Delete**.

App Store

Applications listed below can be imported through "Policy >> Required Application Policy", for deployment to devices.

Add

Edit

Delete

In-House Apps (Android)

Play Store Apps (Android)

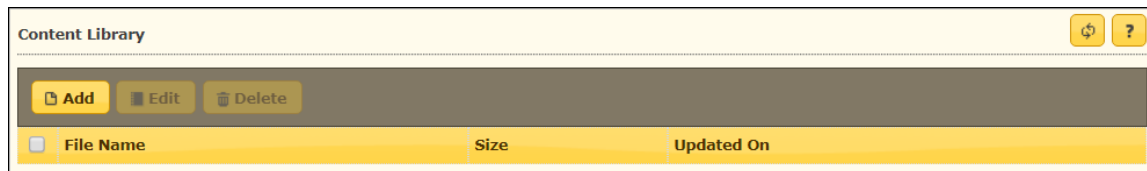
iStore Apps (iOS)

	Application Name	Package Name	Version	Size	Installed	Added On
<input checked="" type="checkbox"/>	eScan Mobile Security	com.eScan.main	7.1.0.11	12950 Kb	0	18 Nov 2019 04:45 PM

The selected application will be deleted.

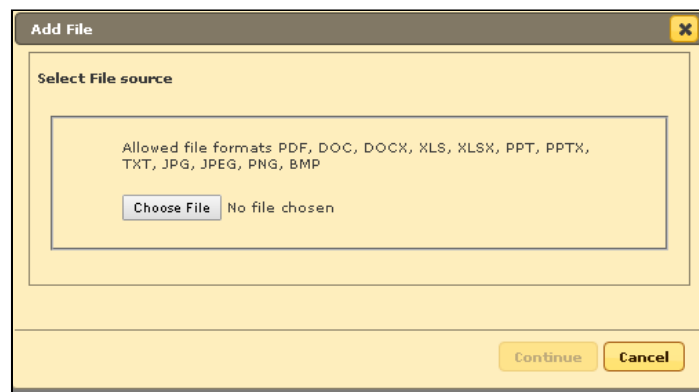
Content Library

The Content Library module lets you deploy documents through the web console. The document types that can be deployed are .pdf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .jpg, .jpeg, .png and .bmp. You can use this feature to share work related documents across multiple devices at the same time.

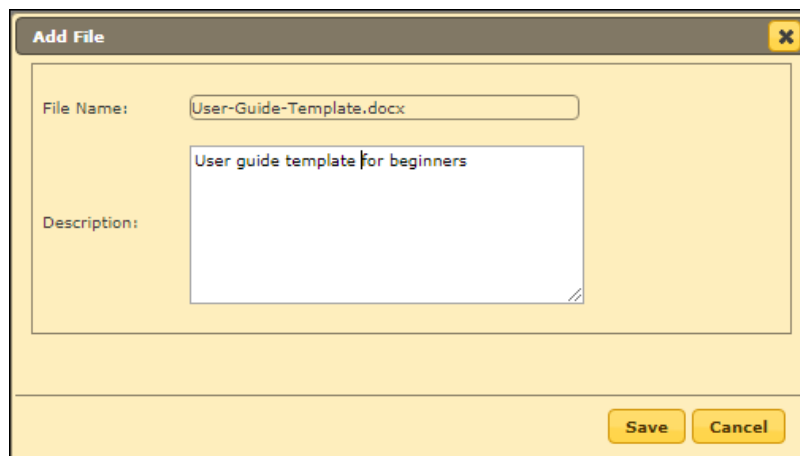


Adding a file

1. Click **Content Library > Add**.
Add File window appears.



2. Click **Choose File** and search your computer for the file.
3. After selecting the file, click **Continue**.
Add File window appears.

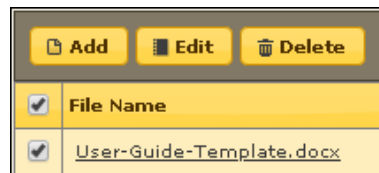


4. Write a description for the document and then click **Save**.
The document will be added to the Content Library.

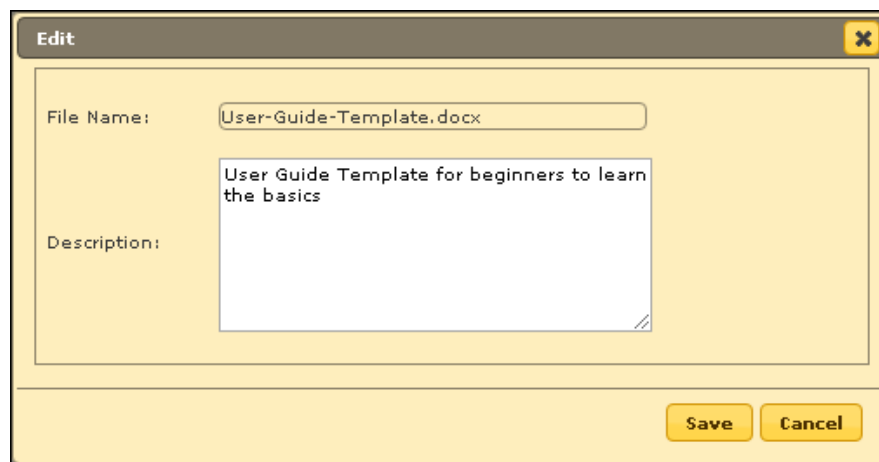
Editing a file description

To edit a file description, follow the steps given below:

1. Select a file and then click **Edit**.



Edit window appears.

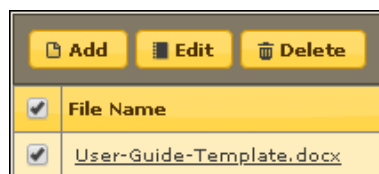


2. Edit the description and then click **Save**. The file description will be updated.

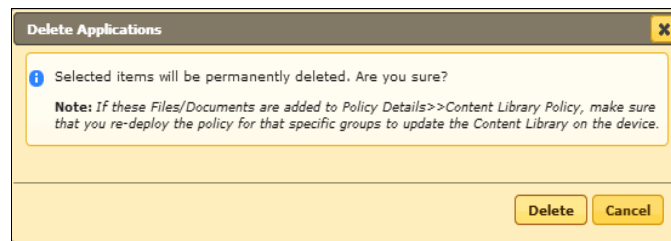
Deleting a file

To delete a file, follow the steps given below:

1. Select a file and then click **Delete**.



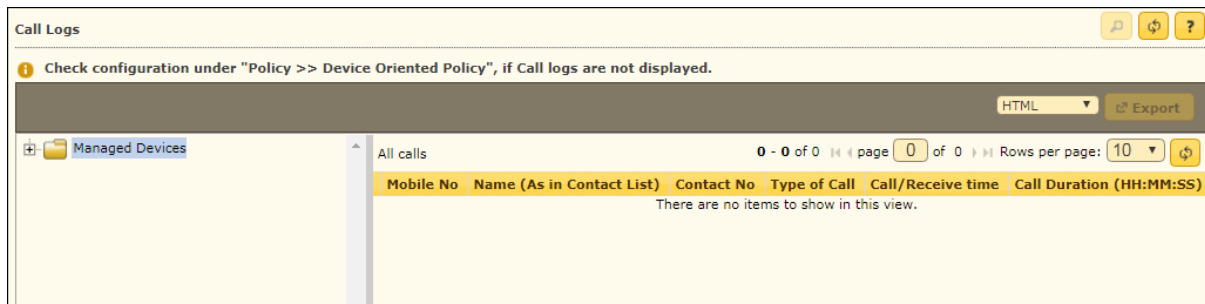
A confirmation prompt appears.



2. Click **Delete**. The file will be deleted.

Call Logs

The Call Logs module lets you maintain call logs of incoming and outgoing calls of all managed devices along with the call duration.

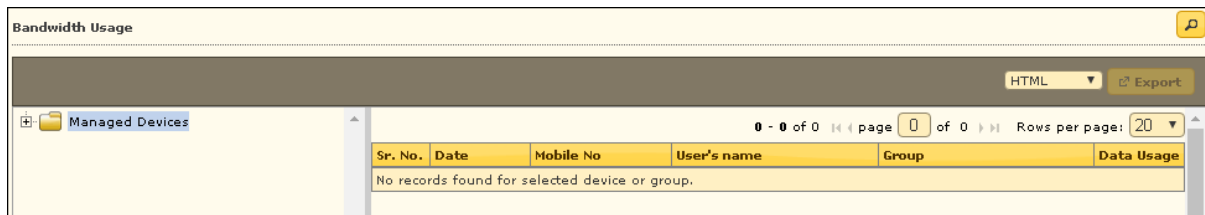


This module displays the list of all the incoming and outgoing calls. It will display the following details:

Column	Description
Mobile no.	This column displays the mobile number.
Name (As in Contact List)	This column displays the contact name as saved in the contact list.
Contact No.	This column displays the contact number with whom the user had a conversation.
Type of Call	This column displays whether the call was incoming or outgoing.
Call/Receive time	This column displays the specific time when the call was made or received.
Call Duration	This column displays the time duration of each call.

Data Usage

The Data Usage module lets you keep a track of cellular data usage of a device.



Column	Description
Date	This column displays the date for which the details are recorded.
Mobile No.	This column displays the mobile number of the device.
Username	This column displays the username of the managed device.
Group	This column displays the group to which the particular managed device belongs.
Data Usage	This column displays the amount of mobile data consumed by the managed device.

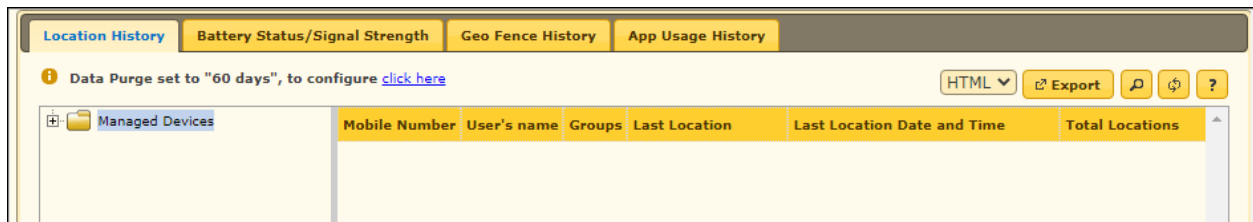
History

The History module consists following tabs:

- Location History
- Battery Status/Signal Strength
- Geo Fence History
- App Usage History

Location History

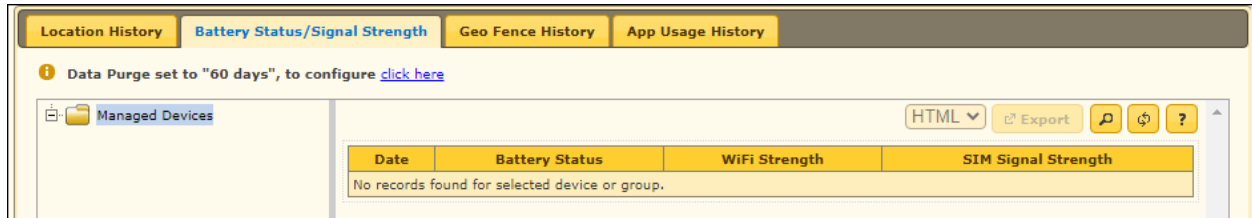
This tab displays the location details of all enrolled devices. It also displays the location where the device was last active and helps you track total number of locations where the device was active.



Column	Description
User's Name	This column displays the user's name of the managed device.
Mobile Number	This column displays the mobile number of the managed device.
Groups	This column displays the group name to which the device belongs to.
Last Location	This column displays the location where the device was last active.
Total Locations	This column displays the total number of the locations where the managed device was active. By clicking the numbers, you can view a detailed device location history recorded on the map along with the Date, Time, Latitude and Longitude. You can also export these details in PDF, XLS, and HTML formats.

Battery Status/Signal Strength

This tab displays the available battery, Wi-Fi, and SIM signal strength of a device.

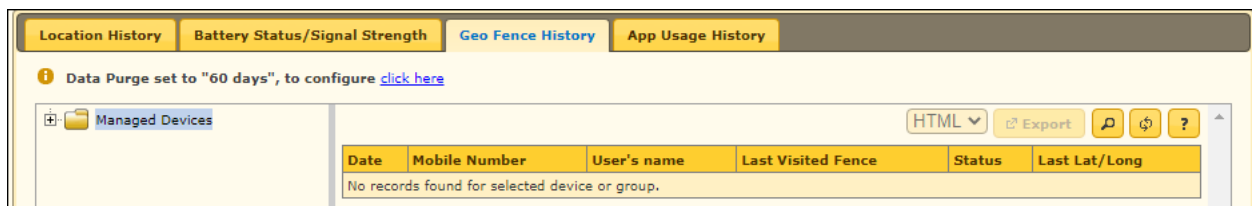


Column	Description
Date	This column displays the date.
Battery Status	This column displays the available battery on a device,
Wi-Fi Strength	This column displays the available Wi-Fi strength of a device.
SIM Signal Strength	This column displays the available SIM signal strength of a device.

Filter

You can also view the details related to the Battery Status/Signal Strength as per the date range.

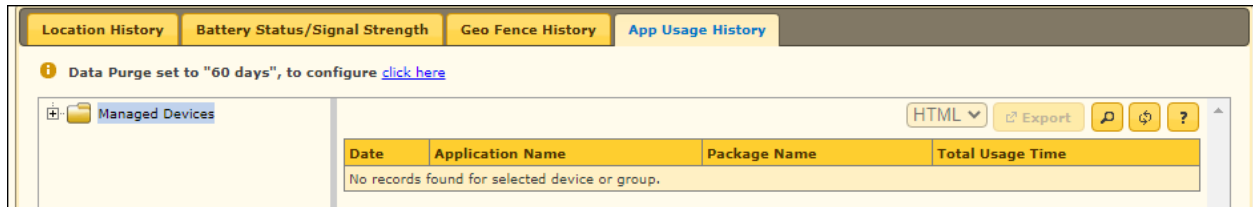
Geo Fence History



Column	Description
Date	This column displays the date.
User's name	This column displays the user name of the device
Last Visited Fence	This column displays the name of the last visited fence.
Status	This column displays the fencing status of a device.
Last Lat/Long	This column displays the coordinates of latitude and longitude of the device visited

	lastly.
--	---------

App Usage History



Column	Description
Date	This column displays the date.
Application Name	This column displays the name of the application.
Package Name	This column displays the package name of the application.
Total Usage Time	This column display the total time the application was used

Fencing Location(s)

Geo-Fencing refers to drawing a virtual barrier around a location using a device's Global Positioning System (GPS) or Internet Protocol (IP) address. Technically, geo-fencing can be any size radius from a particular location, anywhere from 25m to 5000m in stretch. You can define an address on the map and set the radius around that address. If the device is in that region, the policy set by the administrator will be active on the device.

Fencing Location(s)

Add

Edit

Delete

View On Map

Set Default Location

<input type="checkbox"/>	Custom Address	Latitude	Longitude	Radius(m)	Address

Creating a Fencing Location

To create a Fencing Location, it is necessary that a default location must be set first.

1. Click **Fencing Location(s)** and then click **Set Default Location**.
Default Location window appears.

Default Location

Map

Satellite

Enter a location

80, Rd Number 15, Marol MIDC Industry Estate, Andheri East, Mumbai, Maharashtra 400069, India

Map

Satellite

ANDHERI EAST

अंधेरी ईस्ट

SAHAR VILLAGE

साहार विलेज

POWAI

पवई

CHANDIV

चान्दिवली

SAHAR VILLAGE

साहार विलेज

POWAI

पवई

CHANDIV

चान्दिवली

SAHAR VILLAGE

साहार विलेज

POWAI

पवई

CHANDIV

चान्दिवली

Save

2. Enter the location and then click **Save**.

- After setting the default location, click **Add**.
Fencing Location(s) window appears.

Fencing Location(s)

Map Satellite Enter a location

80, Rd Number 15, Marol MIDC Industry Estate, Andheri East, Mumbai, Maharashtra 400047, India

GAUTAM NAGAR CHAKALA INDUSTRIAL AREA (MIDC) MIDC Central Rd MULGAON Rd Number 4 VIJAY NAGAR COLONY ANDHERI EAST KADAM WADI CHRISTIAN WADI

Location Details

Latitude : 19.11983 Longitude : 72.87373

Radius(m) : 200 Meters **Set**

Address : 80, Rd Number 15, Marol MIDC Industry Estate, Andheri

Custom Address :

Save Close

- Enter the location and select the appropriate one from suggestions.
- Click the **Radius** drop-down to select the appropriate radius and then click **Set**.
- In the **Custom Address** field, enter a name for your fencing location.
- After entering all the details, click **Save**.

Editing a Fencing Location

- Select a location and then click **Edit**.

<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="View On Map"/> <input type="button" value="Edit Default Location"/>			
<input checked="" type="checkbox"/>	Custom Address	Latitude	Longitude
<input checked="" type="checkbox"/>	Mumbai Office	19.12000	72.87357

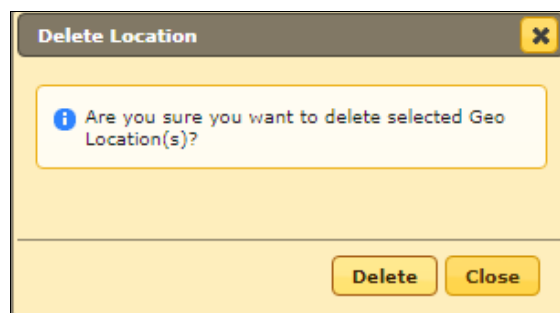
- After making the necessary changes, click **Save**.

Deleting a Fencing Location

1. Select a location and then click **Delete**.

Fencing Location(s)			
<div> Add Edit Delete View On Map Edit Default Location </div>			
<input checked="" type="checkbox"/>	Custom Address	Latitude	Longitude
<input checked="" type="checkbox"/>	Mumbai Office	19.12000	72.87357

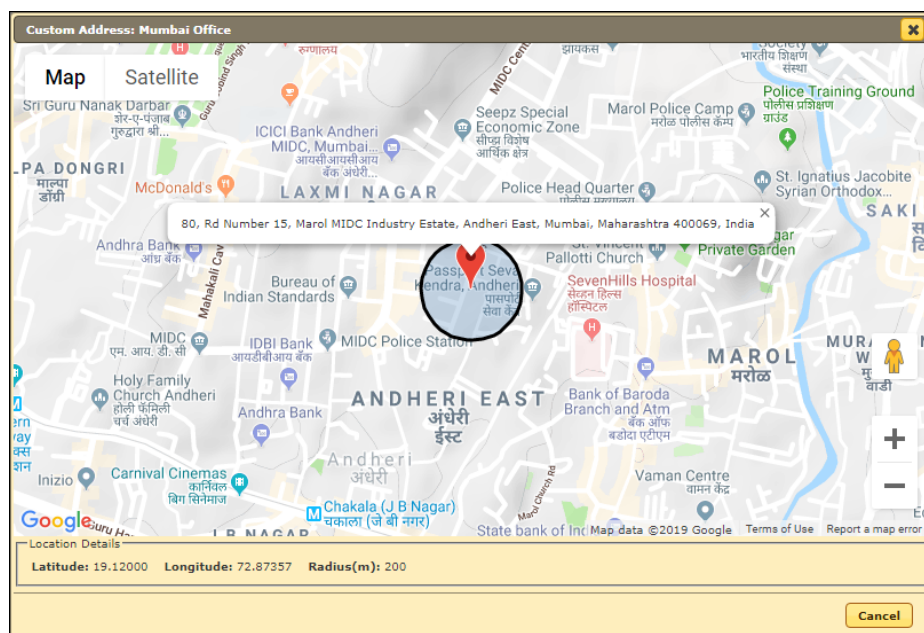
A confirmation prompt appears.



2. Click **Delete**.
The location will be deleted.

View On Map

Clicking **View On Map** lets you view the selected location on the Google Maps.



Administration

The Administration module lets you create User Accounts and User Roles to allocate them Administrative rights for using eScan Management Console as required. With this option, you can allocate roles to the other employees and allow them to carry out required responsibility.

The Administration module consists following submodules:

- User Accounts
- User Roles

User Accounts

With User Accounts submodule, you can 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. You can create new user accounts and also add them from Active Directory.

User Accounts						
<div> Refresh Help </div>						
<div> Create New Account Add from Active Directory Delete 1 - 2 of 2 page 1 of 1 Rows per page: 10 </div>						
<input type="checkbox"/>	User's name	Full Name	Domain	Role	MDM Role	Session Log Status
<input type="checkbox"/>	root	Administrator account created during installation		Administrator	Administrator	View
<div> Create New Account Add from Active Directory Delete 1 - 2 of 2 page 1 of 1 Rows per page: 10 </div>						

Creating a User Account

To create a User Account, follow the steps given below:

1. In the User Accounts screen, click **Create New Account**.
Create User form appears.

Create User Help

User Accounts > Create User

Account Type and Information

User's name*:

Full Name*:

Password*:

Confirm Password*:

Email Address*:

For Example: user@yourcompany.com

Account Role

Role*:

MDM Role*:

Save

Cancel

(*) Mandatory Fields

2. After filling all the details, click **Save**.
The user will be added to the User Accounts list.

Adding a User from Active Directory

1. In the User Accounts screen, click **Add from Active Directory**.
Add Active Directory Users form 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*:

Users > < Selected Users

Account Role

Role*:

MDM Role*:

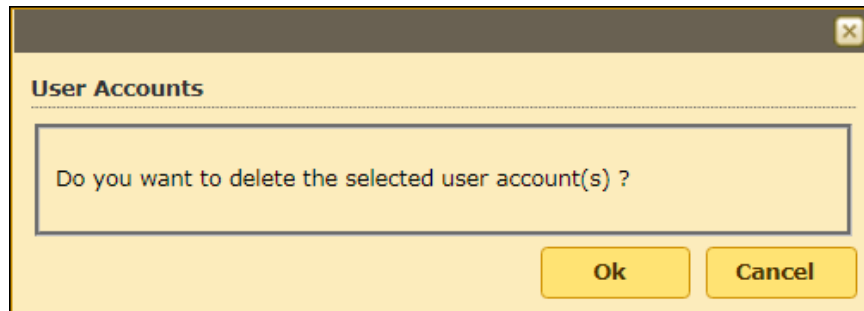
Save Cancel (*) Mandatory Fields

2. After filling **Search Criteria** section details, click **Search**.
3. A list of users will be displayed in the **Users** section.
4. Select a user and then click > button to add the user to **Selected Users** section.
5. Vice versa the added user can be moved from Selected Users to Users by clicking <.
6. Click **Save**.
The user will be added to the User Accounts list.

Deleting a User Account

To delete a user account, follow the steps given below:

1. In the User Accounts screen, select a user and then Click **Delete**.
A confirmation prompt appears.

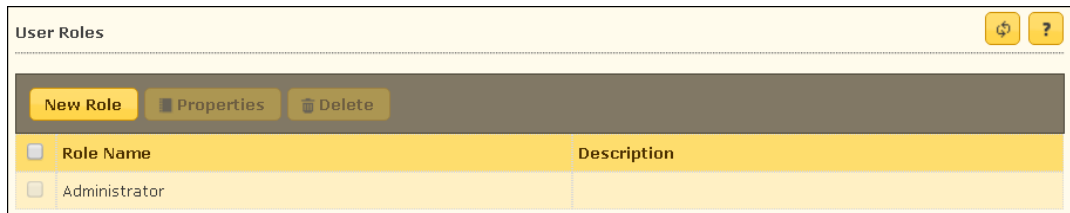


2. Click **OK**.
The User Account will be deleted.

User Roles

The User Roles submodule lets you create a role and assign it to the User Accounts with variable permissions and rights as defined in the role being assigned to them. It can be an Administrator role with set of permissions and rights Group Admin Role or a Read only Role.

You can re-define the Properties of the created role for configuring access to various section of eScan Management Console and the networked Computers. It also lets you delete any existing role after the task is completed by them. It allows the administrator to give permission to subadministrators 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.



Adding a User Role

To add a user role, follow the steps given below:

1. In the User Roles screen, click **New Role**.

New Role form appears.

New Role

Role Details

New Role Name : *

Description :

Select Group :

☐ Select subgroups on selecting Parent group

☐ Managed Devices

OK Cancel

Cancel

2. Enter name and description for the role.
3. Click **Managed Computers** and select the specific group to assign the role.
4. The added role will be able to manage and monitor only the selected group's activities.
5. Click **OK**.

Permissions section appears displaying Main Tree Menu and Client Tree Menu tabs. The Main Tree Menu consists of Managed Mobile Devices and Anti-Theft view and configuration permissions. The Client Tree Menu consists of selected groups on which permissions the user is allowed to take further.

Role Details

New Role Name : *

Test Role

Description :

Monitor

Select Group

Main Tree Menu

Client Tree Menu

Menu	View	Configure
Dash Board	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Managed Mobile Devices	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Manage Backup	<input type="checkbox"/>	<input type="checkbox"/>
Anti Theft	<input type="checkbox"/>	<input type="checkbox"/>
Asset Management	<input type="checkbox"/>	<input type="checkbox"/>
Report Templates	<input type="checkbox"/>	<input type="checkbox"/>
Report Scheduler	<input type="checkbox"/>	<input type="checkbox"/>
Events And Devices	<input type="checkbox"/>	<input type="checkbox"/>
App Store	<input type="checkbox"/>	<input type="checkbox"/>
Content Library	<input type="checkbox"/>	<input type="checkbox"/>
Call Logs	<input type="checkbox"/>	<input type="checkbox"/>

Save

Cancel

New Role

Role Details

New Role Name : *

Test Role

Description :

Monitor

Select Group

☐ Select subgroups on selecting Parent group

Main Tree Menu

Client Tree Menu

Managed Devices

Please Select a Group to set Permission

Save

Cancel

6. Select the check boxes that will allow the role to view/configure the settings.
7. After selecting the necessary check boxes, click **Save**.
The role will be added to the User Roles list.

Role Properties

To view the properties of a role, follow the steps given below:

1. In the User Roles screen, select a role.
This enables **Properties** and **Delete** buttons.

User Roles			
		<input type="button" value="New Role"/> <input type="button" value="Properties"/> <input type="button" value="Delete"/>	
<input checked="" type="checkbox"/>	Role Name	Description	
<input type="checkbox"/>	Administrator		
<input checked="" type="checkbox"/>	Test Role	Monitor	

2. Click **Properties**.
Properties screen appears. Main Tree Menu lets you modify role description, permissions for accessing and configuring Managed Mobile Devices and Anti-Theft modules.
3. To set permissions for groups or subgroups, click **Client Tree Menu**.
Select the group or subgroup to set permission.
4. Click **Save**.
The Role Properties will be updated accordingly.

Deleting a User Role

To delete a user role, in the User Roles screen, select a user role and then click **Delete**.
The User Role will be deleted.

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