

Enterprise EDR (with MDM & Hybrid Network Support)

User Guide

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



24x7 FREE Online Technical Support support@escanav.com https://forums.escanav.com Clients Supported

Cyber Vaccine





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/04.10.2021.Current Software Version:22.0.xxxx.xxxxTechnical Support:support@escanaSales:sales@escanav.cForums:https://forums.eeScan Wiki:https://wiki.escaLive Chat:https://wiki.escaPrinted by:MicroWorld SoftwDate:October, 2021

5BUG/04.10.2021/22.x 22.0.xxxx.xxxx support@escanav.com sales@escanav.com https://forums.escanav.com https://wiki.escanav.com/wiki/index.php/ https://www.escanav.com/english/livechat.asp MicroWorld Software Services Private Limited October, 2021





Content

Introduction	15
Pre-requisites for eScan Enterprise EDR Server	15
System Requirements	16
Installing eScan Enterprise EDR Server	
Installation	19
Components of eScan Server	27
Web Console Login	28
Setup Links	
eScan AV Report	31
Main Interface	32
Setup Wizard	33
Navigation Panel	
Dashboard	43
Deployment Status	43
eScan Status	44
License	44
eScan version	45
Protection Status	46
Update Status	47
Scan Status	48
File Anti-Virus	48
Proactive	49
Mail Anti-Virus	49
Anti-Spam	50
Web Anti-Phishing	51
Mail Anti-Phishing	51
Web Protection	52
Firewall	53
Endpoint Security	53
Privacy	54
Anti – Ransomware	55
Protection Statistics	56
File Anti-Virus	57
Mail Anti-Virus	59
Anti-Spam	59





Web Protection	60
Endpoint Security-USB	61
Endpoint Security-Application	61
Summary Top 10	62
Asset Changes	63
Live Status	64
Configure the Dashboard Display	65
EDR Dashboard	66
Incident - eScan	66
Filtering Incident – eScan Report	67
Exporting the Report	68
Incident-Windows	68
Filtering Incident – Windows Report	69
Exporting the Report	70
Incident-EDR	70
Report Type	71
Filtering Incident – EDR Report	74
Exporting the Report	74
Endpoint Incident	75
Adding Specific Incident for Monitoring	77
Viewing the Details of the Specific Incident	78
Viewing the Details of Monitoring Incident	79
Deleting the Monitoring Incident	79
Network Incident	80
Viewing the Network Incident	82
Filtering the Specific Incident	83
Exporting the Network Incident	
Managed Computers	85
Search	86
Update Agent	86
Features of Update Agents	87
Advantages of Update Agents	87
Adding an Update Agent	
Configuring UA Settings	
Delete an Update Agent	
Create Offline Update	90
Action List	93
Creating a Group	93
Removing a Group	94





Set Group Configuratio	n	
Managing Installations.		
Deploy/Upgrade Client		
Refresh Client		
Moving computer from	one group to other	
Viewing installed softwa	are (on Client computer)	
Removing computers fr	om a group	
Installing eScan on Linu	ix and MAC Computers	
Manual installation of e	Scan Client on network comput	ers108
Installing eScan Client U	Jsing Agent	
Installing other Softwar	e (Third Party Software)	
Uninstall eScan Client (Nindows, Mac, and Linux)	
Synchronize with Active	Directory	
Outbreak Prevention		
Create Client Setup		
Properties of a group		
Group Tasks		
Creating a Group Task .		
Managing a Group Tasl	<	
Assigning a Policy to the	e group	
Client Action List		
Set Host Configuration.		
Deploy/Upgrade Client		
Uninstall eScan Client		
Move to Group		
Remove from Group		
Refresh Client		
Connect to Client (RMN	I)	
Assign Policy Template		
Show Critical Events		
Export		
Show Installed Software	es	
Force Download		
Forensic-Port/Commun	ication	
On Demand Scanning		
Send Message		136
Outbreak Prevention		
Delete All Quarantine F	iles	
Create OTP		





Pause Protection	143
Resume Protection	144
Properties of Selected Computer	145
Anti-Theft	146
Anti-Theft Options	146
Disable Anti-Theft	150
Select Columns	151
Policy Template	152
Managing Policies	152
Creating Policy Template for a group/specific computer	156
Configuring eScan Policies for Windows Computers	157
Configuring eScan Policies for Linux and Mac Computers	254
Assigning Policy Template to a group	
Assigning Policy Template to Computer(s)	
Copying a Policy Template	
Exporting a Policy Template report	
Parent Policy	
Policy Criteria Templates	
Adding a Policy Criteria Template	
Viewing Properties of a Policy Criteria template	
Deleting a Policy Criteria template	
Unmanaged Computers	
Network Computers	
Creating a New Group from the Select Group window	
IP Range	
Adding New IP Range	
Moving an IP Range to a Group	
Deleting an IP Range	
Active Directory	
Adding an Active Directory	
Moving Computers from an Active Directory	
New Computers Found	
Filter Criteria	
Action List	
Report Templates	
Creating a Report Template	
Creating Schedule for a Report Template	
Viewing Properties of a Report Template	
Deleting a Report Template	





Report Scheduler	310
Creating a Schedule	310
Viewing Reports on Demand	313
Managing Existing Schedules	314
Generating Task Report of a Schedule	314
Viewing Results of a Schedule	314
Viewing Properties of a Schedule	315
Deleting a Schedule	315
Events and Computers	316
Events Status	316
Computer Selection	317
Edit Selection	
Software/Hardware Changes	321
Violations	
Settings	
Event Status Setting	
Computer Selection	324
Software/ Hardware Changes Setting	328
Performing an action for computer	328
Tasks for Specific Computers	329
Creating a task for specific computers	329
Viewing Properties of a task	
Viewing Results of a task	
Deleting a task for specific computers	
Asset Management	334
Hardware Report	334
Filtering Hardware Report	
Exporting Hardware Report	336
Software Report	336
Filtering Software Report	
Exporting Software Report	
Software License	
Filtering Software License Report	
Exporting Software License Report	
Software Report (Microsoft)	
Filtering Software Report (Microsoft)	341
Exporting Software Report (Microsoft)	342
Filtering Microsoft OS Report	342
Exporting Microsoft OS Report	343





User Activity	344
Print Activity	344
Viewing Print Activity Log	344
Exporting Print Activity Log	345
Filtering Print Activity Log	345
Exporting Print Activity Report	346
Print Activity Settings	347
Session Activity Report	348
Viewing Session Activity Log	348
Filtering Session Activity Log	348
Exporting Session Activity Report	349
File Activity Report	350
Viewing File Activity Log	350
Filtering File Activity Log	350
Exporting File activity Report	352
Application Access Report	353
Viewing Application Access Report	353
Filtering Application Access Report	354
Exporting Application Access Report	354
Patch Report	355
Patch report	355
Filtering Patch Report	356
Exporting Patch Report	356
All Patch Report	357
Filtering All Patch Report	357
Exporting All Patch Report	358
Notifications	359
Outbreak Alert	359
Event Alert	361
Unlicensed Move Alert	362
New Computer Alert	363
Configure SIEM	363
SMTP Settings	364
Settings	365
EMC Settings	366
Web Console Settings	368
Update Settings	372
General Config	372
Update Notification	373





Scheduling	
Update Distribution	
Auto-Grouping	
Excluding clients from auto adding under Managed Group(s)	
Removing clients from the excluded list	
Defining a group and client selection criteria for auto adding under ma	naged
computer(s)	
Two-Factor Authentication (2FA)	
Enabling 2FA login	
Disabling 2FA login	
Users For 2FA	
Roaming Clients	
Adding Roaming Client	
Administration	
User Accounts	
Create New Account	
Delete a User Account	
User Roles	
New Role	
View Role Properties	
Delete a User Role	
Export & Import	
Export Settings	
Import Settings	
Scheduling	400
Customize Setup	402
Creating a customized setup for Windows	402
Creating a customized setup for Linux	403
Editing Setup Properties (only Windows)	404
Deleting a Setup	405
Audit Trail	406
License	407
Adding and Activating a License	407
Moving Licensed Computers to Non-Licensed Computers	408
Moving Non-Licensed Computers to Licensed Computers	409
eScan Mobility Management	411
Getting Started	412
Dashboard	413
Deployment Status	414





Enrollment Status	415
eScan Status	415
eScan Version (Android - MDM App)	416
eScan Version (Android - Container App)	416
eScan Version (iOS - MDM App)	417
Android Version	417
iOS Version	418
Device Sync Status (Successful)	418
Device Compliance	419
Kiosk Status	419
Protection Status	420
Update Status	421
Scan Status	421
Anti-Virus	422
Web Control	422
Application Control	423
Call and SMS Filter	423
Firewall Status	424
Protection Statistics	425
Anti-Virus	426
Web Control	426
Application Control	427
Call Statistics	427
SMS Statistics	428
Settings	429
Managed Mobile Devices	430
Action List	430
Creating a New Group	432
Adding a New Device	433
Adding Multiple Devices	434
Removing a group	436
Changing Server IP address	436
Synchronizing with Active Directory	438
Client Action List	441
Moving Devices from one group to the other group	441
Checking a Device's Properties	443
Removing a device from group	444
Resending Enrollment Email	444
Changing a User's Name/Email ID	445





Disenrolling a device	445
Select/Add Columns	446
Policy Templates	447
Steps for Defining Policies for the Group	447
Creating New Template	448
Android Template	449
Anti-Virus Policy	450
Call & SMS Filter Policy	452
Web and Application Control	461
App Specific Network Blocking	467
Anti-Theft Policy	468
Additional Settings Policy	470
Password Policy	471
Device Oriented Policy	471
Required Applications Policy	473
Importing an application	473
Deleting an application from "Required Applications Policy"	475
Wi-Fi Settings Policy	476
Enable Wi-Fi Restrictions (For devices with Android version below 6.0)	476
Adding a Wi-Fi SSID	477
Deleting a Wi-Fi network SSID	478
Scheduled Backup (Contacts & SMS)	479
Creating a schedule	479
Modifying a schedule	481
Deleting a schedule	482
Content Library Policy	483
Import a file	483
Kiosk Mode Policy	
Location Fencing	502
iOS Template	503
Device Passcode Policy	504
Restrictions Policy	506
WebClip Policy	511
Adding a WebClip	511
Deleting a WebClip	512
Email Policy	513
Adding Email policy	513
Deleting an Email Policy	517
Wi-Fi Settings Policy	518





Adding a WiFi Settings Policy	518
Deleting a WiFi Settings Policy	519
Content Library Policy	520
Importing a file	520
Deleting a file	520
Required Applications Policy	521
Importing an application	521
Deleting an application	522
Group Tasks	523
Creating a New Group Task	523
Installation and Enrollment of Android Device for MDM Group	525
Adding a device to the console	525
Installation and Enrollment of Android Device for COD and BYOD Group	534
Adding a device to the console	534
Enrolling the added device	535
Differences between COD and BYOD group	543
Installing eScan Container app	544
Installation and Enrollment of iOS Device	551
Adding a device to the console	551
Enrolling the added device	552
Manage Backup	565
Taking a backup from devices to the server	565
Anti-Theft	568
Wipe Data	569
Block Device	570
Unblock Device 💮	
Scream	
Send Message	
Locate Device	
Remove work Profile 💮	573
Asset Management	
Asset Management – Hardware Information	
Viewing Hardware information	
Asset Management – Application Information	
Filtering the Application information	
Asset Management – Export Options for the Generated Reports	
Exporting a Report	





Report Templates	578
Creating a Report Template	578
Editing a Report Template	580
Deleting a Report Template	581
Viewing a Report	581
Report Scheduler	582
Adding a Scheduler	582
Running a schedule	587
Editing a Schedule	588
Deleting a Schedule	588
Viewing the report	589
Viewing results of a report	589
Events and Devices	590
Viewing Events	590
Settings	595
Certificate Management	595
Importing an SSL certificate	596
Email Notification Settings	597
Data Purge	598
Connection Sequence	598
App Store	599
Adding an Android application with In-House Apps (Android) option	599
Adding an Android application with Play Store Apps (Android) option	601
Adding an iOS application	602
Deleting an application from the App Store	603
Content Library	604
Adding a file	604
Editing a file description	605
Deleting a file	606
Call Logs	607
Data Usage	608
History	609
Location History	609
Battery Status/Signal Strength	610
Geo Fence History	610
App Usage History	611
Fencing Location(s)	612
Creating a Fencing Location	612
Editing a Fencing Location	613





Deleting a Fencing Location	614
View On Map	614
Administration	615
User Accounts	615
Creating a User Account	616
Adding a User from Active Directory	617
Deleting a User Account	618
User Roles	619
Adding a User Role	620
Role Properties	623
Deleting a User Role	623
Contact Us	624
Forums	624
Chat Support	624
Email Support	624





Introduction

eScan Endpoint Detection and Response (EDR) is a comprehensive, integrated, and layered endpoint protection solution that combines real-time monitoring and endpoint data analytics with rule-based responses. This helps to analyze and alerts admin about the malicious activity, and allows fast investigation and restricts the attacks on endpoints as soon as detected. It supports automated and manual actions to restrict the potential threats on the endpoint.

eScan EDR solution helps to gain deep insights into the attack to identify the security gaps and demonstrate the impact of the incidents. It provides security team with the tools to proactively identify threats and protect the organizations.

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

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

Pre-requisites for eScan Enterprise EDR 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).

If authentication for the mail server is mandatory for accepting emails, you will NOTE 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 / 11 / 10 / 8.1 / 8 / 7 / Vista / XP SP 2 / 2000 Service Pack 4 and Rollup Pack 1 (For 32-bit and 64-bit Editions)	OS X Snow Leopard (10.6 or later) OS X Lion (10.7 or later) OS X Mountain Lion (10.8 or later) OS X Mavericks (10.9 or later) OS X Yosemite (10.10 or later) OS X El Capitan (10.11 or later) macOS Sierra (10.12 or later) macOS High Sierra (10.13 or later) macOS Mojave (10.14 or later) macOS Catalina (10.15 or later) macOS Big Sur (11.0 or later) macOS Monterey (12.0 or later)	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) Ubuntu 12 and above (32 and 64-bit) Mint 12 and above (32 and 64-bit) Linux Oracle 7.x and above (32 and 64 bit) Red Hat Linux server (32 and 64 bit)
Hardware Requirements for eScan Server: CPU - 2GHz Intel [™] Core [™] Duo processor or equivalent Memory - 4 GB and above Disk Space (Free) – 8 GB and above		
Hardware Requirements for eScan Client:	Hardware Requirements for eScan Client:	Hardware Requirements for eScan Client:
CPU - 1.4 GHz minimum (2.0 GHz recommended) Intel Pentium or equivalent Memory - 1.0 GB and above	CPU - Intel based Macintosh Memory –2 GB and More recommended	CPU - Intel® Pentium or compatible or equivalent Memory –2 GB and above
Disk Space (Free) – 1 GB and above	Disk Space – 2 GB and above	Disk Space – 2 GB free hard drive space for installation of the application and storage of temporary files





eScan Management Console can be accessed by using following browsers:

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

For Android

(Android Endpoints) Platforms Supported:

- Android version: 5.0 and above
- Storage: 40-50 MB

For iOS

(iOS Endpoints) Platforms Supported:

- iOS version: 10.3 and above
- Storage: 40-50 MB

Rooted and Jailbroken devices are not supported.





Installing eScan Enterprise EDR Server

• Installing eScan Enterprise EDR Server from CD/DVD

Installing eScan Enterprise EDR (with MDM & Hybrid Network Support) from the CD/DVD is very simple, insert the CD/DVD in the ROM and wait few seconds for the Autorun to run the installation wizard. In case the installation wizard does not run automatically, locate and double-click the **EDRcwn4k3ek.exe** on CD-ROM. This will run the installation wizard based setup of eScan Enterprise EDR (with MDM & Hybrid Network Support). To complete the installation, follow the instructions on screen.

• Downloading and installing eScan Enterprise EDR Server from internet

To download the setup file click <u>here</u>. To install eScan Server from the downloaded file, double click the **EDRcwnxxxx.exe** and follow the instructions on screen to complete the installation process.





Installation

To install the eScan Enterprise EDR (with MDM & Hybrid Network Support), 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**.

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

The installation wizard welcomes you.

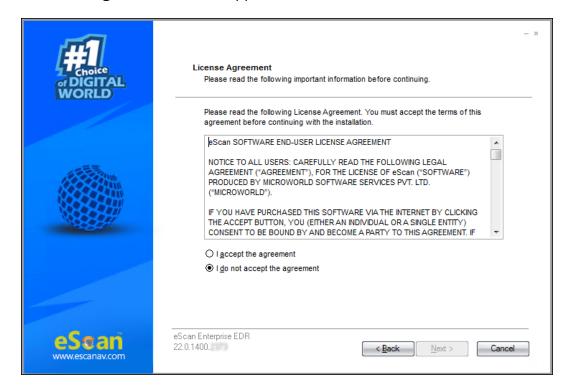
The transfer	 Welcome to the eScan Enterprise EDR Setup Wizard Welcome to the eScan Enterprise EDR Setup Wizard Click Next to continue, or Cancel to exit Setup. 	
eSoan www.escanav.com	eScan Enterprise EDR	

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





License Agreement screen appears.



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

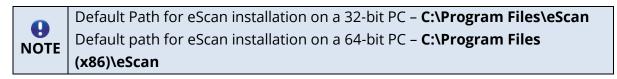
or DIGITAL WORLD	Select Destination Location Where should eScan Enterpr	rise EDR be installed?	
	Setup will install eS	can Enterprise EDR into the following folder.	
	To continue, click Next. If you	u would like to select a different folder, click Browse.	
	<u>Ci∖Program Files∖eScan</u>	Browse	
	At least 1,839.9 MB of free d	lisk space is required.	
eSoan www.escanav.com	eScan Enterprise EDR 22.0.1400.	< <u>B</u> ack Cance	əl





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.



	Ready to Install Setup is now ready to begin installing eScan Enterprise EDR on your computer.	- *
	Click Install to continue with the installation, or click Back if you want to review or change any settings. Destination location: C:\Program Files\eScan	
eSean	eScan Enterprise EDR	
eSoan	eScan Enterprise EDR 22.0.1400	

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.

#1	Welcome to the eScan Management Console Configuration Wizard
DIGITAL WORLD	This installation wizard will guide you through the steps required to install and/or configure Microsoft SQL Server Express for eScan Management Console application on your computer. Note: Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
	Click "Next" to continue.

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





elect computer hosting SQL	Server.
🔵 Use local instance	
Install Microsoft SQL Server E	xpress Edition (recommended)
SQL Server Installation Path	C:\Program Files\Microsoft S(Browse
Choose existing	
SQL Server Name	Browse

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.

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

• 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.



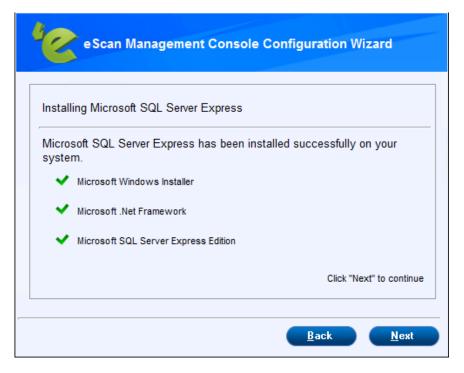


 After selecting an option, click Next to proceed.
 If you selected the recommended option, the configuration wizard will begin installation of the Microsoft SQL Server Express.

e Scan Management Console Configuration Wizard
This wizard will install following prerequisites along with Microsoft SQL Server Express: Microsoft Windows Installer
Microsoft .Net Framework
Microsoft SQL Server Express Edition
Click "Install" to proceed.
<u>B</u> ack <u>N</u> ext

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.

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

Scan Management Co	onsole login information
Enter the login credentials f Scan Management Consol	or the root user to give permission to manage the e.
User name:	root
Description:	Administrator account created during installation
Email address:*	
Password:*	
Confirm Password:*	
	Click "Next" to continue

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.

#1	- %	
	Completing the eScan Enterprise EDR Setup Wizard To complete the installation of eScan Enterprise EDR, Setup must restart your computer. Would you like to restart now?	
eSoan www.escanav.com	eScan Enterprise EDR 22.0.1400.	

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

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







Components of eScan Server

The eScan Server is comprised of following components:

• eScan Server

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

Agent

It manages the connection between the eScan server and the client computers.

• eScan Management Console

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

• Microsoft SQL Server Express Edition

It is a database for storing events and logs already included in the eScan Setup file.

• Apache

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

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

OVE 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:

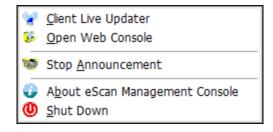
- 1. Launch a web browser.
- 2. Enter the following URL: <IP address of the eScan Server installed system>:10443 Web console login page appears.

	eScal Enterprise EDR - Management Cons	n ole
· · · · · ·	Sign in	
	User Name	4
	Password	
	Login	0000
	eScan AV Report Setup Links	RENGERTS OF
		P
	And the second s	Constanting of the second s

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

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

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



2. Click Open Web Console.

Default browser launches and displays web console login page.





Rests of the options are explained below:

Client Live Updater

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

Date	Time	Machine Na	IP Address	User Name	Event ID	Module Name	Descri -
30 Jul 2021	12:22:26	WHW SISPER	1132 1148 (0.41)	WING SEPTEM	File Anti	[C] eScan M	Windo
30 Jul 2021	12:22:26	WHIN SISPER	1152 1168 (2.67)	WING SIGPRO	File Anti	[C] eScan M	C:\Pro
30 Jul 2021	12:22:27	WHILE SERVER	1112 1148 (2.47)	WING SIGPRE	File Anti	[C] eScan M	Admini
30 Jul 2021	12:22:28	WHILE SERVER	1152 1148 (2.47)	WING SIGPRE	File Anti	[C] eScan M	REMO
30 Jul 2021 👘	12:22:29	WHEN SIGHT	1112 1148 (1.47)	WITH SISTER	File Anti	[C] WinEvent	A logo
30 Jul 2021 👘	12:22:30	WHEN SIGHT	1112 1148 C.47	WITH SEPTEM	File Anti	[C] WinEvent	Remot
30 Jul 2021	12:22:32	WHEN SIGPTO	1112 1148 (2.47)	WING SISPER	File Anti	[C] eScan M	REMO
30 Jul 2021	12:22:36	WHILE SERVICE	1152 1148 (2.47)	WING SIGPRE	File Anti	[C] eScan M	REMO
30 Jul 2021	12:32:03	751136043105		Chevice, Nex.	File Anti	Android	Policy
30 Jul 2021	12:32:03	7511303643105		Chevillae Niew	File Anti	Config(Andr	Auto s
30 Jul 2021	12:32:03	751130363205		Chevillan Nime	File Anti	Anti-Theft (A	Anti-T1
30 Jul 2021 👘	12:32:03	7511 (BLID # 2015)		CARANGE MARK	File Anti	Web and A	Web C
30 Jul 2021 👘	12:32:03	7511 JB (1946) 2045		CARANCE NAME	File Anti	Web and A	Applic
30 Jul 2021	12:32:04	751130304(2015)		Cheville, New.	File Anti	Config(Andr	Protec
30 Jul 2021	12:32:04	7511 3818-8,2935		CARVINE MARK	File Anti	Call & SMS	Call/SI-
30 Jul 2021	12:32:04	7511381843285		Chevillan Manu.	File Anti	Android	Compli
30 Jul 2021	13:32:09	75日18日6月18日		Canvice Name	File Anti	Android	Policy
4		111		-			

Stop Announcement

Clicking this option stops broadcast from and towards the server.

About eScan Management Console

Clicking this option displays Server Up Time and general information.

Shut Down

Clicking this option shuts down the eScan Management console.

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





Setup Links

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

<	
eScan Client Setup (Windows)	\sim
eScan Client Setup (Android)	\sim
eScan Agent Setup (Windows)	\sim
eScan Agent Setup (Linux)	\sim
eScan Agent Setup (MAC)	\sim

• eScan Client Setup (Windows)

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

• eScan Client Setup (Android)

This link can be shared via email to the android users where remote installation is impossible. By clicking this link users can download the EMM application from eScan Client Setup and install it manually on their android device. Users can also directly access the eScan Management console from their Android device.

• eScan Agent Setup (Windows)

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

• eScan Agent Setup (Linux) This link can be shared with the Linux computer user for manual installation.

• eScan Agent Setup (Mac)

This link can be shared with the Mac computer user for manual installation.





eScan AV Report

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

eScan AV Rep	DOTT Sefresh 👔 He
Filter Criteria Select Group	Installation Status All Last Updated All Last Scanned All
	1 - 0 of 0 ((page 1) of 0) → H Rows per page: 10 ∨
<u>Machine Name</u> Group Last Connection Offline Since Installation Stat There are no items	us eScan Version Last Update Last Scanned Last Policy Applied to show in this view.

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

		eScan A	V Report			\$	Refresh	👔 Helj
Filter Criteria								
Select Group			Installation Sta	itus				
🗄 🗹 🪞 Man	naged Computers		All	~				
			Last Updated	~				
			Last Scanned					
			All	~				
Get Details	Reset Export		Search					
Total Machines		5						
Installed Machines		5	Not Installed Machines					0
Last Updated Comp Last Scanned Comp		4	Last Updated Non Com Last Scanned Non Com					1
								-
			1 - 5 of 5	i H (page 1 of	1	I Rows	per page:	10 🗸
Machine Name	Group	Last Connection	Offline Since	Installation Status	eScan Version	Last Update	Last Scan	ned La
4(1)(17-2-1196	Managed Computers	6/24/2021 3:26:20 PM	Offline more than 0 days	Installed	7.1.9	2021/06/24 08:49		83
MINUP-2-136 BECMIN_CLIENT	Managed Computers	6/24/2021 3:26:20 PM 6/23/2021 5:40:54 PM	Offline more than 0 days Offline more than 0 days		7.1.9	2021/06/24 08:49 2021/06/14 15:43	06/23/202	
				Installed			06/23/202	
EBGHN_CUIENT	Managed Computers	6/23/2021 5:40:54 PM	Offline more than 0 days	Installed Installed	54.0.5400.2200	2021/06/14 15:43	06/23/202	

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.

The links in the top right corner are explained below:



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

Username ወ

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

Edit User		👔 Help
Enable thi	s account	
Account Typ	e and Information	
Custom Acco	punt	
User's name:	nat	
Full Name*:	Administrator account created during installation	
New Password:	•	
Confirm Password:	•	
Email Address:	pre-Taille and com	
	For Example: user@yourcompany.com	
Account Rol	e	
Role*:	Administrator 🗸 🗸	
MDM Role*:	Administrator V	
Save	Close	(*) Mandatory Fields



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

Date of Virus Signatures

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





Setup Wizard

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

Setup Wizard	Help
Welcome to the Setup Wizard	
This Wizard helps to create Groups, select computers for respective Groups and installation of eScan on selected Groups.	
Click "Next" to Proceed.	
Next >	

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

Setup Wizard	<u>?</u> Help
Create Group to Manage Computers.	
庄 💼 Managed Computers	
New Grou	up
Click "Next" to Proceed.	
<pre></pre>	





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

	X
Creating New Group	🛜 Help
Create New Group	
Ok Cancel	

Enter the name of the group and click **OK**.

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

Setup Wizard	👔 Help
Create Group to Manage Computers.	
Managed Computers Gaming Users Linux / Mac Samples_Team	
New Group	
Click "Next" to Proceed.	





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

- IP Address/Host name
- Host from Network Computers

Setup Wizard	👔 Help
Add IP/Host to respective Groups.	
Add IP/Host	
🖻 🧰 Managed Computers	
- 🛅 Roaming Users	
🗄 💼 Linux / Mac	
Samples_Team	
Click "Next" to Proceed.	
< Back Next >	

Adding computers via IP Address/Host Name

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

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

Add Computers	🝸 Help
	Add
	Add IP Address Range
	Remove
	-
Ok Cancel	





2. Click Add. Add Computers window appears.

Select Computer	👔 Help
Ok Cancel	

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

OR

4. To add an IP range, click **Add IP Address Range**. Add Computers by IP Range window appears.

Add Computer By IP Range	🝸 Help
Starting IP Address*:	
Ending IP Address*:	· · · · · · · · · · · · · · · · · · ·
Ok Cancel	(*) Mandatory Fields

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





Adding Host Name from Network Computers

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

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

Add Host from Network Computers	<u>?</u> Help
🗄 🗆 🌧 Network Computers	
🗄 🗋 🌧 Microsoft Windows Network	
🛄 🗌 💑 Web Client Network	
Ok Cancel	

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

Add IP/Host	Add Host from Network Computers	
🗄 🪞 Managed Co	omputers	
··· 📢 🖬		
🚺 W1 H Court		
···· 📃 WII in the second	17	
🗄 🧰 Rommu	Line 14	
÷ 📄 PL	(CTORA)	
🔁 QA-11		-





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

Setup Wizard	👔 Help
Select Groups for Installation/Deployment.	
Ė 🗋 🫅 Managed Computers	
👰 QA: INVERTICUE	
📫 Within Ell	
··· 🛃 With Class & Comminent	
🖸 🛅 Roaming Users	
🗄 🗋 🛅 Linux / Mac	
Click "Next" to Proceed.	
< Back Next >	

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

etup Wizard	<table-cell></table-cell>
lient Configuration.	
Auto Reboot after Install	
Show Progress on Client (Only for XP/2000)	
Install Without Firewall	
Disable auto downloading of Windows patches by eScan	
Installation Path	
<default> Add</default>	
Note: Computers with same or newer version of eScan will not be affected.	
Click "Next" to proceed with Installation/Deployment	
< Back Next >	

Client Configuration window appears

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

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





Navigation Panel

***	DashBoard
Ś	EDR Dashboard
* ;^ +	Setup Wizard
<u>i</u>	Managed Computers
ģ	Unmanaged Computers 🗸 🗸
1= =0	Report Templates
	Report Scheduler
Ē	Events & Computers
0	Tasks For Specific Computers
۲	Asset Management
₽Ē	User Activity 🗸 🗸
88	Patch Report
(<u>)</u>)	Notifications 🗸 🗸
ቑ	Settings 🗸 🗸
2	Administration 🗸 🗸
٩	License
0	eScan Mobility Management
	eScan Enterprise EDR





Dashboard

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

EDR Dashboard

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

Setup Wizard

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

Managed Computers

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

Unmanaged Computers

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

Report Templates

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

Report Scheduler

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





Events and Computers

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

Tasks for Specific Computers

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

Asset Management

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

User Activity

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

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. To learn more, <u>click here</u>.

Notifications

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





Settings

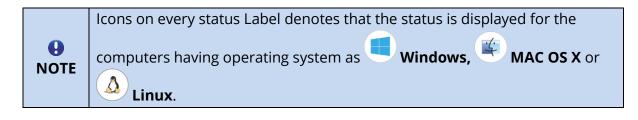
The Settings module lets you configure eScan Console timeout settings, dashboard setting, exclude client settings for eScan. To learn more, <u>click here</u>.

Administration

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

License

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







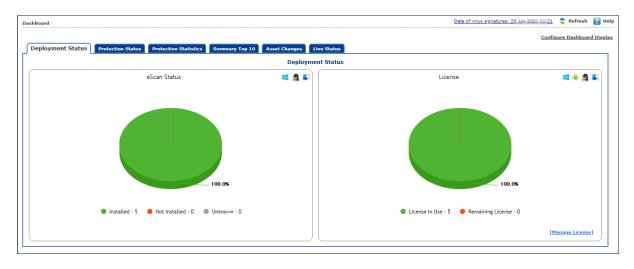
Dashboard

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

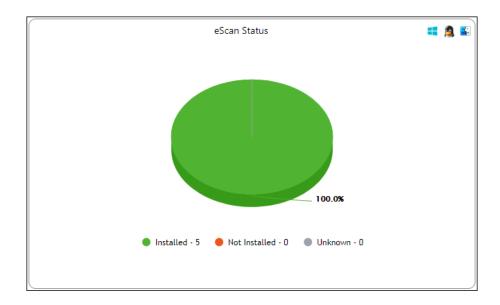
This tab displays information about eScan Client installed on computers, active licenses, and current eScan version number in use.







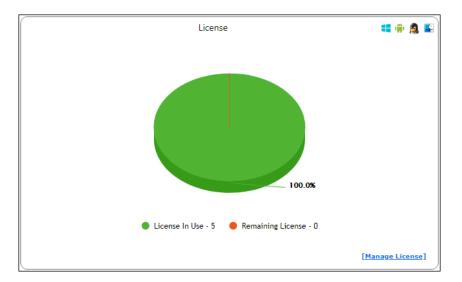
eScan Status



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)

License



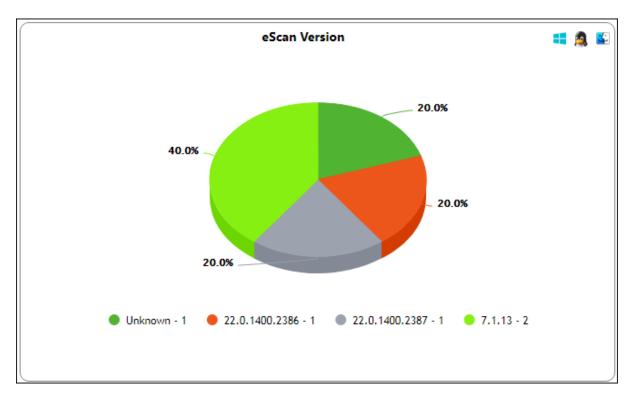
License in Use - It displays the number of licenses that are active. **Licenses Remaining** - It displays the number of remaining licenses.





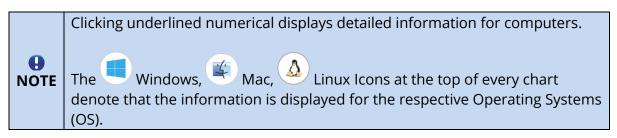
eScan version

The eScan Version chart shows the total number of eScan versions installed on the computers 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
BERVER	-2111-220	Managed Computers
WIN-QADD?	14.0.	Managed Computers
	Close	

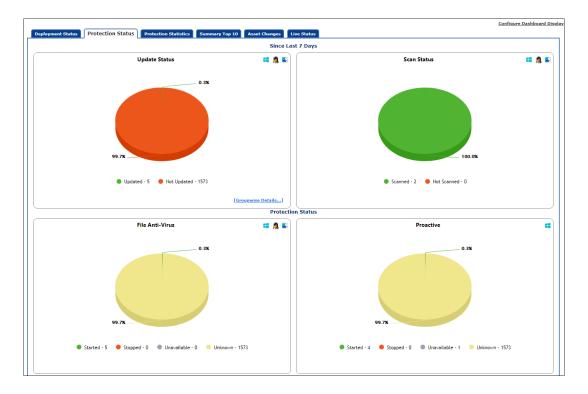






Protection Status

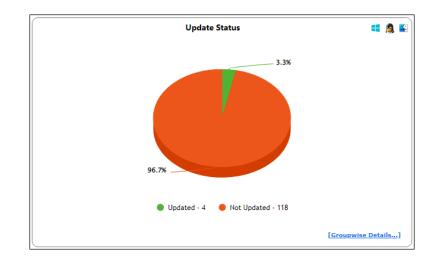
This tab displays the status of eScan Client's modules along with the Update and Scan status since last 7 days.







Update Status



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

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

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

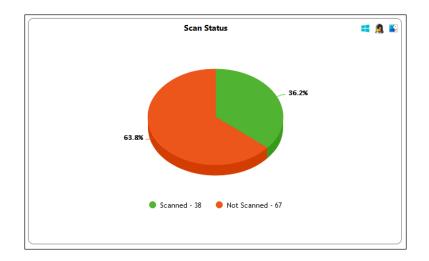
Groupwise Update Status							-	Tuesda	y, Jun	e
🗄 🗂 Managed Computers	🗌 Include Sub Groups 🗹 G	roupwise Details								<u>Print</u>
	Group: Managed Computer	s (Include Sub Grou	ıps)							
	Group Name	Updated	Not Updated	<u>License in Use</u>	EP	<u>E0</u>	<u>СР</u>	<u>co</u>	ш	NA
	Managed Computers	2	0	2	1	0	1	0	0	0
	21 TEXH	0	1	1	0	0	0	0	0	1
	Ed. TEAM	1	0	1	0	0	<u>1</u>	0	0	0
	Samples Team	1	0	1	0	0	1	0	0	0

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





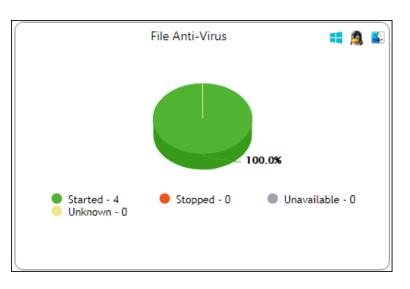
Scan Status



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.

File Anti-Virus



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

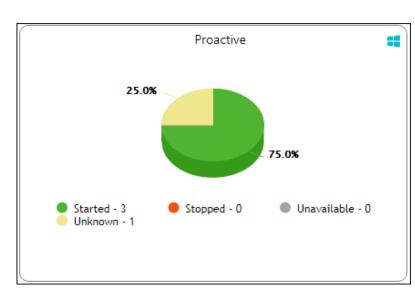
Stopped – It displays the number of computers on which the File Anti-Virus module is in Stopped state.

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





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



Proactive

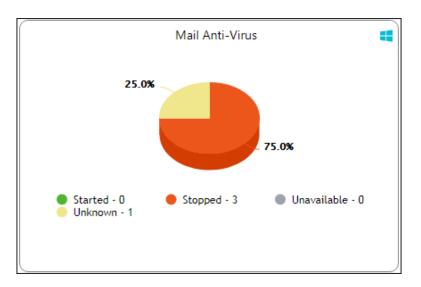
Started - It displays the number of computers on which Proactive scanning service is running.

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.

Mail Anti-Virus







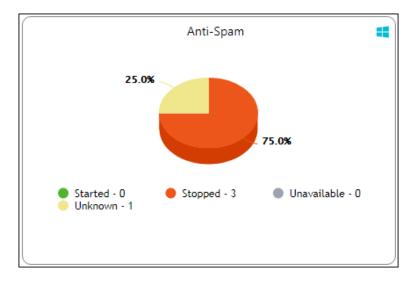
Started – It displays the number of computers on which the Mail Anti-Virus module is in Started state.

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

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

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

Anti-Spam



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

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

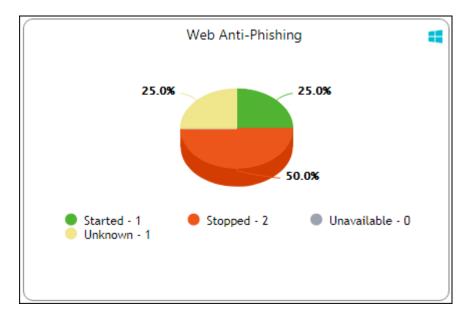
Unknown – It displays the number of computers on which the Anti-Spam module status is Unknown.

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





Web Anti-Phishing



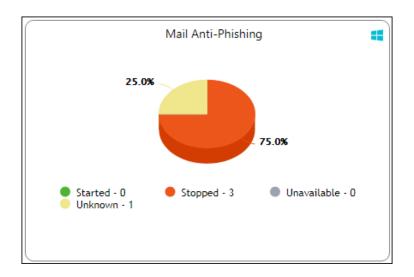
Started – It displays the number of computers on which the Web Anti-Phishing service is started.

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.

Mail Anti-Phishing







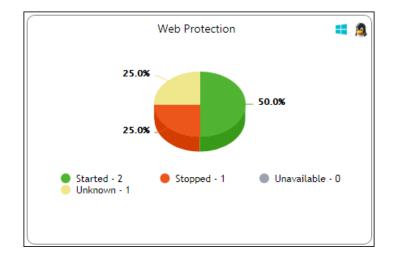
Started – It displays the number of computers on which the Mail Anti-Phishing service is enabled.

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.

Web Protection



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

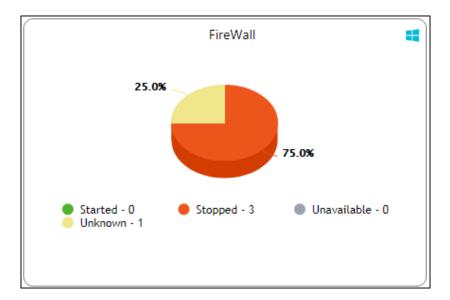
Stopped – It displays the number of computers on which the Web Protection module is in Stopped state.

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

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



Firewall



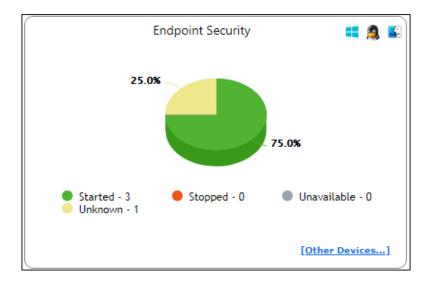
Started - It displays the number of computers on which the Firewall module is in Started state.

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

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

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

Endpoint Security







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

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

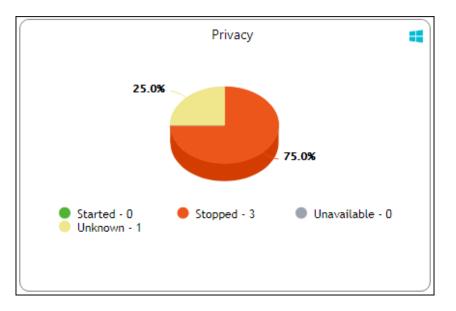
Unavailable – It displays the number of computers on which the Endpoint Security module is unavailable.

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

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

Other Devices	Allowed	<u>Blocked</u>	<u>Unavailable</u>	<u>Unknown</u>	<u>Tota</u>
SD Card	<u>3</u>	<u>o</u>	<u>0</u>	1	<u>4</u>
Web Cam	<u>3</u>	<u>0</u>	<u>0</u>	<u>1</u>	<u>4</u>
Bluetooth	<u>3</u>	<u>0</u>	<u>0</u>	1	<u>4</u>
USB Modem	3	<u>0</u>	<u>0</u>	1	<u>4</u>
Composite Devices	<u>3</u>	<u>0</u>	<u>0</u>	1	<u>4</u>
CD/DVD	<u>3</u>	<u>0</u>	<u>0</u>	1	<u>4</u>
Imaging Devices	3	<u>0</u>	<u>0</u>	1	<u>4</u>
WI-FI	<u>3</u>	<u>0</u>	<u>0</u>	1	<u>4</u>
Printer	3	0	0	1	4

Privacy





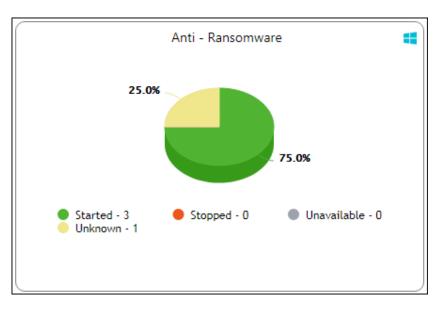


Started - It displays the number of computers on which the Privacy Control module is in Started state.

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

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

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



Anti – Ransomware

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

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

Unavailable – It display the number of computers on which the Anti – Ransomware module unavailable to system.

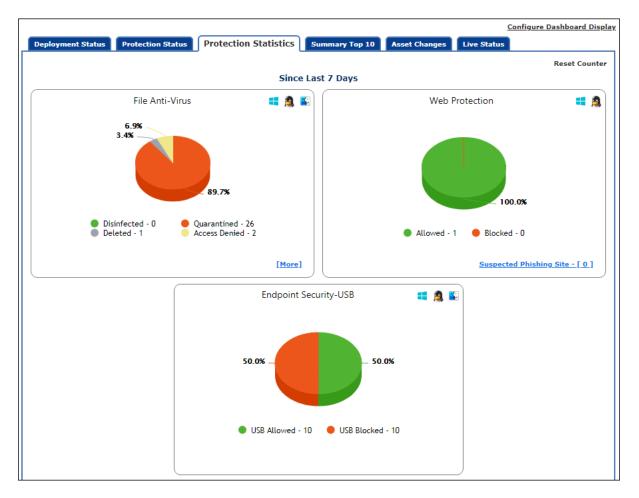
Unknown - It displays the number of computers on which the Anti – Ransomware module status is unknown.





Protection Statistics

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



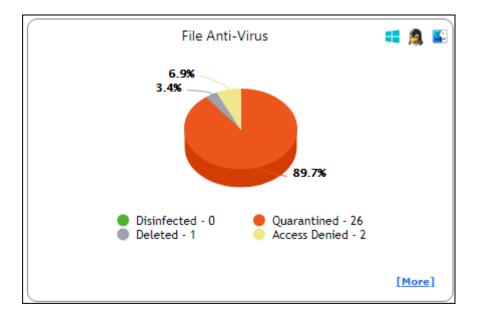
Reset Counter

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





File Anti-Virus



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

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

Protection Statistics >> File Anti-Virus >> Quar	antined	💶 🙇 🗳
Client OS Type All		Print
Machine Name	<u>Status</u>	Group
ESCAR_CLIBRAT	Quarantined (2)	Managed Computers\:
WINGEDCHNEERAER	Quarantined (14)	Managed Computers
WIN-Geddiff	Quarantined (10)	Managed Computers\ AM
	Close	





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

Protection Statistics >> File Anti-Virus >> Quarantined (WINE 10.4 Minute)				
			Print	
Date/Time	File Name	Description	<u>User name</u>	
23/06/21		Infected by Virus:	W	
10:53:14	\\192 11.1.21 and a mail barry if asharif as mulas after, exe	Trojan (Seneric) (S. et a 785 33 (S. et a)	ESCHISER/EE/Administrator	
23/06/21		Infected by Virus:	Witte	
10:53:15	\\192 11.1 21 and a mail terms if aeriant semiclasi and exe	Trojan, Seneral Constitution (04)	EDC#NDEF./EF/Administrator	
23/06/21		Infected by Virus:	W	
10:53:16	\\192, 11 if bt a damai hang it adharif as malas had, exe	Trojan (Seneric) (S. et al 20 (et al (0.0))	ESCHINER/Administrator	
23/06/21		Infected by Virus:	W	
10:53:16	\\192. Its is the mail hang if and and annual notification, exe	Trojan.Autorum (Severic) (35.45036404 ((34))	ESCHIOER/ER/Administrator	
23/06/21		Infected by Virus:	W	
10:53:16	\\192, to it as a new all here it and and a maine all fills, exe	Trojan.Ceneric#Cheb133768 (38)	ESCHIGER/ER/Administrator	

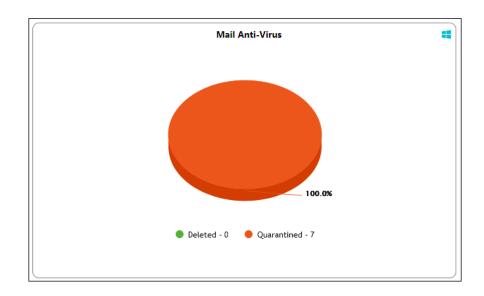
Clicking [More] displays additional protection statistics.

ditional protection statistics	
Malware URL Block	2
Autorun Block	<u>0</u>
Executable Block USB	<u>0</u>
Executable Block Network	<u>0</u>
Executable Block User based	<u>4</u>
Proactive Statistics: Allow	<u>0</u>
Proactive Statistics: Block	2
Exploit Statistics Block	<u>0</u>
Ransomware Statistics Block	<u>Z</u>
Total	<u>15</u>





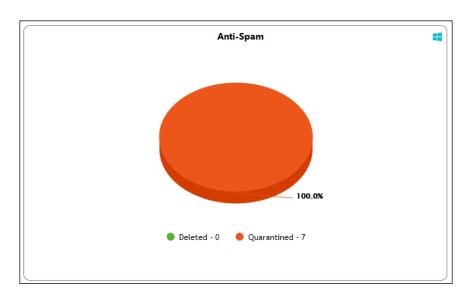
Mail Anti-Virus



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.

Anti-Spam



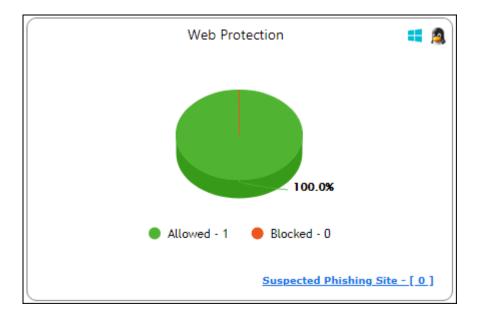
Deleted – It displays the number of files deleted by Anti-Spam module.

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





Web Protection



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

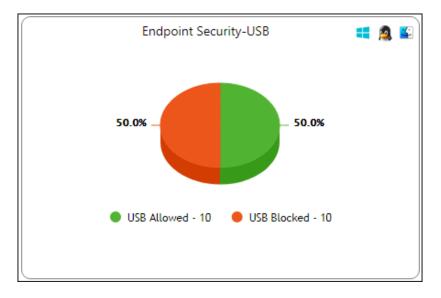
Blocked – It displays the number of websites to which access was blocked by Web Protection module.

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





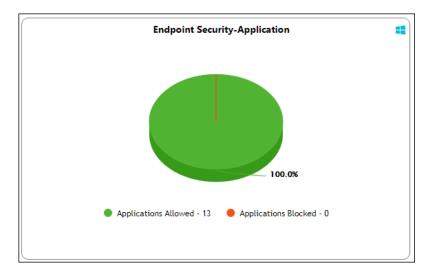
Endpoint Security-USB



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

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

Endpoint Security-Application



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

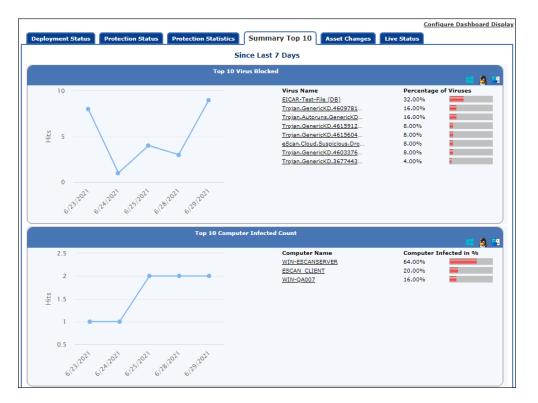
Applications Blocked – It displays the number of applications blocked by Endpoint Security-Application module.





Summary Top 10

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



The tab displays the summary for following parameters:

- Top 10 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.

				Configure Dashboard [
Deployment Status Protection St	atus Protection Statisti	cs Summary Top 10	Asset Changes	Live Status
	-	_	0	
		Since Last 7 Days		
		Hardware Changes		
	Description	Machine Co	ount	
	RAM		1	
	CPU		0	-
	MOTHERBOARD HARD DISK		0	-
	L HARD DISK		v	J
	5			
		Software Changes		
	Machine Name N	ew Installed Softwares	Uninstalled Softwares	
	WITH E SCANNER WEEK.	1	0	
	WINCOMMEN	3	1	
				J

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.

					Configure Dashboard Display
Deployment Status Protection Status	Protection Statistics	Summary Top 10	Asset Changes	Live Status	L
		Live Status			
	l	Live Status	= 🙎	1 🗳	
		100	.0%		
	Onl	line - 4 🛛 🔴 Offline -	0		

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.

	E.
Configure Dashboard Display	
Deployment Status	1
eScan Status	eScan Version
License Summary	
Protection Status	
✓ Update Status	Scan Status
File Anti-Virus	Proactive
Mail Anti-Virus	Anti-Spam
FireWall	Mail Anti-Phishing
Web Protection	Web Anti-Phishing
Endpoint Security	Privacy
Anti-Ransomware	
Protection Statistics	
File Anti-Virus	Mail Anti-Virus
Anti-Spam	Web Protection
Endpoint Security-USB	Endpoint Security-Application
Summary Top 10	
Machine Infected	USB Blocked
Application Allowed by Computer	Application Blocked by Computer
Website Blocked by Computer	Website Allowed by Computer
Application Blocked by App Name	Application Allowed by App Name
Website Blocked by Sites	U Website Allowed by Sites
Website Blocked by Username	Website Allowed by Username
Infected Emails	Spam Emails
Virus Blocked	Exploit Blocked
Live Status	
Live Status	
Graph Type	
Show 3D Graph	
Ok Cancel	

- 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.





EDR Dashboard

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

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

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

Incident - eScan

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

R DashBoard							\$	Refresh 👔 He
Incident - eScan	Incident - Windows	s Incident -	EDR End Point Incident	Network Incident				
 Filter Criteria 	-				▲ Exp	port Option		
		Troj	an. Demeniation Model 10411 (DB): 3.0%					
		Troj	an Develop (DB): 3.0%				Trojan.Automatic Deneration of the Distance (DB): 18.2%	
		Troj	an. Demonstration and introduced (DB): 3.0%					
		1	JRuler.exe:7808 (ppid:7432) : 0.0%					
			15 (DB): 15.2%				Trojan. 68 (DB): 15.2% Trojan. 8 (DB): 15.2%	
	1		1	1				per page: 100
Client Date	Computer Name/Ip	IP Address	<u>User's name</u>	Local Adapter	<u>Wifi Adapter</u>	USB Adapter	File Infected	Action Taken
	WIN COLORADOR IN R	192.000.000	WINCOMMER\Administrator	00-0C-29-20-9A-C3			C:\teating all on.exe	File Quarantine
7/2/2021 12:42:31 PM								
7/2/2021 12:42:31 PM 7/2/2021 3:05:50 PM	WINGSCHNODUNER	192.008.0.039	WI R\Administrator	00-0C-29-20-9A-C3			C:\c.exe	File Quarantin
	WIN COCHNODINER WIN COCHNODINER		WI R\Administrator				C:\cexe C:\exe	File Quarantin
7/2/2021 3:05:50 PM 7/2/2021 3:05:50 PM	WIN EDGANDER/IER	192		00-0C-29-20-9A-C3				
7/2/2021 3:05:50 PM 7/2/2021 3:05:50 PM	WIN EDGANDER/IER	192.048.0.079	WIN CONTRACTOR R\Administrator	00-0C-29-20-9A-C3 00-0C-29-20-9A-C3			C:\\	File Quarantin
7/2/2021 3:05:50 PM 7/2/2021 3:05:50 PM 7/2/2021 3:05:50 PM 7/2/2021 3:05:51 PM	WI R WI R	192	WIN COMMENTER R\Administrator	00-0C-29-20-9A-C3 00-0C-29-20-9A-C3 00-0C-29-20-9A-C3			C:\\aad_wad.exe C:\\aad_wad.exe C:\\aad_wad.exe	File Quarantin File Quarantin File Quarantin
7/2/2021 3:05:50 PM 7/2/2021 3:05:50 PM 7/2/2021 3:05:50 PM	WI R WI R	192.000.0.079 192.000.0.079 192.000.0.079 192.000.0.079	WII R\Administrator WI R\Administrator WI R\Administrator	00-0C-29-20-9A-C3 00-0C-29-20-9A-C3 00-0C-29-20-9A-C3 00-0C-29-20-9A-C3			C/Ver factors for a first factor	File Quarantin File Quarantin File Quarantin File Quarantin





Filtering Incident – eScan Report

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

Incident - eScan Incident - Windows Incident - EDR End P	oint Incident Network Incident		
▲ Filter Criteria		A Export Option	
- Filter Criteria			
Computer Name	* v Include V	✓ IP Address	* Include V
✓ User's name	* Include ¥	MAC Adapter(s)	* v Include v
Description	* Include 🗸	Action Taken	* Include 🗸
Date Range From (MM/DD/YYYY)	06/28/2021		
To (MM/DD/YYYY)	06/28/2021		
	00/20/2021		
Search Reset			(*) View All Items

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

Include/Exclude

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

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

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

E	DR DashBoard							\$	Refresh 👔 Help
	Incident - eScan	Incident - Window	. Tostiont	EDR End Point Incident	Network Incident				
Г		Incluent - Window	s Incident	EDK End Point Incident	verwork incident				
	 Filter Criteria 					A Ex	port Option		
			Troj	an. Deteriol (DB): 3.0%					
			Troj	an (Deterior) (DB): 3.0%				Trojan	
			Troj	an. Demonical Completion (DB): 3.0%					
			١	JRuler.exe:7808 (ppid:7432) : 0.0%					
			Troja	n. Demended et 11 22 (DB): 12.1%	-1				
								Trojan. 48 (DB): 15.2%	
			Troja	n Denericiti estimati (DB): 15.2%	-				
								Trojan8 (DB): 15.2%	
			Troja	n Denericiti et (10)42 (DB): 15.2%				(DD): 13.2%	
								1 - 37 of 37 { { page 1 of 1 } } Nows	er page: 100 🗸
	Client Date	Computer Name/Ip	IP Address	User's name	Local Adapter	Wifi Adapter	USB Adapter	File Infected	Action Taken
	7/2/2021 12:42:31 PM	WINDOWNDR	192.048.0.075	WI WI MINISTRATING R\Administrator	00-0C-29-20-9A-C3			C:\text on.exe	File Quarantine
	7/2/2021 3:05:50 PM	WINGDOMODINER	192.048.0.075	WIN COLONNER\Administrator	00-0C-29-20-9A-C3			C:\leaf all c.exe	File Quarantine
	7/2/2021 3:05:50 PM	WINCOLOUGHIER	192.048.0.039	WII Contractor R\Administrator	00-0C-29-20-9A-C3			C:\\mmillimmil.exe	File Quarantine
	7/2/2021 3:05:50 PM	W10 CDC #10 CPUTER	192.008.0.079	WI WI R\Administrator	00-0C-29-20-9A-C3			C:\\est\fc=]defd:1*fe:12:\e13f.e10[1]e10[1]e10[1]e10[10]e40f*f[2e10]e0[1]e10[10]ee10	File Quarantine
	7/2/2021 3:05:51 PM	WINDOWNSR	192.148.0.179	WINGTON	00-0C-29-20-9A-C3			C:\www.t.exe	File Quarantine
	7/2/2021 3:05:51 PM	WINDERCHARGENER	192.168.0.199	WI I I I I I I I I I I I I I I I I I I	00-0C-29-20-9A-C3			C:\umathcase	File Quarantine
	7/2/2021 3:05:51 PM	WINDERCHARGE	192.000.0.000	WII R\Administrator	00-0C-29-20-9A-C3			C:\ami_db)/ft + fa 25-amt 994d?hen/dbna7_fa7-1225*f, ad. Mathilde295% 51-62	File Quarantine
	7/2/2021 3:05:51 PM	WINDERCHARGENER	192.048.0.099	WI R\Administrator	00-0C-29-20-9A-C3			C:\www.institute.com	File Quarantine





Exporting the Report

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

C Excel O PDF I HTML Export	1	Export Option			
		O Excel	O PDF	HTML	

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



Click the link to open/download the file.

Incident-Windows

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

R DashBoard					💲 Refresh 🛛 👔 I
Incident - eScan Inc	ident - Windows	lent - EDR End Po	oint Incident Network Incident		
 Filter Criteria 				▲ Export Option	
		An account failed	to log on: 10.0%		
	The server accepted a	: User authentication s new TCP connection fr new TCP connection fr new UDP connection f	om client 192.	A logon was attempted using explicit credentials: 40.0% The server accepted a new UDP connection from client :63051: 10.0%	
				1 - 10 of 10 4 4 page 1 of 1	Fill Nows per page: 100
<u>Client Date</u>	Computer Name/Ip	IP Address	User's name	Event Description	Event
/5/2021 10:34:09 AM	With Gald 7	192.048.0.85	WIN-QA007\qa	The server accepted a new TCP connection from client 192. In the server	Logged [131]
/5/2021 10:34:15 AM	WINDERCHNEERURR	192.048.0.099	WI R\Administrator	A logon was attempted using explicit credentials	Logged [4648]
/5/2021 10:34:16 AM	Will Call 7	192.048.0.85	WIN-Quild?" open	The server accepted a new TCP connection from client 192. 40.0 (1990)	Logged [131]
5/2021 10:34:17 AM	WINDERCHNEEPUER	192.048.0.075	WI MINISTRUM R\Administrator	A logon was attempted using explicit credentials	Logged [4648]
5/2021 10:34:17 AM	W39-08007	192.048.0.85	WIN-CollEP on	The server accepted a new UDP connection from client [192.] ## 0 [110] #30100	Logged [131]
5/2021 10:34:17 AM	With Control 7	192.048.0.85	WINGSHITT	Remote Desktop Services: User authentication succeeded:	Logged [1149]
5/2021 10:34:17 AM	W28-Qm207	192.048-0.45	WIR-Quild?" ope	The server accepted a new UDP connection from client [192.] ## 0.5#** #2019	Logged [131]





Filtering Incident – Windows Report

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

▼ Filter Criteria		✓ Export Option	
Filter Criteria			
Computer Name	* v Include V	✓ IP Address	* Include 🗸
✓ User's name	* Include 🗸	Event Id(s)	* 🔻 🗸 Include 🗸
Description	* Include ¥		
Date Range From (MM/DD/YYYY)	07/06/		
To (MM/DD/YYYY)	07/06/		
Search Reset			(*) View All Items

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

Include/Exclude

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

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

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

R DashBoard					🤹 Refresh 🛛 👔
Incident - eScan Inc	ident - Windows Inci	dent - EDR End P	oint Incident Network Incident		
 Filter Criteria 				A Export Option	
		An account failer	to log on: 10.0%		
	1.155 des 21: 10.0%	new TCP connection fr	om client 192.	A lopon was attempted using explicit credentials: 40.0%	
	The server accepted 10.0%	a new UDP connection f	rom client :63050:	The server accepted a new UDP connection from client :63031: 10.0%	
lient Date	Computer Name/Ip	IP Address	User's name	Event Description	→ H Rows per page: 100 Event
/5/2021 10:34:09 AM	With Genill 7	192.000.0.00	WIN-QA007\ga	The server accepted a new TCP connection from client 192.	Logged [131]
/5/2021 10:34:15 AM	WIN COLUMNORMER	192.048.0.079	WI II II II AND AND R Administrator	A logon was attempted using explicit credentials	Logged [4648]
		192.048.0.85	WIN-CADD ² on	The server accepted a new TCP connection from client 192. 44.0.175 (ent.) 7	
5/2021 10:34:16 AM	With Central 7				Logged [131]
	With Edgewidd PulleR	192,048.0.079	W1+ C1 All R\Administrator	A logon was attempted using explicit credentials	Logged [131] Logged [4648]
/5/2021 10:34:17 AM		192.048.0.079	With the second R\Administrator	A logon was attempted using explicit credentials The server accepted a new UDP connection from client [192, 100, 100, 100, 100, 100, 100, 100, 10	
/5/2021 10:34:17 AM /5/2021 10:34:17 AM	WINESCHREIMER				Logged [4648]
7/5/2021 10:34:16 AM 7/5/2021 10:34:17 AM 7/5/2021 10:34:17 AM 7/5/2021 10:34:17 AM 7/5/2021 10:34:17 AM	With EDDWHEEP/ER With Quell 7	192.048.0.85	WIN-QADDPigs	The server accepted a new UDP connection from client [192, 10.0.11] (2001)	Logged [4648] Logged [131]





Exporting the Report

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

- Export Option			
O Excel	O pdf	HTML	Export

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



Click the link to open/download the file.

Incident-EDR

Incident-EDR tab provides the summary report of all the events from the endpoints in the network on the basis of severity for advanced investigation and response. It blocks/remove the suspicious files and then alerts the admin for further investigation and analysis of it.







eScan EDR solution provides different types of report such as Virus, PowerShell, and many more based on the different types of threats and malicious activities. The admin can select the report from the drop-down menu according to the requirement and get the detailed report about the same. The types of reports are as follow:

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

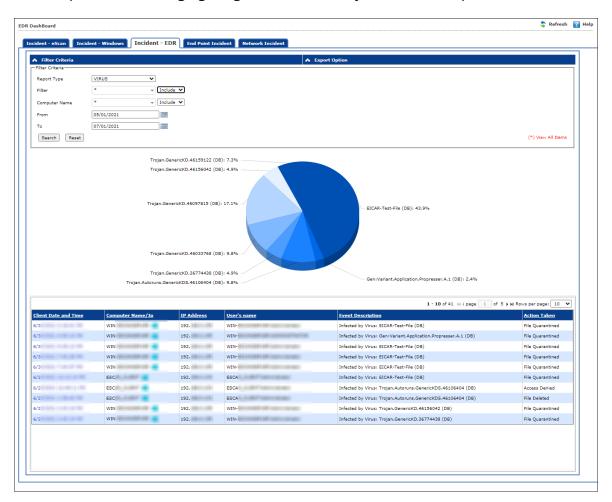
Report Type

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

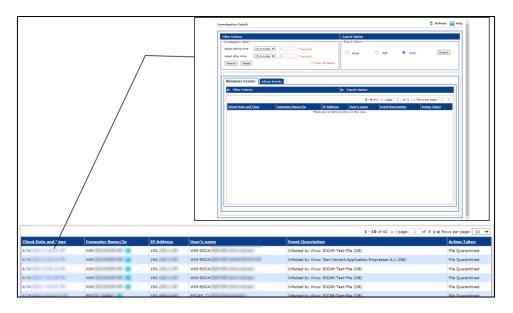




For example, the following figure gives the summary of the virus report.



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







The detailed report will be generated.

١	Windows Events escan Events Network Incidents									
▲ Filter Criteria ▲ Export Option										
1 - 2 of 2 ((page 1 of 1)) Rows per page: 1						r page: 100 🗙				
	Client Date and Time	Computer Name/Ip	<u>IP Address</u>	<u>User's name</u>	Event Description	Action Taken				
	07/05/2021 10:34:17	WIN COLORADOR 📑	192.000.000	W1 R\Administrator	A logon was attempted using explicit credentials	Logged				
	07/05/2021 10:34:15	WIN EDGANGERUER	192.008.0.075	WI R\Administrator	A logon was attempted using explicit credentials	Logged				

Windows Events: It displays the Windows event for the filtered time frame.

eScan Events: It displays the eScan events for the filtered time frame.

Network Incident: It displays the Network Incident events for the filtered time frame.

Filtering Incident – EDR Report for Specific Incident

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

Filter Criteria field expands.

Filter Criteria		
Investigation Detail		
select before time 15 minutes 🗸	2	* hours(s)
select after time 15 minutes 🗸	2	* hours(s)
Search Reset		(*) View All Items

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

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





Exporting Incident – EDR Report for Specific Incident

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

Export Option		
Export Option		
O Excel	HTML	Export

Filtering Incident – EDR Report

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

▲ Filter Criteria			Export Option	
Filter Criteria				
Report Type	VIRUS V	ו		
Filter	*	Include V		
Computer Name	* •	Include 🗸		
From	07/05/2021			
то	07/05/2021			
Search Reset				(*) View All Items

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

Include/Exclude

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

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

Exporting the Report

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

Export Option			
O Excel	O PDF	HTML	Export





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



Click the link to open/download the file.

Endpoint Incident

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

EDR DashBoard	💲 Refresh 🛛 👔 Help
Incident - eScan Incident - Windows Incident -	EDR Endpoint Incidents Network Incidents
Endpoint Incidents	🔅 Settings 🛛 💲 Refresh 👔 Help
Active Incident	Top Incident Image: Constraint of the second seco
Top Incident Technique	Top Affected Computers
Incident Name Severity	Incident Name Severity
PowerShell Blocked LOW	No Incidents to Investigate





Active Incidents

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

Top Incident

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

Top Incident Technique

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

Top Affected Computers

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

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

						I			s per page: 100 🗸
Index		Computer Name/Ip WI R	User's name R\Administrator	IP Address	<u>HostName</u>	<u>HostIp</u>	Incident Date	Incident Count	Incident Severity
		WIN COLOR R	WI R\Administrator			-	07/02/2021	1	Low
		WIN COLORADOR R	WI R\Administrator			-	06/30/2021	2	Medium
		WINDER	WI R\Administrator			-	06/30/2021	1	Low
		WIN COLORADOR R	WI R\Administrator			-	06/30/2021	1	Low
	RansomWare Blocked	WING MIN 7	WING CONDUCTION	192.000.000	-	-	06/29/2021	1	Low





Adding Specific Incident for Monitoring

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

1. From the list of the detected incident, select the specific incident according to the requirement.

Index	Incident	Computer Name/Ip	User's name	IP Address	HostName		Incident Date		per page: 100 ∨
		WIN EDEANOER	WI R\Administrator			-	07/05/2021	1	Low
	RansomWare Blocked	WIN COCHNODINER	WI R\Administrator	192.]	-	-	07/02/2021	1	Low
~	RansomWare Blocked	WIN COLORADOR R	WI R\Administrator	192	-	-	06/30/2021	2	Medium
	RansomWare Blocked	WIH EDGANDER R	WI R\Administrator	192.000.000	-	-	06/30/2021	1	Low
	RansomWare Blocked	WIN COLONNER	WI R\Administrator	192.	-	-	06/30/2021	1	Low
	RansomWare Blocked	WINCOM 7	WI to comit the com	192	-	-	06/29/2021	1	Low

2. Click **Add To Monitor**. The specific incident will be added to the monitoring list.





Viewing the Details of the Specific Incident

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

To view the detailed process tree follow the below steps:

- Select Incident: 7/5/2021 11:14:02 AM View Export To HTML V Export All Incident Report For User Computer Name: WI User Name: WIN CRUZZ 192.000.000 IP Address: Date Time: 7/5/2021 11:13:58 Session Type: Local PowerShell Blocked Incident: **Behavior: Chronology** PID Time File Action Type 4036 11:13:58 explorer.exe Process Run C:\Windows\explorer.ex 11:13:58 3252 cmd.exe C:\Windows\System32\cmd.exe Process Run 11:13:58 3948 powershell.exe Process Run C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe 11:13:59 3948 PowerShell Blocked Process Run C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe **Behavior: Graph** Info Files Registry Integrity Process Name: explorer.exe PID: 4036 Path: C:\Windows\explorer.exe Command Line: C:\Windows\Explorer.EXE url: Client User Name: -Client HostName: Client IP Address: Ð
- 1. Click the incident name under **Incident** column.

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

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

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





Viewing the Details of Monitoring Incident

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

🔺 Filt	ter Criteria									
💼 Dele	te					1 - 1 of 4	📢 page 🚺	of 0.4)	H Rows per page:	10 🗸
Index	Date	EDR Sensor	Condition1	Condition2	Condition3	Condition4	Condition5	Validity	Status	Result
	07/05/2021 16:52:27	05(20	PowerShell Blocked	powershell.exe	powershell.exe -NoProfile	-	-	1 Day	Stop Monitoring	View
	07/05/2021 15:41:13	05 2	MSOffice Child EXE Blocke	ms.exe	-	-	-	1 Day	Stop Monitoring	<u>View</u>
	07/02/2021 15:39:50	02072021153917	Infected by Virus: Trojan	-	C/Inst/nutification.exe	-	-	7 Days	Stop Monitoring	<u>View</u>

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

Status		×
Client Date and Time	7/3/2021 5:11:00 PM	
Computer Name/Ip	WINGSCHRUCER	
User's name	WI	
IP Address	192.000.000	
Client Date and Time	7/5/2021 10:35:31 AM	
Computer Name/Ip	WI I I I I I I I I I I I I I I I I I I	
User's name	WI	•
ок		

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

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

Deleting the Monitoring Incident

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

1. Select the specific incident from the list.

A Filter Oriteria										
							1 of 0.4 → H Rows per pag	je: 10 🗸		
Index	: Date	EDR Sensor	Condition1	Condition2	Condition3	Condition4	Condition5	Validity	Status	Result
	07/05/2021 16:52:27	050 000 0000000000000000000000000000000	PowerShell Blocked	powershell.exe	powershell.exe -NoProfile	-	-	1 Day	Stop Monitoring	View
	07/05/2021 15:41:13	05	MSOffice Child EXE Blocke	ms.exe	-	-	-	1 Day	Stop Monitoring	<u>View</u>

2. Click Delete.

The specific incident will be deleted.





Network Incident

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

EDR DashBoard			💲 Refresh 🛛 👔 Help
Incident - eScan Incident - Windows	Incident - EDR EndPoint Incident Network In	ncident	
Network Incidents			🔅 Settings 🛭 📚 Refresh 👔 Help 🔷
	2	*2	*2
Top Source	Top Destination	Top Incident	All Incident
192. 3 MEDIUM 192. 3 MEDIUM 192. 3 MEDIUM	<u>192.166 0 150</u> 9 HIGH	OS-OTHER Bash CGI environ 9 HIGH	view all records

Top Source

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

rce IP: 192.					
		3			
		Last Observed: 7/27/2021			
3	80 (HTTP)				
	0	80 (HTTP)			





Top Destination

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

 OS-OTHER Bash CGI environment variable injection attempt 			1
First Observed: 7/27/2021			Last Observed: 7/27/2021
See References			
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-7169			
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6278			
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277			
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6271			
192. 66.6 210	3	5 - 10 7	
192. 144 0 231	3	5 8	
192. 444 0 212	3	57469	

Top Incident

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

cident : OS-OTHER Bash CGI environment variable injection attempt			
- 192.144 250			3
First Observed: 7/27/2021			Last Observed: 7/27/2021
See References			
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-7169			
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6278			
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277			
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6271			
192. 44 0.150	3	80 (HTTP)	
+ 192.166.8.251			3
+ 192.168.8.252			3





Viewing the Network Incident

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

Filter Criteria					<u></u>	Export Op	Juon	
Direction		*	-	include 🗸				
Source IP Address		*		Include 🗸				
Source Port		*		include 🗸				
Destination IP Address	5	*	-	include 🗸				
Destination Port		*	-	include 🗸				
Protocol		*	-	include 🗸				
Type of Action		*		include 🗸				
Description		*		include 🗸				
From		07/27/2021						
То		07/27/2021						
Search Reset								(*) View All Items
		Un	known Traffic: 3	83.3%	Potentially Bad Traffi	c: 33.3% (3)		icious Traffi: 33.3%
		Un	known Traffic: 3	13.3%	Potentially Bad Traffi	c: 33,3% (3)		icious Traffi: 33.3% Y Bad Traffic: 33.3%
		Un	known Traffici S	13.3%	Potentially Bad Traffi	c: 33.3% (3)	Potential	
lient Date and Time	Direction	Un Source IP	known Traffici S Source Port	Destination IP			Potential	y Bad Traffic: 33,3%
	Direction		Source Port		Destination Port	Protocol	Potential	y Bad Traffic: 33,3% -9 of 9 ⊣ (page 1 of 1) → Rows per page: 10 ♥
7/27/2021 13:10:28		Source 1P	Source Port	Destination IP 192. MARKED	Destination Port 80	Protocol I HTTP I	Potential 1 Incident Name	y Bad Traffic: 33,3% - 9 of 9 { { page 1 of 1 } } Rows per page: 10 ♥
7/27/2021 13:10:28 7/27/2021 13:10:28	Local	Source 1P 192.	Source Port 5 7 5 7 5 7 5 7	Destination IP 192. MARKED	Destination Port 80 80	Protocol I HTTP I HTTP I	Potential Potential Incident Name Not Suspicious Traffi Unknown Traffic	y Bad Traffic: 33.3% - 9 of 9 (() page 1 of 1)) Rows per page: 10 V Packet Description OS-OTHER Bash CGI environment variable injection attempt
lient Date and Time 7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28	Local Local Local Local	Source IP 192. 192. 192.	Source Part 5 7 5 7 5 7 5 7 5 8	Destination IP 192, 444, 550 192, 444, 550 192, 444, 550 192, 444, 550	Pestination Port 80 80 80 80 80 80	Ртоtocol р НПТР 1 НТТР 1 НТТР 1 НТТР 1 НТТР 1	Potential Potential Incident Name Not Suspicious Traffi Unknown Traffic Potentially Bad Traffic Not Suspicious Traffi	y Bad Traffic: 33.3% P of 9 4 page 1 of 1 } H Rows per page: 10 ♥ Packet Description OS-OTHER Bash CGI environment variable injection attempt OS-OTHER Bash CGI environment variable injection attempt OS-OTHER Bash CGI environment variable injection attempt OS-OTHER Bash CGI environment variable injection attempt
7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28	Local Local Local	Source IP 192. 192. 192. 192.	Source Port 5 7 5 7 5 7 5 8 5 8 5 8	Pestination IP 192, 944,6,370 192, 944,6,370 192, 944,6,370	Destination Port 80 80 80 80 80 80	Protocol 1 HTTP 1	Potential Potential Incident Name Not Suspicious Traffi Unknown Traffic Potentially Bad Traffic Not Suspicious Traffi Unknown Traffic	y Bad Traffic: 33.3% - 9 of 9 4 (page 1 of 1))↓ Rows per page: 10 ✓ Packet Description OS-OTHER Bash CGI environment variable injection attempt OS-OTHER Bash CGI environment variable injection attempt
7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28	Local Local Local Local Local Local	Source 10 192	Source Port 5 7 5 7 5 8 5 8 5 8 5 8	Destination IP 192. set 530 192. set 530 192. set 530 192. set 530 192. set 530	Destination Port 80 80 80 80 80 80 80 80 80 80 80 80 80 80	Protocol 1 HTTP 1	Potential Potential Tracident Name Not Suspicious Traffic Unknown Traffic Potentially Bad Traffic Not Suspicious Traffic Potentially Bad Traffic	y Bad Traffic: 33.3% • 9 of 9 4 (page 1 of 1) → Rows per page: 10 ♥ Packet Description OS-OTHER Bash CGI environment variable injection attempt OS-OTHER Bash CGI environment variable injection attempt
7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28	Local Local Local Local Local Local Local	Source IP 192. 44 19 192. 44 19 192. 44 19 192. 44 19 192. 44 19 192. 44 19	Source Port 5 7 5 7 5 8 5 8 5 8 5 8 5 8 5 8	Destination IP 192. ######## 192. ####### 192. ####### 192. ####### 192. #######	Destination Port 80 80 80 80 80 80 80 80 80 80 80 80	Protocol I HTTP I	Potential Potential Tracident Name Not Suspicious Traffi Unknown Traffic Potentially Bad Traffic Not Suspicious Traffi Potentially Bad Traffic Not Suspicious Traffi	y Bad Traffic: 33.3% • 9 of 9 (page 1 of 1) ⊨ Rows per page: 10 ♥ Packet Description OS-OTHER Bash CGI environment variable injection attempt OS-OTHER Bash CGI environment variable injection attempt
7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28 7/27/2021 13:10:28	Local Local Local Local Local Local	Source 10 192	Source Part 5 7 5 7 5 8 5 8 5 8 5 8 5 8 5 8 5 9 5 9	Destination IP 192. set 530 192. set 530 192. set 530 192. set 530 192. set 530	Destination Port 80 80 80 80 80 80 80 80 80 80 80 80	Рготосо 1 НТТР 1 НТТР 1 НТТР 1 НТТР 1 НТТР 1 НТТР 1 НТТР 1 НТТР 1	Potential Potential Internet Not Suspicious Traffic Unknown Traffic Potentially Bad Traffic Not Suspicious Traffic Potentially Bad Traffic Not Suspicious Traffic Unknown Traffic	y Bad Traffic: 33.3% • 9 of 9 4 (page 1 of 1) → Rows per page: 10 ♥ Packet Description OS-OTHER Bash CGI environment variable injection attempt OS-OTHER Bash CGI environment variable injection attempt

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

Export Option I - 1 of 1 { (page 1 of 1) Rows per page: 100 V Client Date and Time Source IP Source Port Destination IP Destination Port Incident Name Packet Description	Network Incidents	eScan Events	•				
	 Export Option 						
Client Date and Time Source IP Source Port Destination IP Destination Port Incident Name Packet Description							1 - 1 of 1 ((page 1 of 1)) Rows per page: 100 ♥
	Client Date and Time	Source IP	Source Port	Destination IP	Destination Port	Incident Name	Packet Description
07/05/2021 11:44:07 192.		102 100 0 100	40591	192,000.0.000	80	Attempted Administrator Privilege Gain	OS-OTHER Bash CGI environment variable injection attempt.





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

Network Incidents eScan Events							
Export Option							
1 - 5 of 5 (() page 1 of 1)) Rows per page: 100 🗸 🔺							
Client Date and Time	Computer Name/Ip	IP Address	User's name	Event Description	Action Taken		
07/05/2021 11:52:35	With EDC #HOLEFARR	192.008.0.011	WI R\Administrator	MSOffice Child EXE Blocked [Parent-C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE:3808]	Application Terminated		
07/05/2021 11:52:35	WIN COLUMNER	192.008.0.019	WI R\Administrator	MSOffice Child EXE Blocked [Parent-C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE:3808]	Application Terminated		
07/05/2021 11:52:35	WIN ED AN DET AR	192.008.0.075	W1 R\Administrator	MSOffice Child EXE Blocked [Parent-C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE:3808]	Application Terminated		
07/05/2021 11:49:35	WIN EDCHNER	192.	WI R\Administrator	Sensitive OS-File Execution Blocked [Parent-C:\Windows\System32\cmd.exe:7560]	Application Terminated		
07/05/2021 11:44:50	WIN EDCHNODINER	192.008.0.079	WI R\Administrator	Access Blocked: User:Blocked (ES)	Access Denied		

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

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

lter Criteria	Export Option			
nvestigation Detail	Export Option			
select before time 15 minutes V 2 * hours(s)		<u>_</u>	_	
select after time 15 minutes V 2 * hours(s)	O Excel	O PDF	HTML	Export

Filtering the Specific Incident

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

Filter Criteria		▲ Export Option	
Filter Criteria			
Source IP Address	* v Include V		
Source Port	* 👻 Include 🗸		
Destination IP Address	* 🗸 Include 🗸		
Destination Port	* v Include v		
Type of Action	* 🔹 🔹 Include 🗸		
Description	* v Include v		
From	07/05/2021		
То	07/05/2021		
Search Reset		(*)	View All Item

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





Exporting the Network Incident

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

Export Option			
O Excel	O PDF	HTML	Export

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



Click the link to open/download the file.





Managed Computers

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

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

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

Managed Computers		💲 Refresh 🛛 👔 Help
Search Opdate Agent		
Action List 🔻 🛐 Client Action List 🕶	Policy Templates Policy Criteria Templates	<u>QR Code for 2FA</u>
🗄 🦳 🎦 Managed Computers	Name	
Policy	Policy	
Group Tasks	Group Tasks	
Client Computers (2)	Client Computers	
Roaming Users	Group Information	
Group Tasks	AD Sync	Not Configured
🧮 Client Computers	Total Subgroups	13
⊡ 💼 Linux / Mac	Total Computers	0

The screen consists of following buttons:

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





Search

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

arch for Computers				?
Filter				
Computer Name / IP:				
User's name:				
	Find Now			
Client Action List -				
omputer Name Grou	os IP Address User nam	e eScan Status Version Last Connec	tion (YYYY/MM/DD) Installed D	irectory Monitor Status
Unmanaged	Protected	📃 Not Installed / Critical	💻 Unknown status	🛜 Update Agent

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 <u>eScan Update Agents</u>.

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.





Features of Update Agents

- 1. Download the antivirus signature updates from the eScan Server and share with other client machines on the network.
- 2. Download the policy updates from the eScan Corporate Server and share with the client in the group or the network
- 3. The update agent will take event updates from the client computers in the group or network and share it with the eScan Corporate Server.
- 4. Remote Deployment of clients can be done through Update Agents

Advantages of Update Agents

- 1. Update Agent can be installed on any client computer connected to the network (where eScan is already installed).
- 2. Update Agent will take the signature updates from eScan Corporate Server and distribute the same to other managed computers in the group. (Bandwidth is saved).
- 3. Update Agent will alternatively query eScan Update servers on internet for getting updates whenever there is a connectivity problem between the update agent and eScan Corporate Server.

Now in your scenario check how update agent help to achieve update of users who working from home.

Suppose, your eScan Server is located in DMZ network which not allowed to communicate with internal network as well as internet user (Outside users). So achieving update for remote user you need to configure Update agent on the system which is connected in DMZ with eScan server and that system you need to give one static IP (Public IP). So Update agent will take update from eScan Server. And your internal network as well as internet user will take update from primary server and your eScan server also remains in closed environment.

Update agent can be configured as FQDN soNOTEUpdate agent can be configured for multOne update agent can be configured for mult	U U
---	-----





Adding an Update Agent

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

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

		Ε
Jpdate Agent		🛐 Неір
—Select Group Name and		
Update Agent	:	
Group Name:		
Configure UA	A Settings	bbA
Update Agent	IP Address	Assigned to Group(s)
WI COULT	192	Managed Computers

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

elect Computer	*		•	김 He
: 🚞 Managed Comput	ers			
🗆 🙇 ########	96			
🗆 貫 wikesia	10000000000			
🛅 Roaming Users				
🛄 🚞 Linux / Mac				
		Ok		Cancel
* Note: Update Agent car	nnot be set if Ho	stname exceed 15 cl	haracters.	

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

The Update Agent will be set for the selected group.





Configuring UA Settings

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

me for UA clients
me of Primary server to UA / client setup :
Test
date Agents. To apply above changes, delete and re configure the

Ignore Customize/Server IP and Hostname for UA clients

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

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

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

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

Delete an Update Agent

To delete an Update Agent

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

Update Agent		👔 Help
Select Group Name and Update		
Update Agent:		
Group Name:		
Configure UA Setting	<u>15</u>	Add
Update Agent	IP Address	Assigned to Group(s)
WIN CONTRACT	192	Managed Computers\ M





In the Assigned to Group(s) column, click <a>î.
 A confirmation prompt appears.

:10443 says		
Do you want to remove update agent?		
	ОК	Cancel

3. Click **OK**.

The Update Agent will be deleted.

In case of eScan Corporate, this option is available only on system where eScan Corporate Server is installed. You can access this option through eScan Protection Center.

Create Offline Update

With eScan's offline update, administrator can easily update eScan on any system which is not connected to internet. Offline update file can be created through a system that has eScan installed on it and has active internet connection. Once created, the offline update file can be copied to any system and executed just like any other executable to apply eScan update file on that system.

Pre- requisite for creating an offline update

• The system should have eScan SOHO product or eScan Server installed with all the latest updates.

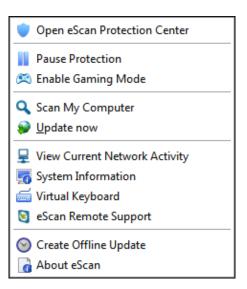
	With default installation of older versions, this feature is not available.
	If older version of eScan is installed, please make sure to download
θ	the latest updates in order to avail this feature.
NOTE	The offline update file that will be created can be executed on any windows system. All latest eScan updates will be installed on the
	system through the Offline update file.

Use following steps to create offline update:

1. Right click on the eScan icon 💔 in the task bar and click **Create Offline Update**.



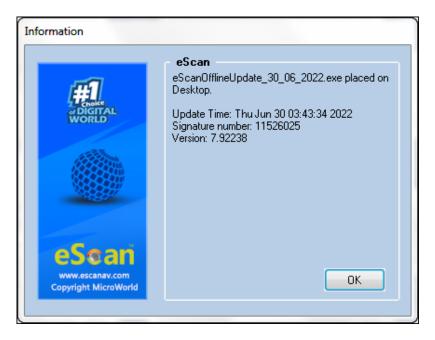




2. It will automatically start creating executable file for updating eScan offline. The file will be created on desktop.



3. Once the update file has been created, you will get the confirmation message.



4. To run the **eScanOfflineUpdate.exe** file on any system, just copy and execute the file on any system where eScan is installed.





5. It will extract the files on to the system

🛞 ESUPDATE [Red	ist] - Updates for eScan and MailScan (www.escanav.com)
Contraction of the second	Extracting plugins\emalware.561 Extracting plugins\emalware.562 Extracting plugins\emalware.563 Extracting plugins\emalware.564 Extracting plugins\emalware.566 Extracting plugins\emalware.567 Extracting plugins\emalware.569 Extracting plugins\emalware.570 Extracting plugins\emalware.571 Extracting plugins\emalware.572 Extracting plugins\emalware.573 Extracting plugins\emalware.573 Extracting plugins\emalware.573
- Const	Destination folder
eSoan	C:\Users\Sudeepa\AppData\Local\Temp Browse Browse
www.escanav.com Copyright MicroWorld	Installation progress
	Install Cancel

6. Click **OK**. After extracting the update files, you will be confirmed through the following message –



In our Products, you can deploy eScan Offline updates along with eScan client (setup.exe) through eScan Management Console. <u>Click here</u>.





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

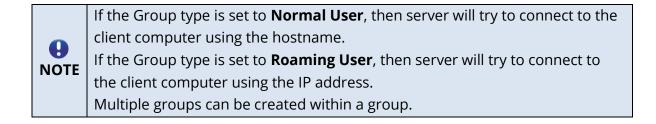
To create a group, follow the steps given below:

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

Creating New Group			Help
New Group Name :			
Group Type :	Normal User	~	
Policy Templates :	Group Default Policy	~	
Policy Templates :		~	

- 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.







Removing a Group

To remove a group, follow the steps given below:

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

Remove Group	
Do you really want to remove	e the group "(an" ?
Ok Cancel	

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



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.

ogin Informatio	n
roup Name:	Managed Computers
emarks:	
ser name:	Administrator
assword:	

- 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. <u>For more click here</u>.
- **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. <u>For more</u> <u>click here</u>.
- 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.

Conditions for third party software installation:



After starting the installation from eScan Management Console, no manual intervention should be required to complete the installation on Client computer. Only automated installations can be done through eScan Management Console.

Care should be taken that the installation file is not huge as it may impact internal network speed of your organization.





Remote Installation of eScan Client

Pre-Installation

To prepare a client computer for the remote deployment of eScan Enterprise EDR Edition (with MDM & 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 / Windows 11

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

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

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

For Windows XP Home

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





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

- 1. Launch Run.
- 2. Enter **secpol.msc**, and then click **OK**. Local Security Settings window appears.
- 3. On the navigation pane, click **Local Policies** folder, and then double-click **Security Options** folder. The security policy appears.
- 4. Double-click **Network access: Sharing and security model for local accounts** policy.
- 5. Select Classic Local users authenticate as themselves option present in the drop-down.
- 6. Click **Apply** > **OK**.
- 7. Double-click Accounts: Limit local account use of blank passwords to console logon only policy.
- 8. Select **Disabled** option.
- 9. Click **Apply** > **OK**.
- 10. If the firewall is enabled, select **File and Printer Sharing** check box, 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** check box.
- 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.

ent Installation	<table-cell> Help</table-cell>
equired packages for Linux Client Installation 🧕	
32 Bit deb. Packages Download	
64 Bit deb. Packages Download	
32 Bit rpm. Packages <u>Download</u>	
64 Bit rpm. Packages <u>Download</u>	
lect Application for Installation:	
Install eScan	
Select eScan Installation Options: 🕂	
Auto Reboot after Install	
Install Without Firewall	
Disable auto downloading of Windows patches by eScan	
	I
Installation Path	
Installation Path <default> Add</default>	
<default> Add</default>	
<default> Add Install Other Software</default>	
<default> Add Install Other Software Linux/MAC Client Setup</default>	
Content of the second secon	
<default> Add Install Other Software Linux/MAC Client Setup Required files for Installation C:\PROGRA~1\eScan\Setup\Launchit.Exe,C:\PROGRA~1\ eScan\Setup\Setup.exe Add</default>	
<default> Add Install Other Software Linux/MAC Client Setup Required files for Installation C:\PROGRA~1\eScan\Setup\Launchit.Exe,C:\PROGRA~1\eScan\Setup\Setup.exe Executable file</default>	

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.
- Click Client Action List > Deploy/Upgrade Client. Client Installation window appears.

	Hel
quired packages for Linux Client Installation 🧕	
32 Bit deb. Packages Download	
64 Bit deb. Packages <u>Download</u>	
32 Bit rpm. Packages <u>Download</u> 64 Bit rpm. Packages <u>Download</u>	
64 Bit rpm, Packages <u>Download</u>	
lect Application for Installation:	
Install eScan	
Select eScan Installation Options: 🗮	
Auto Reboot after Install	
Install Without Firewall	
Disable auto downloading of Windows patches by eScan	
Installation Path	
Installation Path	
Installation Path Coefault> Add	
<default> Add</default>	
Contemporation of the second secon	
<default> Add Install Other Software Linux/MAC Client Setup</default>	
<default> Add Install Other Software Linux/MAC Client Setup Required files for Installation C:\PROGRA~1\eScan\Setup\Launchit.Exe,C:\PROGRA~1\</default>	
<default> Add Install Other Software Linux/MAC Client Setup Required files for Installation C:\PROGRA~1\eScan\Setup\Launchit.Exe,C:\PROGRA~1\ eScan\Setup\Setup.exe Add</default>	

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	This status is displayed when a computer is added to RMM license and the computer can be connected via RMM service.
Eg Two-FA	This status is displayed when a computer is added to 2FA license.
S 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.
C Anti-Theft	This status is displayed when a computer is added to Anti-Theft Portal.





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.
- 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

The installation process of eScan on Linux or Mac computers.

Installing eScan Client on Linux Computers

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

- 1. Login to the EMC with your username and password.
- 2. Click Managed Computers on the navigation panel and select a group.
- 3. Under the group, click Client Computer and select a computer.
- 4. To deploy the setup, click **Client Action List > Deploy/ Upgrade Client**.





5. Download respective agent link from **Required package for Linux Client Installation** option.

Client Installation 🔐 Help	, ^
Required packages for Linux Client Installation 🧕	
32 Bit deb. Packages Download	
64 Bit deb. Packages <u>Download</u>	
32 Bit rpm. Packages <u>Download</u>	
64 Bit rpm. Packages <u>Download</u>	

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

lect Application for Installation:	
Install eScan	
Select eScan Installation Options: 📲	
Auto Reboot after Install	
Install Without Firewall	
Disable auto downloading of Windows patches by eScan	
Installation Path	
<default> V Add</default>	
Install Other Software	
C Linux/MAC Client Setup	
Required files for Installation	
Add	
Executable file	
✓ Edit Script	
Parameters	
Install Agent	
Install local client setup	
Required files for Installation	
Add	
Add	

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



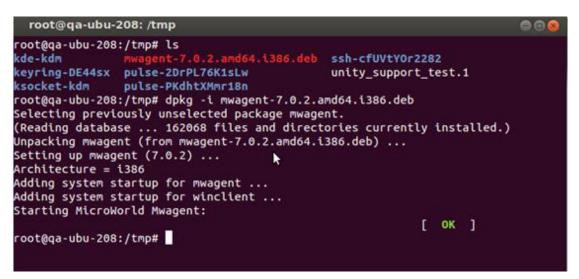


Installing Agent on Linux

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

eScan Client Setup (Windows)	\sim
eScan Client Setup (Android)	\sim
eScan Agent Setup (Windows)	\sim
eScan Agent Setup (Linux)	^
http://WIN-DLP:10443/Setup/Agent_Setup.deb	
http://192.168.0.61:10443/Setup/Agent_Setup.deb	
http://WIN-DLP:10443/Setup/Agent_Setup.rpm	
http://192.168.0.61:10443/Setup/Agent_Setup.rpm	

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



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**.

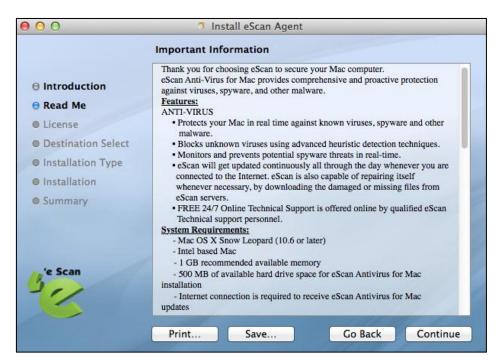
000	Install eScan Agent
	Welcome to the eScan Agent Installer
Introduction	Welcome to eScan Anti-Virus agent installation wizard!
Read Me	
License	
Destination Select	
Installation Type	
Installation	
Summary	
e Scan	
311	
	Go Back Continue



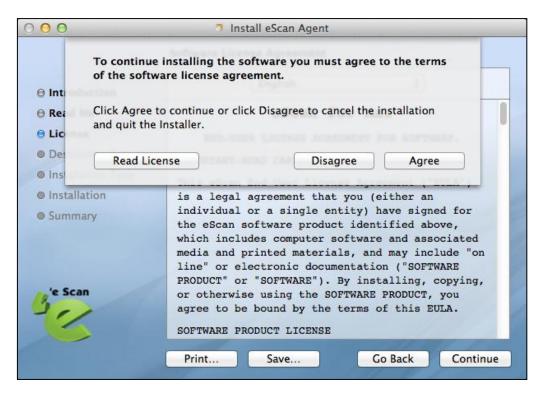


The installation wizard displays Read Me window.

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.



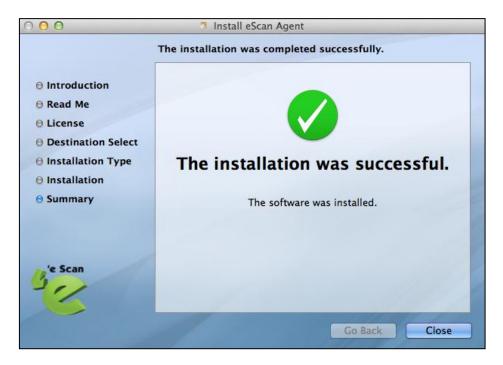




9. Select **eScan Agent Install** check box and click **Continue**.

00	🧿 Install eScan Agent		
	Custom Install on "mac"		
	Package Name	Action	Size
Introduction	🗹 eScan Agent Install	Upgrade	350 KB
🖯 Read Me			
O License			
Destination Select			
Installation Type			
Installation			
Summary			
	Space Required: 350 KB	Remaining: 1.96 GB	3
'e Scan		*	
Sealan			
~			
		1	
		Go Back	Continue

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



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





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** > **Setup Links** of eScan Management Console. Forward this link to the user of the Client computer on mail and guide the user through the installation process.

<	
eScan Client Setup (Windows)	\sim
eScan Client Setup (Android)	\sim
eScan Agent Setup (Windows)	\sim
eScan Agent Setup (Linux)	\sim
eScan Agent Setup (MAC)	\sim

Installing eScan Client Using Agent

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

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

Remotely installing agent on Client computer(s)

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



This option useful in case there are glitches in the network connectivity between server and Client computer. It will overcome those glitches and speed up the client installation on the selected computers.





Manually installing eScan Agent on Client computer(s)

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

<	
eScan Client Setup (Windows)	~
eScan Client Setup (Android)	\sim
eScan Agent Setup (Windows)	\sim
eScan Agent Setup (Linux)	\sim
eScan Agent Setup (MAC)	\checkmark

Installing other Software (Third Party Software)

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

- 1. Open eScan Management Console.
- 2. Click Managed Computers.
- 3. Select a computer from a group where you wish to deploy eScan Offline updates update eScan clients.

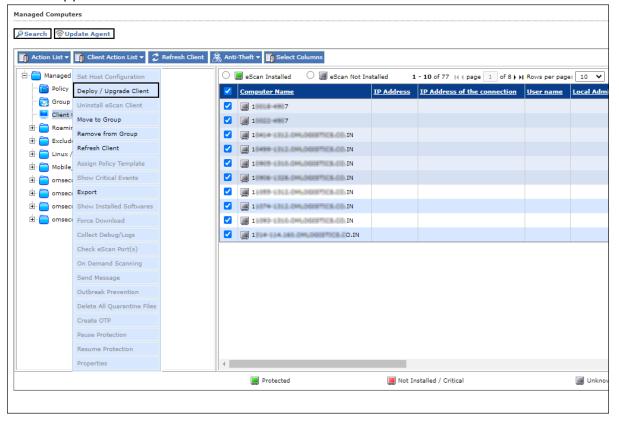
Managed Computers						
Search Opdate Agent						
🛐 Action List 🔻 🋐 Client Action List 🕶 🥏 Refresh Client 🧴	🕈 Anti	-Theft 🔻 🛐 Select Columns				
🗄 🛅 Managed Computers	0	📕 eScan Installed 🛛 🔿 📕 eScan Not Ins	stalled 1	- 10 of 77 🖂 (page 1 of 8) 🕅	Rows per page	: 10 🗸
Policy		Computer Name	IP Address	IP Address of the connection	<u>User name</u>	Local Admi
Group Tasks		1 1 1 1 1 1 1 1 7				
Client Computers (77)		1 1 1 1 7				
🕀 🧰 Roaming Users		10454 \$353.0HL060579C8.00.IN				





4. Click **Client Action List** > **Deploy/Upgrade Client**. Client Installation window

appears.







5. Select Install Other Software option.

elect Application for Installation:	
Install eScan	
Select eScan Installation Options: 📑	
Auto Reboot after Install	
Install Without Firewall	
Disable auto downloading of Windows patches by eScan	
Installation Path	
<default> V Add</default>	
Install Other Software	
Linux/MAC Client Setup	
Required files for Installation	
c:\test\tvnserver.exe Add	
Executable file	
tvnserver.exe	
Parameters	
s	
Install Agent	
Install local client setup	
Required files for Installation	
Add	
Add //	
Everytable file	

6. Click Add.

Add Files window appears.

Add Files	
Add Cancel	





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

Install Other Software	
Linux/MAC Client Setup	
Required files for Installation	
C:\test\tvnserver.exe	Add
Executable file	
TVNSERVER.EXE V	Edit Script
Parameters	
-remove]

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

Client Installation	p
5/3/ 11:09:02 AM : []: Connecting to Computer 5/3/ 11:09:02 AM : []: Deploying other software files to host . Pls Wait 5/3/ 11:09:02 AM : []: Copying file 1 of 1 5/3/ 11:09:03 AM : []: Coppleted 100 % 5/3/ 11:09:04 AM : []: Task 'Install/Upgrade Software on Host' successfully scheduled on	
Close Cancel	

After deployment, eScan client will be installed and updates will be installed automatically on selected managed computers where it was deployed through eScan Management Console.





Uninstall eScan Client (Windows, Mac, and

Linux)

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

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

Client Uninstallation
Ready to Start Uninstallation Click "Uninstall" to Start Uninstallation
Uninstall Cancel

3. Click Uninstall.

The Client Uninstallation window displays the progress.

Client Uninstallation	Help
<pre>8/6/2021 2:41:13 PM : []: Connecting to Computer 8/6/2021 2:41:14 PM : []: Reading Host Details 8/6/2021 2:41:15 PM : []: Version 22.0.1400. 8/6/2021 2:41:15 PM : []: Service Pack 2373 8/6/2021 2:41:15 PM : []: Task 'Uninstall eScan on Host(s)' successfully scheduled on</pre>	
Close Cancel	

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

θ	You can uninstall eScan Client from all the computers in the group by
NOTE	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.

nchronize with Active Directory	
Target Groups :	
Managed Computers	Browse
Source Active Directory Organisation Unit :	
	Browse
60 Minutes (Minimum 5 Minutes)	
Exclude From ADS Sync	
Excluded ADS Sources	Add to Exclude Delete
- Search Filter :	
e.g.: (objectClass=*)	
Install eScan client automatically	
- Select eScan Installation Options:	
Install Without Firewall	
D sync will not add the computers that are already present in any of the groups under Managed co	mputers.Check
Scan\log\ADSsync.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 check box 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.

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.

	😨 He
break Prevention	¹¹
Deploy Outbreak Prevention	store Outbreak Prevention
utbreak Prevention Policies	
Limit access to shared folders (Allow rea	d only access)
Deny write access to local files and folde	t
Block Specific Ports	
Block All Ports (Other than trusted client	-server ports)
Automatically restore outbreak prevention	
Warning: The above outbreak prevention po	licies will be enforced on all the selected computers or groups. Incorrect
configuration of these policies settings can ca	
Warning: The above outbreak prevention po configuration of these policies settings can ca utbreak Prevention Notification	use major problems with the computers.
configuration of these policies settings can ca utbreak Prevention Notification	use major problems with the computers.
configuration of these policies settings can ca utbreak Prevention Notification Notify client users when outbreak prever Message: eScan has detected a security risk outbreak	use major problems with the computers.
configuration of these policies settings can ca utbreak Prevention Notification Notify client users when outbreak prever Message: eScan has detected a security risk outbreak	use major problems with the computers. ntion starts 207/250 on your network. To prevent the security risk from spreading, your eScan
configuration of these policies settings can ca utbreak Prevention Notification Notify client users when outbreak prever Message: eScan has detected a security risk outbreak	use major problems with the computers. ntion starts 207/250 on your network. To prevent the security risk from spreading, your eScan
configuration of these policies settings can ca utbreak Prevention Notification Notify client users when outbreak prever Message: eScan has detected a security risk outbreak	use major problems with the computers. Intion starts 207/250 on your network. To prevent the security risk from spreading, your eScan ay prevent you from accessing network resources.
configuration of these policies settings can ca utbreak Prevention Notification Notify client users when outbreak prever Message: eScan has detected a security risk outbreak	use major problems with the computers. Intion starts 207/250 on your network. To prevent the security risk from spreading, your eScan ay prevent you from accessing network resources.





Limit access to shared folders

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

Deny write access to local files and folder

Select this check box 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 check box 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 check box 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 check box **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.

Deploy Outbreak Pre	vention Restore Outbreak Prevention	
estore Outbreak Prev	vention	
Notify client users	after restoring the original settings	96/250
Message:		
Message: eScan has stopped enf	orcing outbreak prevention policies and has restored pre-outbreak settings.	

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

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





Create Client Setup

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

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

Create Client Setup window appears.

Create Client Setup
Setup Settings
Add Policy
Add Policy
Create Setup Cancel

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

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





Properties of a group

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

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

Properties window appears.

Properties (Managed Computers	;) 🛐 Help	*
General		
Name :	Managed Computers	
Parent Group :		
Group Type :	Normal User 🗸	
Contains :	20 Groups , 5 Computers	
Created :	06/19/2021 4:37:02 PM	

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

- Group Name
- Parent Group
- Group Type Normal or Roaming User
- Contains 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**.

Action List - Client Action List -		QR Code for 2FA
- Managed Computers	Group Tasks	🤹 Refresh 🛛 👔 Help
···· 📄 Policy		
📆 Group Tasks		
📃 Client Computers (3)	🚹 New Task 🗊 Start Task 💕 Properties 📄 Results 🍿 Delete	
🗄 🦳 Roaming Users	Task Name Task Performed Assigned To Whom	Schedule Type
🗄 🧰 Linux / Mac		<u>Scheddle Type</u>





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



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





Managing a Group Task

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

	p Tasks			💲 Refre	esh 김 Help
Ð	New Task	Start Task 🛃 Properties	Results Delete		
	<u>Task Name</u>	Task Performed	Assigned To Whom	Schedule Type	
~	tech	Not Performed Yet	'Managed Computers'	Automatic Scheduler	Task Status

Start Task

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

Delete Task

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

Properties

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

h		?
General Schedule Set	tings	
Task Name	tech	
Task Creation Time:	06/30/21 02:37:25 PM	
Status:	Task not performed yet	
Last Run:		
Save Close		

Results

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

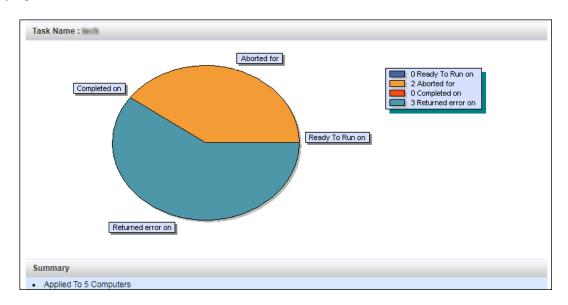
	p Tasks			🗢 Refr	esh 👔 Help
55.	New Task	art Tack	🗏 Basulta 🏛 Dalata		
	Task Name	art Task Properties	Assigned To Whom	<u>Schedule Type</u>	
	facilit.	Completed	'Managed Computers'	Automatic Scheduler	Task Status





Task Status

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



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.

- Computers	Policy	💲 Refresh 🛛 👔 Help
🔯 Group Tasks 💻 Client Computers (3)	Select Template	
🔃 🧰 Roaming Users	Assigned Template	Date And Time of Assigned Template
⊡- 💼 Markating_Taam ⊡- 💼 m_Ttan	SAMPLES	Jun 29 2021 12:25:45 PM
🕀 🧰 Carles III 🗄 🧰 Sameles Team	Criteria Change Criteri Criteria to be set in case of conflict	a 🕆 Remove
- 📄 Policy - 💮 Group Tasks	Criteria to be set in case of conflict Criteria Assigned Policy Te	mplate Date And Time of Assigned Criteria
Client Computers (1)		





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

Policy	👔 н
licy Template Selection	
Group Default Policy	
QA SAMPLES	^
elect Cancel	

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

Select Policy Criteria	👔 Help
Set this criteria as a default criteria in case of conflict	
Policy Template Selection	
Group Default Policy	
·	
Criteria Template Selection	
deme .	
· · ·	
Select Cancel	

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





Client Action List

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

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

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





Set Host Configuration

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

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

- 1. Select the computer.
- Click Client Action List > Set Host Configuration.
 Set Host Configuration window appears.

emarks: Administrator	ogin Information		
ser name: Administrator	omputer Name:		
	emarks:		
	ser name:	Administrator	
assword:	assword:		

- 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.
- Click Client Action List > Deploy/Upgrade Client. Client Installation window appears.

nt Installation	1 H
quired packages for Linux Client Installation 🧕	
32 Bit deb. Packages Download	
54 Bit deb. Packages <u>Download</u>	
32 Bit rpm. Packages Download	
64 Bit rpm. Packages <u>Download</u>	
ect Application for Installation:	
Install eScan	
Select eScan Installation Options: 📒	
Auto Reboot after Install	
C Auto Reboot alter Install	
Install Without Firewall	
0	a Gran
Disable auto downloading of Windows patches by	eScan
Disable auto downloading of Windows patches by	eScan
Disable auto downloading of Windows patches by	eScan
 Disable auto downloading of Windows patches by Installation Path 	
Disable auto downloading of Windows patches by Installation Path <default></default>	
Disable auto downloading of Windows patches by Installation Path <default> Install Other Software</default>	
Disable auto downloading of Windows patches by Installation Path Cefault> Install Other Software Dinux/MAC Client Setup	Add
Disable auto downloading of Windows patches by Installation Path Cefault> Install Other Software Linux/MAC Client Setup Required files for Installation C:\PROGRA~1\eScan\Setup\Launchit.Exe,C:\PROGRA escan\Setup\Setup.exe	
Disable auto downloading of Windows patches by Installation Path Cefault> Install Other Software Linux/MAC Client Setup Required files for Installation C:\PROGRA~1\eScan\Setup\Launchit.Exe,C:\PROGRA	

3. Select Install eScan option.

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

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

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

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





Uninstall eScan Client

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

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

Client Uninstallation window appears.

Client Uninstallation
Ready to Start Uninstallation Click "Uninstall" to Start Uninstallation
Uninstall Cancel

3. Click Uninstall.

The Client Uninstallation window displays the progress.

Client Uninstallation	
9/26/2019 4:47:37 PM : 9/26/2019 4:47:37 PM : 9/26/2019 4:47:37 PM : 9/26/2019 4:47:37 PM : 9/26/2019 4:47:37 PM :]: Reading Host Details []: Version 14.0.1400.2220 []: Service Pack 2220
Close Cancel	

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

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





Move to Group

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

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

Remove from Group

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

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

Refresh Client

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

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

Connect to Client (RMM)

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

- 1. Go to Managed Computers.
- 2. Select the client computer which you want to add to RMM License.
- Click Client Action List > Connect to Client (RMM).
 RMM disclaimer appears.
- 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.





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.

licy Configuration	P 1
Policy Template Selection	
Assigned Group Policy(ESCAN_DEFAULT_POLICY) QA SAMPLES	· · · · · · · · · · · · · · · · · · ·
	~
Select	

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.
- 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.

🛐 Action List 🔻 🋐 Client Action List 🔻 📿 Refresh Client	😤 An	ti-Theft 🔻 🛐 Select C	columns		
🚊 🫅 Managed Computers	0	💻 eScan Installed	🔿 📃 eScan No	t Installed 1 - 3 of 3 i∉ (p	age 1 of 1) > Row
Policy		Computer Name	IP Address	IP Address of the connection	<u>User name</u>
		WATZYN-ILL	192.000.000		WIN-10 President
Client Computers (3)		MIRH-GUP	192.008.048		WIN
🗄 💼 Roaming Users		M01-Q8007	192.000.007		
D. D. Whatsage_Access_Droug					

 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.

Excel		O PDF	
Select All Columns			
Computer Name	IP Address	IP Address of the connection	🗹 User name
Local Administrator User(s)	🗹 eScan Status	Version	Last Connection
Installed Directory	Monitor Status	🗹 Anti-Spam	🗹 Mail Anti-Virus
✓ Web Protection	Endpoint Security	Firewall	🗹 Last Update
✔ Update Server	Client OS	✓ Status	🖌 Last Policy Applied
Last Policy Applied Time	Last eBackup Status		

- 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.

🛐 Action List 🔻 🛐 Client Action List 🔻 💈 Refresh Client	💦 Ant	i-Theft 🔻 🚺 Select C	Columns		
🗄 🛅 Managed Computers	0	💻 eScan Installed	🔿 📃 eScan No	t Installed 1 - 3 of 3 📧 (p	age 1 of 1 → > Row
🛅 Policy		Computer Name	IP Address	IP Address of the connection	<u>User name</u>
🔂 Group Tasks		📕 WARN-5.5	192.008.0.075		WIN
Client Computers (3)		MIN-GLF	192.008.046		WIN
🖻 🧰 Roaming Users		M01-Q8007	192.		
0. Whateage_terms_Droup		·			

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

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

Installed Softwares	_? Hel
Computer Name: WI with an and the second	Total No.Of Installed Programs: 12
Currently Installed Programs	
Advanced IP Scanner 2.5	
Dropbox	
eScan Corporate - 360	
Google Chrome	
Microsoft SQL Server 2008 R2	
Microsoft SQL Server 2008 R2 Native Client	
Microsoft SQL Server 2008 R2 Setup (English)	
Microsoft SQL Server 2008 Setup Support Files	
Microsoft SQL Server Browser	
Microsoft SQL Server VSS Writer	
Microsoft Visual C++ 2017 Redistributable (x86) - 14.12.25810	
VMware Tools	





Force Download

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

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

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

🛐 Action List 🗸 🋐 Client Action List 👻 🍣 Refresh Client	💦 Ant	ti-Theft 🔻 🋐 Select C	columns		
🗄 🗂 Managed Computers	0	💻 eScan Installed	🔿 📃 eScan No	t Installed 1 - 3 of 3 i∢ (p	age 1 of 1 → ⊨ Row
🛅 Policy		Computer Name	IP Address	IP Address of the connection	<u>User name</u>
🔂 Group Tasks		📕 WATER- B.B.	192.000.000		WIN I President
··· 📕 Client Computers (3)		MIN-GLF	192.000.000		WIN
E - Caming Users		M010-QM0107	192		
E- Vitalange_terman_Droop			1		1

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







Forensic-Port/Communication

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

7/8/2021	12:35:51	M : Processing with gro	un:O		
		M : Connecting to Comp		n.111 7	
		M : Successfully Export		The Constant 7	

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

E	Computer Name	Last EBackup Status	Forensics Report
) 📕 W 19- Cell 17 🎅	Job Name:Test Bak - Date:2 John Backup - O -Status:Backup Finished., No files to upload on [No new files found for backup.]	View

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

WIN GRINT	· · · · · · · · · · · · · · · · · · ·	Refresh 🔋 Help
Search files in selected Date Range From 06/06/2021	MM/DD/YYYY To 07/06/2021	arch Reset
Delete Report Type Forensics - Port/Communication Report 🗸		
File Name	Created On (Date and time)	Size
eScan Forensics Anti-Malware	22 Jun 2021,11:52 AM	308 КВ
eScan Forensics Port	22 Jun 2021,11:19 AM	327 KB
Close		





On Demand Scanning

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

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

On Demand Scanning window appears.

On Demand Scanning (Forensic-Antimalware Scann	ing)	김 Help
Scan Option		
🗌 Spyware And Adware 📒	🗌 Computer StartUp 📒	
🗌 Memory Scan 📒 🙇	🗌 Registry 📒	
🗌 System Folder 📕	🗌 Scan network drives ╉	
🗌 Scan Local Drives 🖶 🙇		
🗌 Scan System Drive 📑		
🗌 Scan Data Drives 📒 🙇		
Scan Option		
🗌 Scan Archives 📒 🙇		
🗌 Auto Shut Down After Scan Completion 🚦		
🗌 Scan Only 🗮 🙇		
Scan Cancel		

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.

Action List 🕶 🛐 Client Action List 🕶 📿 Refresh Client 🤰	🚴 Ant	i-Theft 🔻 🚺 Select C	olumns		
🗄 🦳 🎦 Managed Computers	0	💻 eScan Installed	🔿 📃 eScan No	t Installed 1 - 3 of 3 🗔 🖗	age 1 of 1 + + Row
Policy		Computer Name	IP Address	IP Address of the connection	<u>User name</u>
Group Tasks		📕 WARN-53	192.000.000		WIN-10 President
Client Computers (3)		MON-GUP	192		WIN
🗄 🧰 Roaming Users		- W1281-QHI2127	192.000.007		
🖻 🧰 Whateage_times_Droug					

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

	E
Message Text :	350/350
1	
	Send Cancel

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.

Deploy Outbreak Prevention	Restore Outbreak Prevention
utbreak Prevention Policies	
Limit access to shared folders (All	ow read only access)
Deny write access to local files an	d folder
Block Specific Ports	
Disale All Deater (Others there beyond	client-server ports)
Block All Ports (Other than trusted	
Automatically restore outbreak pro Narning: The above outbreak preven configuration of these policies settings	evention after 1 v hours(s) tion policies will be enforced on all the selected computers or groups. Incorrect can cause major problems with the computers.
Automatically restore outbreak pre Warning: The above outbreak preven configuration of these policies settings utbreak Prevention Notification	tion policies will be enforced on all the selected computers or groups. Incorrect can cause major problems with the computers.
Automatically restore outbreak pre- Warning: The above outbreak preven configuration of these policies settings utbreak Prevention Notification	tion policies will be enforced on all the selected computers or groups. Incorrect can cause major problems with the computers.
Automatically restore outbreak pre- Warning: The above outbreak preven configuration of these policies settings utbreak Prevention Notification Notify client users when outbreak Message: eScan has detected a security risk out	tion policies will be enforced on all the selected computers or groups. Incorrect can cause major problems with the computers.
Automatically restore outbreak pre- Warning: The above outbreak preven configuration of these policies settings utbreak Prevention Notification Notify client users when outbreak Message: eScan has detected a security risk out	tion policies will be enforced on all the selected computers or groups. Incorrect can cause major problems with the computers. prevention starts 207/250 break on your network. To prevent the security risk from spreading, your eScan

Limit access to shared folders

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

Deny write access to local files and folder

Select this check box 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 check box 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 check box 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 check box **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.

Deploy Outbreak Pre	vention Restore Outbreak Prevention	
Restore Outbreak Pre	vention	
Notify client users Message:	after restoring the original settings	96/250
_	orcing outbreak prevention policies and has restored pre-outbreak settings.	
eScan has stopped en	orang outsites prevention poinces and has restored pre-outbreak settingsi	

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

To notify clients about Outbreak Prevention restoration, select the check box **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.

🋐 Action List 🔻 🋐 Client Action List 👻 💈 Refresh Client	💦 Ani	ti-Theft 🔻 🛐 Select C	columns		
🗄 🗂 Managed Computers	0	💻 eScan Installed	🔿 📃 eScan No	t Installed 1 - 3 of 3 🗔 🖗	age 1 of 1 ⊨ ⊨ Row
Policy		Computer Name	IP Address	IP Address of the connection	<u>User name</u>
Group Tasks		📕 WARR-11.	192.		WIN I President
Client Computers (3)	0	MIN-GUP	192.000.040		WIN CALF
🗈 🦳 Roaming Users		M01-Q8007	192		
ErWhattenpp_terman_Errorp					

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

10/1/2019 12:53:20 PM : Processing with group : Sample Group 10/1/2019 12:53:20 PM : Connecting to Computer 10/1/2019 12:53:20 PM : Quarantine files successfully deleted	Help

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.

te One Time Password Computer Name:* ESTate Culture Valid for:* 10 mins V Select Option Select Option File Anti-Virus + RE Allow to Change Ipt	
Valid for:* 10 mins V	
Valid for:* 10 mins V	
- Select Option	
🗌 File Anti-Virus 💶 🕿 🗓 👘 💭 🔲 Allow to Change Ip	
Web Protection	
EPS App Control EPS USB	
🗌 Mail Anti-Virus & Anti-Spam	
New Password	
Password	

- 3. In the **Valid for** drop-down, select the preferred duration to bypass the protection module.
- 4. In **Select Option** section, select the module you want to disable.





5. Click **Generate Password**. An OTP will be generated and displayed in **Password** field.

Password generator	
Generate One Time Password	
Computer Name:*	QA-EDR
Valid for:*	10 mins V
Select Option	
🗌 File Anti-Virus 👯 👰 🖳	Allow to Change Ip
🗌 Web Protection 📒 👧	Firewall
EPS App Control	🗆 EPS USB 🚝 👧 🌇
🗌 Mail Anti-Virus & Anti-Spam	
New Password	
Password	3AAUDHTDQDB9 Password is case-sensitive
Generate Password Close	(*) Mandatory Field

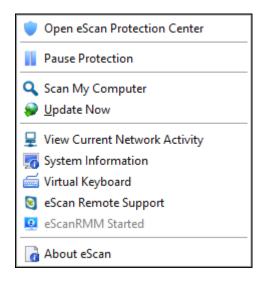




Entering an OTP

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.

	×
K	eScan Protection Center
Enter eScan Administrator Password	
•••••	
Duration	
15 minutes V	
	OK Cancel

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

The selected module will be disabled for set duration.







Pause Protection

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

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

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

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

🛐 Action List 🔻 🛐 Client Action List 👻 🌮 Refresh Client 🖄 Anti-Theft 👻 🛐 Select Columns					
🗄 🫅 Managed Computers	0	💻 eScan Installed	🔿 📃 eScan No	ot Installed 1 - 3 of 3 🖂 (p	age 1 of 1) → Row
Policy		Computer Name	IP Address	IP Address of the connection	<u>User name</u>
Group Tasks		📕 WATER- B.B.	192.000.000		WIN
		MIN-GLF	192.000.040		WIN
🗄 🛅 Roaming Users		M010-QA017	192.		
È- 🛑 Ministrine È- 🛑 Ministryp_honese_Droup			1	1	1

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

(Client Status
	7/8/2021 12:53:15 PM : Processing with group : Q M 7/8/2021 12:53:15 PM : Connecting to Computer W 7 7/8/2021 12:53:15 PM : Successfully Paused Protection on W 7





Resume Protection

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

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

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

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

🛐 Action List 🔻 🛐 Client Action List 🔻 🤣 Refresh Client 🕅 Anti-Theft 👻 🋐 Select Columns					
🗄 🗂 Managed Computers	0	💻 eScan Installed	🔿 📃 eScan No	t Installed 1 - 3 of 3 🗔 🤅 p	age 1 of 1 ⊨ ⊨ Row
Policy		Computer Name	IP Address	IP Address of the connection	<u>User name</u>
Group Tasks		W/29-51	192. 48. 191		WIN-10 President
Client Computers (3)		MIN-GLP	192		WIN-CALP New
년- 🧰 Roaming Users		M010-QADD7	192		
🖻 - 🧰 1996autona È - 🚞 Mhalongg "Accana, Shoo			1		1

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

Client Status			
•			
	7/8/2021 12:54:31 PM : Processing with group : Q M		
	7/8/2021 12:54:31 PM : Connecting to Computer W		
	7/8/2021 12:54:31 PM : Successfully Resumed Protection on W		





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.

perties	?	н
SCAN_CLIENT		
eneral		
Computer Name	ES (mm_Culture)	
IP Address	192	
User name	ESIGN, CLIER Million at stor	
Operating System	Windows XP Professional x64 Edition 64-bit	
V-Status		
Anti-Virus Installed	Installed (Client) - eScan Corporate for Windows	
Version	14.0.1400	
Installed Directory	C:\Program Files (x86)\eScan	
Update Server	192	
Last Update	2021/06/29 13:27	
otection		
File Anti-Virus	Enabled	
Mail Anti-Virus	Disabled	
Anti-Spam	Disabled	
Web Protection	Enabled	
Firewall	Disabled (Allow All)	
Endpoint Security	Enabled	



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





Anti-Theft

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

🋐 Action List 🗸 🋐 Client Action List 🗸 💈 Refresh Client	😤 Anti	Theft 🔻 🗻 Select C	olumns			
🗄 🛅 Managed Computers	0	eScan Installed	🔿 📃 eScan No	t Installed 1 - 3 of 3 🖂 (pa	age 1 of 1 ⊧ ⊧∣ Rom	ws per page: 10 💙
···· 🛅 Policy		Computer Name	IP Address	IP Address of the connection	<u>User name</u>	Local Administrator User
- 🔂 Group Tasks		🜉 WAT2N-B.B.	192.000.000		WIN-10 President	tration/President
- Elient Computers (3)		MIN-GUP	192.008.049		WIN-Duff and	A attraction and
🖻 💼 Roaming Users		MIN QADD?	192.008.0.007			
🗄 - 🦰 Whateau, Strong						
	•					
		Protected	_	Not Installed / Critical	💻 Unkn	own status

Anti-Theft Options

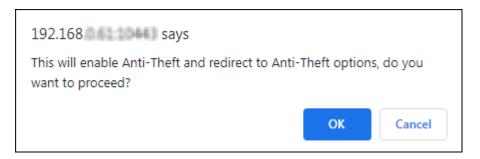
To add computers in an Anti-theft, follow the steps given below:

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

The computer will add in Anti-Theft Portal.

Anti-Theft	
Following is Email Id which will be use to Enable Anti-Theft o	n
client Computer, If you want you can change Email Id. Email ID : com	
Ok Cancel	

5. A confirmation prompt appears.







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

WELDHALL-JOHAN	Device Lost Reset Configure Data wipe		
My eScan			-
Locate Locate View Details O			
Action Features			-
Lock Lock View Details ©	Scream Scream View Details O	Alert Alert View Details O	Data wipe Data wipe View Details O

Anti-Theft Portal

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

VAUDNALL-JOKKA	Device Lost	Reset Configu	ıre Data wipe			
My eScan						-
Locate Locate View Details ©						
Action Features						-
Lock Lock View Details ©	Screa	m Scream View Details		Alert	Alert View Details •	ata wipe v Details O

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





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

100000000000000000000000000000000000000		Device Lost	Reset	Configure Data wipe	
My eScan					-
Locate	0				
Locate					
View Deta	ails 🔿				

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

Set Device as lost	×
If you set your device as stolen, below command will be sent to the device.	
Are you sure you want to set this device as lost?	
Confirm	lose

- Locate: This option will allow you to locate the system in case of loss/theft. Click on the Locate option on the anti-theft portal and the last known location of the system will be displayed on the map. Procedure to Locate the system:
 - Click Locate, the status will change to Request Pending; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to locate the system is in progress.
 - 2) View Details displays the Last Location of your system on a map. It also shows details of last two successful executions of the Locate command.





- **Screenshot**: This option will take a screen shot of the system whenever it is synced to the server.
 - Click Screenshot, the status will change to Request
 Pending; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to take a screenshot is in progress.
 - 2) **View Details** displays the last two screenshots from the successful execution of the screenshot command.
- **Take Photo**: This option will allow you to take a snapshot of the current user of the system from the webcam on clicking the camera option on the anti-theft portal.
 - 1) Click **Camera**, the status will change to Request Pending; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to take a snapshot is in progress.
 - 2) View Details displays the last two snapshots taken from your system. Click **Reset** to reset the **Action Features** on the system; these actions can be performed on the system when it has been lost or stolen.

Action Features			-
Lock	Scream	Alert	Data wipe
Lock () View Details O	Scream 3 View Details 3	Alert 1 View Details 3	Data wipe () View Details ●

There are following action features.

• Lock: The Lock feature will block the system from any further access. You will have to unblock the system by entering the pin provided on the anti-theft portal. On the anti-theft portal, select your System Alias name and then click Lock to remotely block your system, to unblock your system you will have to enter the Secret Code provided at the time of executing the lock command.





- **Scream**: Scream will allow you to raise a loud alarm on the system; this will allow you to trace the system if it is in the vicinity. Click **Scream** option to remotely raise a loud alarm on your system.
- Alert: This option will allow you to send an alert message (up to 200 characters) to the lost system. This alert message will be displayed on the screen; you can write and send any message for example: Request a call back or send your address or any kind of message to the current holder of your system. With this option there will be higher chance of your lost system being returned. Click Alert option to remotely send a message to your lost system. Type in your message in the send message section and click confirm.
- Data wipe: The Data Wipe feature will delete all the selected files and folders that have been added to the list to be deleted from the portal. Click data wipe option to remotely wipe all the selected files and folders or only delete the cookies and click confirm. Select the Delete Cookies check box to delete cookies or select the Datawipe check box to wipe the data and click on Confirm.

Disable Anti-Theft

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

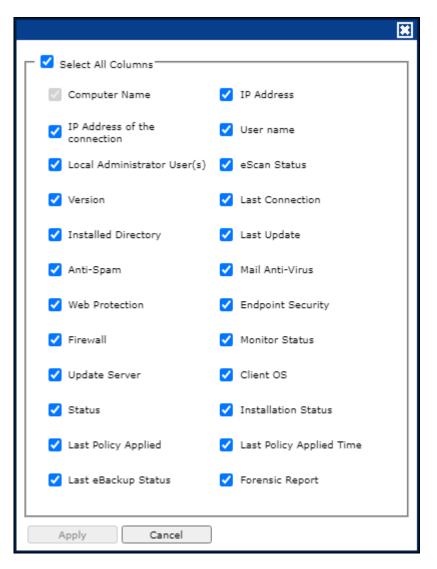
- 1. Go to Managed Computers.
- 2. Select the desired computers in Anti-theft Portal.
- 3. Click Anti-Theft > Disable Anti-Theft.





Select Columns

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



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





Policy Template

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

Managing Policies

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

Defining Policies Windows computers

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

File Anti-virus

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

Mail Anti-Virus

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

Anti-Spam

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

Web Protection

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

Firewall

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

Endpoint Security

The Endpoint Security module monitors the application on client computers. It allows/ restricts USB, Block list, White list, and defines time restrictions for applications. To learn more, <u>click here</u>.





Privacy Control

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

Advance Security

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

Administrator Password

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

ODS/Schedule Scan

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

MWL Inclusion List

Inclusion List contains the name of all executable files which will bind itself to MWTSP.DLL. All other files are excluded. To learn more, <u>click here</u>.

MWL Exclusion List

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

Notifications & Events

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

Schedule Update

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

Tools

Tools policy let you configure eBackup Settings. To learn more, <u>click here</u>.





Defining Policies Mac or Linux computers

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

File Anti-Virus



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

Endpoint Security



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

On Demand Scanning



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

Schedule Scan



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

Schedule Update

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

Administrator Password

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





Web Protection

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

Network Security



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



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.
- Select the desired group and then click **Policy Template**.
 Policy Template window appears.

Templates				💲 Refresh
New Template	operties Parent Policy 👘 D	Delete Assign to Group(s)	Assign to Computer(s)	y Template Export To 💙
Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
Name of Template	<u>Created On</u> Jun 19 2021 06:07:27 PM	<u>Modified On</u> Jun 29 2021 01:01:43 PM	<u>Assigned to Group(s)</u>	Assigned to Computer(s)

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

ew Template			김 Help
Select Rule-Sets			
Enter Template Name:*			
			-
File Anti-Virus	Edit	Mail Anti-Virus	
Assign From Select Policy		Assign From Select Policy	
Anti-Spam	Edit	Web Protection	
Assign From Select Policy V		Assign From Select Policy	
FireWall	Edit	EndPoint Security Edit	
Assign From Select Policy 🗸		Assign From Select Policy	
	Edit	Advance Security	
Assian From Select Policy	Edit		
Assign From Select Policy V		Assign From Select Policy	
_ _			_
Administrator Password	Edit	ODS/Schedule Scan	

- 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.

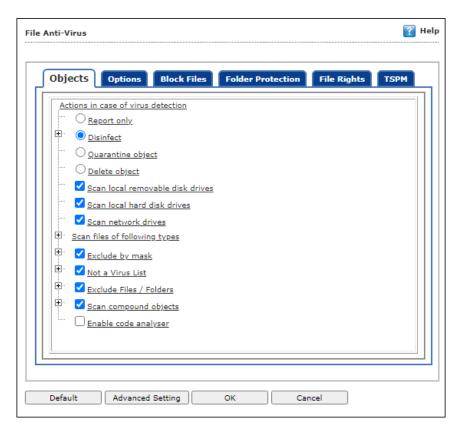
File Anti-Virus

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:

File Anti-Virus	Help
Objects Options Block Files Folder Protection File Rights TSPM	
 Save report file Show pack info in the report Show clean object info in the report Limit size to (KB) (avpM.rpt) Enable Auto backup / Restore Limit file size to (KB) Proactive Behaviour Monitor Display attention messages Enable Malware URL Filter Enable Ransomware Protection 	
Default Advanced Setting OK Cancel	





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 Autobackup 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.

ects Options Block	K Files Folder Protection File Rights TSPM	
Disable Autoplay on USB :	and Fixed Drives	
Deny access of executa User defined whitelist	tables on USB Drives	
File Name		Add
		Delete
		RemoveAll
Deny access of executa	tables from Network	
User defined whitelist		
Folder Name	Include Subfolder	Add
Folder Name	Include Subfolder	
Folder Name	Include Subfolder	Delete
		Delete
Deny Access of followin	ing files	Delete
 Deny Access of followin Quarantine Access-den 	ing files	Delete RemoveAll
Deny Access of followir Quarantine Access-den File Name	ing files	Delete
 Deny Access of followin Quarantine Access-den 	ing files	Delete RemoveAll Add
Deny Access of followir Quarantine Access-den File Name	ing files	Delete RemoveAll Add Delete

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**.

Add Folder	
C:\Documents and Settings\Remya\My Documents	
🖉 Include Subfolder	
Add 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.

- 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-Vir	us		👔 Helş
Objects		File States Folder Protection File Rights TSP	
	Folder Name	Include Subfolder	Add Delete RemoveAll
Default	Advanced Settin	g 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.

Virus		
jects Options Block Files F	older Protection File Rights TS	РМ
Enable eScan Remote File Rights		
Do not allow remote users to modify th	he following local files	
File / Folder Name	Include Subfolder	Add
•.EXE		Delete RemoveAll
.сом		
		•
Allow Modification for following Files		
File / Folder Name	Include Subfolder	Add Delete
	V	RemoveAll
WINDIR%\TEMP\	V	•
Enable eScan Local File Rights		
Do not allow local users to modify the	following files	
File / Folder Name	Include Subfolder	Add Delete
		Delete

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.

jects Options Block Files Folder Protection	File Rights TSPM
Enable Terminal Service Protection Module	
Allow Local IP : Allow local IP of same subnet 🗸	
	Add
WhiteListed IPs	Delete
Block All Foreign IP	
Not Allowed List :	
NA List	Add
FreeRDP	Delete RemoveAll
Rdesktop	
a	
Windows7	-
RDP blocked from foreign country	
Whitelist Foreign Country for RDP : (e.g. India or Tunisia or Ur	nited States)
Country Names	Add
	Delete RemoveAll
	Kentoveni
Show RDP block alert	
Block brute force attack	

Enable Terminal Service Protection Module

Select this check box to activate TSPM module.





Allow Local IP

This dropdown menu has following options:

Allow Local IP :	Allow local IP of same subnet $ullet$	
	Allow only whitelisted IPs	
	Allow local IP of same subnet	
WhiteLis	Allow local IP for all subnet	

• Allow only whitelisted IPs: Select this option to allow only whitelisted IPs to connect to the endpoints.

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

Add IP	**************************************
IP Address*:	
Ok Cancel	(*) Mandatory Fields

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

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

Block All Foreign IP

Select this check box to block all the foreign IP address from communicating from the endpoint within the network.

Not Allowed List

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

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





RDP blocked from foreign country [Default]

This check box blocks all the RDP connection attempts from the foreign country.

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

This option allows to whitelist the country names, so that RDP connections from those countries can be allowed.

Show RDP block alert [Default]

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

Block brute force attack [Default]

This check box allows to block the connection in case of any brute force attack.

Advanced Settings

Clicking Advanced Settings lets you configure advanced settings for console.

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

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

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

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

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





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

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

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

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

Clear Quarantine folder after Days specified

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

Clear Quarantine Folder after Size Limit specified in MB

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

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

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

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

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

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

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

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

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

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

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

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

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





Define Virus Alert Time (in seconds)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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





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

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

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

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

Enable Cloud (1 = Enable/0 = Disable)

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

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

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

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

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

Whitelisted AutoConfigURL

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

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

Selecting this option disables Add-ons and Extension blocking.

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

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

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

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

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

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

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

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

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

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





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

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

Ð	Only if it is enabled the setting " NetworkSharesReadOnlyAccess " and
NOTE	"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.

Mail Antivirus Settings	Help
Block Attachments Types Add PRETTY*.EXE Delete NAVI*.EXE Advanced FIX200*.EXE Advanced MINE.* TR**.EXE SUPP*.EXE Advanced Port Settings Port Settings for eMail Outgoing Mail(SMTP) [25] Incoming Mail(POP3) [10] Scan Outgoing Mails Scan Outgoing Mails	
Default Ok Cancel	

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:

	Ξ				
Advanced Scan Options					
Delete all Attachments in eMail if Disinfection is not possible Selete entire eMail if Disinfection is not possible					
Delete entire eMail if any Virus is found					
Quarantine Blocked Attachments					
Delete entire eMail if any Blocked Attchement is found Quarantine eMail if Attachments are not Scanned Image: Comparison of the second se					
Quarantine Attachments if they are Scanned Exclude Attchements (White List)					
Add					
Delete					
Save Cancel					

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.

dvano	ed
	Send Original Mail to User
	Do not check content of Replied or Forwarded Mails
	Check Content of Outgoing mails Phrases
	Spam Filter Configuration
	Check for Mail Phishing
	Treat Mails with Chinese/Korean character set as SPAM
	Treat Subject with more than 5 whitespaces as SPAM
	Check content of HTML mails
	Quarantine Advertisement mails Advanced
	Mail Tagging Options
\bigcirc	Do not change email at all.
	Both subject and body is changed. [Spam] tag is added in Subject. Actual spam content is embedded in Body.
\bigcirc	"X-MailScan-Spam: 1" header line is added. Actual spam content is embedded in Body.
۲	Only [Spam] tag is added in Subject. Body is left unchanged.
\bigcirc	"X-MailScan-Spam: 1" header line is added. Body and subject both remain unchanged.

Advanced

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

Send Original Mail to User [Default]

This 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.

Advanced Spam Filtering Options	
 Enable Non Intrusive Learning Pattern (NILP) chect 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 Add bl.spamcop.net Delete b.barracudacentral.org Remove All	Auto-Spam Whitelist Add *@analytics.bounces.googl *@irctc.co.in *@sourcenext.co.jp *@sourcenext.com *@sourcenext.com





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

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

Enable email Header check [Default]

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

Enable X Spam Rules check [Default]

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

Enable Sender Policy Framework (SPF) check

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

Active				O Block Web Access	
Filter Categories	Allow	Block		Site Names playboy.com	
Category Name	Туре	<u>Status</u>	^	playboycom	
Pornography	Block 🛩	Customize			
Gambling	Block 🗸	Customize			
Alcohol	Block 🗸	Customize			
Violence	Block 🗸	Customize			
Drugs	Block 💙	Customize			
Retires black estates	Diral at	Customine	-		-
Add Delete				Add Delete Save	

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.

Protection	👔 H
Start Stop	🗌 Start Phishing Filter 🗌 Start Malware URL Fi
Filtering Options Scanning Options Define Time-Restriction	
Actions U Log Violations Shutdown Program in 30 Secs.	Port Setting Internet Access (HTTP Port) 80,8080,3128,6588,4480,88
Default Advanced Setting OK Cancel	

Actions

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

Log Violations [Default]

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

Shutdown Program in 30 Secs

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





Port Setting

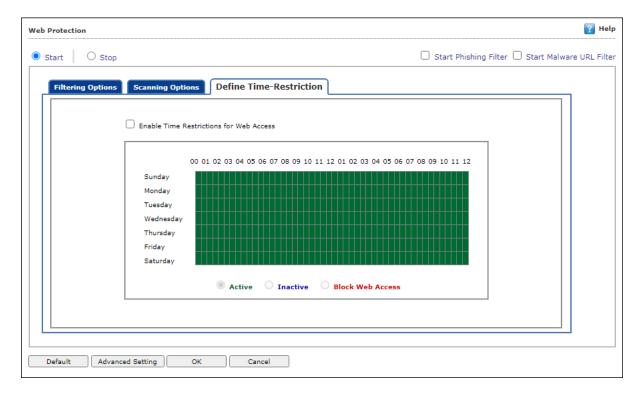
This section lets you specify the port numbers that eScan should monitor for suspicious traffic.

Internet Access (HTTP Port)

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

Define Time Restriction

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



Enable Time Restrictions for Web Access

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

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

Active

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





Inactive

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

Block Web Access

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

Phishing and Malware URL Filter

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

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

Web Protection	👔 Help
Start Stop	Start Phishing Filter Start Malware URL Filter

Advanced Settings

Clicking Advanced displays Advanced Settings.

Ignore IP address from Web-scanning

Select this option to enter IP address form Web-Scanning

Enable Unknown Browser detection

Select this option to enable/disable unknown browser detection

Enable allowing of WhiteListed Site during BlockTime

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

Enable Online Web-Scanning Module

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

Disable Web Warning Page Select this option to enable/disable web warning page

Enable HTTPS Popup

Select this option to enable/disable HTTPS Popup

Show External Page for Web blocking (Page to be define under External Page) Select this option to enable/disable external page for web blocking





External Page Link for Web blocking (Depends on Show External Page) Select this option to enter external page link for web blocking

Force inclusion of Application into Layer scanning (MW Layer) Select this option to enter Force inclusion of Application into Layer scanning

Enable HTTP Popup (1 = Enable/0 = Disable) Select this option to enable/disable HTTP pop-ups.

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

Allow access to SubDomain for Whitelisted sites(Only HTTP Sites) Select this option to enable/disable access to SubDomain for Whitelisted sites.

Allow access to SubDomain for Whitelisted sites(Only HTTPS Sites) Select this option to enable/disable access to SubDomain for Whitelisted sites.

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

Block EXE download from HTTP Sites (1 = Enable/0 = Disable) Select this option to enable/disable block download of .exe files from HTTP websites.

Block HTTP Traffic only on Web Browser Select this option to enable/disable block HTTP Traffic on Web Browser

Allow website list (Depends on "Block HTTP Traffic only on Web Browser") Select this option to enter to block HTTP Traffic on Web Browser.

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

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

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

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

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

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

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

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





Firewall

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

eWall			<mark>?</mark> Hel
Allow All O Limited Filter O Interactive Filter			
Zone Rule Expert Rule Trusted MAC Address Lo	ocal IP List Application Rule		
Name	IP Address/Host Name	Туре	Zone
Allow Local Network 192.168.*.*	192.168.0.1-192.168.254.254	IP Range	Trusted
Add Host Name Add IP Add IP Range	Modify Remove		
Show Application Alert			

The Firewall feature of eScan protects your data when you:

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

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





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

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

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

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

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

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.

Zon	e Rule Exper	t Rule Trusted MAC	Address Local IP Li	st Application R	ule		
	Firewall Rule				Rule Action Summary	A	
\Box	UDP Rule				Permits UDP packets on Any I	Interface between "My Netw	
	ARP packet exchan	ge - For mapping IP addre	dress	Permits ARP packets on Any I	interface		
\Box	NetBios (LAN File S	haring) - Access files and	, from your computer	Permits TCP and UDP packets	on Any Interface between "		
\Box	NetBios (LAN File S	haring) - Access files and	Blocks TCP and UDP packets on Any Interface between "A				
\Box	ICMP messages				Permits ICMP packets on Any Interface between "My Netv		
	ICMPV6 messages				Permits ICMPV6 packets on A	ny Interface between "My N	
\Box	DHCP/BOOTP packs	et exchange			Permits UDP packets on Any I	Interface between "Any Addi	
•	FTP Control - For d	ownloading and uploading	files		Permits TCP packets on Any I	nterface between "My Netwo	
	Add Disable	Modify	Remove	Shift up	Shift down	Enable	

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:

Firewall Rule	
General Source Destination Advanced	
Rule Name	ן ר
Rule Action	
Permit Packet Deny Packet	
	~
Apply Rule on Interface	~
OK Cancel	

General tab

In this section, specify the Rule settings:

Rule Name – Provide a name to the Rule.

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

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

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





Source tab

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

Add Firewall Rule	
General SOURCE Destination Advanced	
Source IP Address	1
O My Computer	
O Host Name	
O Single IP Address	
O Whole IP Range	
O Any IP Address	
My Network	
Source Port	
Any	
○ Single Port	
O Port Range	
O Port List	
	4
OK Cancel	

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.

When the selected Source IP Address and Source PortNOTE matches together.

Destination tab

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

General Source	Destination	Advanced	
-Destination IP Address			
O My Computer			
O Host Name			
○ Single IP Address			
O Whole IP Range			
Any IP Address			
My Network			
Destination Port			
Any			
O Single Port			
O Port Range			
O Port List			

Destination IP Address -

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

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





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

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

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

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.

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





Advanced tab

This tab contains advance setting for Expert Rule.

eneral Source Destination Advanced		
Enable Advanced ICMP Processing		
ICMP Type		
	In	Out
Destination Unreachable		
Echo Reply (ping)		
Echo Request (ping)		
Information Reply		
Information Request		
Parameter Problem		
Redirect		
Source Quench		
TTL Exceeded		
 The packet must be from/to a trusted MAC address Log information when this rule applies 	:	

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

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

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

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

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

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

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





Trusted MAC Address

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

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. 00-13Edit – 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.

Allow All 🔋 🔍 Lim	ted Filter O Intera	active Filter			
Zone Rule Expert	Rule Trusted MAC Ac	ddress Local IP List	Application Rule		
0000:0000:0000:00	00:0000:0000:0000:0001				
127.*.*					
192.168.*.*					
FE80:0000:0000:00	00:0000:0000:0000:0000				
		Class All			
EES0:0000:0000:00	00:0000:0000:0000 Remove	Clear All			

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.

Zone Rule Expert Rule	Trusted MAC Address Local IP List Ap	oplication Rule	
Application	Description	Path	Access

Defining permission for an application

To define permission for an application,

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

Add N	New Applicatio	n	
Арр	lication name wi	ith path	
			ןכ
	Ask	🔘 Permit	
			_
(OK Can	cel	

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

The permission for the application will be defined.

Removing permission of an application

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





Other Buttons

- **Clear All** This option will clear/delete all the information stored by the Firewall cache.
- **Show Application Alert** Selecting this option will display an eScan Firewall Alert displaying the blocking of any application as defined in the Application Rule.
- **Default Rules** This button will load/reset the rules to the Default settings present during the installation of eScan. This will remove all the settings defined by user.
- **Advanced Settings**: This button allows you to configure the advanced settings such as block port scan and disable Trojan rule.

dvanced Setting				
	Name	Value		
	Disable Trojan Rule	1 🗸		
\Box	Block Portscan	0 🗸		





Endpoint Security

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

ndPoint Security		🝸 Help
● Start │ ○ Stop		
	DLP (Attachment Control)	
Enter Application to Block List of Blocked Applications		
+ Custom Group	Allow This Group	Block
+ Computer Game	Allow This Group	Delete
+ Instant Messengers	Allow This Group	
+ Music Video Players	Allow This Group	
+ P2P Applications	Allow This Group	
Default Advanced Setting	OK Cancel	

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.



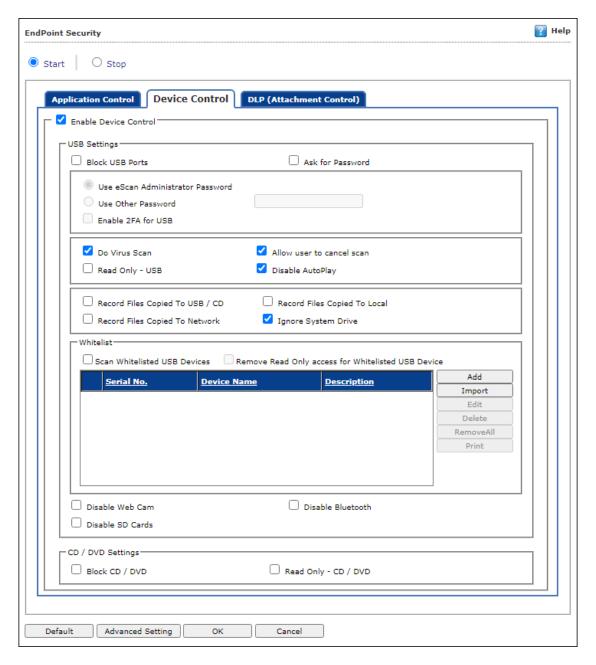


Datewise Restrictions

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.







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.
- Enable 2FA for USB: This option is available only when you select the Ask for Password check box. Click this option if you want enable 2FA feature for the USB.

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.

Read Only - USB

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





Disable AutoPlay [Default]

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

Record Files Copied To USB/CD

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

Record Files Copied To Network

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

Record Files Copied To Local

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

Ignore System Drive

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

Whitelist

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

Scan Whitelisted USB Devices

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

Remove Read Only access for Whitelisted USB Device

Select this option to remove the read-only access for the whitelisted USB Device.





Add

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

USB Whitelist					
•	<u>Serial No.</u>	<u>Device Name</u>	<u>Host Name</u>	<u>Client Date and</u> <u>Time</u>	<u>Description</u>
	34,10,40948	General Field Only USB Device	W 111 (mill 7	25/06/21 4:40:09 PM	
		A			
OK Cancel Custom Edit					

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

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

USB Whitelist		
Serial No.		
Device Name		
Description		
	OK Cancel	
	Cancel	

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





Import

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

Disable Web Cam: Select this option to disable Webcams.Disable SD Cards: Select this option to disable SD cards.Disable Bluetooth: Select this option to disable Bluetooth.

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.

Click **Default** to apply default settings done during eScan installation. It loads**NOTE** 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.

art O Stop	
Application Control Device Control DLP (Attachment Control)	
Attachment Allowed	
Attachment Blocked	
Enter Process Name : Eg. Thunderbird.exe	
Add Delete	
Blacklisted Process	
	-
	-
Attachments will be allowed from below sites irrespective of the above settings	
Attachments will be allowed from below sites irrespective of the above settings Enter Site Name : Eg. Gmail.com,Yahoo	
Enter Site Name : Eg. Gmail.com,Yahoo	
Enter Site Name : Eg. Gmail.com,Yahoo Add Delete	
Enter Site Name : Eg. Gmail.com,Yahoo	
Enter Site Name : Eg. Gmail.com,Yahoo Add Delete	
Enter Site Name : Eg. Gmail.com,Yahoo Add Delete	
Enter Site Name : Eg. Gmail.com,Yahoo Add Delete	
Enter Site Name : Eg. Gmail.com,Yahoo Add Delete	
Enter Site Name : Eg. Gmail.com,Yahoo Add Delete	
Enter Site Name : Eg. Gmail.com,Yahoo Add Delete	↓
Enter Site Name : Eg. Gmail.com,Yahoo Add Delete	×
Enter Site Name : Eg. Gmail.com,Yahoo Add Delete	×

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

Name	Value
Allow Composite USB Device	1 🗸
Allow USB Modem	1 ¥
Enable Predefined USB Exclusion for Data Outflow	1 ¥
Enable CD/DVD Scanning	1 💙
Enable USB Whitelisting option on prompt for eScan clients	0 🗸
Enable USB on Terminal Client	1 🗸
Enable Domain Password for USB	0 🗸
Show System Files Execution Events	0 🗸
Allow mounting of Imaging device	1 🗸
Block File Transfer from IM	1 🗸
Allow WIFI Network	1 🗸
Whitelisted WIFI SSID (Comma Separated)	
Allow Network Printer	1 🗸
Whitelisted Network Printer list(Comma Separated)	
Disable Print Screen	0 🗸
Allow eToken Devices	1 🗸
Include File Extension for File Activity Monitoring (e.g EXE)	





Allow Composite USB Device (1 = Enable/0 = Disable) Select this option to allow/block use of composite USB devices.

Allow USB Modem (1 = Enable/0 = Disable) Select this option to allow/block use of USB modem.

Enable Predefined USB Exclusion for Data Outflow Select this option to enable/disable use of predefined USB.

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

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

Enable USB on Terminal Client (1 = Enable/0 = Disable) Select this option to enable/disable USB on terminal client.

Enable Domain Password for USB Select this option to enable/disable domain password for USB

Show System Files Execution Events Select this option allow/block system files execution events

Allow mounting of Imaging device (1 = Enable/0 = Disable) Select this option to allow/block mounting of imaging devices.

Block File Transfer from IM (1 = Enable/0 = Disable) Select this option to allow/block file transfer from Instant Messengers.

Allow Wi-Fi Network (1 = Enable/0 = Disable) Select this option to allow/block use of Wi-Fi networks.

Whitelisted WIFI SSID (Comma Separated) Select this option to whitelist WIFI SSID

Allow Network Printer (1 = Enable/0 = Disable) Select this option to allow/block use of network printers.

Whitelisted Network Printer list(Comma Separated) Select this option to whitelist network printer list

Disable Print Screen Select this option to enable/disable use of printer screen





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

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

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

Select this option to include File Extension for File Activity Monitoring

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

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

Auto Whitelist BitLocker encrypted USB Devices

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

Ask Password for whitelisted Devices only

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





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.

ivacy Control		🝸 F
General Advanced		
Scheduler Options		
You can set to run this Tool Automatically a Options Below.	at Various times. Select the times you would	l like Auto Erase to run from the
Run at System Startup	Run Everyday at 0:00 am	٥٧
Clear Auto-Complete Memory Clear Last Run Menu Clear Temporary Folders Clear Last Find Computer Clear Browser Address Bar History	Clear Last Search Menu Clear Recent Documents Clear Favorites Clear Open/Save Dialog Box History Empty Recycle Bin	Clear Cache Clear Cookies Clear Plugins Clear ActiveX Clear History <u>Select All</u>
	_	
Default OK Cancel		

It consists following tabs:

- General
- Advanced

General tab

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

Scheduler Options

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

Run at System Startup

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





Run Every day at

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

Auto Erase Options

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

Clear Auto Complete Memory

Auto Complete Memory refers to the suggested matches that appear when you enter text in the Address bar, the Run dialog box, or forms in web pages. Hackers can use this information to monitor your surfing habits. When you select this 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 below option as well.

Select All/ Unselect All

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





Advanced tab

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

General Advanced MS Office MS Word	Windows	Others Windows Media Player Play List	Help
MS Excel MS PowerPoint MS FrontPage MS Access	Clipboard Data Start Menu Order History Registry Streams MRU (Most recently used) Application Log	U Windows Media Player History	
		<u>Select All</u>	
Default OK	Cancel		

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.

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

Policy Details also lets you do the following for Windows Operating System.





Advance Security

Following tabs with multiple threat protection options that are present in the EDR Policy:

- Advance Threat Protection
- Block Downloads from Internet
- Archive File Protection
- Block Files Using sha256

Advance Threat Protection	Block Downloads from Internet	Archive File Protection	Block Files Using sha256	
Block Unsigned Exe Downloaded Fi	om Internet			
Block Unsigned Exe From USB				
✔ Unsigned Exe White List (Cloud)				
Whitelisting for unsigned exe Download	ded From Internet/on USB			
Add whitelisted files or folder			Add	
			Delete	
			RemoveAll	
 Block WScript From Running Down Block Adobe Office Child Exe Block Custom Child Exe 	loaded Apps			
Add custom child exe			Add	
			Delete	
			RemoveAll	

The following section will describe the tabs and options in detail.

Advance Threat Protection

This tab allows you to block and whitelist the execution of EXE files downloaded from Internet or present in the USB. Along with its Advanced Threat Protection tab that enables to restrict the WScript and Adobe reader from the execution of child processes.

Block Unsigned Exe Download from Internet

This option blocks the execution of untrusted/unknown executable files that are downloaded from the internet.





Block Unsigned Exe from USB

This option blocks the execution of untrusted/unknown executable files from portable storage devices like USB drives.

Unsigned Exe White list (Cloud)

This option allows the execution of whitelisted executable files based on the eScan Cloud database. It is enabled by default.

Whitelisting for unsigned exe Downloaded From Internet/on USB

This option allows the user to whitelist the unknown executable files. After enabling the above listed options, you can configure this option.

Whitelisting for unsigned exe Downloaded From Internet/on USB			
Add whitelisted files or folder	Add		
	Delete		
	RemoveAll		

- Add: To add an unknown executable file, enter the name of the file and click Add. The file will be added in the list.
- **Delete:** To delete an executable file, select the particular file from the list and click **Delete**.
- **Remove All**: To remove all the files from the list, click **Remove All**.

Block WScript From Running Downloaded Apps

This option allows you to blocks the execution of any potentially malicious scripts (.js, PowerShell) that running from the downloaded apps.

Block Adobe Office Child Exe

This option allows you to block the generation of any child process (VB macros, exploit code, PowerShell commands) by Adobe Reader and Office apps.





Block Custom Child Exe

This option lets you to add or delete the custom child EXE.

- After enabling this option, you can configure the following options:
 - Add: To add custom child EXE, enter the name and click Add.
 - **Delete**: To delete any child EXE, select the file and click **Delete**.
 - **Remove All**: To remove all the file at once, click **Remove All**.

Block Downloads From Internet

This tab allows you to block or restrict the internet downloaded files and files downloaded from email clients.

EDR Policy	Help
Advance Threat Protection Block Downloads from Internet Archive File Protection Block Files Using sha256	
 □ Block Internet Downloaded Files ✓ Exclude Email Clients 	
Default OK Cancel	

Block Internet Downloaded Files

This option allows you to directly block the files while downloading from internet.

Exclude Email Clients

This option allows the execution of attachment and auto-run executable files that are downloaded via email clients (Outlook, Thunderbird, and more). It is enabled by default.

Archive File Protection

This tab allows or blocks the running of password-protected archive files (zip, rar, 7zip, and more).

EDR Poli	cy	👔 Help
Ad	Ivance Threat Protection Block Downloads from Internet	Archive File Protection Block Files Using sha256
Ca	se of Password Protected Archives:	Allow All Allow All Allow only default archive types Allow only excluded extensions Block All
Def	ault OK Cancel	





Following options can be configured:

Allow All

This option is enabled by default and allows running of all the password-protected archive files.

Allow only default archive types

This option allows the access of only default archive types and file name with extensions that are added in the list.

Advance Threat Protection Block Downloads	from Internet Archive File Protection Block Files Using sha256
Case of Password Protected Archives:	Allow only default archive types 💙
Action :	Access denied Access denied
Add Custom Unsafe Extensions	Qurantine archive
	Add
	Delete
	RemoveAll

Action

This drop-down option allows you to select the action to be taken in case of password protected archive file that does not belong to default type or whitelisted file extensions.

- **Access Denied:** This option will deny the access to the archive files that are not default type or whitelisted file extensions.
- **Quarantine archive:** This option will quarantine all the archive files other than default types or whitelisted file extensions.

Add Custom Unsafe Extensions

This option allows you to add custom unsafe archive in the list.

- Add: To add custom unsafe extension, enter the extension and click Add.
- **Delete**: To delete any custom extension, select the extension and click **Delete**.
- **Remove All**: To remove all the extension at once, click **Remove All**.





Allow only excluded extensions

This option allows the access of only the archive files extensions that are added in the excluded list.

olicy	
Advance Threat Protection Block Downloads from	m Internet Archive File Protection Block Files Using sha256
Case of Password Protected Archives:	Allow only excluded extensions
Action :	Access denied Access denied
□ Ignore Default Extensions	Qurantine archive
Exclusion List For Custom Extensions	Add
	Delete
	RemoveAll
Default OK Cancel	

Action

This drop-down option allows you to select the action to be taken in case of passwordprotected archive file that does not belong to excluded file extensions.

- Access Denied: This option will deny the access to the archive files that are not added in the exclusion list.
- **Quarantine archive:** This option will quarantine all the archive files that are not added in the exclusion list.

Ignore Default Extensions

This check box will allow the access of default archive extensions by including them in the blacklist.

Exclusion List for Custom Extensions

This option allows you to add custom extension file type in the list.

- Add: To add custom extension, enter the extension and click Add.
- **Delete**: To delete any custom extension, select the extension and click **Delete**.
- **Remove All**: To remove all the extension at once, click **Remove All**.





Block All

This option blocks the access of all the password-protected archive files types.

OR Policy	🛐 Help
Advance Threat Protection Block Downloads from Internet	Archive File Protection Block Files Using sha256
Case of Password Protected Archives: Action :	Block All Access denied Qurantine archive
Default OK Cancel	

Action

This drop-down option allows you to select the action to be taken on the passwordprotected archive file types.

- **Access Denied:** This option will deny the access to all the password-protected archive files.
- **Quarantine archive:** This option will quarantine all the password-protected archive files.

Block Files Using sha256

This tab allows you to block the files that are encrypted using SHA256 encryption based on the hash value of it.

_	Block Downloads from Internet Archive File Protection Block Files Using sha256
Enable SHA256 Prote Filter Categories	ion '
Category Name	Hashes Comment
CLOP ransomw	6d115ae4c32d01a073185df95d3441d51065340ead1eada0efda6975214d1920
ThiefQuest r	6d8d5aac7ffda33caa1addcdc0d4e801de40cb437cf45cface5350710cde2a74
	70f42cc9fca43dc1fdfa584b37ecbc81761fb996cb358b6f569d734fa8cce4e3
	a5f82f3ad0800bfb9d00a90770c852fb34c82ecb80627be2d950e198d0ad6e8b
	85b71784734705f6119cdb59b1122ce721895662a6d98bb01e82de7a4f37a188
	2ceeedd2f389c6118b4e0a02a535ebb142d81d35f38cab9a3099b915b5c274cb
	Add Delete
Add Delete	2ceeedd2f389c6118b4e0s02s535ebb142d81d35f38csb9s3099b915b5c274cb

Enable SHA256 Protection

This option lets you enable the SHA256 protection to block the files having identical hash key.





Filter Categories

This option will be enabled after selecting the **Enable SHA256 Protection** option. You can use this option to add or remove SHA256 categories and the hash values that has been added to the particular category.

Category Name

- Add: To add a filter category, enter the category name and click Add.
- **Delete**: To remove filter category, select the category name and click **Delete**.

Hash files

To add/remove the hash file in particular category, select the category and then add or delete the file.

• Add: To add a hash value, select the category in the **Category Name** column. Enter the hash value and comments (optional) and click **OK**.

Add Hash Key		
Hash Key:		
		ן נ
Comment:		۰ I
		1
ок	Cancel	

• **Delete**: To remove a hash file, select the category in the **Category Name** column. Select the hash file and click **Delete**.





Administrator Password

Administrator Password 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.

hange Password	
eScan Password Two-Factor Authentication	
O Set Password	Blank Password
Enter new Password	
Confirm new Password	
Password is case-sensitive	
Use separate uninstall password Enter uninstall password Confirm uninstall password	
afault Advanced Setting OK Canc	21

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





Two-Factor Authentication

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

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.

eScan Authe	ntication
C DIGITAL WORLD	Two-Factor Authentication
	Enter your passcode:
eSoan www.escanav.com	Verify
Copyright MicroWorld	Wed, 04 Aug 2021 01:17:00 PM UTC

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

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

You can enable the 2FA feature for existing Policy Templates by selecting aNOTE 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.

Change Password		?] I
eScan Password Two-Factor Au	thentication	
Enable Two-Factor Authentication		
RDP SafeMo	de 📃 User Logon	Unlock
Use Other Password Use Online Two-Factor Authenticat		
 All Users Particular Users Note : Users can be added via Setti 	ngs > Two-Factor Authentication > Us	sers for 2FA option
Default Advanced Setting OK	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

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

To learn more about adding user and enabling the 2FA, click here.

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

To use this feature, follow the steps given below:

- 1. Install the Authenticator app from Play Store for Android devices or App Store for iOS devices.
- 2. Open the Authenticator app and tap **Scan a barcode**.
- 3. Select the 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.

- Scan the onscreen QR code via the Authenticator app.
 A Time-based One-Time Password (TOTP) appears on smart device.
- 6. Forward this TOTP to personnel for login.





Advanced Setting

Clicking Advanced Setting displays Advance setting.

	Name	Value	
	Enable Automatic Download		
	Enable Manual Download	1 ¥	
0	Enable Alternate Download	1 ¥	
	Set Alternate Download Interval(In Hours)	6	
	Disable download from Internet for Update Agents	0 🗸	
	Stop Auto change for download from Internet for Update Agents	1 ¥	
\Box	Enable Download of AntiSpam update first on clients	1 ¥	
	No password for pause protection	0 🗸	
\Box	Download Signature Updates from Internet and Policy from Primary Server	0 🗸	
	Change ICON to eScan	0 🗸	
\Box	Stop Patch Notification	0 🗸	
	Set IPONLY	0 🗸	
Π	Enable HTTPS Download	0 🗸	

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

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

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

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

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

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

Set Alternate Download Interval (In Hours)

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

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

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





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

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

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

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

No password for pause protection

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





ODS/Schedule Scan

ODS (On Demand Scanning)/Schedule Scan provides you with various options like – checking for viruses, and making settings for creating logs and receiving alerts. You can also create task in the scheduler for automatic virus scanning.

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

It consists following tabs:

- Options
- Scheduler

Virus Check Alert		
In the case of an infection:	Automatic	~
Priority of scanner:	Normal (normal runtime)	~
File types:	Automatic type recognition	~
Use separate exclude list for ODS:	Add / Delete	
Limit CPU Usage	Enable for ODS only	~
CPU Percentage Value :	20 🗸	
CPU Percentage Value :	20 🗸	

Options

Options tab lets you make the settings for checking viruses and receiving alerts. There are two tabs – Virus Check and Alerts. You can do the following activities.

- Virus check
- Alerts





Virus Check

It lets you configure the settings for checking viruses. To set virus check,

- 1. Specify the following field details.
 - In the case of an infection: Select an appropriate option from the dropdown 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,
 - o High (short runtime)
 - o 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.

ODS/Schedule Scan	🕜 Help
Options Scheduler	
Virus Check Alert	
Alert	ק
Warn, if virus signature is more than 3 days old.	
Warn, if the last computer analysis was more than 3 days ago	
Log Settings	
Prepare Log	
Only infection to be logged	
Full log	
Default Advanced Setting Save Cancel	





To set alerts,

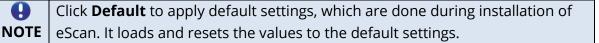
- 1. Under **Alert** section, Select the [Default] **Warn**, if virus signature is more than x days old check box, and then enter the number of days in the x days old field, if you want to receive alerts when virus signature exceeds the specified days. By default, value 3 appears in the field.
- 2. Select 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 appear 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.

Click **Default** to apply default settings, which are done during installation of **NOTE** 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.

Option	s Schedule	r		
	Name	Schedule	Next start	
	Clear All	Add task	Delete task	Edit







Clear All - This button wil	ll clear all the listed tasks.
Add Task	

Job Ana	ysis extent Schedule Virus scan	
Name	Active	
	n foreground 🗹 Allow user to cancel scan n background	
	virus detected 🗸	,
Scan only	v when idle Automatically shutdown machine after scar in to delete and to change properties of this job	1

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.

tomatic virus scan	T H
Job Analysis extent Schedule Virus scan	1
Scan Startup	
Scan memory, registry and services	
Scan local hard drives	
🗹 Scan System Drive	
🗹 Scan Data Drives	
Scan network drives	
Save Cancel	

- 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.

ob Analysis extent	Schedule Virus scan	
Execute		
Once	O Weekly	
	O Monthly	
O Daily	O With system startup	
Date and time	12:00 pm	
07/01/2021	12:00 pm	





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

Click the left < and right > sign to navigate to the previous or next month andNOTE 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.

atic virus scan Job Analysis extent Schedul	e 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		
e 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 dropdown 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.

Advanced Settings

Autorun System Scanning if System not scanned for days defined

This option let you define days for autorun system scanning if system is not scanned.

Ignore Battery Status

Select this option to Ignore Battery Status.

Scan USB when All Drive option selected

Select this option to scan USB when all drive options are selected.

Remove LNK

This option lets you Enable/Disable Removal of LNK.

Start Background Scan in System Mode

Select this option to start background scan in system mode.

Enable Scan Caching

This option lets you Enable/Disable scanning of cache.

Check for Corrupted Files

Select this option to check for corrupted files.

Scan in low Priority Mode

It lets you Enable/Disable the scan in low priority mode on the computer.

Enable Unhiding of USB Files & Folder

This option let you enable/disable unhiding USB files & folders.

Enable Missed schedule scan JOB's to run

This option let you enable/disable missed schedule scan JOB's to run.





MWL (MicroWorld WinSock Layer)

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

MWL Inclusion List

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

Click **Default** to apply default settings, done during eScan installation. It loads**NOTE** 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

MWL Inclusion List	🔋 Help
telnet.exe msimn.exe outlook.exe eudora.exe winpm-32.exe	Add Delete RemoveAll
whiphiszlexe phoenix.exe thebat.exe jrew.exe	
□ Jre.exe □ inetinfo.exe	





Add files to Inclusion List

To add executable files to the Inclusion List,

- 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.
- 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**.

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

You can do the following activities.

- Adding files to Exclusion List
- Deleting files from Exclusion List
- Removing all files from Exclusion List

MWL Exclusion List		👔 Help
]
		Add
VHTTPD32.DLL		Delete RemoveAll
NS-ADMIN.EXE		
NS-SLAPD.EXE		
TCPSVCS.EXE		
SVCHOST.EXE		
C ESERV.EXE		
DOWNLOAD.EXE		
C RP.EXE		
SPOOLER.EXE	-	
Default Ok Cancel		•





Adding files to Exclusion List

To add executable files to the Exclusion List,

- 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,

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

Removing all files from Exclusion List

To remove all executable files from the Exclusion List,

1. Click Remove All.

A confirmation prompt appears.

2. Click **OK**.

All executable files get removed from the Exclusion List.





Notifications and Events

Notifications & Events		👔 Help
Notifications Events		
Virus Alerts	Warning Mails	٦
Show Alert Dialog-box	presidente 2 est en com)
Mail Server Settings SMTP Mail Server SMTP Port User Authentication(Opt.) Authentication Password(Opt.) Virus Warning To Sender Virus Warning To Sender Virus Warning To Sender	Delete Mails From User Add Delete RemoveAll	
 Virus Warning To Recipient Content Warning To Sender Content Warning To Recipient 		
attrem.snd		
<pre>#Lines starting with # are comment lines. #This file specifies warning sent to Mail-Sender by #@Scan when it deletes attachments. # The attachment(s) that you sent with the following mail was deleted by eScan (not delivered to the recipient) ====================================</pre>		•
Default Advanced Setting OK O	Jancel	

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.





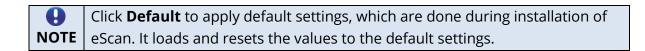
Events

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.

Notifications & Events	김 Help
Notifications Events	
Do not allow client to send event for	_
Executable Allowed	
 ✓ WebSite Allowed ✓ Cleaned Mail 	
Default Advanced Setting OK Cancel	







Advanced Settings

<u>Name</u>	<u>Value</u>
nable Caching of Unsent Events	1 🗸
show 'Secured by eScan' on startup	1 🗸
Show eScan Splash window	0 ¥
Send Only Defined Event Ids	
nable Gaming Mode	0 🗸
5	nable Caching of Unsent Events how 'Secured by eScan' on startup how eScan Splash window end Only Defined Event Ids

Enable Caching of Unseen Events (1 = Enable/0= Disable)

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

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

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

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

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

Send Only Defined Event Ids

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

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

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





Schedule Update

The Schedule Update lets you schedule eScan database updates.

Automatic Download		Schedule Download		
Daily				
Weekly	Mon	Tue	Wed	🗌 Thu
	📃 Fri	Sat Sat	Sun	
Monthly	1 .			
At	12:00 am	© V		

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

-OR-

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

Advanced Settings

Set bandwidth limit for download (in kb/sec)

It lets you define bandwidth limit for download on managed computers, if you have limited internet connection or other network issues.

Retry schedule download (Default retry interval is 15 minutes)

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





Tools

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

Tools	👔 Help
EBackup RMM Settings	
Add Backup Set	
Backup Name Next Start Created On	^
	Ψ.
(*) eBackup policy is not applicable for Policy Ok Cancel	Criteria Templates.

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.





The eBackup option has following tabs to configure:

Job

This tab you can schedule the eBackup option.

	ce and Exclusion Backup location
Active Name	
Scheduler	
Once	O Weekly
Hourly	O Monthly
O Daily	O With system startup
Date and time	▼ Date 07/08/2021 Time 4:57 PM ©▼
Set Restore Passw	ord Note* : Password can be set only while adding new job.

Active

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

Scheduler

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

Date and time

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

Set Restore Password

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





Backup Source and Exclusion

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

Add Backup Set				<u>?</u> Help
Job Backup Source and Exclusion Folder Settings	Backup location	File/Folder Exclusion Add File/Folder Folder O Exclude by mask	Add Delete RemoveA	
Save Cancel]

File Type and Folder Exclusion

This subtab allows to exclude the files/folder for backup.

Folder Settings

- Add File Type for Backup: Select the type of files for backup. By default, Office Documents option is selected.
- **File/Folder Exclusion**: In this section, you can exclude a specific folder or a file format from getting backed up. You can add, delete, and remove the files for the same.





Backup Location

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

Add Backup Set	🝸 Help
Job Backup Source and Exclusion Backup location Local/Network Google Drive DropBox OneDrive	
Store backup on Local/Network drive Local Drive Settings Destination Path for Backed up Files. UserName Password	
Note : Only Drive name or full UNC path is Allowed. Eg: 1. "c:\" 2. "\\192.168.0.96\external\backup"	
Save	

Local/Network

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

 Network storage 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.





Google Drive

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

Job Backup Source and Local/Network G00g	Exclusion Backup location DropBox OneDrive	
Store backup on Googl	Drive.	
-Google drive settings		
Select gmail account :		~
Refresh token :		
	Check Storage Login	
Remove gmail account :		~
	Mark for deletion Unmark	
*Note: the selected email w	I be permantly deleted only after saving the policy.	
	e Google Drive, select the appropriate Google account. If you have a Google a on also lets you create an account if you want to use account other than your	



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





DropBox

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

Job Backup Source and Ex		
Local/Network Google D	rive DropBox OneDrive	_
Store backup on DropBox		
DropBox settings		٦
Select DropBox account :	×.	
Refresh token :		
	Check Storage Login	
Remove dropbox account :	V	
	Mark for deletion Unmark	
*Note: the selected email will	be permantly deleted only after saving the policy.	
	DropBox, select the appropriate DropBox account. If you have a DropBox account, click "Login". Additionally, the eate an account if you want to use account other than your existing accounts.	

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





OneDrive

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

ob Backup Source and Exc Local/Network Google Dri	usion Backup location	
Store backup on OneDrive.		
OneDrive Settings		
Select OneDrive account :		~
Refresh token :		
	Check Storage Login	
Remove onedrive account :		~
	Mark for deletion Unmark	
*Note: the selected email will b	e permantly deleted only after saving the policy.	
Note: To store backup on the O	eDrive. select the appropriate OneDrive account. If you have a OneDrive account.	click "Login", Additionally, the
	reDrive, select the appropriate OneDrive account. If you have a OneDrive account, te an account if you want to use account other than your existing accounts.	click "Login". Additionally, the

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

Add Backup Set

9

NOTE

To create a Backup Set,

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

You can add the backup set for existing Policy Templates by selecting a PolicyNOTE 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. In Job tab, enter a name.
- 6. In the Scheduler section, select a preferred interval for backup execution.
- 7. Click **Backup Source and Exclusion** tab and configure the same accordingly.





- 8. Click **Backup Location** tab, select the appropriate option to save the backup file.
- 9. Click **Save**.

The Backup Set will be created.

By default, Active option is selected. If Active option is not selected, aNOTE 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:

Tools	Help
EBackup RMM Settings	
Manual Start	
O Auto Start	
User Acceptance Required	
Show RMM Connection Alert	
Ok Cancel	

- **Manual Start**: If this option is selected, client endpoint users have to manually start the RMM service to establish a RMM connection.
- **Auto Start**: If this option is selected, RMM service will be started automatically and all client endpoints will be connected to your main eScan server.
- User Acceptance Required: If this 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**.



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

Disclaimer	_
** The eScan RMM option is available for any number of devices during trial period.However, this option is not part of default eScan Corporate License. To use eScan RMM during contract period customer needs to purchase an Add-on License.	
eScan RMM allows administrator to connect to the client system using web browser. It help administrator to see user(s) screen and/or control user(s) computer remotely to offer precise assistance. During trial period Administratorget direct option connect to client by selecting Connect to Client(RMM) option available under "Client Action List". Once Administrator add the eScan RMM Add-on License to console, Administrator get option to add Client(s) toRMM license and get option to connect client under "Client Action List".	
Accept	el







 Read the disclaimer thoroughly and then click Accept.
 Your default browser opens eScan Remote Access window (Google Chrome, Mozilla Firefox, MS Edge, etc.)

eScan Remote Access Google Chrome Onot secure	dian Materia	which the Real	of Red Public Inte	atur futur		 Q
¹ C						
			\checkmark	1	Ť	Ţ
	Reconnect	Disconnect	De-Activate View Only	Screen Quality Settings	Send Key Combo	Hide

Following notification appears on client endpoint displaying IP address of RMM connecting endpoint and connection ID (If **Show RMM Connection Alert** option is selected).

eScar	RMM	
	Active Connection [ID:	-1
	10:	

RMM - Auto Start

If **Auto Start** option is selected, then client endpoints get automatically connected to your eScan server.

- Go to Managed Computers, select the target endpoint and then click Client Action List > Connect to Client (RMM). RMM disclaimer appears.
- 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.







Configuring eScan Policies for Linux and Mac Computers

eScan lets you define settings for File Anti-Virus, Endpoint Security, On Demand scanning and Schedule Scan module for Linux and Mac computers connected to the network. Click **Edit** to configure the eScan module settings for computers with respective operating systems.

□ File Anti-Virus 🙉 💟 Assign From Select Policy 🗸	Edit	EndPoint Security Se	Edit
ODS Settings 🙇 💟 Assign From Select Policy 🗸	Edit	Schedule Scan 🧟 😰 Assign From Select Policy 🗸 🗸	Edit
Schedule Update 🙉 Assign From Select Policy 🗸	Edit	Administrator Password	Edit
Web Protection Assign From Select Policy	Edit	Network Security Assign From Select Policy	Edit

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





File Anti-Virus 🍛 🛎

n the case of an infection:	Disinfect (if not possible, quarantine)	~
Scan Settings		
🗆 Archives 🙇 🖺	🗌 Mails 些	
🗹 Packed 🙇 🖺	🗌 Cross file system 🙇	
🗌 Follow symbolic links 👰		
Display attention messages		
 Display attention messages lumber of days log should be kept 	365	
· · · · · · · · · · · · · · · · · · ·		
🗌 Exclude by mask 🗳		
		Add
		Delete
		RemoveAll
🗆 Exclude Files / Folders 🙇 🖺		
		Add
		Delete
		RemoveAll
Add Directory for realtime scan	2	
		Add
/home		Delete
/tmp		RemoveAll

Actions in case of infection [Drop-down]

It displays a list of actions eScan should take, in case of virus detection.

In the case of an infection:	Disinfect (if not possible, quarantine) 🗸	
Scan Settings	Log only Disinfect (if not possible, log) Disinfect (if not possible, delete file) Disinfect (if not possible, quarantine) Delete Quarantine	
Follow symbolic links		





By default, Disinfect (if not possible, quarantine file) option is selected. Following are the types of actions:

- **Log Only:** This option indicates or alerts the user about the infection detected (No Action is taken; only logs are maintained).
- **Disinfect (if not possible, log):** This option tries to disinfect and if disinfection is not possible it logs the information of only the infected object.
- **Disinfect (if not possible, delete file):** This option tries to disinfect and if disinfection is not possible it deletes the infected object.
- **Disinfect (if not possible, quarantine file):** This option tries to disinfect and if disinfection is not possible it quarantines the infected object.
- **Delete:** This option deletes the infected object.
- **Quarantine:** This option quarantines the infected object.

Scan Settings

- **Mails** It indicates scanning the mail files. By default, it is selected. Select this 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.

Application Control

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

Start Start Stop Application Control Device Control File Integrity Monitor Enable Application Control	
Enable Application Control 🙇	
Enter Application/Package to Block	
List of Blocked Applications/Packages Application/Package Name	Add
reprised in sense name	Delete
	Remove All
Default OK Cancel	

Enable Application Control

Select the check box to enable the application control feature.

Enter Application/Package to block

Enter the application or package name to add them in the list of application/packages blocked.

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

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





Device Control

The Device Control tab helps to allow/block the USB/CD/DVD access.

Ipoint Security			<u>?</u> +
Start O Stop			
Application Control	evice Control File Integ	rity Monitor	
┌ 🙇 🗳 ────			
Enable Device Cont	rol		
USB Control			
Allow All	O Blo	ock All	Ask Password
Use Escan Admin			
Use Other Passwo	rd		
Blacklist	USB Devices		
Serial No.	Device Name	Description	Add
		beschption	Edit
			Delete RemoveAll
			Print
Monitor to USB	a	Autoscan to USB	
CD / DVD Settings 🧕 —			
	0		
O Block CD / DVD	O Read Only	- CD / DVD	Disable
Default OK	Cancel		

Enable Device Control: Select this check box to configure the Device Control settings.

- **USB Control**: This option lets you to allow, block, or ask password for the USB device connected to the endpoint. It has following options:
 - **Allow All:** Select this option to allow all the connected USB devices.
 - **Block All:** Select this option to block all the connected USB devices.
 - Ask Password: Select this option to set password for the connected USB devices. This will ask password before allowing USB devices to connect to the system. You can either set a password or use the administrator password using options Use Other Password and Use Escan Administrator Password respectively.
- **Blacklist:** This option lets 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.

USB Whitelist		
Serial No.		
L		
Device Name		
Description		
Description		
	OK Cancel	

- **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.





File Integrity Monitor

ndpoint Security	👔 Hel
Start O Stop	
Application Control Device Control File Integrity Monitor	·]
— 🗌 Enable FIM 🧟 ———————————————————————————————————	
File Integrity Check Alert Create New Baseline	
Enter Directory Name	
	Add
Directories Name	Delete
/іь	Remove All
/etc	
/bin	
/sbin	
Default OK Cancel	

Enable FIM

Select this check box to enable the File Integrity Monitor option.

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

Enter Directory Name

Enter the directory name to add it to the integrity monitoring.

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

To delete a specific directory from monitoring, select the directory, and click **Delete**. To remove all the directory from monitoring, click **Remove All**.

Default

This button 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.

S Settings 🧟 🖺		<u>?</u> He
In the case of an infection:	Disinfect (if not possible, quarantine) 💙	
Priority of scanner:	Normal (normal runtime) 🗸	
Exclude by mask		
		Add
		Delete
		RemoveAll
Exclude Files / Folders		
		Add
		Delete
		RemoveAll
Scan Options		
✓ Include sub directories	🗆 Mails	
	Archives	
Cross filesystem	Packed	
Follow symbolic links	Memory Scan	
Default OK	Cancel	

Actions in case of infection [Drop-down]

It indicates a type of action which you want eScan real-time protection to take, in case of virus detection.

In the case of an infection:	Disinfect (if not possible, quarantine) 🗙	
Priority of scanner:	Log only Disinfect (if not possible, log) Disinfect (if not possible, delete file)	
	Disinfect (if not possible, delete file) Disinfect (if not possible, Rename File)	
Exclude by mask	Disinfect (if not possible, quarantine)	
	Delete Infected File Rename Infected File	Add
	Quarantine	Delete
		RemoveAll
L		





By default, Disinfect (if not possible, quarantine file) option is selected. Following actions can be taken:

- Log Only: It indicates or alerts the user about the infection detected.
- **Disinfect (if not possible, log):** It tries to disinfect and if disinfection is not possible it logs the information of only the infected object.
- **Disinfect (if not possible, delete file):** It tries to disinfect and if disinfection is not possible it deletes the infected object.
- **Disinfect (if not possible, Rename file):** It tries to disinfect and if disinfection is not possible it renames the infected object.
- **Disinfect (if not possible, quarantine):** It tries to disinfect and if disinfection is not possible it quarantines the infected object.
- Delete Infected File: It directly deletes the infected object.
- **Rename Infected File:** It directly renames the infected object.
- **Quarantine:** It directly quarantines the infected object.

Priority of Scanner – You can select the priority of scanning as **High (short runtime)**, **Normal (normal runtime)**, or **Low (long runtime)**.

- **High (short runtime)** Has a short runtime.
- Normal (normal runtime) Has a normal runtime.
- Low (long runtime) Has a long runtime.

Exclude by Mask – Select this check box if you want eScan real-time protection to exclude specific files, and Remove any or all Added Files whenever required.

Exclude Folders and Files – Select this check box if you want eScan real-time protection to exclude Folders and files from scanning. eScan lets you add; Remove any or all Added Files or Folders whenever required during On Demand Scanning.

Scan options

- **Mails** It indicates scanning the mail files. By default, it is selected. Select this check box if you want eScan real-time protection to scan mails.
- **Archives** It indicates the archived files, such as zip, rar, and so on. Select this check box if you want eScan real-time protection to scan archived files.
- **Packed** It indicates the compressed executable.
- **Memory Scan** This option ensures eScan scans the system's memory for any infection from malwares.
- Include Sub Directories This option ensures eScan scans all the sub directories recursively under every directory and not only the first level of directories.
- **Heuristic** Heuristic scanning is almost identical to signature scanning, which instead of looking for specific signatures looks for certain instructions or





commands within a program/application. This results in the detection of potentially malicious function in program/application.

- **Cross File System** that facilitates scanning of files over cross-file systems.
- **Follow Symbolic Links:** scans the files following the symbolic links.
- **Memory Scan**: This will scan the memory of the system.

You can restore default eScan settings by clicking **Default**.

Schedule Scan 🌢 🛎

Name	Schedule Type	Schedule	On

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

ime		
Schedule Analysis e	extent Virus scan	
- 🧟 🖺		
Once Hourly	 Weekly Monthly 	
O Daily		
Date and time Month : 7 V Date : (2 V 12:00 pm	

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

Automatic virus scan	🛐 Help
Name Schedule Analysis extent	
Scan Options 🙇 🖺	
✓ Include sub directories	Mails
Heuristic	Archives
Cross filesystem	Packed
Follow symbolic links	Memory Scan 🙇
Save Cancel	

Using this tab you can define the scan options for Linux and Mac computers connected to the network.

• **Include sub Directories** – This option lets you include sub directories while conducting an automatic scan.





- **Heuristic Scan** Heuristic scanning is almost identical to signature scanning, which instead of looking for specific signatures looks for certain instructions or commands within a program/application. This results in the detection of potentially malicious function in program/application.
- **Cross File System** that facilitates scanning of files over cross-file systems.
- Symbolic Link Scanning scans the files following the symbolic links.
- **Mails** It indicates scanning the mail files. By default, it is selected. Select this check box if you want eScan real-time protection to scan mails.
- **Archives** It indicates the archived files, such as zip, rar, and so on. Select this check box if you want eScan real-time protection to scan archived files.
- **Packed** It indicates the compressed executable. Select this check box if you want eScan real-time protection to scan packed files.
- **Memory Scan** This option will only scan the memory of the system.

Virus Scan

matic virus scan	
Schedule Analysis extent Viru	us scan
In the case of an infection: 🙇 😰	Disinfect (if not possible, quarantine) 💙
Priority of scanner: 🙇 鉴	Normal (normal runtime) 🗸 🗸
🗌 Exclude by mask 🧝 🗳	
	Add
	Delete
	RemoveAll
🗌 Exclude Files / Folders 🙇 📡	
	Add
	Delete
	RemoveAll
ave	

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	<u>?</u> Help
Automatic Download Start at 12:00 pm OT Every 1 v hours(s)	
Schedule Download	
Once Weekly	
Hourly Monthly	
Daily	
Date and time Month : 1 V Date : 1 V 12:00 AM	
Default Ok Cancel	

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





Administrator Password

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

vord

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 nonwork-related websites during work hours. You can configure the following settings.

Start/Stop

It lets you enable/disable **Web-Protection** module. Click the appropriate option.

Web Protection		🛐 H	lelp
🔿 Start 🖲 Stop			
			7
Allow O Block			
Filter Categories Allo	w Block	Site Names	
Category Name	Туре		
Pornography	Block 🗸		
Gambling	Block 🗸		
Alcohol	Block 🗸		
Violence	Block 🗸		
Drugs	Block 🗸		
Retires black estance.	Diash àé		
Add Delete		Add Delete Save	
]
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.





Network Security

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

Allow All O Limited Filter O Interactive Filter Zone Rule Expert Rule Trusted MAC Address Local IP List					
Name	IP Address/Host Name Type Zone				
Allow Local Network 192.168.*.*	192.168.0.1-192.168.254.254	IP Range	Trusted		





Firewall

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

Network Security 🧟			<table-cell> Help</table-cell>
FireWall Reverse Shell Block Port Scan			
O Allow All 📔 🖲 Limited Filter 📔 O Interactive Filt	er		
Zone Rule Expert Rule Trusted MAC Address	Local IP List		
Name	IP Address/Host Name	Туре	Zone
Allow Local Network 192.	192 192.168 - 19	IP Range	Trusted
Add IP Add IP Range Mo	dify Remove		
🗌 Enable Trojan Rule			
Default Save Cancel			

You can configure the following settings to be deployed to the eScan client systems. **Allow All** – Clicking **Allow All** disables the eScan Firewall i.e. all the incoming and outgoing network traffic will not be monitored/filtered.

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

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





Following tabs are available:

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

Zone Rule

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

- Add Host Name This option lets you add a "host" in the zone rule. After clicking Add Host Name, enter the HOST name of the system, select the zone (Trusted/Blocked) and enter a name for the zone rule. Click OK to create the zone rule.
- Add IP This option lets you add an IP address of a system to be added in the zone rule. After clicking Add IP, enter the IP address of the system, select the zone (Trusted/Blocked) and enter a name for the zone rule. Click OK to create the Zone Rule.
- Add IP Range This option lets you add an IP range to be added in the zone rule. After clicking Add IP Range, add the IP Range (i.e. a range of IP that the zone rules should be applied), select the zone (Trusted/Blocked) and enter a name for the zone rule. Click **OK** to create the zone rule.
- **Modify** To modify/change any listed zone rule(s), select the zone rule to be modified and then click **Modify**.
- **Remove** To remove any listed zone rule(s), select the zone rule and then click **Remove**.





Expert Rule

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

twork Security 🧟	8 F
○ Allow All	
Zone Rule Expert Rule Trusted MAC Address Local IP List Firewall Rule Firewall Rule Firewall Rule Firewall Rule Firewall Rule	Rule Action Summary
UDP Rule	Permits UDP packets on Any Interface between "!
ARP packet exchange - For mapping IP address to a hardware (MAC) address	Permits ARP packets on Any Interface
NetBios (LAN File Sharing) - Access files and folders on other computers, from your computer	Permits TCP and UDP packets on Any Interface be
NetBios (LAN File Sharing) - Access files and folders on my computer, from other computers	Blocks TCP and UDP packets on Any Interface bet
ICMP messages	Permits ICMP packets on Any Interface between "
ICMPV6 messages	Permits ICMPV6 packets on Any Interface betwee
DHCP/BOOTP packet exchange	Permits UDP packets on Any Interface between "/
FTP Control - For downloading and uploading files	Permits TCP packets on Any Interface between "
Add Modify Remove Shift up Enable Disable	Shift down
Enable Trojan Rule	
Default Save Cancel	

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

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





The following buttons are available to configure an Expert Rule:

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

dd Firewall Rule	
General Source Destination Advanced	_
Rule Name	
Rule Action	
Protocol TCP and UDP	
Apply Rule on Interface	
]
OK Cancel	

General tab

In this section, specify the Rule settings:

Rule Name – Provide a name to the Rule.

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

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

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





Source tab

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

Add Firewall Rule	
General SOURCE Destination Advanced	
Source IP Address	1
O My Computer	
O Host Name	
O Single IP Address	
O Whole IP Range	
O Any IP Address	
My Network	
Source Port	
Any	
○ Single Port	
O Port Range	
O Port List	
	4
OK Cancel	

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.

When the selected Source IP Address and Source PortNOTE matches together.

Destination tab

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

General Source	Destination	Advanced	
-Destination IP Address			
O My Computer			
O Host Name			
🔿 Single IP Address			
🔿 Whole IP Range			
O Any IP Address			
My Network			
Destination Port			
Any			
O Single Port			
O Port Range			
O Port List			

Destination IP Address -

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

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





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

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

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

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.

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





Advanced tab

This tab contains advance setting for Expert Rule.

neral Source Destination Advanced		
Enable Advanced ICMP Processing		
ICMP Type		
	In	Out
Destination Unreachable		
Echo Reply (ping)		
Echo Request (ping)		
Information Reply		
Information Request		
Parameter Problem		
Redirect		
Source Quench		
TTL Exceeded		
The packet must be from/to a trusted MAC address Log information when this rule applies		

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

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

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

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

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

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

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





Trusted MAC Address

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

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

work Security 🙎 👔	lelp
FireWall Reverse Shell Block Port Scan	_
O Allow All 🔋 🖲 Limited Filter 🔹 O Interactive Filter	
Zone Rule Expert Rule Trusted MAC Address Local IP List	
FE80:0000:0000:0000:0000:0000:0000	
192.	
127	
0000:0000:0000:0000:0000:0000:0001	
Add Remove Clear All	
Enable Trojan Rule	-
Default Save Cancel	

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

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

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

Enable Trojan Rule

Select this check box, to enable the Trojan Rule.





Reverse Shell

This tab allows you to allow/restrict the reverse shell attack and prevent the zero-day attack.

work Security 🙎	
FireWall Reverse Shell Block Port Scan	
O Start • Stop	
Enable White List	
	Add
bash	Delete
python	RemoveAll
peri	•
Enable Black List	
	Add
apache	Delete
apache2	RemoveAll
httpd	
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 check box 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 check box 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

This tab allows admin to configure the port scan option.

eWall Reverse Shell Block Port Scan	
Enable Block Port Scan Excluded IP(Port Scan)	Add
	Delete
Default Save Cancel	

Enable Block Port Scan

Select this check box to enable the port scan option. You can add and delete the IP addresses that need to exclude from the port scan.

- Add: To add an IP, enter the IP address and click Add.
- **Delete**: To delete an IP, select the IP address and click **Delete**.
- Remove All: To remove all the excluded IP addresses, click Remove All.

Tools 🙆

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

ols	김 He
RMM Settings	
Manual Start	
O Auto Start	
User Acceptance Required	
Show RMM Connection Alert	
Ok Cancel	

• **Manual Start**: If this option is selected, client endpoint users have to manually start the RMM service to establish a RMM connection.





- **Auto Start**: If this option is selected, RMM service will be started automatically and all client endpoints will be connected to your main eScan server.
- User Acceptance Required: If this 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.





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.

					×
Policy Templates				💲 Refresh 📔	👔 Help
📑 New Template 📑 Prope	rties 🛃 Parent Policy 👘 Delet	e 🛃 Assign to Group(s) 🛃 Ass	ign to Computer(s) 🛃 Copy 1	emplate Export To 💙	
	a - 1 - 1 a	u - 10-			
Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)	
QA	Jun 19 2021 06:07:27 PM	Jun 29 2021 01:01:43 PM	Q/A_TEAM		
SAMPLES	Jun 29 2021 12:25:32 PM	Jun 29 2021 12:25:32 PM	Samples_Team		

3. Click Assign to Group(s).

Select Group window appears.

Assign template to group	🝸 Help
Select Group	
🗄 🗌 🚞 Managed Computers	
Ok	Cancel

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.

Action List - Client Action List -	💕 Policy Templates 📑 Policy Criteria Ter	emplates		
Managed Computers Policy Group Tasks Client Computers (4)	Policy Select Template			
⊞- 🛑 Roaming Users ⊡- 🛑 Linux / Mac	Assigned Template Date And Time of Assigned Template Group Default Policy Jul 02 2021 11:24:52 AM			
	Select Criteria Change Criteria Remove (*) Criteria to be set in case of conflict			
	Criteria Assigned Policy Ter	emplate Date And Time of Assigned Criteria		

3. In the right pane, click **Select Template**. New Policy window appears.

New	Policy	👔 Help
Po	licy Template Selection	
	Group Default Policy	
Se	elect Cancel	

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.

licy Templates				💲 Refresh 🛛 👔 H
🕂 New Template 🛛 🛃 Pro	perties Parent Policy 👘 De	elete 🛃 Assign to Group(s)	Assign to Computer(s) P Cop	y Template Export To V
Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
Name of Template	Created On Jun 19 2021 06:07:27 PM	Modified On Jun 29 2021 01:01:43 PM	Assigned to Group(s)	<u>Assigned to Computer(s)</u>
Name of Template SAMPLES			<u>Assigned to Group(s)</u> Cd_Ttell	<u>Assigned to Computer(s)</u>

- 2. Click Assign to Computer(s).
- 3. Assign Template to computer window appears.

Assign template to group	🝸 Help
Select Group	
🗄 🗋 Managed Computers	
Ok Ca	incel

4. Click Managed Computers.

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





Copying a Policy Template

To copy a Policy Template,

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

olicy Templates				🗢 Refresh 👔 He
<table-of-contents> New Template 💕 Prop</table-of-contents>	perties Parent Policy 👘 De	elete 🛃 Assign to Group(s)	Assign to Computer(s)	y Template Export To 💙
Name of Template	<u>Created On</u>	Modified On	Assigned to Group(s)	Assigned to Computer(s)
Q8.	Jun 19 2021 06:07:27 PM	Jun 29 2021 01:01:43 PM	QA_TEXH	
SAMPLES	Jun 29 2021 12:25:32 PM	Jun 29 2021 12:25:32 PM	Sangles_Team	

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.

Exporting a Policy Template report

To copy a Policy Template,

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

y Templates				💲 Refresh 🛛
New Template 🛃 Pro	perties 🕎 Parent Policy 💼 🛙	Delete Y Assign to Group(s)	Assign to Computer(s)	y Template Export To ♥
Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
Name of Template	Created On Jun 19 2021 06:07:27 PM	<u>Modified On</u> Jun 29 2021 01:01:43 PM	Assigned to Group(s)	<u>Assigned to Computer(s)</u>

- 2. Click Export To.
- 3. Select the file format from the drop-down menu (HTML, PDF, and Excel).
- 4. The Policy template report will be generated.







Parent Policy

The Parent Policy lets you to implement a change in policy setting to multiple policies at the same time. For example, if you want to make a policy change in a single module like File Anti-Virus in multiple policies; you can do this all at a time using Parent Policy. To configure Parent Policy, follow the steps given below:

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

2. In the Policy Template window, click **Parent Policy**.

				Ε
Policy Templates				💲 Refresh 🛛 👔 Help
<table-of-contents> New Template 📑 Prope</table-of-contents>	rties 🔐 Parent Policy 👘 Delete	💕 Assign to Group(s) 📑 Assi	gn to Computer(s) 📑 Copy To	emplate Export To 💙
Name of Template	<u>Created On</u>	Modified On	Assigned to Group(s)	Assigned to Computer(s)
V	Jun 19 2021 06:07:27 PM	Jun 29 2021 01:01:43 PM	QA_TEXN	
SAMPLES	Jun 29 2021 12:25:32 PM	Jun 29 2021 12:25:32 PM	Samples_Team	

indows Linux / Mac			
File Anti-Virus	Edit	Assign To Select Policy	Edit
Anti-Spam Assign To Select Policy	Edit	Assign To Select Policy -	Edit
FireWall Assign To Select Policy	Edit	EndPoint Security Assign To Select Policy	Edit
Privacy Control Assign To Select Policy	Edit		
Assign TO Delett Policy	v		

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

3. Select and edit the required module according to your preferences.





4. Click **Assign To** drop-down and select the policies for which the parent policy changes should be applied.

V File Anti-	Virus Edit	ו
Assign To	Select Policy 👻	
🗌 Anti-Spa		
Assign To	✓ Check All X Uncheck All ✓	
G FireWall		D
Assign To		
Privacy (
Assign To		

5. Click **OK**. The Parent policy will be updated and changes will be applied to all the policies selected.

Before disabling a module in Parent Policy, ensure that policies areNOTE unchecked from Assign To drop-down.





Policy Criteria Templates

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

Adding a Policy Criteria Template

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

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

Properties	前 Delete Criteria	Assign To 🗸		
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.

Policy Criteria	🝸 Help
Criteria Name: Description:	
Conditions for criteria:	
Save Close	

- 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 co	omputer are listed below	
O If the client computer does not have any	y of the addresses listed below	
	<u>Content</u>	A
4		
Add Edit	Delete	
	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	<u>?</u> Help
Type : Management Server Connection V	
 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	
Condition Username	^
	-
Add AD users Edit Delete	>
Ok	

Adding Local Users

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

Username		
Username : Ok	Cancel	





- 2. Enter a Username.
- 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		김 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*:	289	
Search		
Search Results		
	Selected Users	
Ok Cancel	(*) Man	datory Fields

- 2. Enter data in mandatory fields.
- 3. Click **Search**.
- 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

Specify criteria	김 Help
Type : Machine Name	
If the client computer has one of the machine name listed below Condition	
Machine Name	^
	-
Add Delete	<u> </u>
Ok Cancel	

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

Select Computer Select Computer Select Computer Roaming Users China Computers China Computer China Computer	Help
	Add Remove

 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**.

Poli	Policy Criteria Sefresh 👔 Help					
	👔 New Criteria 😰 Properties 👔 Delete Criteria 👔 Assign To 🔻					
~	Name of Criteria	<u>Created On</u>	Modified On	Assigned to Group(s)	<u>Assigned to Computer(s)</u>	
	deme	Jul 📑 2025 04:21:58 PM	Jul 📑 2020 04:21:58 PM	Group Default Policy Managed Computers		

Policy Criteria window appears.

Policy Criteria		🝸 Help
Criteria Name: Description:	dema	
Conditions for crit		
If the clien	t computer can connect to the management server	
Save	Close	

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





Deleting a Policy Criteria template

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

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

Poli	Policy Criteria Sefresh 👔 Help							
	New Criteria 💕 Prope	erties 前 Delete Criteria 🛐	Assign To 🔻					
~	Name of Criteria	<u>Created On</u>	Modified On	Assigned to Group(s)	Assigned to Computer(s)			
	deme	Jul 📲 2022 04:21:58 PM	Jul 📑 2012 04:21:58 PM	Group Default Policy Managed Computers				
	•	·	·	·				

Assign Criteria to Group window appears.

ect Policy Template	
Group Default Policy	
	-

3. Click Group Policy Template > OK.





Assign Criteria to group window displays Managed Computers folder tree.

Assign Criteria to group	👔 Help
-Select Group	
🗄 🗹 🦳 Managed Computers	
	Ok Cancel
	Cancer

- 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.

Po	licy Crite	ria				💲 Refresh 🛛 👔 Help
	👔 New Criteria 😰 Properties 👔 Delete Criteria 🛐 Assign To 🔻					
	Name	of Criteria	<u>Created On</u>	Modified On	Assigned to Group(s)	Assigned to Computer(s)
	deme		Jul 📲 2022 04:21:58 PM	Jul 📲 2012 04:21:58 PM	Group Default Policy Managed Computers	

- 6. Select the template.
- 7. Click Delete Criteria.

A confirmation window appears.

Policy Criteria
Do you want to delete selected policy criteria(s)?
Ok Cancel

8. Click **Ok**.

The Policy Criteria Template will be deleted.





Unmanaged Computers

To install eScan Client, define policies and tasks on the basis of group, it is necessary to move computers to the created groups. You can move the computers from

Unmanaged Computers to desired groups created in the **Managed Computers** using the following submodules:

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

Network Computers

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

- 1. In the navigation panel, click **Unmanaged Computers** > **Network Computers**.
- 2. Click Microsoft Windows Network.
- 3. Select the workgroup from where you want to move computers to the group created in Managed Computers section. A list of computers appears.

Network Computers	 				💲 Refresh 🔋	👔 Hel
₽ Search						
Action List Refresh Client						
Metwork Computers	Computer Name	<u>Groups</u>	IP Address	<u>User name</u>	<u>eScan Status</u>	-
Mware Shared Folders	III #80/80				Unknown status	
Microsoft Windows Network Microsoft Windows Network Microsoft Windows Network	ACCOUNTENINA				Unknown status	
Web Client Network	A				Unknown status	
THE CHERT RECTOR	A AND PC				Unknown status	
	COMPLEX				Unknown status	
	C ## 67				Unknown status	

- 4. Select the computer(s) you want to move to the desired groups.
- 5. Click **Action List** > **Move to Group**. Select Group window appears.





6. Click **Managed Computers** tree to view the groups.

	3
Select Group	👔 Help
Move Computer(s) to Group	
🗄 - 🛅 Managed Computers	
New Group Ok Cancel	

 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**.

	**
Select Group	김 Help
Move Computer(s) to Group	
🗄 🦳 Managed Computers	
New Group Ok Cancel	

Creating New Group window appears.

	X
Creating New Group	👔 Help
Create New Group	
Ok Cancel	

- 2. Enter a name for the group.
- 3. Click **OK**. A new group will be created.





IP Range

The **IP Range** submodule lets you scan the desired IP address or range of IP address and add the required computers to any of the managed groups. It also lets you add, search and delete an IP range.

Adding New IP Range

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

1. In the IP range screen, click **New IP Range.** Specify IP Range window appears.

	×
Specify IP Range	🝸 Help
Starting IP Address*:	
Starting IP Address 1	
Ending IP Address*:	
OK Cancel	(*) Mandatory Fields

- 2. Enter the Starting and Ending IP address.
- 3. Click **OK**. The IP Range will be added.

	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
O NOTE	selected IP Range will be added to the IP Range tree.
NOTE	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

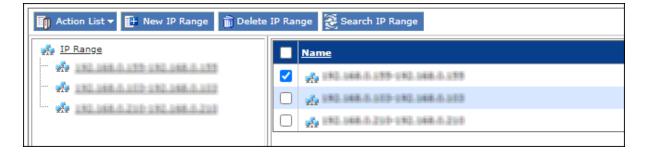
To move an entire IP range to a group, follow the steps given below:

- 1. Select an IP range.
- 2. Select the check box 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.

Properties
🔂 Add 🔂 Modify 🗊 Delete
Active Directory Domain Controller Address
ОК

3. Click Add. Login Settings window appears.

Login Settings		Help
AD IP Address *:		
User name *:		
Password *:		
Confirm Password *:		
Use SSL Auth.:		
AdsPort*:	389	
OK Cancel	(*) Mandatory	Fields

4. Fill in the required Login Credentials and click **OK**.





The details including IP Addresses from active directory will be added instantly.

	:
Properties	🕜 Help
H Add Modify Delete	
Active Directory Domain Controller Address	
192.000	
OK	

- 5. Select the Active Directory and click **OK**. The selected Active Directory will be added to the Active directory tree.
- 6. To view the details, click the **Active Directory**.

tive Directory								🗢 Refresh	👔 Не
👔 Action List 🔻 📝 Properties 🛛 🕄 Refr	esh Cli	ient							
: 🎪 Active Directory		Computer Name	Groups	IP Address	User name	eScan Status	Version	Last Connection (YYYY/M	IM/DD
🗄 🌺 DC=arry (1) = teatian (1) = arry		i teathcaith			Unknown status				
🏫 Chieduiltin	Ľ				onknown status				
🚓 (DhimComputere									
- 🏠 CuisCunain Contailas									
🗠 🙀 Chintanaightantaith/thinkige									
Chiedan and and a state									
💏 (Chini, and multinum)									
🗠 🔬 Olisimerapel Service noon									
- 🚓 Olientita Qualee									
🚓 Oliatingram Cala									
···· 🚓 (Chini Zupakarni									
Chimisteere									

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.

w C	Computers Found									💲 Ref	fresh 김 H
Sea	arch										
	Action List 💙 🔥 Filter C	riteria									
1	Computer Name	IP Address	User name	Last Seen	Belongs To	eScan Status	Version	Last Connection	Installed Directory	Monitor Status	Anti-Spam
		192,008,0.130		02 Jul 2021 13:54:27	Server	Unknown status					
		192 048 0.27		02 Jul 2021 13:54:45	Server	Unknown status					
		192 008 0 00		02 Jul 2021 13:54:26	Server	Unknown status					
		192 048 8 370		02 Jul 2021 13:54:28	Server	Unknown status					
		192 000 0 000		02 Jul 2021 13:54:27	Server	Unknown status					
)		192,008,0.376		02 Jul 2021 13:54:28	Server	Unknown status					
		192 18 1 2 1		02 Jul 2021 13:54:28	Server	Unknown status					
		192,008-0.238		02 Jul 2021 13:25:43	Server	Unknown status					
		192 008 0 129		02 Jul 2021 13:54:27	Server	Unknown status					
כ		192.008.0.48		02 Jul 2021 13:54:27	Server	Unknown status					
		192 008 0 020		02 Jul 2021 13:54:27	Server	Unknown status					
כ		192,008,0.76		02 Jul 2021 13:54:27	Server	Unknown status					
כ		192 048 0.000		02 Jul 2021 13:54:46	Server	Unknown status					
)		192 048 0.46		02 Jul 2021 13:54:27	Server	Unknown status					
											•
	📃 Unmanaged		📃 Prot	ected		📕 Not Installed	/ Critical			Unknown status	

Filter Criteria

The Filter Criteria lets you filter new computers found according to date range.

Filter Criteria	iteria
Date Range From (MM/DD/YYYY) To (MM/DD/YYYY)	07/02/2021
Search Reset	

- 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.

Repo	ort Templates	🖉 Properties 🤤 Refresh	김 Help
Ð	New Template 🗊 Create Schedule 📝 Properties 🗊 Delete		
	Template Name		
\Box	Virus Report 🚝 🧟 🖺		
	Update Report 🚛 🙇 些		
\Box	Scan Report 👯 🧟 🔛		
	Web Protection Report 💶 🙇		
\Box	Application Control Report 👯		
	Attachment Control Report 📕		
\Box	Anti-Spam Report		
	Mail Anti-Virus Report		
\Box	USB Control Report 📫 🧟 些		
	Group Summary Report 👯 🧟 🖺		
\Box	Hardware Report 🗮 🧟 🗳		
	Software Report 📫 🧟 鉴		
\Box	File Activity Report		
	Computers with Critical Status Report 📒 🙇 🖺		
\Box	Asset Changes (Software) Report 丰 🙇 些		
	Asset Changes (Hardware) Report = 🙇 些		
	Top 10 Summary Report 🚝 🧟 鉴		
	Anti-Ransomware Report 📕		
\Box	Application Access Report 🗮		
	Session Activity Report 📒		
	eBackup Report 📕		
	Endpoint Incident Report		





Creating a Report Template

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

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

New Template screen appears.

Templates >New Template	
<u></u>	
nte Name	
New Template Name :* New Template	
Template	
rempiere	
Report Type	
🔍 Virus Report 丰 🙇 🖺	🔿 Anti-Spam Report 📕
🔿 Update Report 💶 🙇 些	O Mail Anti-Virus Report
🔾 Web Protection Report 📑 🙇	🔿 USB Control Report 📫 🙇 🖺
🔿 Group Summary Report = 🙇 🖺	O Application Control Report 🚝
🔿 Hardware Report = 🙇 🖺	🔿 Attachment Control Report 🗲
🔿 Scan Report 🚝 🙇 🖺	🔿 Software Report 🚝 🧟 🖺
🔿 Computers with Critical Status Report 🗮 🙇 🖺	🔿 File Activity Report 🗮
🔿 Asset Changes (Hardware) Report 👥 🙇 🕵	🔿 Asset Changes (Software) Report 📑 🧟 🖺
🔿 eBackup Report 💶 🙇 🗳	🔿 Top 10 Summary Report 📑 🧟 🖺
🔿 Endpoint Incident Report 🚛	🔿 Anti-Ransomware Report 📑
	O Application Access Report 🗮
	🔿 Session Activity Report
Period & Sort By	
Date Options	
	This Week This Year
	Date Range
O Last Month	
Date	Virus
Computer O	Action Taken
Options	
Show only On Demand Scan Results	

- 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, <u>click here</u>.

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.

operties				 ? H
port Templa	ates > Virus Report Properties	5		
G				
	General Report Period	& Sort By		
	Report Name			
	Report Name :	Virus Report		
	Details			
	Selected Template Type	8	VIRUS REPORT	
	Created:		6/30/2021 5:33:18 PM	
	Modified:		6/30/2021 5:33:18 PM	
Save	Cancel			

UNOTE

Depending upon the Report Template enter, the Properties varies.

3. After making the necessary changes, click **Save**. The Report Template's properties will be updated.

Deleting a Report Template

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

- 1. Select the template you want to delete.
- 2. Click **Delete**.
 - A confirmation prompt appears.
- 3. Click **OK**. The Report Template will be deleted.



Default Report Templates cannot be deleted.





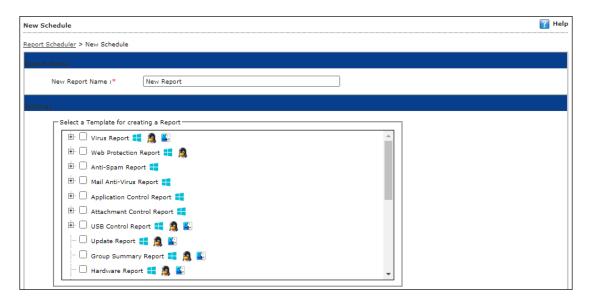
Report Scheduler

The Report Scheduler module lets you create schedule, update and run the task according to your preferences.

Creating a Schedule

To create a Schedule,

 In the Report Scheduler screen, click New Schedule. New Schedule screen appears.



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





- Select Condition	
Generate a Report for Groups	
Generate a Report for a List of Computers	
Select Target Groups	
🗄 🖓 🗋 Managed Computers	

5. In the Send Report by email section, fill the required information to receive reports via email.

Report Sender*:	presidente generation com	
Report Recipient*:		Add
	prantenie z en en com	Delete
Mail Server IP Address:	192.000	
Mail Server Port:	25	
User Authentication:		
Password Authentication:		
* For Example: user@yourcompany.com		

- 6. Select the preferred report format.
- 7. In Report Scheduling Settings section, make the necessary changes.





Report Se	cheduling Settings		
[Enable Scheduler	O Manual Start	
	DailyWeekly	Mon Tue Wed Thu	
	O Monthly C Last Day of Month		
[• At	12:00 pm	
Save	Cancel		(*) Mandatory Fields

8. Click Save.

New schedule will be created.





Viewing Reports on Demand

To view a report or a set of reports immediately,

1. Click **Report Scheduler** > **View & Create**.

New Schedule screen appears.

Report Scheduler > New Schedule	
Settings	
- Select a Template for creating a Report	1
🗄 🗌 Virus Report 💶 🙇 🖺	
🗄 🗌 Web Protection Report 📢 🙉	
🗄 🗹 Anti-Spam Report 📒	
🗄 🗋 Mail Anti-Virus Report 🚛	
🗄 🗹 Application Control Report 👯	
🗄 🗆 Attachment Control Report	
🗄 🗆 USB Control Report 🚝 🙇 鉴	
🖸 Update Report 💶 🙇 鉴	
Group Summary Report 📒 🙇 🖺	
]
 Select Condition Generate a Report for Groups 	
Generate a Report for a List of Computers	
Select Target Groups	
😟 🗋 Managed Computers	
]
Create Schedule Cancel View	(*) Mandatory Fields

- 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		🤤 Refres	
🛐 Start Task 📄 Results	Properties 👔 Delete	🕂 New Schedule 🚺 View & Create	
Schedule Name	Report Recipient	Scheduler Type	View
New Taylort	presidente and end com	Automatic Scheduler	<u>View</u>

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.

	🝸 Help
Time	
7/7/2021 1:35:05 PM	
7/7/2021 1:21:47 PM	
7/7/2021 1:17:39 PM	
7/7/2021 1:12:01 PM	
7/7/2021 1:08:25 PM	
7/7/2021 1:02:29 PM	
7/7/2021 12:53:48 PM	
7/7/2021 12:37:36 PM	
	7/7/2021 1:35:05 PM 7/7/2021 1:21:47 PM 7/7/2021 1:17:39 PM 7/7/2021 1:12:01 PM 7/7/2021 1:08:25 PM 7/7/2021 1:08:25 PM 7/7/2021 1:02:29 PM 7/7/2021 12:53:48 PM





Viewing Properties of a Schedule

To view the properties of a schedule,

- 1. Select a schedule.
- 2. Click **Properties**.

Properties screen appears.

Properties		김 Help
Report Scheduler >Properties		
General Schedule Settir	gs Groups	
Schedule Name :*	New Tennet	
Created:	07/03/21 11:17:33 AM	
Status:	Task not performed yet	
Ok Cancel		(*) 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) ?
Ok Cancel

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 & Computers		🤹 Refresh 🛛 👔 Help
Settings 🚺 Edit Selection	•	
Events & Computers	Events & Computers	
Ė 🛅 Events Status	Events Status	
 · · ·	Computer Selection	
	Software/Hardware Changes	
	Violations	
•		
	1 Information	🚫 Critical

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.

Events & Computers		💲 Refresh	_? Help
·			
Settings Difference Edit Selection	*		
Events & Computers	Computer Selection		
🗄 🛅 Events Status	Computers with the "Critical Status"		
Computers Selection	Secondary Server Status (Not Updated)		
Computers with the	Ken i i i		
Computers with Live	Computers with the "Warning Status"		
···· [Computers with the ···· 🚺 Database are Outda	🔂 Database are Outdated		
Many Viruses Detect	2 Many Viruses Detected		
No eScan Antivirus 1	RNo eScan Antivirus Installed		
Not Connected for a lc	(Lee		
Protection is off	2.Not Connected for a long time		
Update Agent Status	2Not Scanned for a long time		
	DProtection is off		
	记 Update Agent Status		
•			
	1 Information	Critical	

The Computer Selection subfolder consists following sections:

- Computers with "Critical Status"
- Secondary Server Status (Not Updated)
- Computers with Live Status
- Computer with "Warning Status"
- Database is outdated
- Many Viruses Detected
- No eScan Installed
- Not connected for a long time
- Not scanned for a long time
- Protection is off
- Update Agent Status





This section displays computers marked with Critical status.

Computers with critical status

This section displays computers marked with Critical status.

Secondary Server Status (Not Updated)

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

Computers with Live status

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

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

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



The required action can be performed only if the endpoint system is online. The Symbol indicates that the endpoint is online and Symbol indicates that the system is offline.

The following actions can be performed on the online system according to the need of the user:

- **Log off**: This option will log off the system from the current user.
- **Force Log off**: This option will log off the current user forcefully.
- Lock Machine: This option will lock the system automatically.
- **Shutdown Machine**: This option will shut down the system.
- Force Shutdown Machine: This option will shut down the system forcefully.
- Restart Machine: This option will restart the system.
- Force Restart Machine: This option will restart the system forcefully.
- **Hibernate Machine**: This option will hibernate the system that will consume less power than sleep mode and resumes back to the previous states when you start-up the system.





• **Stand By Machine**: This option will put the machine in the standby mode. The standby mode is similar to as that of Hibernate mode.

Computers with warning status

This section displays computer with a warning status.

Database is outdated

This section displays computers whose virus database is outdated.

Many Viruses Detected

This section displays the computers whose virus count has exceeded.

No eScan installed

This section displays computers on which eScan is not installed.

Not connected for a long time

This section displays the computers which didn't connect to the eScan server for the set duration.

Not scanned for a long time

This section displays the computers which weren't scanned for the set duration.

Protection is off

This section displays the computers on which File Protection is disabled.

Update Agent Status

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

The additional settings vary depending upon the Computer Status.





Edit Selection

This drop-down menu allows to configure various option based on selected options. The following options are present in the menu:

• **Protection**: This option displays the protection status of the selected computer.

? Help
E

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

Recent Events (1 - 10 of 622 ()						
<u>Date</u>	<u>Time</u>	<u>User's name</u>	<u>Event Id</u>	Module Name	Description	<u>c</u>
1 7/3/2021	12:52:35	mail	File Anti-Virus (10154)	update	New virus database taken and applied (2025/07/05 67-52) (7.89055)	U
1 7/3/2021	12:52:35	real	File Anti-Virus (10740)	winclient	/regit/MicroWorld[Hittp:///282.568.dl.598.3225//wwC/ito/K	e
1 7/3/2021	12:52:34	mail	File Anti-Virus (10154)	update	New virus database talen and applied (2025/07/05.07-52) (7.89053)	υ
1 7/3/2021	12:52:34	real	File Anti-Virus (10740)	winclient	jingh/https://iaidi/http:///1932.048.01.099-2225/Min6//AAK	e
1 7/3/2021	11:30:18	mail	File Anti-Virus (10154)	update	New virus database taken and applied (2021/07/03 05:05) (7.89035)	υ
1 7/3/2021	11:30:18	real	File Anti-Virus (10740)	winclient	/regit/Micro/Micro/Upittp:///252.568.dl.598.d2225/MinC/MoNC	e
1 7/3/2021	11:30:18	mail	File Anti-Virus (10740)	winclient	/regit/MicroWierfd[]http:///150.548.dt.590.0225//wwC//wWK	e
1 7/3/2021	11:30:18	mail	File Anti-Virus (10154)	update	New virus database talam and applied (2021/07/03 05:05) (7.89035)	υ
1 7/3/2021	10:30:14	mail	File Anti-Virus (10740)	winclient	/agit/MicroWorld[Hittgr///1882.0488.05.0585-02231/MinC/iRvN	e
1 7/3/2021	10:30:14	mail	File Anti-Virus (10154)	update	New virus database taken and applied (2021/07/03 05-05) (7.49035)	U

- Deploy/Upgrade Client: To learn about this option, click here.
- **Check Connection**: This option will verify if the client machine is online or offline.





	(
Connecting to ComputerAN Connection : Successful	
Connection : Successful	

- **Remove from Group**: To learn about this option, <u>click here</u>.
- Connect to Client (RMM): To learn about this option, click here.
- Force Download: To learn about this option, click here.
- On Demand Scanning: To learn about this option, click here.
- Send Message: To learn about this option, click here.
- Properties: To learn about this option, click here.

Software/Hardware Changes

This subfolder displays all software/ hardware changes that occurred on computers. It consists following sections:

- Software Changes
- Hardware changes
- Existing System Info

Events & Computers		💲 Refresh 🛛 👔 Help
Settings Edit Selection	•	
🗄 🛅 Events & Computers	Software/Hardware Changes	
	Software Changes	
🗄 🛅 Software/Hardware Cl	Hardware Changes	
	Existing System Info	
🗄 葿 Date / Time Violations		
	1 Information	Critical

Software Changes

This section displays software changes i.e. installation, uninstallation or software upgrades.





Hardware changes

This section displays hardware changes that occurred on computers. For example, IP address. Hard Disk, RAM etc.

Existing System Info

This section displays a computer's existing hardware information.





Violations

Date/Time Violations

This subfolder consists Date/Time Violations that displays client computers whose users attempted to modify date and time.

Events & Computers								💲 Refresh 🛛 👔 Help
Edit Selection 🗸								
Events & Computers	▲ Filter Cri	teria			^	Export Option		
E Computers Selection	Date / Time Vio	lations Eve	ents			1 - 1 of 1 ∣∢ page	1 of 1 ⊨ Ro	ws per page: 10 🗸
E Goftware/Hardware Changes	<u>Date</u>	<u>Time</u>	Machine Name	IP Address	<u>User's name</u>	Event Id	Module Name	Client Action
Date / Time Violations Date / Time Violations	7/6/2021	13:05:53	WIN-QA007 丰	192	WING MULTING	File Anti-Virus (1805)	eScan Monitor	Device/Computer Modif

Settings

You can define the Settings for Events, Computer Selection and Software/Hardware changes by clicking on the **Settings** option and defining the desired settings using the Tabs and options present on the Events and Computer settings window.

Event Status Setting

Basically, events are activities performed on client's computer.

Events & Computers Settings		👔 Help
Events Status Computer Selection	Software/Hardware Changes	
Events		
Events Name Recent Number Of Records	1000	
Save Close		





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

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

Steps to define event status settings:

Perform the following steps to save the event status settings:

- 1. Select the appropriate **Events Name**.
- 2. Enter the number of events that you want to view in a list, in the **Number of Records** field.
- 3. Click **Save**. The settings get saved.

Computer Selection

Events & Computers Settings	👔 Help
Events Status Computer Selection Software/Hardware Changes	
Computers	
Check for eScan Not Installed	
Check for Monitor Status Check for Not Scanned Check for Not Scanned	
Check for Database Not Updated Check for Not Connected	
Database Not Updated from more than 7 days System Not Scanned from more than 7 days System Not Connected from more than 7 days Number Of Records 1000	
Save Close	





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 check box to view the list of client systems under managed computers on which eScan has not been installed.
- **Check for Monitor Status**: Select this check box to view the client systems on which eScan monitor is not enabled.
- **Check for Not Scanned**: Select this check box to view the list of client systems which has not been scanned.
- **Check for Database Not Updated**: Select this check box to view the list of client systems on which database has not been updated.
- **Check for Not Connected**: Select this check box 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 check box to view the list of client systems which has not been scanned.
- **Check for Database Not Updated**: Select this check box to view the list of client systems on which database has not been updated.
- **Check for Not Connected**: Select this check box to view the list of eScan client systems that have not been communicated with eScan server.
- **Check for Protection off**: Select this check box to view the list of client systems on which protection for any module is inactive.
- **Check for Many Viruses**: Select this check box 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 check box if you want to view the client systems on which eScan monitor is not enabled.
- **Check for Mail Anti-Phishing**: Select this check box 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 check box 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 check box if you want to view the list of client systems on which **Mail Anti- Spam** protection is inactive.
- **Check for Endpoint Security**: Select this check box if you want to view the list of client systems on which **Endpoint Security** protection is inactive.
- **Check for Firewall**: Select this check box if you want to view the list of client systems on which **Firewall** protection is inactive.
- **Check for Proactive**: Select this check box if you want to view the list of client systems on which **Proactive** protection is inactive.
- **Check for Web Protection**: Select this check box 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 check boxes, 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.

ents Status	Computer Selection	Software/Hardware Changes	
-Updates			
	Hardware Changes Softw	vare Changes 🗸	
	r Of Days	1 days	
Numbe	r Of Records	1000	
Save	Close		

The Software/ Hardware Changes enable you to do the following activities:

Type of Software/Hardware Changes

- Software changes
- Hardware changes
- Existing system info

To Change software/hardware settings, follow the steps given below:

- 1. Click the **Software/Hardware Changes** tab.
- 2. Specify the following field details.
 - **Software/Hardware Changes**: Click the drop-down and select the changes made.
 - **Number of Days**: Enter the number of days, to view changes made within the specified days.
 - **Number of Records**: Enter the number of client systems that you want to view in the list.
- 3. Click **Save**. The settings get saved.

Performing an action for computer

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

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





Tasks for Specific Computers

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

Tasks For Specific Compu				💲 Refresh	김 Help
H New Task Start	Task Properties	Results <u> </u> Delete			
Task Name	Pending	Completed	Schedule Type		

Creating a task for specific computers

To create a task for specific computer(s), follow the steps given below:

- 1. In the navigation panel, click **Tasks for Specific Computers**.
- 2. Click **New Task**.





New Task Template form appears.

sk Template		
or Specific Computers	>New Task Template	
ame		
Task Name:*	New Task	
	(
ed Tasks		
File Anti-Virus	Status = 🧟 🖺	
Enabled		
Disabled		
Mail Anti-Virus	Status 📕	
Enabled		
Disabled Anti-Spam Sta	hua 💶	
	tus 🜉	
Enabled Disabled		
Web Protection	Status 💶 👧	
Enabled		
Enabled Disabled		
	rity Status 뜸 🧟 些	
Enabled		
Disabled		
Firewall Status	4	
🔍 Disable Fi	rewall	
🗌 Enable Lir	nited Filter Mode of Firewall	
	teractive Filter Mode of Firewall	
Alternate Down	nload Status द ्द 🙇 些	
Enabled		
Disabled		
Start/Stop And		
Start Serv		
Stop Serv		
Set Update Se		
Add Server Na Remove Serve		168.0.155
_		
🗌 Scan 👥 🙇 🕻		
	mory Scan 👥 🙇	Registry
	stem Folder 📫	Scan network drives
	in Local Drives	Computer StartUp
	Scan System Drive 拱	
	Scan Data Drives = 🧟 🖺	
Option		
	n Archives द ्द 🕵 些	
	to Shut Down After Scan Completion 🚦	•
Sca	in Only 🗮 🙇 🖺	
	Des related the data and A	
Force Client to	Download Update 📒 🙇 🖺	

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





5. In the **Select Computers/Groups** section, select the computers/groups on which the tasks should be run and then click **Add**.

Select Computers/Groups							
Select Computers/Groups	Add						
		4	•				

6. In the **Tasks Scheduling Settings** section, configure the schedule settings.

sk Scheduling Settings					
Enable Scheduler		(Manual Start		
Daily					
O Weekly	Mon	🗌 Tue	Wed	Thu	
	🗌 Fri	Sat	Sun		
O Monthly	1 💙				
At	12:00 pm				
Save Close				(*) Man	datory Field

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





Viewing Properties of a task

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

For Specific Computers > Properties		
General Schedule Machines	Settings	
Task Name	New Task	
Task Creation Time:	07/ 04:32:27 PM	
Status:	Task not performed yet	
Last Run:		

This section will have following tabs to configure:

- **General**: This tab provides task name, 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 (New Task)								
Tasks For Specific Computers > Task Results								
Client Computers	Group	Status	Date/Time					
AN	Managed Computers	Not Performed Yet						
ED#_OLIENT	Managed Computers	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.

sks For Specific Computers				💲 Refresh	- · ·		
🔂 New Task 🛐 Start Task 🛃 Properties 📑 Results							
<u>Task Name</u>	<u>Pending</u>	<u>Completed</u>	<u>Schedule Type</u>				
New Tesk	2	0	Automatic Scheduler	I	ask Status		

2. Click **Delete**.

A confirmation prompt appears.

X
Tasks For Specific Computers
Do you want to Delete the Selected Task(s) ?
Ok Cancel

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.

lardware Report	Software Report	Software Lic	ense Software Report (Micro	soft)
Filter Criteria			Export Option	
Computer Details			1 - 5 of 5 🖂 (pag	e 1 of 1) > Rows per page: 100 ♥
Computer Name	Group	IP Address	<u>User's name</u>	Operating System
Анын 💿 тб 🙇	Managed Computers	192.108.2000	root	Ubuntu Linux 16.10 64-Bit
ESCHALCUIDHT	Samples_Team	192.000.000	ES and CLER demonstrator	Windows XP Professional x64 Edition 64-bit
PR. Statement	Managed Computers	192.000.000	PRASMAN Commission tor	Windows 7 Home Basic Edition 32-bit
WI COLORADOR 📑	Managed Computers	192.008.0.075	WII COLORED OF ADministrator	Windows 8 Professional 32-bit
WING-MINT =	Q=M	192.008.0.00	WIN-Control of some	Windows 8.1 Professional 64-bit

The tab displays following details of managed computers:

- Computer Name
- Group
- IP Address
- User name
- Operating System
- Service Pack
- OS Version
- OS Installed Date
- Internet Explorer
- Processor
- Motherboard
- RAM
- HDD
- Local MAC Adapter(s)
- Wi-Fi MAC [Adapter]
- USB MAC [Adapter]





- PC Identifying Number
- Motherboard Serial No
- Network Speed
- Disk Free Space
- PC Manufacturer
- PC Model
- MB Manufacturer
- Graphic Card Details
- Machine Type
- BitLocker Status
- Keyboard Vendor
- Software

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

Filtering Hardware Report

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

♥ Filter Criteria			^	Export Option			
Filter Criteria	I	nclude All 💉			#Add Asse	t Informati	ion
Computer Name	*	Include 💙	✓	Internet Explorer	*	Include	~
🗹 User's name	*	Include 💙	✓	OS Version	*	Include 1	~
Operating System	*	Include 🗸	<	Processor	*	Include 1	~
Motherboard	*	Include 💙	✓	Local Adapter	*	Include 1	~
RAM	*	Include 💙	<	Wifi Adapter	*	Include 1	~
Group	*	Include 🗸	<	USB Adapter	*	Include 1	~
PC IdentifyingNumber	*	Include 🗸	<	Motherboard Serial No	*	Include 1	~
🗹 OS Type	*	Include 🗸	✓	HDD			
IP Address	*	Include 🗸	<	OS Installed Date			
Service Pack	*	Include 🗸	✓	Disk Free Space			
PC Manufacturer	*	Include 🗸	✓	PC Model	*	Include 1	~
MB Manufacturer	*	Include 🗸	✓	Graphic Card Details	*	Include 1	~
Machine Type	*	Include 🗸	✓	BitLocker Status			
Search Reset]				(*) V	iew All Iten	ns

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			
O Excel	O PDF	HTML	Export

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



Click the link to open/download the file.

Software Report

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

Hardware Report Software Report Software L	icense Software Report (Microsoft)
∧ Filter Criteria	A Export Option
Software Details	1 - 10 of 10 ((page 1 of 1)) Rows per page: 10 ♥
Software Name	Computer Count
Brave	1
Client Authentication Agent	1
Dropbox	1
eScan Corporate - 360	1
eScan Corporate for Windows	2
Google Chrome	3
Microsoft SQL Server 2008 R2	1
Microsoft SQL Server 2008 R2 Native Client	1
Microsoft SQL Server 2008 R2 Setup (English)	1

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.

♥ Filter Criteria		Export Option		
Filter Criteria Software Name Computer Name OS Type	*	Include V Include V	Group By Software Name Computer Name Group	
Search Reset				(*) View All Items

The Software Report can be filtered on the basis of **Software Name** or **Computer Name**.

Software Name

Entering the Software name displays suggestions. Select the appropriate software.

Computer Name

Click the drop-down and select the preferred computer(s).

OS Type

Enter the OS type.

Group By

The results can be grouped by Software name, Computer name or Group. If Group option is selected, the report can be filtered for a specific group.

After entering data in all fields, click **Search**. The Software Report will be filtered according to your preferences.





Exporting Software Report

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

▲ Filter Criteria		✓ Export Option
Export Option		
O Excel	HTML	Export Detailed Report

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.

A success message appears.



Click the link to open/download the file.

Software License

The Software License tab displays list of Software Licenses of managed computers.

Hardware Report Software Report	Software License Software Report (Microsoft)				
Filter Criteria K Export Option					
	1 - 4 of 4 14 (page 1	of 1 → → Rows per page: 100 ¥			
License Key	Software Name	Computer Count			
YG TAB COTTAG BEER PRAY AND ANALY	Windows 7 Home Basic Edition 32-bit 📒	1			
NG BRW SHORE FEDRIA KEPTRE SREE4	Windows 8 Professional 32-bit 📒	1			
GCM D DIVINI TOCON COMBO 104 "9	Windows 8.1 Professional 64-bit	1			
VCR30 where ended a 300 + 400 M	Windows XP Professional x64 Edition 64-bit	1			

The log displays License Key, Software Name and Computer Count.

To see more details of the computer's license key installed, click the numerical value in License Key or Computer Count column.





Filtering Software License Report

To filter Software Report, click **Filter Criteria** field. Filter Criteria field expands.

✔ Filter Criteria		▲ Export Option
Filter Criteria		
Software License Key	*	Include 🗸
Software Name	*	Include V Group By
Computer Name	*	Include V Group
IP Address	*	Include 🗸
OS Type	*	Include 🖌
Search Reset		(*) View All Items

Software License Key

Entering the license key displays suggestions. Select the appropriate key.

Software Name

Entering the Software name displays suggestions. Select the appropriate software.

Computer Name

Click the drop-down and select the preferred computer(s).

IP Address

Entering the IP address displays suggestions. Select the appropriate IP address.

OS Type

Enter the OS type.

Include/Exclude

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

After entering data in all fields, click **Search**. The Software License Report will be filtered according to your preferences.





Exporting Software License Report

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

▲ Filter Criteria			♥ Export Option		
Export Option					
C Excel C PDF	HTML	Export Ex	ort Detailed Report	Vindows OS	Microsoft Office

Select whether you want report for Windows OS and Microsoft Office.

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.

A success message appears.



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.

lardware Report	Software Report	Software License	Software Report (Microsoft)
MS Office Softw	vare Report 🕅	crosoft OS	
 Filter Criteria 		^	Export Option
		1 - 1 of 1	1 < (page 1 of 1) > Rows per page: 20 ♥
Software Name			Computer Count

The tab consists following subtabs:

MS Office Software Report – It displays Microsoft software name and computer count.

Microsoft OS – It displays Operating System, Service Pack, OS version and computer count.





Filtering Software Report (Microsoft)

To filter Software Report (Microsoft), click **Filter Criteria** field. Filter Criteria field expands.

♥ Filter Criteria		🔺 Export Opti	Export Option	
Filter Criteria				
Software Name	Microsoft Office*	Include 💙	Group By	
Computer Name	*	✓ Include ∨	Group	
Search Reset				(*) View All Items

Computer Name

Click the drop-down and select the preferred computer(s).

Group By

If Group option is selected, the report can be filtered for a specific group.

After entering data in all fields, click **Search**.

The Software Report (Microsoft) will be filtered according to your preferences.





Exporting Software Report (Microsoft)

To export the Software Report (Microsoft), click **Export Option**. Export Option field expands.

▲ Filter Criteria		✓ Export Option
Export Option		
O Excel	HTML	Export Detailed Report

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.

A success message appears.



Click the link to open/download the file.

Filtering Microsoft OS Report

To filter the Microsoft OS report, click **Filter Criteria** field. Filter Criteria field expands.

♥ Filter Criteria		Export Option		
Filter Criteria				
Operating System	*	Include 🗸		
Computer Name	*	Include 💙	Group By	
Service Pack	*	Include 💙	Group	
OS Version	*	Include 💙		
Search Reset				(*) View All Items

Operating System

Entering the operating system name displays list of suggestions. Select the appropriate OS.

Computer Name

Click the drop-down and select the preferred computer(s).

Service Pack

Entering the service pack name displays list of suggestions. Select the appropriate Service Pack.





OS Version

Entering the OS version displays list of suggestions. Select the appropriate OS version.

Include/Exclude

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

After filling all the fields, click **Search**. The Microsoft OS report will be filtered according to your preferences.

Exporting Microsoft OS Report

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

 Filter Criteria 		👻 Export Opt	tion
Export Option			
O Excel	O PDF	HTML	Export

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 also provides the reports of the running applications. It consists following submodules:

- Print Activity
- Session Activity
- File Activity
- Application Access Report

Print Activity

The Print Activity submodule monitors and logs print commands sent by all computers. It also lets you filter the logs on the basis of Computer name, Printer and Username. Furthermore, the module lets you export a detailed print activity report in XLS, PDF, and HTML formats. The log report generated consists of Print Date, Machine Name, IP Address, Username, Printer Name, Document Name along with number of Copies and Pages.

rint Activity	Setting	s 🤹 Refresh 👔 He
▲ Filter Criteria	Export Option	
	1 - 1 of 1 ∢ (page 1 of 1) > R	ows per page: 10 💙
Printer Name	Copies	<u>Pages</u>
NPIBERCIE (HP Lasariat 400 MH2G+)	5	5

Viewing Print Activity Log

To view the Print log of a Printer, click its numerical value under **Copies** or **Pages** column.

Print Activity window appears displaying details.

Print Activity >> N	IBAC28 (HP Law	erjiet 400 MADS	*()			
Machine Name : *(Inclu	de)			Export To:	Select 🗸	Export
				1 - 5 of 5 ∢ (page 1 of 1)	N Rows per page:	10 🗸
<u>Client Date</u>	Machine Name	IP Address	<u>User name</u>	Printer Name	Document Name	<u>Copies</u>
05/08/21 4:23:03 PM	Q in all its	192. ***	QA 21 H Administration	NPIBBRCOB (HP LaserDat 400 WHEL+)	Untitled - Notepad	1
05/08/21 4:22:40 PM	Q.M. CEDIR.	192	Q = C = H = d = in all sel or	NPIBBRCOB (HP LaserDat 400 W425+)	Untitled - Notepad	1
05/08/21 4:22:09 PM	Q in state	192. *******	Q. C. H. M. Historian and or	N	Untitled - Notepad	1
05/08/21 4:21:42 PM	Qilletter	192	Qn 011 minimizeror	NPIBBRCOB (HP LaserCel 400 W425x)	Untitled - Notepad	1
05/08/21 4:21:31 PM	Q# == #	192. 48.0.117	Q = E = A _ A _ A _ A _ A _ A _ A _ A _ A _ A	NFIBERCOB (HP LaserCall #30 WHESH)	Untitled - Notepad	1





Exporting Print Activity Log

To export this generated log,

- 1. Click the **Export to** drop-down.
- 2. Select a preferred format.
- 3. Click Export.

A success message appears.



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		A Export Optic	n	
Filter Criteria				
Computer Name Printer	*	▼ Include ♥ Include ♥	Group By Printer	
User name	*	Include 🗸	O User name	
Date Range				
From (MM/DD/YYYY) 07/03/2021				
To (MM/DD/YYYY) 07/03/2021				
Search 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.

▲ Filter Criteria		♥ Export Option
Export Option		
O Excel	HTML	Export Export Detailed Report

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.

A success message appears.



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.

lias Name		Alias List		Printer List	
	Add		Remove	Add	Remove
Carner Lat 1 100					
4	•	•	►.	•	•
Save					

- 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.

 Filter Criteria 			🔺 Export Opt	ion	
				1 - 10 o	f11 < < page 1 of 2 ▶ ▶ Rows per page: 10 ▶
Operation Type	Client Date	Computer Name/Ip	Group	IP Address	Description
Session LogOn	03/07/21 12:50:17 PM	WIN-Quint?	Q#TE#M	192	User LogOn User's name: W1
Session LogOff	03/07/21 10:55:49 AM	WIR COURT	Qin_manM	192.048.0.88	User LogOff User's name: WI
Remote Session Disconnect	03/07/21 10:55:48 AM	WING MINT	Q4M	192. 48.0.49	
Remote Session Connect	03/07/21 10:55:47 AM	WIN-QADD*	Q#_TE#M	192	Remote Session Connect User's name: WI Name of Remote PC: WI IP of Remote PC: 192.
Remote Session Disconnect	03/07/21 10:55:34 AM	WIN COURS	Q.eTEAM	192.000.0.00	
Remote Session Connect	03/07/21 10:55:33 AM	WIN-QADD?	Q#_TEMM	192.008.0.89	Remote Session Connect User's name: WI Name of Remote PC: WI IP of Remote PC: 192.
Start up	03/07/21 10:43:23 AM	WINCESCHUER	Managed Computers	192.000 0 0 0 0	
Session LogOn	03/07/21 10:43:09 AM	WINCOMMERCE	Managed Computers	192.048.0.075	User LogOn User's name: W1
Start up	03/07/21 10:42:13 AM	WIN-CONDUCT	Q#_TE#M	192. 188 (1.89	
Shut Down	03/07/21 10:37:44 AM	WINDOWNDOWNER	Managed Computers	192.048.0.075	

Filtering Session Activity Log

To filter session activities, click **Filter Criteria** field. Filter Criteria field expands.

♥ Filter Criteria		Export Option	
Filter Criteria			
Computer Name	* v Include V	✓ IP Address	* Include 🗸
Operation Type	* v Include v	Group	* Include 🗸
Description			
🔤 Date Range			
From (MM/DD/YYYY)	07/03/2021		
To (MM/DD/YYYY)	07/03/2021		
Search Reset			(*) 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.

▲ Filter Criteria	👻 Export Opti	on
Export Option		
O Excel	HTML	Export

Select the preferred option and then click **Export**.

A success message appears.



Click the link to open/download the file.





File Activity Report

The File Activity module displays a report of the files created, copied, modified, and deleted on managed computers. Additionally in case of a misuse of any official files can be tracked down to the user through the details captured in the report. Select and filter the report based on any of the details captured.

Viewing File Activity Log

In the navigation panel, click **User Activity** > **File Activity Report**.

The log displays list of files and the type of operation performed on them. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

					1 - 1	.0 of 51 ∢ (pag	pe 1 of 6 >>> Rows per page: 10	~
Client Date	Computer Name/Ip	Group	IP Address	<u>User's name</u>	File Action Type	Drive Type	Source File	D
6/19/2021 6:11:04 PM	PRASHANT-QA	Qn_manM	192	PRASE and a number ator	Сору	Fixed Drive	C:\Users\Administrator\	C:
6/19/2021 6:11:13 PM	PRASING	Q=_==M	192.000.000	PRASMENT of a second ator	Modify	Fixed Drive		C:
6/19/2021 6:11:18 PM	PRESIDENT	QAM	192	PRASMENT of administrator	Delete	Fixed Drive		C:
6/21/2021 11:17:06 AM	With Canada	Q#M	192.008.0.00	WINCOMMUNIC	Modify	Fixed Drive		C:
6/22/2021 11:04:10 AM	With Canada	Qe_manM	192. 48.8.8	W1 Hard and the same	Delete	Network Drive		W
6/22/2021 11:04:10 AM	With Contracts	Q#M	192.008.0.07	WINGSAU	Delete	Network Drive		W
6/22/2021 11:04:10 AM	With condition	Qn_manM	192. 48.8.8	With a graduate the second	Delete	Network Drive		W
6/22/2021 11:05:11 AM	With a second second	Q#TERM	192.	With constraints and	Delete	Network Drive		W
6/23/2021 11:29:58 AM	With California	QAM	192.000.000	With condition and	Create	Fixed Drive	NewFile	C:
6/23/2021 11:33:55 AM	Without Market	Qit_TERM	192,008.0.05	W1911-1_m1111 ²⁰ 100	Modify	Fixed Drive		C:

Filtering File Activity Log

To filter file activities, click **Filter Criteria** field. Filter Criteria field expands.

♥ Filter Criteria		▲ Export Option	
Filter Criteria			
Computer Name	* Include 🗙	IP Address	* Include 🗸
✓ User's name	* Include 🗸	Group	* Include 🗸
File Action Type	* 🔹 Include 🗸	Drive Type	* v Include V
Source File	* Include ¥	Destination File	* Include 🗸
Application	* Include 🗸		
Date Range From (MM/DD/YYYY) To (MM/DD/YYYY)	07/03/2021 IIII 07/03/2021 IIIII		
Search Reset	bove fields (Note: By enabling this option page l	oading can get delayed)	(*) 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.

▲ Filter Criteria		✓ Export Option	
Export Option		· · · · · · · · · · · · · · · · · · ·	
O Excel	O PDF	HTML	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.

 Filter Criteria 	 Export Option
	1 - 9 of 9 (page 1 of 1 > > Rows per page: 100 ♥
Application Name	Total Duration (DD:HH:MM:SS)
Dropbox	00:00:06:10
Google Chrome	00:04:04:12
Internet Explorer	00:04:20:22
Notepad	00:00:00:23
Qt Qtwebengineprocess	00:00:03:47
Remote Desktop Connection	00:00:00:44
Secunia PSI Tray	00:02:22:45
Windows Command Processor	00:00:21:22
WordWeb	00:02:30:56

By clicking on the duration present under **Total Duration (DD:HH:MM:SS)** column, you will get the details of the computer name accessed the app and duration.

Application Name >> Dropbox	
Export To:Select V Export	
	1 - 1 of 1 ((page 1 of 1)) Rows per page: 100 ♥
Computer Name	Total Duration (DD:HH:MM:SS)
WIN EDGenhalden af R	00:13:50:41

Again, if you click on the duration, you will get detailed view of the app accessed by the computer along with the date, time, and application path.

Export To:Select V Export				
1 - 1 of 1 ((page 1 of 1)) Rows per page: 100			e 1 of 1) > Rows per page: 100 *	
Application Name	<u>Start Time</u>	End Time	Total Duration (DD:HH:MM:SS)	Application Path
And set.exe	09/07/21 11:51:05 AM	09/07/21 12:05:14 PM	00:00:14:08	C:\Program Files\mail_mail_mail_mail.exe
And set .exe	09/07/21 11:51:05 AM	09/07/21 12:05:14 PM	00:00:14:08	C:\Program Files\

You can export this report in various format such as PDF, CSV, and HTML.





Filtering Application Access Report

To filter file activities, click **Filter Criteria** field. Filter Criteria field expands.

♥ Filter Criteria	🔺 Export Op	Option	
Filter Criteria		Group By	
Application Name	* Include 🔪	Application Name	
Computer Name	* v Include v	Computer Name	
🖉 Date Range			
From (MM/DD/YYYY)	07/03/20	2021	
To (MM/DD/YYYY)	07/03/20	2021	
Search Reset		(*) View All Item	ns

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.

ch Management Patch Report	l Patch Report		💲 Refresh 🛛 👔
 Filter Criteria 		▲ Export	Option
			1 - 20 of 272 (age 1 of 14) → Rows per page: 20 V
Patch Name	Applied Count	Not Applied Count	Not Applicable Count
KB958644	0	0	5
KB929969	0	o	5
KB958687	0	0	5
KB921883	0	0	5
KB912919	o	0	5
KB902400	0	0	5
KB905749	0	0	5
KB899588	0	o	5
KB890047	0	0	5
KB885250	0	0	5
KB873333	0	0	5
KB888113	0	0	5

Patch report

The Patch report tab displays the Patch Name, Applied Count, Not Applied Count and Not Applicable Count. Clicking the numerical displays the patch name, details about the computer, the group it belongs to, IP address and User's name.

Computer List >> Not Applicable Count For >> KB958644					
Export To:Select V Export					
1 - 5 of 5 ∢ (page 1 of 1) → Rows per page: 20 ¥					
Computer Name	Group	<u>IP Address</u>	<u>User's name</u>	<u>Operating System</u>	
AH.# 2 136	Managed Computers	192.000 2 000	ree	Ubuntu Linux 16.10 64-Bit	
ESCHN_CLIENT	Managed Computers	192.008.0.019	ESCAR, CLIENT Administrator	Windows XP Professional x64 Edition 64-bit	
PF address of the	Managed Computers	192.000 0 010	PREDition of administration	Windows 7 Home Basic Edition 32-bit	
WIN EDCHNOENJER	Managed Computers	192.008.0.019	WHITE SCHNEEP JEEP Jeannahore	Windows 8 Professional 32-bit	
WIR-QADE?	Managed Computers	192.008 0 49	W Proceeding to the second	Windows 8.1 Professional 64-bit	





Filtering Patch Report

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

♥ Filter Criteria	▲ Export Option
→ Filter Criteria Patch Name	Group By Patch Name Computer Name
Search Reset	(*) 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.

▲ Filter Criteria		▼ Export Option
Export Option		
	HTML	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.

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

p	atch Management	💲 Refresh 🛛 👔 Help
	Patch Report All Patch Report	
	▲ Filter Criteria	Export Option
		0 - 0 of 0 ((page 0 of 0)) Nows per page: 20 ♥
	Patch Name Compute	
	There are no item	s to show in this view.

Filtering All Patch Report

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

✔ Filter Criteria	▲ Export Option	
Pilter Criteria	* Include V * Include V	Group By
Computer Name	• • Include •	Computer Name (*) View All Items
	Note : To enable All Patch Report Configure policy under File Antiv	irus>Advanced Setting>Send Windows Security Patch Events.

Enter the **Patch Name** and **Computer Name** to be included in the filtered report.

•	To enable All Patch Report Configure policy by going to File Antivirus-	
NOTE	Advanced Setting>Send Windows Security Patch Events.	

Include/Exclude

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

After making the necessary selections, click **Search.**

The Patch Report will be filtered according to your preferences.





Exporting All Patch Report

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

▲ Filter Criteria		✓ Export Option
Export Option		
O Excel	HTML	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.





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:

 In the navigation panel, click Notifications > Outbreak Alert. Outbreak Notification screen appears.

Ou	DutBreak Notification		
O	utBreak Alert Settings		
	Send Notification, If virus count exceeds threshold value within the defined time duration		
	Count 25 Time Duration 1 Day(s) V	Configure SMTP Settings	

- 2. Select the check box **Send notification**.
- 3. Enter the preferred values in Count and Time Limit field.

Auto	Auto Isolation Settings		
	Auto Isolation for Outbreak Send Outbreak, If virus count exceeds threshold value within the defined time duration Count 25 Time Duration 1 Day(s) V View Auto Isolated Endpoints Automatically restore outbreak prevention after 24 View Auto Isolated Endpoints		
	Client(s) list excluded from Auto Isolation Add Add Remove		
	e.g.: Host Name Host Name with wildcard IP Address		
	IP Address Range Save Cancel		





- 4. In **Auto Isolation Settings** section, select check box **Auto Isolation for Outbreak**.
- 5. Enter the preferred values in Count and Time Limit field.
- 6. Select the value in **Automatically restore outbreak prevention after hours(s)** field.
- 7. You can also add/remove clients list to exclude it from auto isolation in the below table. To do the same refer the following:
 - Enter the host name, IP Address, or IP address range and click **Add**.
 - To delete a particular client, select the client and click **Remove**.
- 8. After configuring accordingly, click **Save.** Outbreak Alert Settings will be saved.

In order to receive notification emails, it is necessary to configure SMTP
settings.
Learn more about SMTP Settings by clicking <u>here</u> .
To view the Auto-Isolated Endpoints, click View Auto Isolated Endpoints
hyperlink. The list of auto-isolated endpoints will be displayed.





Event Alert

This submodule lets you enable email notifications about any event that occurs on the client computers connected to the server.

_	vent Notification	👔 Help
	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 S	Settings							
	Enable email alert Notification <u>Configure SMTP Settings</u> Send Information only in subject line								
Select Event Ids Select activities for which email alert is required									
		Event Id	Description	·					
		100	ESCAN_DUMMY_EVENT						
		1	MWAV_FOUND_MALWARE						
		2	MWAV_FOUND_VIRUS_AND_DELETED						
		3	MWAV_FOUND_VIRUS_AND_CLEANED						
	\Box	4	MWAV_FOUND_ADWARE						
5 MWAV_FOUND_ERROR			MWAV_FOUND_ERROR						
		6	MWAV_FOUND_VIRUS_AND_RENAMED						
		7	MWAV_FOUND_ADWARE_AND_DELETED						
		8	MWAV_LAST_COMPUTER_SCAN						
		9	MWAV_START						
		10	MWAV_SUMMARY						
		501	SCHED_MWAV_FOUND_MALWARE						
		502	SCHED_MWAV_FOUND_VIRUS_AND_DELETED						
		503	SCHED_MWAV_FOUND_VIRUS_AND_CLEANED						
	\Box	504	SCHED_MWAV_FOUND_ADWARE	•					





4. Select the required hosts or group.

	All Hosts Selected Hosts		
	Select Computers		
	🗄 🗌 🧰 Managed Computers		
L		 _	
	Save Cancel		

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.

Unlicense Move Notification							
Unlicense Move Alert Settings							
Send notification for unlicensed computers.	Configure SMTP Settings						
Save Cancel							

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.

New Computers Notification	👔 Help
New Computers Alert Settings	
Send new Computers added notification within the shown time Time Limit 1 Day(s) V	Configure SMTP Settings
Save Cancel	

To enable the new computer alert, follow the steps given below:

- 1. In the navigation panel, click **Notifications > New Computer Alert**.
- 2. Select the check box **Send new Computers added notification within the shown time**.
- 3. Enter the preferred values in Time limit field.
- 4. Click Save.

The New Computer Alert Settings will be saved.

Configure SIEM

SIEM technology provides real-time management of security events generated for hardware changes and applications installed/uninstalled/upgraded where eScan is installed. eScan is equipped with variety of features that facilitate real-time monitoring, correlating captured events, notifications and console views and provides long-term storage, analysis and reporting of data.

Configure SIEM		👔 Help
Settings		
Enable event forward to SIEM / SYSLOG Server Add IP Address Add Hostname		
SIEM / SYSLOG Server IP Address	192]
SIEM / SYSLOG Server UDP port	5	

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 check box.





- 3. After selecting the check box, it will enable the rest of the options that can be configured. You can enter the details of the SIEM/SYSLOG Server.
- 4. Click **Save**.

The SIEM settings will be saved.

SMTP Settings

This submodule lets you configure the SMTP settings for all the email notifications.

SMTP Settings		김 Help
SMTP Settings		
Sender:	presidente com	
Recipient:	pra la la com	
SMTP Server:	192.	
SMTP Port:	25	
Use SMTP Authent User name: Password: Test		
Save Cancel		

To configure the SMTP settings, follow the steps given below:

- 1. In the navigation panel, click **Notifications** > **SMTP Settings**.
- 2. Enter all the details.
- 3. Click Save.

The SMTP Settings will be saved.

To test the newly saved settings, click **Test**.





Settings

The Settings module lets you configure general settings. It contains following submodules.

- **EMC Settings**: This submodule lets you define settings for FTP sessions, Log Settings, Client Grouping and Client connection settings.
- Web Console Settings: This submodule lets you define settings for web console timeout, Dashboard Settings, Login Page settings, SQL Server Connection settings, SQL Database compression settings.
- **Update Settings**: This submodule lets you define settings for General Configuration, Update Notifications, and Scheduling.
- **Auto-Grouping**: This submodule lets you define settings for Grouping of computers after installation of eScan client is carried out.
- **Two-Factor Authentication**: This submodule lets you to add extra layer of protection to your endpoints.
- **Roaming Client**: This submodule allows the remote client to download all the updates via Cloud while Server uploads all the required client updates to Cloud.





EMC Settings

The **EMC** (eScan Management Console) **Settings** lets you configure the eScan Management Console. You can configure the FTP settings, Bind to IP Settings, Log Settings, Client Grouping and Client Connection Settings.

You can bind announcement of FTP server to particular IP by selecting the IP address in the list. However, you can choose to leave it as 0.0.0.0, which mean it will announce on all available interface/IP.

EMC Settings	👔 Help						
EMC Settings							
FTP Settings Settings Image: Allow log upload from clients Bind IP Image: Allow log upload session allowed by clients 0.0.0.0 Image:							
LOG Settings Delete the user settings and user log files after uninstalling. No of days Client logs should be kept 5							
Client Grouping Group Clients by NetBIOS O DNS Domain							
Client Connection Settings Increase Thread count 10 (1-100) Increase Query Interval 10 (In seconds) (1-100)							
Restore default values							
Save Cancel							

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 check box. After selecting the check box, 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** check box.

After performing the necessary changes, click **Save**. The EMC Settings will be updated.





Web Console Settings

Web Console Settings submodule lets you configure web console Timeout, Dashboard, Login Page, SQL Server Connection, SQL Database compression, and Password Policy Settings.

Web Console Settings		👔 Help
Web Console Timeout Setting		
Enable Timeout Setting		
Automatically log out the Web Console after	0 V minutes	
DashBoard Setting		
Show Status for Last 7 days (1 - 365)		
Login Page Setting		
Show Client Setup Link		
Show Agent Setup Link		
Show eScan AV Report Link		
Logo Settings		
Logo : eSaañ		
The logo needs to have the size 300		
and needs to be in .png or .jpg (RG	B Color) format.	
Change Default		
Sql Server Connection Setting		
Microsoft Windows Authentication Mode		
Microsoft Windows Authentication Mode SQL Server Authentication Mode		
SQL Server Authentication Mode	eScanSQLSERVER	Browse
Host Name/IP Address:	127.0.0.1	
Login name	sa	
Password	•••••	Test Connection
	·	
SQL Database Purge Settings		
Enable Database Purge	1024 (500 - 3027)	
Database Size threshold in (MB) Purge data older than specified days, if above		
threshold is met	7 days (7 - 365)	
RMM Settings		
 Activate View Only 		
O De-Activate View Only		
Screen Quality	Medium 🗸	
Screen Ratio	80% 🗸	
Password Policy Settings		
Password Age :	90 days (30-180 days)	0 = Password Never Expires
Password History :	3 (3-10 Passwords)	0 = No password history is maintained
Maximum Failed login attempts :	3 (3-10 times)	0 = Unlimited failed attempts allowed
	Default	
Note: The above restrictions are not applicable	to "Root" login.	
Save		

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 check boxes of respective links.

Logo Settings

This setting allows you to add the organization logo in PNG or JPEG format. So the console and reports will have the uploaded logo for customization.

To have the default eScan logo, click **Default**. To have customized logo, click **Change**.

SQL Server Connection settings

This setting lets you select an authentication mode between Microsoft Windows Authentication Mode to SQL Server Authentication Mode. Select the **SQL Server Authentication Mode** and define **Server instance** and **Host Name** along with the credentials for connecting to the database.

Server Instance

It displays the current server instance in use. To select another server instance, click **Browse**. Select an instance from the list and click **OK**.

Hostname/IP Address

It displays the Hostname or IP Address of the server instance computer.

Enter the credentials in **Username** and **Password** fields. To check whether correct credentials are entered, click **Test Connection**.

SQL Database Purge Settings

This setting lets you define the maximum SQL database size in MB and purge data older than the specified days. To enable SQL Database Purge Settings, select **Enable Database Purge** check box.

Enter the preferred value in **Database Size threshold in (MB)** field.

Enter the preferred number of days in **Purge data older than specified days, if above threshold** is met field.





RMM Settings

This setting lets you configure default RMM setting for connecting to client via RMM service:

Activate View Only

By default, after taking a remote connection, you can only view the endpoint screen and are unable to perform any activity.

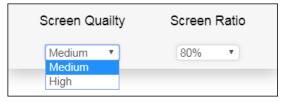
De-Activate View Only

To perform activity on an endpoint after taking remote connection, click **De-Activate View Only**.

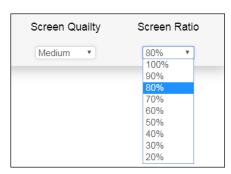
Screen Quality Settings

This option lets you configure the screen as per your requirements. It consists following suboptions:

• Screen Quality can be set to Medium or High.



• Screen Ratio can be set to anywhere from 20% to 100%.





To build a safe RMM connection between a Client to Server, Client to Update Agent, and Update Agent to Server, ensure that ports 2219, 2220 and 8098 are open.





Password Policy Settings

This setting allows the admin to configure the password settings for other users.

- **Password Age**: Enter the preferred value (between 30-180); this will prompt user to reset the password after specified number of days. Here, 0 indicates that password never expires.
- **Password History**: Enter the preferred value (between 3-10); this maintains the password history for specified count. Here, 0 indicates, no password history is maintained.
- **Maximum Failed login attempts**: Enter the preferred value (between 3-10); this will restrict the user from logging after specified attempts. Here, 0 indicates unlimited login attempts.



This setting will not be applicable for the root login

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.

FTP Ittp xy Settings Download via Proxy TTP HTTP Proxy Server IP : 192. Port: 3 Login Name : Password :	neral Config Update I	Notification Scheduli	ing Update Distribution	
HTTP HTTP HTTP Proxy Server IP: Password : FTP Login Name : Port: 1021 Login Name : anonymous	xy Settings		• нттр	
FTP Proxy Server IP:	HTTP	192.000 0.01		
	Port: Login Name :	anonymous	User@siteaddress OPEN siteaddress PASV Mode	

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** check box. 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.

eneral Config	Update Notification	Scheduling	Update Distributio	n		
Update Notificati	on					 1
Sender:	prisitianite 2 and and	com				
Recipient:						
SMTP Server:	192.			SMTP Port:	25	
User name: Password :						
Password :						
Password :						

Update Notification

To receive email notifications from eScan about virus signature database update, select this option.

Sender

Enter an email ID for sender.

Recipient

Enter the 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 check box and enter the login credentials in the **Username** and **Password** fields.

After filling the necessary data, click **Save > Update**. The Update Notification will be saved and updated.

Scheduling

The Scheduling tab lets you schedule updates with Automatic or Schedule Download mode.

Update Settings					김 Help			
		uling Update Dist]			
Query Interval	120 V minutes	5						
Schedule Download								
Weekly	Mon	Tue Sat	Wed Sun	Thu				
O Monthly	1 V of the	month						
At 12:00 pm C▼								
Save	Cancel Upda	ite						

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

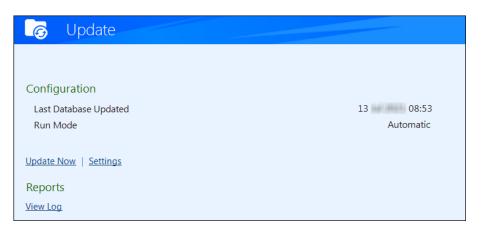
The Update Distribution tab allows the admin to enable and disable the sharing of eScan Virus signature to be distributed to air-gapped/isolated network.

-Setting O Enable Share	Disable Share	
-Anti-spam/product Updates		
Anti-spam/product Updates :	C:\PUB\Update	
-AntiVirus Updates 32 bit share path :	C:\PUB\AVX	
	only if 64 bit Linux and MAC system are in network)	
64 bit share path :	C:\PUB\MAC\AVX	

Select **Enable Share** in **Setting** section, this will allow the distribution of eScan Virus Signatures to the isolated/air-gapped network. After enabling this, it is mandatory to set the update mode to the network in network that is isolated/air-gapped through eScan Protection Center.

To update it, follow the below steps:

1. Open the eScan Protection Center in air-gapped network; click **Update** option present in the Quick Link section.







2. Click Settings. Update Settings window appears.

Select Mo	ode © FTP	⊘ HTTP	Network
	tings wnload via Proxy		L
HTTP	HTTP Proxy Server IP : 192.		Port: 3
	Login Name :		Password :
FTP	FTP Proxy Server IP:		Port: 1
	Login Name:		Logon Type O User@siteaddress
	anonymous		OPEN siteaddress
	Password:		PASV Mode Socks

3. Select Network option and set the Source UNC Path as \\ServerName\esupd or \\ServerIP\esupd.

E.g.: **\\192.0.2.0\esupd**

After setting UNC path for the air-gapped network, the update will be available automatically to the Isolated/Air-gapped network.





Auto-Grouping

The Auto grouping submodule consists following subsections:

- Auto Add Client setting
- Client(s) list excluded from Auto adding under Managed Group(s)
- Group and Client selection criteria for Auto adding under Managed Group(s)

uto Grouping					🤤 R(efresh 👔 He
Auto Add Client setting						
 Auto adding client(s) under Manage 	ed Group(s)					
Client(s) list excluded from Auto a	dding under Mana	aged Group(s)				
	Add					
SUPPORT PC	Remove					
e.g.: Host Name	J					
Host Name with wildcard IP Address						
IP Address Range						
Group and Client selection criteria	for Auto adding u	inder Managed Group(s)				
Group Name		Client Criteria				
	Add			Add	Run Now	
	Remove		-	Remove		
	Browse					
	Up					
e.g.: group1	Down	e.g.: Host Name	*			
group1\subgroup		Host Name with wildcard IP Address IP Address Range				
Save						

Auto Add Client setting

Selecting the check box **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 criteri	a for Auto adding u	under Managed Group(s)		
Group Name		Client Criteria		
	Add			Add Run Now
	Remove		-	Remove
	Browse			
	Up			
	Down		-	
e.g.: group1		e.g.: Host Name		2
group1\subgroup		Host Name with wildcard IP Address		
		IP Address IP Address Range		

 Under the Group Name, enter the group's name and click Add. OR

Click **Browse** and select the group from the existing list.

0 To browse through the list of groups, click **Up** or **Down**. NOTE

- 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**.



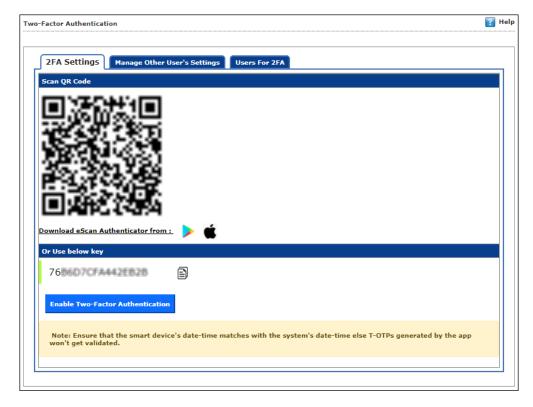


Two-Factor Authentication (2FA)

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 <u>Play Store</u> or for iOS devices from <u>App Store</u> 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.





Ensure that the smart device's date and time matches with the system's date and time or else TOTPs generated by app won't get validated.





We recommend that you save/store the Account Key in offlineIMPORTANT 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**.
- Open the Authenticator app.
 After basic configuration following screen appears on smart device.

÷		000
	an account	
0	Scan a barcode	
	Enter a provided key	

3. Select a preferred option. If you tapped **Scan a barcode**, scan the onscreen QR code via your smart device. If you tapped **Enter a provided key**, enter the Account Key and then tap **ADD**.

After scanning the Account QR code or entering Account Key the eScan server account gets added to the Authenticator app. The app then starts displaying a Time-based One-Time Password (TOTP) that is valid for 30 seconds.

Authenticator	
Account Added	
536151	13

4. Click Enable Two-Factor Authentication.





Verify TOTP window appears.

	٤
Two-Factor Authentication	
Verify T-OTP	
11:43:18 AM	
Enter T-OTP Verify T-OTP	

- 5. Enter the TOTP displayed on smart device and then click **Verify TOTP**. The 2FA login feature gets enabled.
- 6. To apply the login feature for specific users, click **Manage Other User Settings** tab. The tab displays list of added users and whether 2FA status is enabled or disabled.



Two-Factor Authentic		🛐 Help
2FA Settings	Manage Other User's Settings	2FA
<u>User's name</u>		2FA Status
kaitutta		
root		
L		

 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.

Two-Factor Authentication Verify T-OTP	
44.45.04	
11:45:34 AM	
Enter T-OTP	
Verify T-OTP	

3. Enter the TOTP and then click **Verify TOTP**. The 2FA feature gets disabled.

0	After disabling the 2FA feature and enabling it again, the 2FA login status
NOTE	will be reinstated for added users.





Users For 2FA

This tab helps to add the users and apply 2FA to the endpoints via policy template. The users can be added directly or from Active directory.

	-Factor Authentication 😨 Help						
2F	2FA Settings Manage Other User's Settings Users For 2FA						
	Add User Madd from Active Directory ☐ Delete						
	<u>User's name</u>	Description	Created Date	Assigned Policy Template	<u>QRCode</u>		
	anital	admin	7/2/2021 6:24:41 PM		View		
L							

Method 1: Adding user

To add users for the same, follow the below steps:

- 1. Go to Settings > Two-Factor Authentication > Users For 2FA.
- 2. Click Add User.

Add User window appears.

		🗄
Add User		
Username Description		
Ok	Cancel	

- 3. Enter the **Username** and **Description**.
- 4. Click **OK**.





Method 2: Adding User from Active Directory

To add users from Active Directory, follow the below steps:

- 1. Go to Settings > Two-Factor Authentication > Users For 2FA.
- 2. Click Add from Active Directory.

Add Active Directory Users window appears.

Add Active Directory Users		👔 Help
> Add Active Directory Users		
Search Criteria		
User's name*:		
	For Example: user or user*	
Domain*:		
AD IP Address*:		
AD Admin User name*:		
	For Active Directory account: domain\username	
AD Admin Password*:		
Use SSL Auth.:		
AdsPort*:	389	
Search		
Search Results		
Users	Selected Users	
Ok Cancel	(*) Manda	atory Fields

- 3. Enter the required information.
- 4. Click **Ok**.

The Active Directory Users will be added.





Roaming Clients

Roaming Clients submodule provides protection for the remote endpoints when not connected to the organization network, adding another layer of security. According to the needs of the business, admins might want to continue the protection of roaming client on the organization network. Using this feature admin can provide protection for such clients connected to both organization network and also to internet via cloud.

This feature is quite helpful for the remote clients. Apart from it, it does not require any additional machine set up apart from the (on-premise) EPS Server in the network. All the communication is handled by the EPS Server via Cloud to the client having stable internet connection.

Here, the remote clients will update their status, download the latest configuration from the EPS Server via Cloud.

Roaming Clients		🝸 Help
Roaming Clients		
-	_	e clients update their status, download latest when the clients are outside your organization network
Roaming Service State	15	
Not Connect	ed. You must connect to the EPS cloud platform in o	order to use Roaming Service.
Company Name:*		
Email Address:*		Generate Secret Code
Secret Code:*		Code is valid for 10 Minutes only.
Connect to cloud pl	atform	
Note: For enabling	Roaming Service kindly allow "cl.escanav.com	" in firewall.

This service allows admin to apply policies to the client from EPS Server. All events from the clients such as Application Control Scan, Vulnerability Scan, Virus Scan, etc. are collected and managed on EPS server via Cloud Platform.





Adding Roaming Client

To add roaming client, it is mandatory to connect to the Cloud Platform. Follow the below steps, to do the same:

- 1. Go to **Settings** > **Roaming Clients**.
- 2. Enter the company name and email address.
- 3. Click Generate Secret Code.

Roaming Clients		👔 Help
Roaming Clients		
	2	the clients update their status, download latest en when the clients are outside your organization network
Roaming Service Stat	us	
Not Connect	ed. You must connect to the EPS cloud platform i	n order to use Roaming Service.
Company Name:*	Shiiliteen	
Email Address:*	sh-line com	Generate Secret Code
Secret Code:*		Code is valid for 10 Minutes only.
Connect to cloud p	atform	
Note: For enabling	Roaming Service kindly allow "cl.escanav.co	m" in firewall.

A secret security code will be generated and sent to given email address.



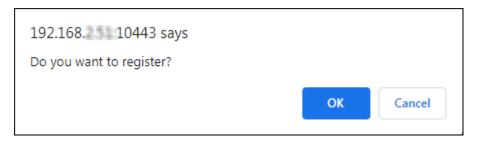




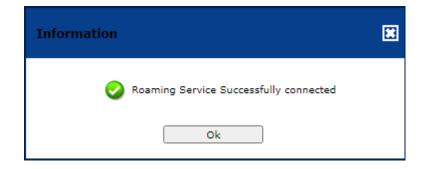
4. Enter the secret code received via email, click **Connect to cloud platform**.

Roaming Clients	🝸 Help
Roaming Clients	
In this section, You can set EPS clients as roaming. This feature will let th configuration from the EPS Server via Cloud based Roaming Service even and connected through internet.	
Roaming Service Status	
Not Connected. You must connect to the EPS cloud platform in o	rder to use Roaming Service.
Company Name:* Shull am	
Email Address:* shall an generation com	Generate Secret Code
Secret Code:" -	Code is valid for 10 Minutes only.
Connect to cloud platform	
Note: For enabling Roaming Service kindly allow "cl.escanav.com	" in firewall.

5. A confirmation window appears. Click **OK**, this will authenticate and allows to connect to Cloud Platform.



An information window appears.



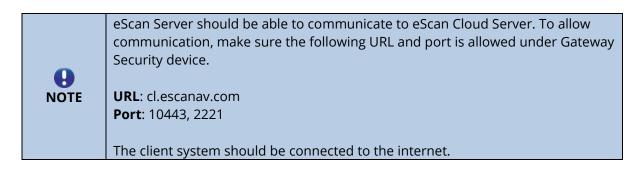




6. After connecting to the cloud platform successfully, you can manually enable and disable the roaming service.

ming Clients	
aming Clients	
	t EPS clients as roaming. This feature will let the clients update their status, download latest Server via Cloud based Roaming Service even when the clients are outside your organization network ernet.
aming Service Status	
Your local EPS is si	uccessfully connected to the Cloud based Roaming Service, you may now use this service.
V	
Company Name:*	Shulldam
Company Name:* Email Address:*	Shuham shuham com
Email Address:*	shi ha com
	shi ha com
Email Address:*	shi ha com
Email Address:* Connect to cloud platfor Note: For enabling Roar	shimmer com
Email Address:* Connect to cloud platfor Note: For enabling Roar	shimmer com
Email Address:*	m ming Service kindly allow "cl.escanav.com" in firewall.
Email Address:* Connect to cloud platfor Note: For enabling Roar aming Mode	m ming Service kindly allow "cl.escanav.com" in firewall.

7. Click **Download Roaming Client Setup** to download the setup file. Install the set up file in the client system to make it as roaming client and it should be connected to the internet.



Installing Roaming Clients

To install Roaming Clients setup, follow the below steps:

- 1. Go to Settings > Roaming Clients > Download Roaming Client Setup.
- 2. Transfer the file to the client system.
- Double-click and install the setup file.
 It will connect to eScan Cloud Server and automatically gets added and managed by eScan EPS Server.





Administration

The Administration module lets you create User Accounts and allocate them Admin rights for using eScan Management Console. In a large organization, installing eScan client on all computers may consume lot of time and efforts. With this option, you can allocate rights to the other employees and allow them to install eScan Client, implement Policies and Tasks.

The Administration module consists following submodules:

- User Accounts
- User Roles
- Export & Import
- Customize Setup
- Audit Trail

User Accounts

For a large organization, installing eScan Client and monitoring activities may become a difficult task. With User Accounts submodule, you can create new user accounts and assign Administrator role to added users and reduce the workload. This submodule displays a list of users and their details like Domain, Role, Session Log and Status.

User	Accounts					💲 Refresh	🝸 Helj
-							
	Create New Acco	unt 💽 Add from Active Directory <u>Delete</u>	1	-1 of 1 ⊣ page	1_of1 ⊨	Rows per page:	10 🗸
	<u>User's name</u>	Full Name	Domain	<u>Role</u>	MDM Role	Session Log	<u>Status</u>
	root	Administrator account created during installation		Administrator	Administrator	View	
Ð	Create New Acco	unt 🛃 Add from Active Directory 前 Delete	1	-1of1 _M page	1 of 1 🕅	Rows per page:	10 🗸





Create New Account

To create a User Account,

 In the User Accounts screen, click Create New Account. Create User form appears.

Create User		? Help
<u>User Accounts</u> > Create User		
Account Type and Information		
User's name*:		
Full Name*:		
Password*:		
Confirm Password*:		
Email Address:*		
	For Example: user@yourcompany.com	
Account Role		
Role*: Administrator	♥	
MDM Role*: Administrator	v	
Save Cancel	(*) Mandator	ry Fields

After filling all the details, click Save.
 The user will be added to the User Accounts list.

Delete a User Account

To delete a user account

1. In the User Accounts screen, select the user you want to delete.

Jser	Accounts					💲 Refresh	👔 Hel
Ð	Create New Acco	ount 🋃 Add from Active Directory 👔 Delete		1 - 2 of 2 ∢ page	e 1 of 1 ⊨∣ Ro	ows per page: (10 🗸
	<u>User's name</u>	<u>Full Name</u>	<u>Domain</u>	<u>Role</u>	MDM Role	Session Log	<u>Status</u>
<	k	K		Administrator 🗸	Administrator 🗸	View	V .
	root	Administrator account created during installation		Administrator	Administrator	View	
Ð	Create New Acc	ount 🙀 Add from Active Directory 👘 Delete		1 - 2 of 2 ∢ pag	e 1 of1⊮ Ro	ows per page: (10 🗸





2. Click **Delete**.

A confirmation prompt appears.

User Accounts
Do you want to delete the selected user account(s) ?
Ok Cancel

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.

	Roles	🗢 Refre	-
₽	New Role Properties		
	Role Name	<u>Description</u>	
	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,

 In the User Roles screen, click New Role. New Role form appears.

<u>User Roles</u> >New Role Role Details
Role Details
New Role Name :*
Description :
Select Group :
🖻 🗌 🧰 Managed Computers
Ok
Cancel





- 2. Enter name and description for the role.
- 3. Click **Managed Computers** and select the specific group to assign the role. The added role will be able to manage and monitor only the selected group's activities.
- 4. Click **OK.**

Permissions section appears displaying Main Tree Menu and Client Tree Menu tabs. The Main Tree Menu consists of Navigation Panel Access permissions while the Client Tree Menu consists of selected groups on which permissions the user is allowed to take further.

Main Tree Menu Client Tree Menu		
Menu	View	Configure
DashBoard		
Managed Computers	S	
Unmanaged Computers		
Network Computers		
IP Range		
Active Directory		
Report Templates		
Report Scheduler		
Events & Computers		
System Action List		
Tasks For Specific Computers		
Asset Management		
User Activity		
Print Activity		
Session Activity Report		
File Activity Report		
Application Access Report		
Patch Report		
Notifications		
Outbreak Alert		
Event Alert		

- 5. Select the 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		💲 Refresh 🛛 👔 Help				
🔂 New Role 💕 Properties 👔 Delete						
	Role Name	Description				
	Administrator					
	Kahili					

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**.

Menu	View	Configure
menu		
DashBoard		
Managed Computers	V	
Unmanaged Computers		
Network Computers		
IP Range		
Active Directory		
Report Templates		
Report Scheduler		
Events & Computers		
System Action List		
Tasks For Specific Computers		
Asset Management		
User Activity		
Print Activity		
Session Activity Report		
File Activity Report		
Application Access Report		

4. To modify client configuration permissions, click **Client Tree Menu**. **Client Tree Menu**





Define the Actions that the created role can configure for the allocated group. The menu has Action List, Client Action List, Select Policy Template, Policy Criteria, and Group Tasks.

Permissions	rmissions					
Main Tree Menu Client						
Managed Computers	[Managed Computers/Samples_Team] Menu	Configure				
E. Linux / Mac	Action List					
I 🛅 <u>Ma</u> duatina. Taa <u>m</u>	New Sub Group					
	Set Group Configuration					
	Deploy / Upgrade Client					
	Uninstall eScan Client					
	Remove Group					
	Synchronize with Active Directory					
	Outbreak Prevention					
	Create Client Setup					
	Properties					
	Client Action List					
	Set Host Configuration					
	Deploy / Upgrade Client					
	Uninstall eScan Client					
	Move to Group					
	Remove from Group					
	Refresh Client					
	Show Critical Events					
	Export					
	Show Installed Softwares					

5. To let the role configure these actions, under the Configure column select the check boxes of corresponding actions.

6. Click **Save**.

The Role Properties will be updated accordingly.





Delete a User Role

To delete a user role

1. In the User Roles screen, select the user role you want to delete.

	🤝 Refresh 📲	Help
New Role 🛃 Properties 👔 Delete		
Role Name	Description	
Administrator		
Kallill		
	New Role Properties in Delete	New Role Properties Delete

2. Click **Delete**.

A delete confirmation prompt appears.

E	З
Delete Role	
	1
Do you want to delete the selected Role(s)?	
Ok Cancel	

3. Click **OK**.

The User Role will be deleted.





Export & Import

The Export & Import submodule lets you to take a backup of your eScan server settings, in case you want to replace the existing eScan server. You can export the Settings, Policies and the Database from existing server to a local drive and import it to the new server.

Export Settings

This tab lets you export the eScan Server Settings, Policies, and Database. To export the eScan Server settings, follow the steps given below:

1. In the Export Import Settings screen, click **Export Settings** tab.

WMC Settings	and Delision	
Database	and Policies	
Export		
View Exported File	<u>s</u>	
Export files path:	C:\PROGRA~1\COMMON~1\microworld\apache2\EMCWebAdm	

2. To backup **WMC Settings and Policies** and **Database**, select both the check boxes.

The backup file will be exported to the path shown in **Export files path** field. To change the file path, click **Change Path**. Enter the file path and click **Add**.

3. 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.

File Name Ch	pose File No file chosen	
✓ WMC Settings	and Policies	
Database		
Import		
View Exported File	<u>15</u>	
1. Select file to im	port (EservConf [YYYYMMDDhhmm][_SCHD].zip)	

2. Click Choose File.

The Import Settings tab lets you import only Settings and Policies or Database.

- 3. To import **WMC Settings and Policies** and **Database**, select both the check boxes.
- 4. Click Import.

The backup file will be imported. A success message is displayed after complete import.



After successfully taking a backup, eScan asks you to restart the server.





Scheduling

This tab lets you schedule auto-backing up of Settings, Policies, and Database.

	d Policies			tabase
Daily				
🔾 Weekly	Mon	Tue	Wed	🗌 Thu
	🗌 Fri	Sat	Sun	
Monthly	1 🗸			
Sender:				
Recipient:				
SMTP Server:				
SMTP Port:				
User name: Password:				
Password:				
Test				
Enable Optional S	ettings			
Enable Optional S Select how many bac			2 🗸	
Select how many bac		er than or equal to :	2 🗸	МВ 🗸

To create a Schedule for export, follow the steps given below:

- 1. Select **Enable Export Scheduler** check box.
- 2. Select the check boxes 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 check box and fill in the necessary details. If the SMTP server requires authentication, select the Use SMTP Authentication check box 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

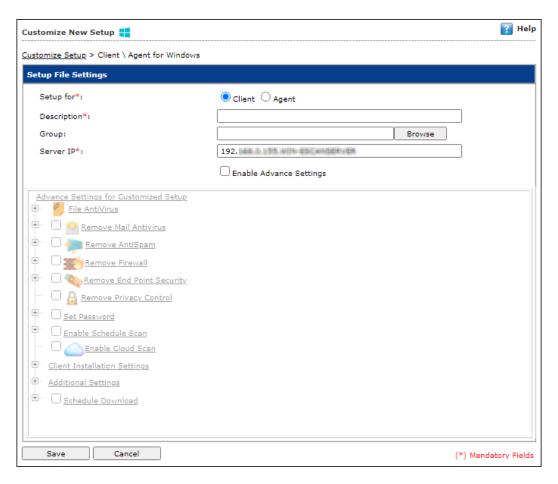
This submodule lets you create a customized setup for a Client or an Agent with fewer modules and deploy it to various locations. This can be very useful, if there are locations to which a server is unable to push the setup or locations that are unable to connect to the server directly. The custom setup can be downloaded as a file and sent to different locations.

reate Customized Setu	dr						💲 Refres	h 🝸 H
Client \ Agent for Windo	ws 🏭 Client \ Ag	ent for Linux 🧕	Properties	5 🗎 Delete				
Setup Name	Group Path	Server IP	OS Type	Distribution	Description	Created On	Download	*

Creating a customized setup for Windows

To create a customized setup for Windows, follow the steps given below:

 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** check box. Doing so enables the bottom field. Select the setting check boxes you want to provide.
- 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:

 In Create Customized Setup screen, click Client\Agent for Linux. Customize New Setup screen appears.

Customize New Setup 🧕		👔 Help
Customize Setup > Linux		
Setup File Settings		
Description*: Distribution*: Source Setup file path*: Group*: Server IP:	RedHat ✓ C:\Program Files\eScan\Setup\Agent_Setup.rpm Browse 192.	
Save Cancel		(*) Mandatory Fields

- 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:

	te Customized Setup							💲 Refresh	? He
Clie	nt \ Agent for Windows 📒 Client	\ Agent for L	.inux 🧕	🌱 Propert	ies 🚡 Delete	2			
	<u>Setup Name</u>	<u>Group</u> <u>Path</u>	<u>Server</u> <u>IP</u>	<u>OS</u> Type	<u>Distribution</u>	Description	Created On	<u>Download</u>	*
~	Setup_01001010_0010e0797.exe		125.000	Windows		Sample	08/05/2021 13:01	<u>Download</u>	

- 1. In the Create Customized Setup screen, select the Windows setup you want to edit.
- 2. Click **Properties**.

Edit Customized Setup screen appears.

Edit Customized Setup 🚦		👔 Help
<u>Customize Setup</u> > Client \ Agent for Windows		
Setup File Settings		
Setup for*:	Client Agent	
Description*:	Sample	
Group:	Browse	
Server IP*:	123 cmm	
	Enable Advance Settings	
Advance Settings for Customized Setup Image: Set Password Image: Set Password <td< td=""><td></td><td></td></td<>		
Save Cancel		(*) Mandatory Fields

3. Make the necessary changes and then click **Save**. The setup will be updated.





Deleting a Setup

To delete a setup, follow the steps given below:

1. In the Create Customized Setup screen, select the setup you want to delete.

	te Customized Setup							💲 Refresh	<table-cell> н</table-cell>
Clie	nt \ Agent for Windows 🗾 Client	\ Agent for	Linux 🧕	💕 Propert	ies 📋 Delete	2			
~	<u>Setup Name</u>	<u>Group</u> <u>Path</u>	<u>Server</u> <u>IP</u>	<u>OS</u> <u>Type</u>	<u>Distribution</u>	<u>Description</u>	Created On	<u>Download</u>	-
~	Setup_01001010_0010+0"9".exe		123.000	Windows		Sample	08/05/2021 13:01	<u>Download</u>	

2. Click Delete.

A confirmation window appears.

Create Customized Setup
Do you really want to Delete?
Ok Cancel

3. Click **Ok**.

The setup will be deleted.





Audit Trail

The Audit Trail submodule let you record the security relevant data, operation, event, Action, policy updates. Audit logs are used to track the date, time and activity of each user, including the policy/criteria that have been changed. A record of the changes that have been made to a database. You can get audit trail of user activity across all these systems.

lit Trail Report	t								💲 Refresh 🔋
Filter Crite	ria				▲ Export (Options			
							1 - 4 of 4 ।∢ (pa	ge 1 of 1 → ⊨ Row	s per page: 50 🗸
User Name	Session Id	IP Address	Client Date	Client Time	Audit Type	Policy/Criteria Name	Module Name	Action	View Action
mail	[E5A0 10143*0 100436]	192.168	(18/19)/21	12 38 56	Log Off			Console LogOut	
rasit	[DCHC-28 *0420048353B]	192.168	(18)(18)(21	12 38 00	Login			Console LogIn	
rast	[6C(+10+10+10)0135]	192.168	(10) (10) 21	12 - 2	Login			Console LogIn	
	[6C(1) 18-10 (1) 35]	192.168 8 88	08/08/21	12	Log Off			Console LogOut	

Filter all Audit Trail report

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

♥ Filter Criteria		▲ Export Options	
Filter Criteria			
🖾 User Name	* Include 🗸	IP Address	* Include ¥
🗹 Audit Type	* v Include V	Policy/Criteria Name	* Include 🗸
Module Name	* Include 🗸		
Date Range			
From (MM/DD/YYYY) To (MM/DD/YYYY)	09/09/2021		
	05/05/2021		
Search Reset			(*) View All Items

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

Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the report. After making the necessary selections, click **Search**.

The Hardware Report will be filtered according to your preferences.

Exporting Hardware Report

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

▲ Filter Criteria		♥ Export Option	
Export Option			
O Excel	O PDF	HTML	Export

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



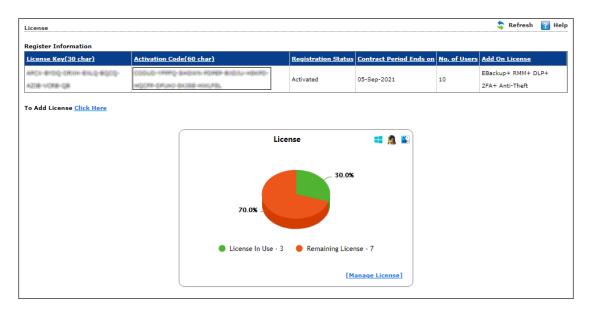
Click the link to open/download the file.





License

The License module lets you manage user licenses. You can add, activate, and view the total number of licenses available for deployment, previously deployed, and licenses remaining with their corresponding values. The module also lets you move the licensed computers to non-licensed computers and vice versa. Here you can also view the number of add-on license along with the name of it. For example, as you can see here there are 15 add-on licenses for eBackup feature. The add-on license is available for eBackup, 2FA, and DLP features.



Adding and Activating a License

To add and activate a license

1. In the License screen, click the **Click Here** link.

To Add License <u>Click Here</u>

Add License Key dialog box appears.

Add 30 Character License Key.		
	ОК	Cancel

Enter the license key and then click **OK**.
 The license key will be added and displayed in the **Register Information** table.

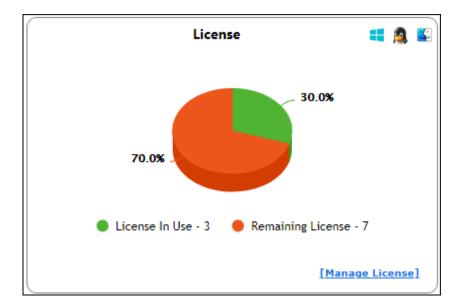




Moving Licensed Computers to Non-Licensed Computers

To move licensed computers to non-licensed computers,

1. In the License statistics box, click **Manage License**.



Manage License window appears.

1anage License			? F	lelp
Licensed Computers / Devices (3)	Filter Licer	nse All 🗸	Move to Non-License	e
Machine Name		Group		^
🗆 📃 umumu 🧟		Managed Computers		
🗌 🗮 QA-BDR 📫		Managed Computers		
WING MARCETTRIN!		Managed Computers		
Non-Licensed Computers / Devices (0)	Filt	ter License All 🗸	Dive to License	
	No Reco	ord Found		^
				Ŧ
Close				





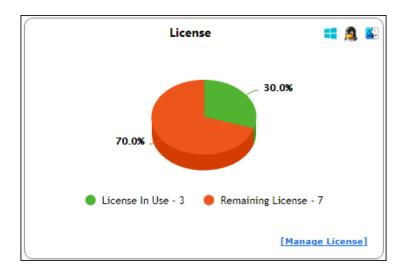
- 2. Under the Licensed Computers section, select the computer(s) that you want to move to Non-Licensed Computers section.
- 3. Click Move to Non-License.
- 4. The selected computer(s) will be moved to Non-Licensed computers section.

1anage License			🛜 Help
Licensed Computers / Devices	(2) Filter Licer	nse All 🗸	Dove to Non-License
Machine Name		Group	<u>^</u>
🗆 📃 uaunitu 🙇		Managed Computers	
		Managed Computers	
Non-Licensed Computers / Devices (1) Filter License			
Machine Name	Group	Unlicense Date Time	Description
🗆 📒 (pa esta 📢	Managed Computers\###	05/08/2021 16:43:00	

Moving Non-Licensed Computers to Licensed Computers

To move licensed computers to non-licensed computers, follow the steps given below:

1. In the License statistics box, click Manage License.







Manage License window appears.

Manage License 👔 Help					
Licensed Computers / Devices	Licensed Computers / Devices (2) Filter License All 🔹				
Machine Name		Group	·		
🗆 📃 uaunitu 🙇		Managed Computers			
		Managed Computers			
			~		
Non-Licensed Computers / Dev	rices (1) Filt	er License All	Move to License		
Machine Name	Group	<u>Unlicense Date Time</u>	Description		
	Managed Computers\	05/08/2021 16:43:00			
Close			*		

- 2. Under the Non-Licensed Computers section, select the computer(s) that you want to move to Licensed Computers section.
- 3. Click Move to License.
- 4. The selected computer(s) will be moved to Licensed Computers section.

Manage License 👔 Help			
Licensed Computers / Devices (3) Filter Lice	inse All		
Machine Name	Group		
	Managed Computers		
	Managed Computers\		
wik-condentration	Managed Computers		
	•		
Non-Licensed Computers / Devices (0) Fi	Iter License All		
No Rec	ord Found		
	*		
Close			





eScan Mobility Management

eScan Mobility Management (EMM) introduces a comprehensive mobile security solution that helps organizations maintain compliance while reducing IT intervention and effort. It provides a centralized system for device management and data security for complex and diverse mobile device. It allows you to enforce security policies for mobile devices from the same management platform.

Using granular, policy-based controls and deploying sophisticated threat protection, it allows to proactively enabling mobile productivity without compromising security. Following are the benefits of MDM:

- Deploy, protect, and manage Company-Owned Devices (COD) and Bring Your Own Devices (BYOD).
- Implement a various device control without having to physically handle the user's device.
- Secure data and resources, enhance user productivity, reduce costs, and maintain communications.
- Remotely locate, lock and wipe data on lost or stolen devices.
- Manage device app via App Store and monitor network data usage, call, SMS, etc.
- Keep an eye on the device by applying fencing parameters such as time, location, and Wi-Fi.
- Generates in-depth reports of mobile devices as per the requirement.





Getting Started

Click **eScan Mobility Management** in the Navigation Panel. Select Platform prompt appears.

eScan EMM is ready for Android Devices	
Start with Android (without iOS)	
To manage iOS devices you need to add a Trusted CA Certificate	
Start with iOS	

Clicking **Start with iOS** takes you to the **Settings** module > **Certificate Management** tab. To learn more about it, <u>click here</u>.

Clicking **Start with Android (without iOS)** displays the **eScan Mobility Management Console**.

If you clicked **Start with Android (without iOS)**, 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 <u>here</u>.





Dashboard

The Dashboard displays eScan MDM application's real-time Deployment Status, Protection Status and Protection Statistics for managed devices.

DashBoard		Date of v	irus signatures (EMM): Not Updated 🛛 😝 🕼
Deployment Status Protection Status Pr	rotection Statistics		
	Since L	ast 7 Days	
Updat	e Status	Scan Status	
	Updated 0 Not Updated 0 Unknown <u>1</u> Total <u>1</u>		Scanned 0 Not Scanned 0 Unknown <u>1</u> Total <u>1</u>
	Protect	tion Status	
Anti	-Virus	Web Control	
	Started 1 Stopped 0 Unknown 0 Total 1		Started 0 Stopped 1 Unknown 0 Total 1





Deployment Status

This tab displays detailed pie chart view and statistics of the following -

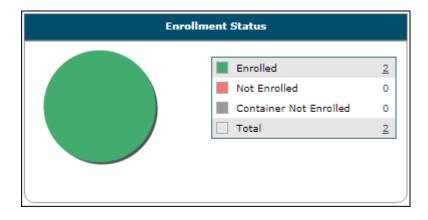
- Enrollment Status
- eScan Status
- eScan Version (Android MDM App)
- eScan Version (Android Container App)
- eScan Version (iOS MDM App)
- Android Version
- iOS Version
- Device Sync Status (Successful)
- Device Compliance
- Kiosk Status

DashBoard		Date of virus signatures (EMM): Not Updated	\$ \$
Deployment Status Protection Status	Protection Statistics		_
Enroll	ment Status	eScan Status	
	Enrolled 2 Not Enrolled 0 Container Not Enrolled 0 Total 2	Installed 2 Not Installed 0 Unknown 0 Total 2	
eScan Version	(Android - MDM App)	eScan Version (Android - Container App)	
	7.2.0.49 1 7.2.0.70 1 Unknown 0 Total 2	Unknown 2 Total 2	





Enrollment Status



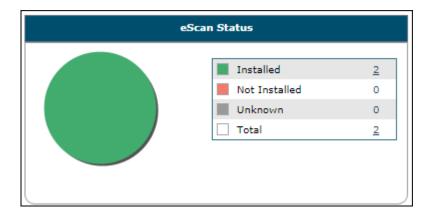
Enrolled – It displays the number of devices that are enrolled.

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.

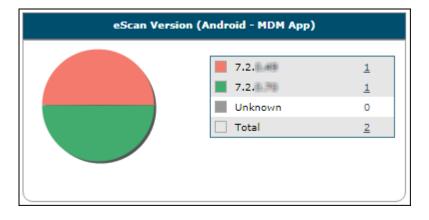
Not Installed – It displays the number of devices on which eScan MDM application is not installed.

Unknown – It displays the number of devices on which the eScan MDM application installation status is unknown.





eScan Version (Android - MDM App)

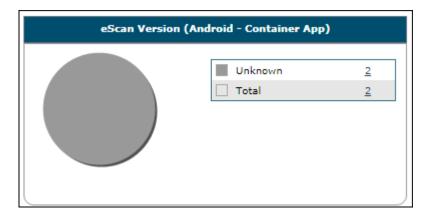


Version Numbers – It displays the Android MDM application's version number installed on devices.

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)



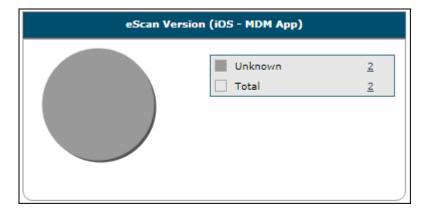
Version Numbers – It displays the eScan Container application's version number installed on devices.

Unknown – It displays the number of devices on which the eScan Container application's version number is unknown.





eScan Version (iOS - MDM App)

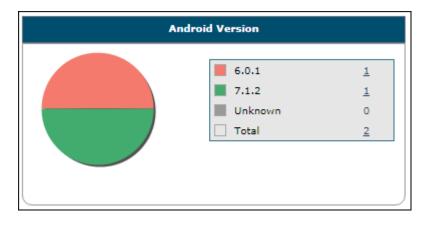


Version Numbers – It displays the iOS MDM application's version number installed on devices.

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



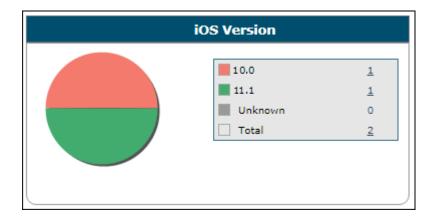
Version Numbers – It displays the Android OS version numbers and the number of devices which are running it.

Unknown – It displays the number of devices on which the Android OS version is unknown.





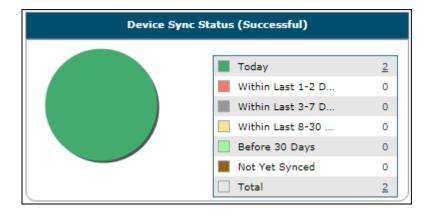
iOS Version



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)



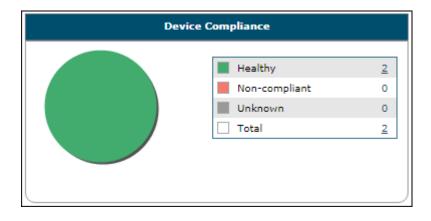
It displays the last sync status of the managed device with the server. You can view the statistics of the devices that are synced with the eScan server for Today, Within Last 1-2 Days, Within Last 3-7 Days, Within Last 8-30 Days, Before 30 Days.

Not Yet Synced – It displays the number of devices that are not yet synced with the eScan server.



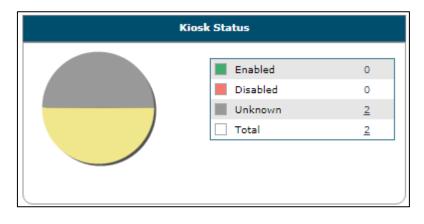


Device Compliance



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 mode is enabled. **Disabled** – It displays the number of devices on which the Kiosk mode is disabled. **Unknown** – It displays the number of devices on which the Kiosk mode status is unknown.





Protection Status

This tab displays detailed pie chart view and statistics of the following -

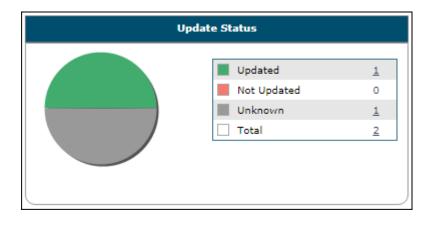
- Update Status
- Scan Status
- Anti-Virus
- Web Control
- Application Control
- Call & SMS Filter
- Firewall Status

ashBoard Date of virus signatures (EMM): Not Updated 😝 🧔				
Deployment Status Protection Status Protection	ection Statistics			
	Since La	ast 7 Days		
Update S	tatus	Sca	in Status	
	Updated 0 Not Updated 0 Unknown <u>1</u> Total <u>1</u>		Scanned 0 Not Scanned 0 Unknown 1 Total 1	
	Protect	on Status		
Anti-Vi	rus	Wei	b Control	
	Started 1 Stopped 0 Unknown 0 Total 1		Started 0 Stopped <u>1</u> Unknown 0 Total <u>1</u>	





Update Status



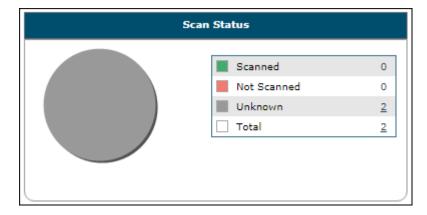
Updated – It displays the number of devices on which the Anti-Virus signatures are updated.

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.

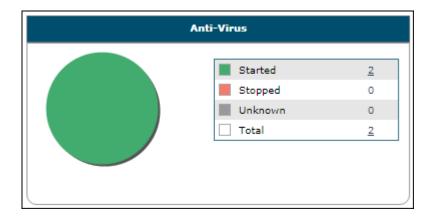
Not Scanned – It displays the number of devices which are not scanned.

Unknown – It displays the number of devices on which the scan status is unknown.





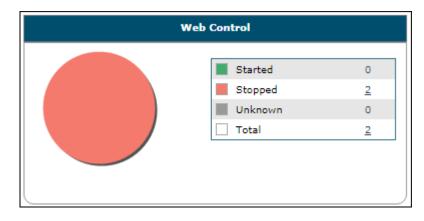
Anti-Virus



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.

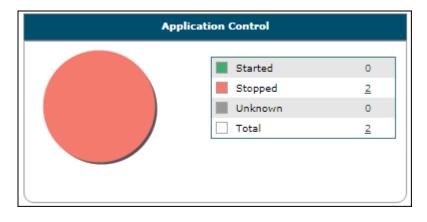
Stopped – It displays the number of devices on which the Web Control module is stopped.

Unknown – It displays the number of devices on which the Web Control module status is unknown.





Application Control



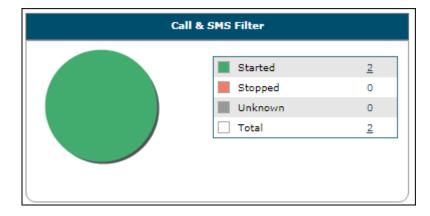
Started – It displays the number of devices on which the Application Control module is started.

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

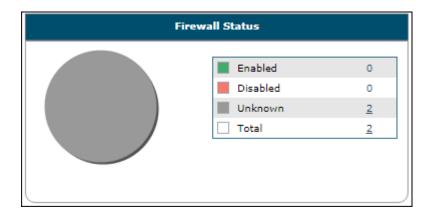


Started – It displays the number of devices on which the Call and SMS filter is started.
Stopped – It displays the number of devices on which the Call and SMS filter is stopped.
Unknown – It displays the number of devices on which the Call and SMS filter status is unknown.





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.

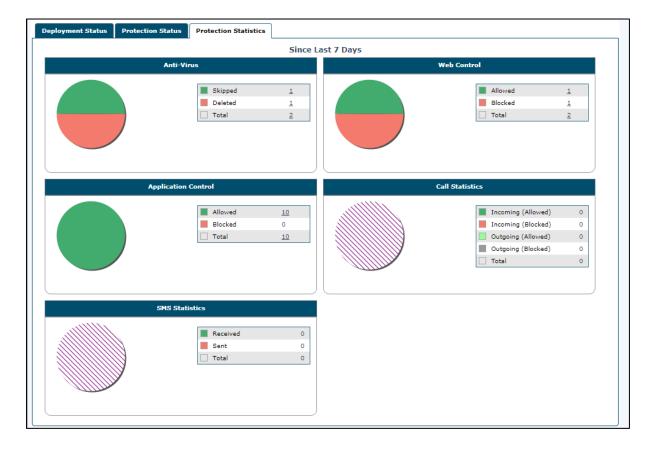




Protection Statistics

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





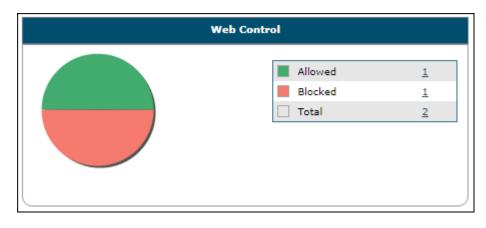


Anti-Virus

Skipped <u>1</u> Deleted <u>1</u> Total <u>2</u>	Anti-Virus		
		Deleted	_

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



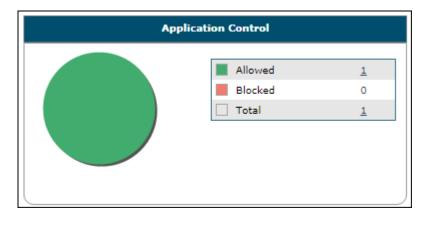
Allowed – It displays the number of websites allowed on a device.

Blocked – It displays the number of websites blocked on a device.



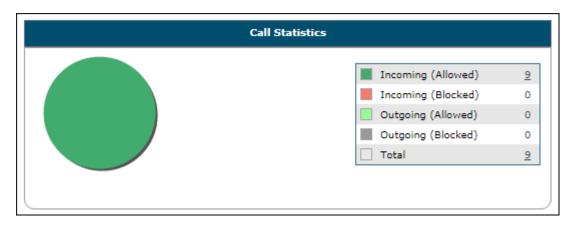


Application Control



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

SMS Statistics				
	Received	0		
	Sent	0		
	Total	0		

Received – It displays the number of messages received on a device.

Sent - It displays the number of messages sent from a device.





Settings

The Settings let you configure the modules to be displayed see in all tabs.

1. Click settings icon 🚨.

Configure Dashboard Display window appears.

onfigure Dashboard Dis	play	
Deployment Status		
eScan Status	l l	🖌 eScan Version (Android - MDM App)
eScan Version (And App)	droid - Container	🖌 eScan Version (iOS - MDM App)
Android Version		iOS Version
Device Sync Status	s (Successful)	Device Compliance
Kiosk Status		
Protection Status		
Update Status	C.	Scan Status
🗹 Anti-Virus	C.	Veb Control
Application Control		Call & SMS Filter
Firewall Status		
Protection Statistics		
🗹 Anti-Virus		Veb Control
Application Control		Call Statistics
SMS Statistics		

2. Select the module(s) to be displayed 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

Managed Mobile Devices		P († ?	
Action List Client Action List	Select/Add Columns 🔲 Policy Templates		
🗄 🔚 Managed Devices	Group Information		
🛄 Policy	LDAP/Active Directory Sync	Not Configured	
Group Tasks	Total Subgroups	0	
Client Devices	Total Devices	0	
	Group Type	MDM	
	Name		
	Assigned Policy Template: Managed Devices_Policy D View Policy Template		
	Group Tasks		
	Client Devices		

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		
New Group	devices.		
Add New Device	This option lets you add new devices to the selected groups.		





Add Multiple Devices	This option lets you import (*.txt, *.csv) 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
Remove Group	format. This option lets you remove a group from the Managed Devices.
Kemove droup	
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	This option lets you synchronize the managed devices with the
with	source active Directory Organization unit, the minimum sync
LDAP/Active	interval is five minutes and you can also exclude ADS source
Directory	paths 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). In this group type, the User installed apps in the Personal profile will always be blocked as company is the device owner. 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,





user installed apps in the Personal profile will be restricted within the set Geo/Wi-Fi location. This restrictions will be removed once the device out of the Geo/Wi-Fi location.

For differentiation between applications required to be installed, enrollment procedures and policies for the respective group type, <u>click here</u>.

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.

Create New Group			×
New Group Name :*			
Group Type:	 мом 	Осор	O BYOD
Select Template			
Default_Policy MDM	~		
* Mandatory Field			
		_	
		Sav	e 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.

Add New Device [Group Name: test_MDM] [Group	p Type: MDM]
Mobile Number*	
	Add Add More Close

- 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.

The mobile number required here is only for indicative purposes and it needNOTE 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.

Add Multiple Devices	×
Select File source	
Select file for import (*.txt,*.csv):	
Choose File No file chosen Upload	
Eg: 9821000000,×y×,×yz@domainname.com 9821000001,abc,abc@domainname.com	
Note:Device(s) added through this option will be seen as Android devices (when in not enrolled state) and will change to iOS, if an iOS device is enrolled against the number.	
Ok Can	cel
UK	Cer

3. Click **Browse** and select the **.txt** and **.csv** file consisting required details.

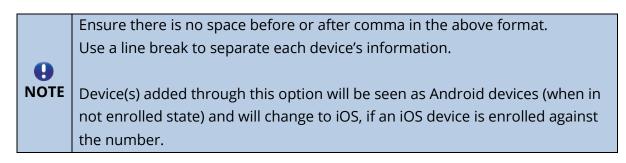




4. Click **OK**. Add Multiple Devices window appears.

Add Multiple Devices	×
Select File source	
Select file for import (*.txt,*.csv): Choose File No file chosen upload	
✓ File "MDM.txt" uploaded successfully	
Ok Canc	el

5. All devices from the **.txt** and **.csv** file will be added to the group. After the successful addition, the following window will be displayed.



Add Multiple De	evices	×	
04 Aug 2021 04:	04 Aug 2021 04:24 PM: Adding new device 78 8 04 Aug 2021 04:24 PM: New Device 78 8 added successfully		
Total devices Device added Not added	: 1 : 1		
		Close	





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.

hange Server IP Address on device	(s)	X
IP Address: 192.1	Change To	
Apply To	O List of Devices	
Select Group(s)		
	Apply Cancel	





- 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**.

Change Server IP Address on device(s)
IP Address: 192. Change To 192
Apply To-
Select Group(s)
Apply Cancel

6. The group's or device's IP address will be changed.





Synchronizing with Active Directory

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

 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 :	
Managed Devices' Browse	
Source LDAP/Active Directory Organisation Unit :	
Browse	
Synchronization interval :	
60 Minutes (Minimum 5 Minutes)	
Exclude From LDAP/Active Directory Sync	
Exclude Flom EDAP/Active Directory Sync	
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**.

Synchronize with LDAP/Active Directory	×	3
Synchronize with LDAP/Active Directory		
Select Source LDAP/Active Directory	× _	
Select Source LDAP/Active Directory	?	
	Configure	
Active Directory		
DC====,DC=local(192.	1	
🚽 🛃 Climbullin		
- 💑 CheCangulare		
- Ouedonain Controllera	1	
ChefaneignZecuritj/Hindgele	1	
🕂 🔬 Chie Depair Teel		
🔿 🛃 Chiedhiadhuature		
🕂 👷 ChinizadibridTaund		
🖓 Chemeragel Service Accounte		
🗛 Outettionauft Exchange Security Druge		
Chelfersent Eicharge System Chjeda		
Cueffan Citati		
Chentric Quates		
🛃 🖓 Chiefhogram Cala		
China Sustam		
Ok Cancel		





4. Set the Synchronization Interval as per your requirement.

hronize with LDAP/Active Directory	
nchronize with LDAP/Active Directory	
Target Groups :	
Managed Devices\Test_AD	Browse
- Source LDAP/Active Directory Organisation Unit :	
DC=,DC=local(192.)	Browse
-Synchronization interval :	
60 Minutes (Minimum 5 Minutes)	
Exclude From LDAP/Active Directory Sync	
Excluded LDAP/Active Directory Sources	
OU=(Segal Task, SC+asha, SC+local	Exclude
	Delete

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.

Select OU to Exclude	×
🗄 🦣 Active Directory	
DC=,DC=local(192,	
··· Chesalin	
··· CheCampulara	
··· Duedenain Centraliere	
Chi=EuraignEasurityEtincipals	
🗸 OV=Depairment	
··· Diebifastructure	
··· Chi=Lastitudfound	
Oli=Managed Service Accounts	
OuterMonault Exchange Security Drouge	
Otremoreauft Exchange System Objecte	
··· Distriction Character	
··· Distrigram data	
··· Che Bustem	
	Ok Cancel

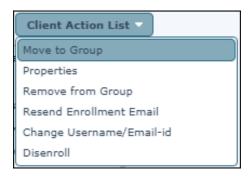
2. Select the group you want to exclude and then click **OK**.





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:

 Select the group in which the device(s) is already added and then click Client Devices.







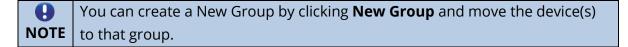
 Select the device you want to move to another group and then click Client Action List > Move to Group.

Client Action List
Move to Group
Properties
Remove from Group Resend Enrollment Email
Change Username/Email-id
Disenroll

3. Select Group window appears.

Select Group	×
🖃 💼 Managed Devices	
💼 t=== M	
	New Group Ok Cancel

4. Select the group to which you wish to move the device(s) and then click **OK**.







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.

General	
Mobile Number	75 Dube 0 5
User's name	Device_Harmen
Column1	-
Column2	-
Column3	-
Column4	-
Mac Number	C4: the child and a share
Email Id	neme ;; com
Enrollment Date	30 Jul 2021 12:29 PM
AV Setting	
eScan Install	Installed
eScan Version	7.2.0.70
Last Connection	30 Jul 2021 04:32 PM
Last Update	-
Last Scanned	-
Protection	
Anti-Virus	Enabled
Web Control	Disabled
Application Control	Disabled
Call & SMS Filter	Enabled
Miscellaneous	
Battery Status	14%
WiFi Strength	99%
SIM Signal Strength	No Network



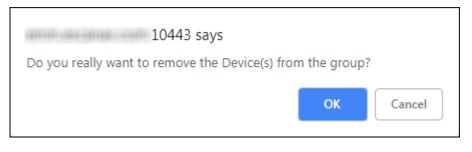


Removing a device from group

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.

If a device is removed, all details related to that device are also deleted fromNOTE 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.
- 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 User's name/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.

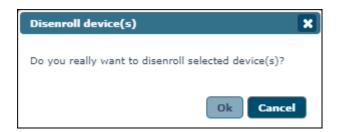
Change Details X
Mobile Number
75 5
User's name* Device_
Email Id*
ne e com
OS Type Android iOS
* Mandatory Field
Save Details Cancel

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.
- Click Client Action List > Disenroll.
 A confirmation prompt appears.



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.

elect/Add Customized Columns	
Select All	
Mobile Number	Anti-Virus
🗹 User's name	✓ Web Control
	Network Block Status
	Application Control
	Call & SMS Filter
	Last Connection
🗹 QR Code	Last Update
Device Added Date	Last Scanned
Enrollment Status	✓ Update Server
Enrollment Date	Client OS
Mac Number	Policy Applied Date
Email Id	GPS Status
✓ Kiosk Status	eScan Status
Battery Status	eScan Version
✔ WiFi Strength	Container Version
✓ 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 Templates

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.

naged Mobile Devices		ب
Action List 🔻 🛛 Client A	ction List 🔻 🛛 Select/Add Columns	Policy Templates
Managed Devices	Group Policy	
Sa maria	Assigned Template	Date And Time of Assigned Template
	Managed Devices_Policy	19 Jul 2021 03:12 PM

Clicking **Select Template** displays a list of available templates.

Select Policy T	emplate		×
Group Name:	Managed Devices		
Group Type:	MDM		
Default_Policy	BYOD		-
Default_Policy	COD		
Default_Policy	MDM		
Managed Devi	ces_Policy		
			-
		Select	Cancel

Clicking Policy Templates displays Policy Template screen and lets you create, copy, and assign template to specific group or devices.

New Template Propertie	s 🗑 Delete 🛛 A	ssign to Group(s) Ass	ign to Device(s) Copy T	emplate	
Name of Template	Applicable for Group type	Created On	Modified On	Assigned to Group(s)	Assigned to Device(s)
) Default_Policy BYOD	BYOD	19 Jul 2021 03:12 PM	19 Jul 2021 03:12 PM	-	-
) Default_Policy COD	COD	19 Jul 2021 03:12 PM	19 Jul 2021 03:12 PM	-	-
) Default_Policy MDM	MDM	19 Jul 2021 03:12 PM	19 Jul 2021 03:12 PM	Managed Devices	-
			1	1	





Creating New Template

To create a new template, follow the steps given below:

1. Click **New Template**.

Create Policy Template window appears.

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	
WiFi Settings Policy	
> Scheduled Backup (Contacts & SMS)	
Content Library Policy	
> Kiosk Mode Policy	
Location Fence	
	-
Save Cancel	

- 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
WiFi 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.

Scan Settings	
Protection	Enabled V
Scanning for files on installation is enabled	
Scan Type	(All Files 🗸
Automatic Scan	
Startup Scan	Disabled 🗸
Schedule Scan	Disabled 🗸
Scan Day	Sunday 🗸
Select Scan Time	21:14
Schedule Update Settings	
Schedule Update	Daily 🗸
Jpdate Day	Sunday 🗸 🗸
Jpdate Time	13:00
Update from Internet server	

Options	Description
	Using the options present under the Anti-Virus Policy, the
Scop Sottings	administrator can define settings for enabling or disabling virus
Scan Settings	protection on devices along with settings for file types to be
	scanned on managed devices.
Protection	
Scanning for files	Select Enabled or Disabled to enable or disable protection on
on installation is	managed devices in the group.
enabled	
Automatic Scan	Use options present under the Anti-Virus Policy to scan devices
Automatic Stan	on startup or schedule the scan as per requirement.
Startup Scan	Select from drop-down to enable or disable scanning on device
Startup Star	startup, as per your requirement.
	Select a schedule to scan managed devices. You can conduct a
Schedule Scan	weekly or daily scan as required or even disable the scan
	schedules.
	Select a particular day of the week to scan the managed devices
Scan Day	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	
Schedule Opdate	or weekly basis or disable the update schedule.	
	Select a particular day of the week to update the managed	
Update Day	devices present in the group. This check box will be activated	
	only if you select weekly update.	
	Set time for the devices to take virus signature database update	
Update Time	from the server. It will be helpful in saving network congestion	
	where large numbers of devices are added in the MDM Server.	
Update from	Select this check box to update the virus signature database	
Internet server	from the Internet server.	
Update only if	Select this check box to update virus signature database only if	
Wi-Fi is available	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 & SMS Filter Policy		
- Call & SMS Filter (Incoming)		
Call & SMS Filter Mode (Both List V)		
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		
Call Filter (Outgoing)		
Call Filter Mode Off 🗸		
Whitelist		

Call and SMS filter Mode set to Off

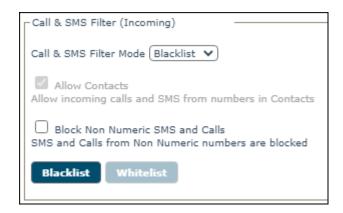
Call & SMS Filter (Incoming)
Call & SMS Filter Mode Off
Allow Contacts Allow incoming calls and SMS from numbers in Contacts
Block Non Numeric SMS and Calls SMS and Calls from Non Numeric numbers are blocked
Blacklist Whitelist

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 nonnumeric numbers.

To block incoming calls from known numbers and SMS consisting specific keywords, click **Blacklist**.

Call and SMS Blacklist window appears.

Call & SMS Blacklist	×
Add Delete Remove All	
Blocked Phone Number Filter Forbidden Text	-
	-
	Close





Click **Add**.

Block Incoming window appears.

lock Incoming			2
	O Calls	Calls & SMS	
Blocked Phone N	umber		_
Forbidden Text			_

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**.

All		
Filter	Forbidden Text	-
Calls & SMS	-	
Calls	-	
SMS	dear	
		_
		· ·
	Filter Calls & SMS Calls	Filter Forbidden Text Calls & SMS - Calls -





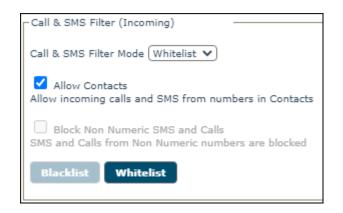
To delete a specific number from the Blacklist, select the number and click **Delete**.

Call & SMS Blacklist			
Add Delete Remove	All		
📕 Blocked Phone Number	Filter	Forbidden Text	^
980. 104 100 100	Calls & SMS	-	
86 86 86 86 8	Calls	-	
74 14 14	SMS	dear-	
			-
			Close

The selected number will be deleted.

To remove all the added numbers in a single-click, click **Remove All**.

Call and SMS filter mode set to Whitelist



Check Allow Contacts check box and then click Whitelist.





Call and SMS Whitelist window appears.

6	all & SMS Whitelist			×
	Add Delete Remove All			
	Allowed Phone Number	Filter	Allowed Text	^
				-
				Close

Click Add.

Allow Incoming window appears.

Allow Incoming		1	×
● SMS	Calls	Calls & SMS	
Allowed Phone N	lumber		
Allowed Text			
L			
Note: Wildcard %	6 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**.

All		
Filter	Allowed Text	-
SMS	hell+	
Calls	-	
Calls & SMS	-	
		-
		Clos
	Filter SMS Calls	Filter Allowed Text SMS heim Calls -

To delete a specific number from whitelist, select the number and click **Delete**.

97***		
	SMS	hel-
78	Calls	-
87es 11. bes	Calls & SMS	-

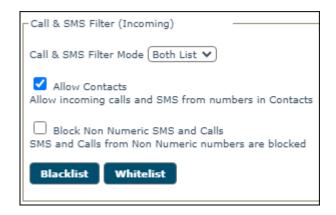
The number will be deleted.

To remove all numbers in a single-click, click **Remove All**.





Call and SMS filter mode set to Both List



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.

Outgoing calls	×
Add Delete Remove All	
Allowed Phone Number	-
	-
_	
l l l l l l l l l l l l l l l l l l l	lose

Click Add.

Allow outgoing window appears.

Enter the phone number and then click **Add**.





The number will be added to the Whitelist.

6)utgoing c	calls	×
	Add	Delete Remove All	
		Allowed Phone Number	*
		98	
			*
			lose

To delete a specific number, select a number and then click **Delete**.

Ou	itgoing c	alls		×
	Add	Delete Remove	All	
	Z	Allowed Phone Num	e r	
		98		F
			Cid	se

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.

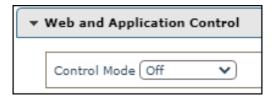
ntrol Mode (Both 🗸				 	
Allow / Block Application List					
Allow / Block Website categories					
- Filter Categories					
Category Name	Allow	Block	A		
Select All					
Advertisements and Popups	۲	0			
Alcohol and Tobacco	0	0			
Anonymizers	0	۲			
Arts	۲	0			
Botnets	0	0	.		

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.







Control mode set to Website

Setting the Control Mode to Website lets you allow and block website categories.

Control Mode (Website 💙) - Allow / Block Website categories				
Filter Categories				
Category Name	Allow	Block	*	
Select All				
Advertisements and Popups	۲	0		
Alcohol and Tobacco	0	۲	1	
Anonymizers	0	۲	1	
Arts	۲	0		
Botnets	0	۲	_	

Allow List: Websites added to this list can be accessed in browser. You can modify, delete and also remove the list of websites.

Allow List	×
Websites added to the Allow List will be Allowed regardless of the settings done under "Allow / Block Website categories"	
Add Modify Delete Remove All	
	*
	-
Clos	æ





Click Add.

Add in allow list window appears.

Add in allow list X
Add the URL of a specific website to allow from filtering or being blocked by eScan Note: The allow list website will not be filtered in future
Example: www.companyname.com
Save Cancel

Enter the URL in the field and then click **Save**.

To edit the existing allowed website, select the particular website and click **Modify**.

To delete a particular website, select the website and click **Delete**.

To remove all the website from the list in a single-click, click **Remove All**.

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.

Block List	×
Websites added to the Block List will be blocked regardless of the settings done under "Allow / Block Website categories"	
Add Modify Delete Remove All	
	•
	-
Clos	æ





Click Add.

Add in block list window appears.

Add in block list	×
Add the URL of a specific website to be blocked	
Example: www.companyname.com	
Save	Cancel

Enter the URL and then click **Save**.

To edit the existing blocked website, select the particular website and click **Modify**.

To delete a particular website, select the website and click **Delete**.

To remove all the website from the list in a single-click, click **Remove All**.

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.

	n List			
ote :				
 System apps will be 3. User Installed apps v If action is set to "As App is uninstalled. 	alow list will be Allowed/Blocked as per action sp Allowed by default unless explicitly added to "Bk vill be Blocked by default unless explicitly added k Uninstall" the device will prompt the User to u ion is set for System App, the app will be Blocke	ock" action. to "Allow" action. ninstall the App and		
Select Applications		~	+ Add	Select All
Delete				Count: 0
	Application Name		Allow Bl	ock Ask Uninstall
	Select All			
i te: If Application is NO	T in the "Available Applications" list, you can ad	d the package name	with the "Enter Pa	ckage Name" optior
ote: If Application is NO Enter Package Name:	T in the "Available Applications" list, you can ad	d the package name	with the "Enter Pa	ckage Name" option

Select the applications from the drop-down menu and click **Add**. To delete a particular application, select the application and click **Delete**.

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.

If Application is NOT in the "Available Applications" list you can add theNOTE package name with the "Enter Package Name" option.





Enter the application's package name in the field and click **Add.** After adding the package name that is not available in Available Application List, select the action **Allow**, **Block**, or **Ask Uninstall** option.

Control mode set to Both

Setting the Control Mode to Both lets you allow/block website categories and applications.

eb and Application Control			
Control Mode (Both 🗸			
Allow / Block Application List			
- Allow / Block Website categories			
Filter Categories			
Category Name Select All	Allow	Block	Â
Advertisements and Popups		0	
Alcohol and Tobacco	0	۲	
Anonymizers	0	۲	
Arts	۲	0	
Botnets	0	۲	-
			-
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 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.

To delete a package from the list, select the specific package and then click **Delete**.

🗑 Delete 🛛 Remove All				
C	Package Name	*		
	com. and not drama			
) com. and not final tea			
	com. and not again a			
		1		

To remove all packages, click **Remove All**.





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.

Enable Anti-Theft Location History Enable Location History Capture location History Capture location details - Time based Configure Note : Location cordinates 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: Send Email notification on SIM card change To Hoble No.: Send Email Id: Custom Email Id: Custom Email Id: Custom Email Id:	١nt	ti-Theft Policy			
□ Enable Location History Interval 20 Mins ♥ □ Capture location details - Time based Configures Note : Location cordinates 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. Interval 20 Mins ♥ Unisatell Protection Slock Device Ak "Admin Access Password" (Do not block device) Anti-Theft WIPE Settings Image: Constant account Image: Constant account □ Delete all configured email accounts Image: Constant account Image: Constant account Sinter Add domain name in comma seperated format Sey, yourcompany.com, gmail.com, yahoo.com Sin watch settings Send SMS notification on SIM card change Image: Constant account Image: Constant account Image: Constant account Image: Constant account Image: Constant account Sim watch settings Send SMS notification on SIM card change Image: Constant account Image: Constant account Image: Constant account Image: Constant account Image: Constant account Image: Constant account Image: Constant account Image: Constant account Image: Constant account Image: Constant account Image: Constant account<	Enable Anti-Theft				
Capture location details - Time based Configures Note : Location cordinates 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 Image: Streen Overlay" permission is required for displaying the GPS alert screen on the device. Uninstall Protection Image: Streen Overlay" permission is required for displaying the GPS alert screen on the device. Uninstall Protection Image: Streen Overlay" permission is required for displaying the GPS alert screen on the device. Uninstall Protection Image: Streen Overlay" permission is required for displaying the GPS alert screen on the device. Uninstall Protection Image: Streen Overlay" permission is required for displaying the GPS alert screen on the device. Uninstall Protection Image: Streen Overlay Ask "Admin Access Password" (Do not block device) Anti-Theft WIPE Settings Image: Delete all configured email accounts Delete all configured email accounts Delete all configured email accounts Image: Delete Add domain name in comma separated format ego. yourcompany.com, gmail.com, yahoo.com Sim watch settings Send SMS notification on SIM card change Image: Send Email notification on SIM card change Image: Administrator Email Id: Image: Administrator Email Id: Image: Administr	Г	Location History			
Note : Location cordinates 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 Image: Streen Overlay" permission is required for displaying the GPS alert screen on the device. Uninstall Protection Image: Streen Overlay" permission is required for displaying the GPS alert screen on the device. Uninstall Protection Image: Streen Overlay" permission is required for displaying the GPS alert screen on the device. Uninstall Protection Image: Streen Overlay" permission is required for displaying the GPS alert screen on the device. Uninstall Protection Image: Streen Overlay" permission is required for displaying the GPS alert screen on the device. Anti-Theft WIPE Settings Image: Delete all configured email accounts Delete specific domain names: Image: Delete Add domain name in comma separated format egi. yourcompany.com, gmail.com, yahoo.com Sim watch settings Image: Send Email notification on SIM card change Image: Administrator Email Id: Image: Administrator Email Id:		Enable Location History Interval 30 Mins 🗸			
Show GPS alert block screen Note : "Screen Overlay" permission is required for displaying the GPS alert screen on the device. Uninstall Protection Shock 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: eg. yourcompany.com, gmail.com, yahoo.com Sim watch settings Send SMS notification on SIM card change To Mobile No.: Administrator Email Id:		Capture location details - Time based Configure			
Note : "Screen Overlay" permission is required for displaying the GPS alert screen on the device. Uninstall Protection Image: State Sta		Note : Location cordinates will be captured by the device(s) only during the selected time slots.			
Uninstall Protection Uninstall Protection Uninstall Protection Uninstall Protection Uninstall Protection Uninstall Access Password" (Do not block device) Acti-Theft WIPE Settings 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:		Show GPS alert block screen			
 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: Enter 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.: Mobile No.: Administrator Email Id: Administrator Email Id: 		Note : "Screen Overlay" permission is required for displaying the GPS alert screen on the device.			
Ask "Admin Access Password" (Do not block device) Anti-Theft WIPE Settings Image: Delete all configured email accounts Delete specific domain account Enter domain names: Image: Delete Add domain name in comma seperated format eg. yourcompany.com, gmail.com, yahoo.com Sim watch settings Send SMS notification on SIM card change Image: To Mobile No.: Image: Administrator Email Id:	Г	Uninstall Protection			
Anti-Theft WIPE Settings Polete all configured email accounts Delete specific domain account Enter 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:		V Block Device			
 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: 		Ask "Admin Access Password" (Do not block device)			
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 Mobile No.: Administrator Email Id:	Γ'	Anti-Theft WIPE Settings			
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:		✓ Delete all configured email accounts			
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:		Delete specific domain account			
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:		Enter domain names:			
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:					
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:					
Sim watch settings Send SMS notification on SIM card change To Mobile No.: Send Email notification on SIM card change Administrator Email Id:					
Send SMS notification on SIM card change To Mobile No.: Send Email notification on SIM card change Administrator Email Id:	L				
To Mobile No.: Send Email notification on SIM card change Administrator Email Id:					
Send Email notification on SIM card change Administrator Email Id:					
Administrator Email Id:		To Mobile No.:			
Administrator Email Id:					
Administrator Email Id:					
Custom Email Id:		Administrator Email Id:			
Custom Email Id:					
		Custom Email Id:			

Options	Description
Enable Anti-Theft	By default, this check box is selected.
Enable Location	Select this check box to track the location history.
	NOTE : Location coordinates will be captured by the device
History	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.
	Select this checkbox to show the GPS alert and lock the
Show GPS alert block	screen.
screen	NOTE : Screen Overlay permission should be enabled on the
	device in order to work.
Block Device	Select this option if you want the device to be blocked if a
DIUCK DEVICE	user tries to uninstall the MDM application.





Ask "Admin Access	Select this option if you don't want the device to be blocked
	if a user tries to uninstall the MDM application. The
Password" (Do not	application will ask the user to enter the Admin Access
block device)	Password.
Delete all configured	Select this check box to delete all email accounts configured
email accounts	on the managed device.
Doloto sposific	Select this check box to delete email accounts of specific
Delete specific domain account	domain. After selecting this check box, enter the domain
domain account	name in Enter domain names field.
	Select this check box to receive a text message informing
Send SMS notification	about SIM card change. The text message will be sent to the
on SIM card change	number added by you.
	Add the desired number in To Mobile No. text box
Send Email	Select this check box to receive an email informing about
	SIM card change. The notification email will be sent to the
notification on SIM	administrator's email ID or the custom email ID that the
card change	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	

Use this option to enable or disable the above options on selected managed devices.

Options	Description
Show	Selecting this check box will display all notifications on devices.
Notification	Selecting this check box will display all notifications on devices.
Sound	Selecting this check box will play notification sound for eScan
300110	MDM application events.
Write Logs	Selecting this check box will enable MDM application to write
WITCE LOgs	extensive logs to the eScan log file.
Sync at Device	Selecting this check box will sync the device with the eScan server
Reboot	after it reboots.
Sync Frequency	You can set the Sync Frequency in minutes and let the device sync
Sync Frequency	with the eScan server.



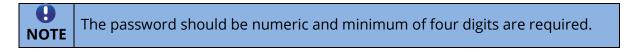


Password Policy

Password Policy lets you define Administrator Access Password that allows an authorized user to configure settings of eScan Module on respective Managed devices.

•	Password Policy	
	Admin Access Password]
	Show Password	
	Note: Password has to be numeric and minimum 4 digits are required.	
	······································	

Enter the password in Admin Access Password field.



Device Oriented Policy

Device Oriented Policy lets you enable GPS and disable Camera, Bluetooth, and USB Connectivity on a device.

▼ Device Oriented Policy

Device Oriented Policy		
Enable GPS (For devices with Android version below 4.0)		
Disable Device Settings**	Block Access to Android Settings	
**Web And Application Control Mode should be set to Both/Application		
Block Device Features		
Disable Camera (For device with Android version 4.0 and Above)		
Disable Bluetooth & Bluetooth Discovery		
Disable USB Connectivity (For devices with Android version below 4.0)		
Send Call Details to Server, including Call/SMS filter events		

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	Select this check box to disable the Bluetooth
Discovery	and Bluetooth discoveries.
Disable USB Connectivity (For	Select this check box to disable USB
devices with Android version	Connectivity.
below 4.0)	connectivity.
Send Call Details to server,	Select this check box if you want device(s) to
including Call/SMS filter events	send their Call/SMS details to the server.





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.

Required Applications Policy					
🛓 Import 🗑 Delete					
Application Name	Application Id	Арр Туре	Version	Added On	
					-
4					- F

Importing an application

1. Click Import.

Import Application window appears.

ilable applications				Total: 1
Application Name	Application Id	Арр Түре	Version	Added On
eScan Mobile Security	com.eScan.main	Play Store	-	04 Aug 2021 04:30 PM

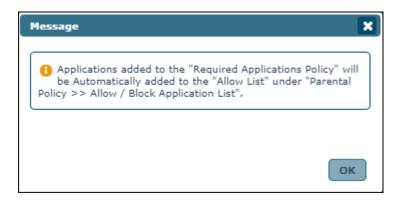
- 2. Select the application(s).
- 3. Click **Save**.

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".



 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**.

Application Name Application Id App Type Version Added On	
eScan Mobile Security com.eScan.main Play Store - 04 Aug 2021 04:30 PM	

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 check box 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.

ViFi Settings Policy		
Disable WLAN / WiFi		
WiFi Restrictions		
Enable WiFi Restrictions (For devices wi	th Android version below 6.0)	
Note: Device(s) will be allowed to connect	ONLY to listed WiFi network name (SSIDs)	
+ Add 🗑 Delete		
WiFi Network Name (SSIDs)		▲
		.
4		•
Lock Device / Sound Alarm		
Lock Device	Sound Alarm	
Note: Device(s) will lock / sound alarm wi	hen NOT connected to either of the listed WiFi network name (SSIDs)	
+ Add 🗊 Delete		
WiFi Network Name (SSIDs)		▲
		-
4		►





Adding a Wi-Fi SSID

 Select the check box Enable Wi-Fi Restrictions and then click Add. Add window appears.

ľ	Add X
	Enter WiFi network name (SSIDs):
	Note: WiFi network name (SSID) are case sensitive
	Add Cancel

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.

Add Networks	×
Available Networks	
WiFi Network Name (SSIDs)	*
🗌 automotio	
	-
4	Þ
Sav	e Close

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**.

+ Add 🗊 Delete	
✓ WiFi Network Name (SSIDs)	
automatic	

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 can be scheduled for daily/weekly basis.

•	Scheduled Backup (Contact	ts & SMS)		
	+ Add 🔳 Modify	jj Delete		
	🔲 Job Name	Schedule Type	Schedule Time	·
				-
	4			►

Creating a schedule

1. Click Add.

Add new job window appears.

Add new job	×
Job Name:	•
▼ Job Settings	
Select Backup	1
□ sms	1
Contacts	I
► Job Scheduler Settings	I
	1
Save	

- 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**.

dd new job	
Job Name:	_
▶ Job Settings	
	\equiv
▼ Job Scheduler Settings	
	,
O Daily	
O Weekly Mon Tue Wed Thu	
Fri Sat Sun	
Disable Schedule	
At 05:30	
	ancel
Save	ancer





Modifying a schedule

1. To modify a schedule, select the specific schedule and then click **Modify**.

	+ Add 🛛 📲 Modify 🗋 Delete				
~	Job Name	Schedule Type	Schedule Time	4	h.
 	d	Daily	05:30		
					۳.
				Þ.	

Modify backup job window appears.

Job Settings	
▼ Job Scheduler Settin	gs
Daily	
O Weekly	Mon Tue Wed Thu
O Disable Schedule	Fri Sat Sun
At 05:30	B
AL 05:50	

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**.

+ Add 📱 Modify	🗑 Delete		
🗹 Job Name	Schedule Type	Schedule Time	
den en e	Daily	05:30	
			*
4			

A confirmation prompt appears.

×
el

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, <u>click here</u>.

▼ Content Library Policy		
± Import 🗊 Delete		
File Name	Added On	· · · · · · · · · · · · · · · · · · ·
		-
4		

Import a file

To import a file from Content Library, click **Import**. Select the file and then click **Save**.

Import Files	×
Available Files	Total: 1
File Name	Added On
ED1_1++++_1++.doc	20 Jul 2021 12:58 PM
	Save Cancel

To delete a file, select the specific file and then click **Delete**.

🛨 Import 🗊 Delete		
🔽 File Name	Added On	
ED#doc	20 Jul 2021 12:58 PM	

The selected file will be deleted.





Kiosk Mode Policy

▼ Kiosk Mode Policy		
Enable Kiosk Mode		
Application(s) to be added to Kiosk		
Use Single App Mode		
	▼ + Add	
		Count: 0
Application Name		· · · · · · · · · · · · · · · · · · ·
		Ψ.
4		► I
Force user to install all apps as required by Kiosk policy (Unchecking will allow user to enter Kiosk mode even if any of the app is not installed)		

To configure Kiosk Mode Policy, select **Enable Kiosk Mode** check box.

Application(s) to be added to Kiosk

This section allows an application to be accessed in Kiosk mode.

Use Single App Mode

Select this check box to use kiosk in single app 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

If this option is checked, the user will not be allowed to enter the Kiosk mode unless all the listed apps are installed on the device.



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.

	+ Add	
	mes added to the list will be allowed if launched from within any other apps added to kiosk mode. will not be visible in Kiosk mode.	
Delete		
Package I	lame	
4		

Add

Enter the name of the 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.

All non-launchable system apps will be allowed if launched from within anyNOTE other app added to Kiosk mode.

rHardware Key Control			
Disable Power button			
Disable Volume buttons			
Allow User to Turn ON/OFF			
ViFi	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.

Unchecking options won't display Control to the user on the Kioskapplication.

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.





Install eScan Kiosk Lockdown Application

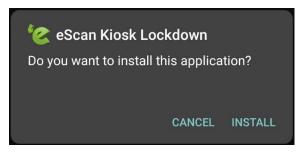
To run the eScan Kiosk Lockdown application in your device, it is necessary that you have installed eScan Device Management application and your device is enrolled in eScan Mobility Management console. Also, ensure that the Kiosk Mode Policy is deployed to the device via the console.



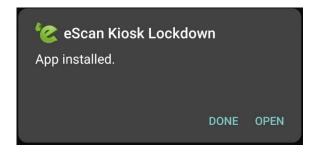
The below screenshots are taken from Android 10 on dark theme. The app permissions, screens and text may vary depending upon the android version, applied theme and device manufacturer.

After the app has been downloaded on device, follow the below given installation procedure –

Installation prompt appears.



1. Tap INSTALL.







 After the application gets installed, tap **OPEN**.
 After opening the app, Welcome screen appears with End User License Agreement (EULA).



3. Tap **OPEN AGREEMENT**. Read the EULA carefully and then tap **ACCEPT**.

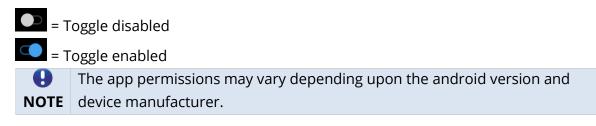




4. You will have to grant permissions to the app manually. Tap **Permit Drawing Over Other Apps.**

eScan Kiosk Lockdown	
Permit Drawing Over Other Apps	>
App Usage Access	>
Write Setting Permission	>
Allow to write DND setting	>
Device Admin Permission	>
Allow app installation permission	>
Please allow all above permissions for this applic	ation to
function properly and a better experience.	
PROCEED	

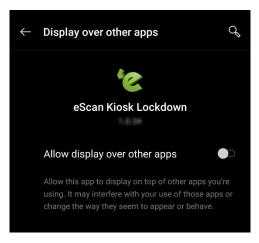
Tapping the displayed options will take you to the respective options in Settings, wherein you will have to tap the toggle button to grant all requested permissions.







5. Tap the **Allow display over other apps** toggle and then go back.



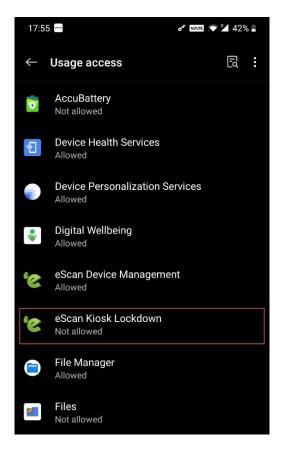
6. Tap App Usage Access.

eScan Kiosk Lockdown	
Permit Drawing Over Other Apps	~
App Usage Access	>
Write Setting Permission	>
Allow to write DND setting	>
Device Admin Permission	>
Allow app installation permission	>
eSean	
Please allow all above permissions for this ap function properly and a better experien	
PROCEED	

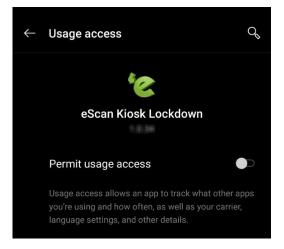




7. Tap eScan Kiosk Lockdown.



8. Tap **Permit usage access** toggle and then go back.





The option **Permission usage access** maybe **Allow usage tracking** in your device. This option may vary depending upon the device manufacturer/android version.

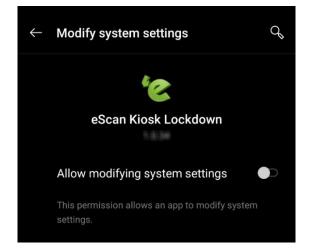




9. Tap Write Setting Permission.

eScan Kiosk Lockdown	
Permit Drawing Over Other Apps	~
App Usage Access	~
Write Setting Permission	>
Allow to write DND setting	>
Device Admin Permission	>
Allow app installation permission	>
eSean	
Please allow all above permissions for this ap function properly and a better experier	oplication to nce.
PROCEED	

Modify system settings screen appears.







10. Tap **Allow modifying system settings** toggle and then go back.

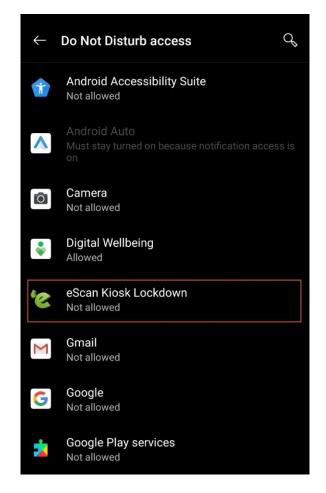
eScan Kiosk Lockdown	
Permit Drawing Over Other Apps	~
App Usage Access	~
Write Setting Permission	~
Allow to write DND setting	>
Device Admin Permission	>
Allow app installation permission	>
eSean	
Please allow all above permissions for this appl function properly and a better experience	
PROCEED	



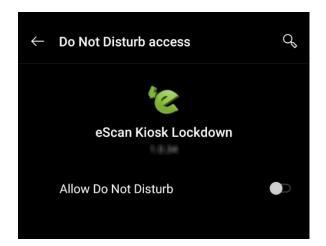


11. Tap Allow to write DND setting.

Do Not Disturb access screen appears.



12. Tap eScan Kiosk Lockdown.







13. Tap **Allow Do Not Disturb** toggle.

A prompt appears.

Allow access to Do Not Disturb for eScan Kiosk Lockdown? The app will be able to turn on/off Do Not Disturb and make changes to related settings.

14. Tap **ALLOW** and then go back.

eScan Kiosk Lockdown	
Permit Drawing Over Other Apps	~
App Usage Access	~
Write Setting Permission	~
Allow to write DND setting	~
Device Admin Permission	>
Allow app installation permission	>
eSeaň	
Please allow all above permissions for this app function properly and a better experien	
PROCEED	





15. Tap Device Admin Permission.

Activate device admin app screen appears.

Activate device admin app? eScan Kiosk Lockdown After activating admin, you will be able to block application uninstalling. Lockdown to perform the following operations: Erase all data Erase the phone's data without warning by performing a factory data reset. Change the screen lock Change the screen lock Monitor screen unlock attempts Monitor the number of incorrect passwords typed. when unlocking the screen, and lock the phone or erase all the phone's data if too many incorrect passwords are typed. Lock the screen Control how and when the screen locks. Set storage encryption Require that stored app data be encrypted. • Disable cameras Activate this device admin app

Cancel

Uninstall app





16. Tap **Activate this device admin app** option and then go back.

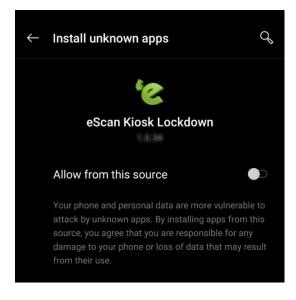
eScan Kiosk Lockdown	
Permit Drawing Over Other Apps	~
App Usage Access	~
Write Setting Permission	~
Allow to write DND setting	~
Device Admin Permission	~
Allow app installation permission	>
eSean	
Please allow all above permissions for this appl function properly and a better experience	
PROCEED	



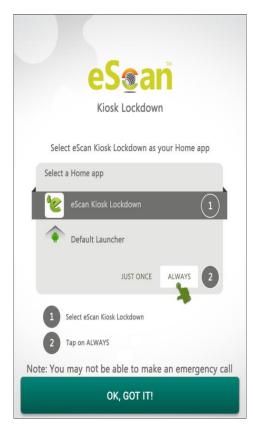


17. Tap **Allow app installation permission**.

Install unknown apps screen appears.



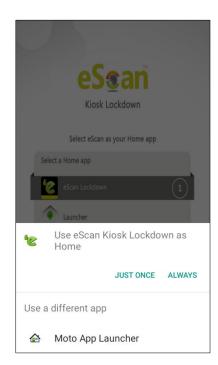
18. Tap **Allow from this source** toggle and then go back. After all permissions are granted, an instructional image appears.







- 19. Read the instructions in the image and then tap **OK, GOT IT!**
- 20. The application asks you to use eScan Kiosk Lockdown as Home App. Tap **ALWAYS.**



The device now runs in Kiosk mode and only the apps deployed via Kiosk Mode Policy are visible.



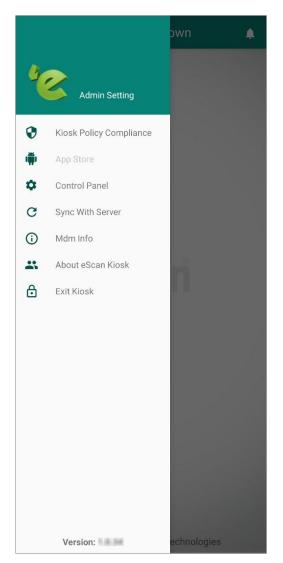




O NOTE The above image is for representational purposes only.

Tapping the bell icon A displays notifications related to Kiosk application. For example, application updates if any available. If an update for application is available, the user will be redirected to Google Play and install updates manually.

Tapping the menu icon \blacksquare displays general info and configuration menu.



The menu options are explained below:

Kiosk Policy Compliance

It displays

- Policy applied date, day and time
- Applications deployed via Kiosk Mode Policy and their package name





App Store

It displays the applications deployed via Kiosk Mode Policy but not yet installed on device. Tap the application to download and install it on your device.

Control Panel

It displays the Brightness, Volume, Bluetooth and Wi-Fi controls. Brightness control lets user set the display brightness to Low, Medium or High. Volume control lets the user set the device volume to Mute, Normal or Vibrate. Bluetooth and Wi-Fi control allows user to switch them ON and OFF.

Sync with Server

It lets user sync the device with server and comply device with the latest updated policy.

MDM Info

It displays the eScan MDM details such as Mobile Number, Server Name, Install and Expiry date, Last sync date and time details and MDM version number in use.

About eScan Kiosk

It displays general information about the Kiosk application, developer information and copyrights notice.

Exit Kiosk

This option allows device user to exit Kiosk mode by entering the Admin Password.





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, <u>click</u> <u>here</u>.

Latitude	Longitude	Radius(m)	
			*
	Latītude	Latitude Longitude	Latitude Longitude Radius(m)

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.

If Block device when outside of the set fence is unchecked then device willNOTE not be blocked but only events will be sent to the server.





iOS Template

Create Policy Template	×
Policy Template Name:	Â
Select Group Type:	l
Android Template iOS Template	
Device Passcode Policy	
Restrictions Policy	I
Web Clip Policy	I
> Email Policy	I
WiFi Settings Policy	
Content Library Policy	
Required Applications	
	÷
	Ť
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.

evice Passcode Policy		
Enable		
Allow Simple Value	Ves O No	
Require Alphanumeric Value	Ves No	
Minimum Passcode Length	Select	~
Minimum Number of Special characters	Select	~
Maximum Passcode Age (days 1-730, or blank)	0	
Allowed idle time, before Auto-Lock	Select 🗸	Mins
Number of Passcodes to be maintained in the history (1-50, or blank)	0	
Grace Period for Device Lock	Select	~
Maximum Number of Failed Attempts (Before all data is erased)	Select	~

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

Pevice Functionality	
Allow Installing Apps	● Yes ○ No
Allow Use of Camera	● Yes ○ No
Allow FaceTime	● Yes ○ No
Allow Screen Captur	● Yes ○ No
Allow Automatic Sync While Roaming	● Yes ○ No
Allow Siri	● Yes ○ No
Allow Siri while device locked	● Yes ○ No
Allow usage of Touch ID to unlock device (iOS 7 and above)	● Yes ○ No
Allow Passbook while device locked (iOS 6 and above)	● Yes ○ No
Show Control Center in lock screen (iOS 7 and above)	● Yes ○ No
Show Notification Center in lock screen (iOS 7 and above)	● Yes ○ No
Show Today view in lock screen (iOS 7 and above)	• Yes O No
Allow Voice Dialing	● Yes ○ No
Allow In App Purchase	● Yes ○ No
Force User to enter iTunes Store password	O Yes 🖲 No
Allow Multiplayer Gaming	● Yes ○ No
Allow Adding Game Center Friends	● Yes ○ 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 <u>here</u>.

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 <u>here</u>.

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

_ Application	
Allow Use of iTune Music Store	● Yes ○ No
Allow Use of Safari	● Yes ○ No
- Safari Settings	
Enable Autofill	● Yes ○ No
Force Fraud Warning	🔾 Yes 🖲 No
Enable JavaScript	● Yes ○ No
Allow Pop-ups	● Yes ○ No
Accept Cookies	Always

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

_ iCloud	
Allow Backup	● Yes ○ No
Allow Document Sync	● Yes ○ No
Allow Photo Stream	● Yes ○ No
Allow Shared Stream(iOS 6 and above)	● Yes ○ No

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

● Yes ○ No
● Yes ○ No
● Yes ○ No
O Yes 💿 No
O Yes 🔍 No
● Yes ○ No
● Yes ○ No

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

Allow Explicit Music Podcasts: Set this option to **Yes** to allow explicit music podcasts to be played on a device.

Ratings by Region



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.

▼ Web Clip Policy		
┌ □ Enable		
+ Add 🗊 Delete		
Webclip Policy Name	·	
	_	
4		

Select **Enable** check box to enable the configuration of Web Clip Policy.

Adding a WebClip

Check **Enable** and then click **Add**. WebClip Policy window appears.

Web Clip Policy	×
Web Clip Label *	
URL to be Linked *	
Removal of Web Clip	● Enable ○ Disable
Allow Full Screen	O Yes 🔍 No
	Save Cancel

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.

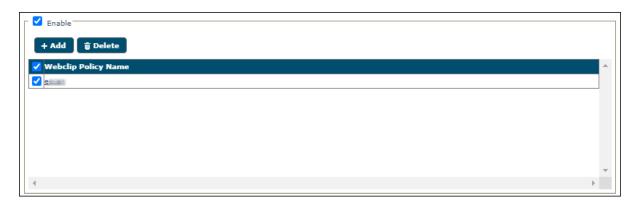
Allow Full Screen: Select Yes to allow full screen and No to disable full screen.

After entering all the details, click **Save**. The new web clip policy will be added.

+ Add 🗑 Delete	
Webclip Policy Name	

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.

▼ Email Policy		
Enable The Add Delete		
Email Policy Names		
4	• •	

Check **Enable** to configure the Email Policy.

Adding Email policy

To add email policy, follow below steps:

1. Check **Enable** and then click **Add**. Email Policy window appears.

[Email Policy		×
	Account Name *	[*
	Account Type	IMAP 🗸	
	Path Prefix		
	User Display Name		1
		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)	· Oves 🖲 No	_
		Save Cance	





Fill the following appropriate details:
 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.

- Enter the Incoming Mail and Outgoing Mail details.
 To learn more about Incoming Mail, <u>click here</u>.
 To learn more about Outgoing Mail, <u>click here</u>.
- 4. After filling the details, click **Save**.





Incoming Mail

- Incoming Mail	
Mail Server *	
Port *	143
Username	
	Note : "%username%" or "%email%" will fetch the appropriate Username/Email mapped to the device
Authentication Type	Password 🗸
Password	
Use SSL	⊖Yes ●No

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

Outgoing Mail		
Mail Server *		
Port *	25	
Username		
	Note : "%username%" or "%email%" will fetch the appropriate Username/Email mapped to the device	
Authentication Type	Password 🗸	
Password		
Use Outgoing Password Same as Incoming	⊖ _{Yes} ● No	
Use Only in Mail	⊖Yes	
Use SSL	⊖ Yes	

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.

Deleting an Email Policy

To delete an email policy follow below steps:

1. Select the particular Email Policy from the list.

+ Add 🗊 Delete	
🗹 Email Policy Names	

2. Click **Delete**.

The email policy will be deleted.





Wi-Fi Settings Policy

The Wi-Fi Settings Policy lets you manage how a user connects their devices to a Wi-Fi network.

▼ WiFi Settings Policy	
Enable + Add To Delete	
Wifi Policy Name	*
4	+

Check **Enable** to configure the WiFi Setting Policy.

Adding a WiFi Settings Policy

To add a WiFi Settings Policy, follow below steps:

1. Click **Enable** and then click **Add**.

Wi-Fi Settings Policy window appears.

WiFi Settings Policy	×
Wireless Network Identification * Automatically Join Network Hidden Network Security Type	● Yes ○ No ○ Yes ● No Any (Personal) ►
Password Configure Proxy Wireless Network Identification	None
	Save Cancel





2. Enter the following details:

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
- 3. After entering the appropriate details, click **Save**.

The WiFi Settings Policy will be saved.

Deleting a WiFi Settings Policy

To delete a WiFi Settings Policy, follow below steps:

1. Select the particular WiFi Settings Policy from the list.

E	+ Add 🗇 Delete
<	Wifi Policy Name
\checkmark	asilonalis

2. Click Delete.

The WiFi Settings Policy will be deleted.





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, <u>click here</u>.

▼ Content Library Policy		
┌ □ Enable		
± Import		
File Name	Updated On	▲
		-
4		• •

Select **Enable** check box to configure the Content Library Policy.

Importing a file

1. Check **Enable** and then click **Import**.

Import Files window appears.

L×
•

2. Select a file and then click **Save**.

Deleting a file

Select a file and then click **Delete**.

± Import 🗍 🗑 Delete	
🗸 File Name	Updated On
C ED dec doc	20 Jul 2021 12:58 PM

The selected file will be deleted.





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**.

▼ Required Applications		
┌ □ Enable		
± Import 🗊 Delete		
File Name	Updated On	·
		· ·
4		Þ

Import Application window appears.

Import Application					×
Available applications				Total: 1	
Application Name	Application Id	Арр Туре	Version	Added On	
eScan Mobile Security	com.eScan.main	Play Store	-	04 Aug 2021 04:30 PM	
				Save	Cancel

- 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**.

equired Applications		
± Import		
✓ File Name	Updated On	
eScan Mobile Security	04 Aug 2021 04:33 PM	
	· · · · · · · · · · · · · · · · · · ·	
4		
4		

The selected application will be deleted.





Group Tasks

The Group Tasks option lets you create and schedule tasks for the devices in a group.

anaged Mobile Devices			P ¢
Action List 🔻 Client Actio	n List 🔻 🛛 Select/Add (Columns 🕒 Policy Templates	
Managed Devices Managed Devices Managed Devices Managed Devices	Group Tasks	Start Task #Properties	
Client Devices	Task Name	Task Performed	Schedule Type

Creating a New Group Task

 Select a group and then click Group Tasks > New Task. The New Task window appears.

Scan Full Scan Memory Scan Update Task Scheduling Settings	▼ Task Settings		
	Full Scan		
Task Scheduling Settings	Update		
	▶ Task Scheduling Setting	js	

- 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.





4. In **Task Scheduling Settings**, schedule the created task by selecting the appropriate options.

▼ Task	Scheduling Settings
	Enable Scheduler O Manual Start
0	Daily Weekly Mon Tue Wed Thu Fri Sat Sun Monthly IV
At	8 🗘 30 🗘 AM 🗸

5. Click **Save**.

The task will be created instantly.

Selecting a task enables following options:

Group Tasks 🖷		?
🗅 New Task	► Start Task # Properties	🗍 Results 🛛 🝵 Delete Task
🗹 Task Name	Task Performed	Schedule Type
🗹 ta 🗰 📗	Task not performed yet	Automatic Scheduler

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 s	
Properties	task.
Results	Click Results to view detailed results of the selected task.
Delete	Click Delete Task to delete the selected task from the list of tasks.
Task	Click Delete Task to delete the selected task from the list of tasks.





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

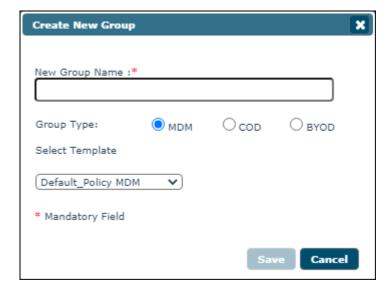
Adding a device to the console

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**.



- 3. Select the group.
- 4. Click Action List > Add New Device.





Add New Device window appears.

Add New Device [Group Name: Managed Devices] [(Group Type: MDM] X
Mobile Number*	
	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								P (\$?
Action List Client Action List Select/	'Add Columns 🛛 🗅 Poli	cy Templates					т	otal Devices: 1	L
Hanaged Devices					1 - 1 of 1	e page 1 of	1 → > Rows pe	r page: 10 🔹	•
🔃 Policy 	🔲 Mobile Number	User's name QR Co	de Device Added Date	Enrollment Status	Enrollment Date	IMEI/Android ID	Mac Number	Email Id	eS
Client Devices (1)	78 - 18	adams <u>View</u>	04 Aug 2021 04:24 PM	Not Enrolled	-	-	-	adams@g.com	No
test_MDM									

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.

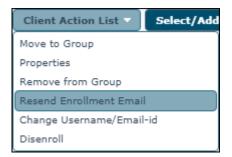




Enrolling the added device

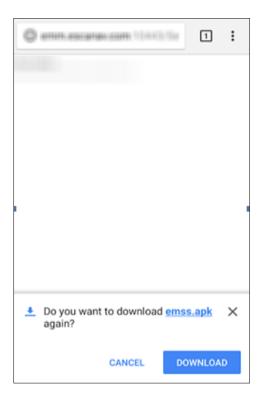
After a device is added to the console, an enrollment email is sent to the specified email ID. This email contains enrollment details and steps to download the MDM application. It also contains the QR code which directly fetches the enrollment details by scanning it from the device.

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:

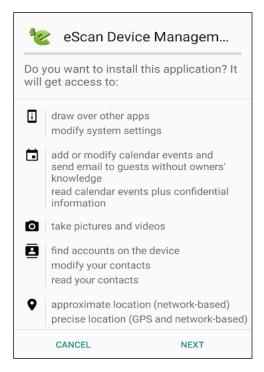
1. Tap the shared URL in the email. A prompt appears asking you to download the eScan MDM application. Tap **DOWNLOAD**.



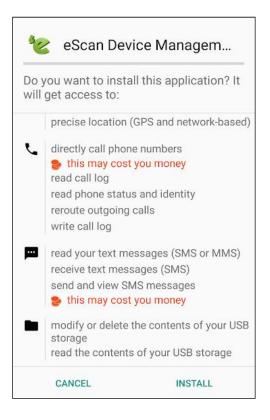




2. Tap the downloaded file and read thoroughly about the permissions asked by the application. To proceed, tap **NEXT**.



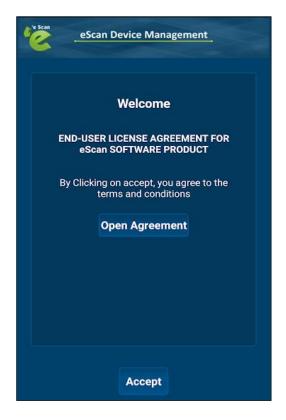
3. After reading the application's access permissions, tap INSTALL.







Welcome screen appears.



- 4. Tap **Open Agreement** and read the agreement completely.
- 5. After reading the agreement, tap **Accept**. Enrollment Details form appears.

e sca	eSc	an Device	Managemen			
			nt Details rough QR coo	ie		
	Mobile	Number	*			
	Server*					
	2221					
	Country	/				
	1	2	3	-		
	4	5	6	<u> </u>		
-	7	8	9	$\langle \times \rangle$		
	,	0		\rightarrow		





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 device is scanned, the enrollment process starts automatically.

e Scar	eScan Device Management	:
	Enrollment Details Fill entries through QR code	
	900000000	
	emm.escanav.com,192.168.0.6/	
	2221	
	Country	
	Version : 6.0.5.25 * Field is mandatory Default Port is 2221	
	Enroll Device	

7. Device Enrollment begins. Wait till the device gets enrolled.



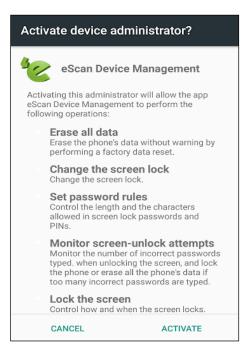




Device Administrator prompt appears.



It is recommended that you tap **Next**.
 Activate Device Administrator prompt appears.

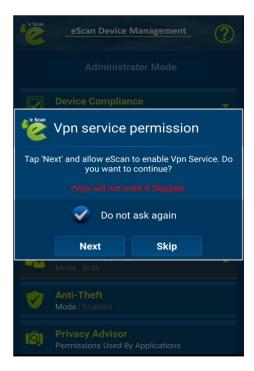


9. Read about the permissions completely and then tap ACTIVATE.





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

Create New Group	Create New Group
New Group Name :* Group Type: O MDM O COD O BYOD Select Template	New Group Name :* Group Type: O MDM O COD O BYOD Select Template
Default_Policy COD Mandatory Field Save Cancel	Default_Policy BYOD * Mandatory Field Save Cancel

- 3. Select a group.
- 4. Select the policy template from the dropdown menu.
- Click Action List > Add New Device.
 Add New Device screen appears.
- 6. 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 **the Mobile Number** column; this indicates that the device is not enrolled.

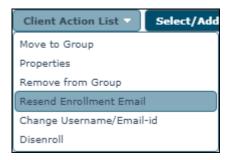
Enrolling the added device

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:

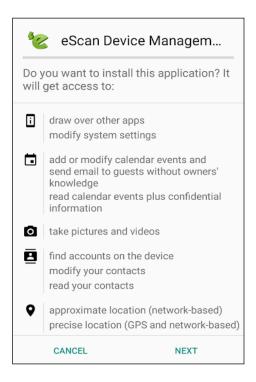
1. Tap the shared URL in the email. A prompt appears asking you to download the eScan MDM application. Tap **DOWNLOAD**.





🖉 emm.escanav.com 10443/5z	:
Do you want to download <u>emss.apk</u> again?	×
CANCEL	ND .

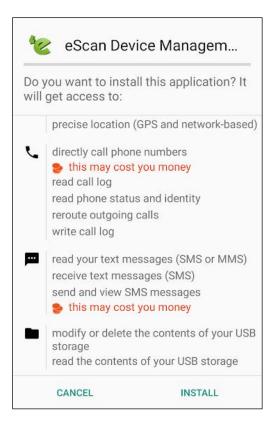
2. Tap the downloaded file and read thoroughly about the permissions asked by the application. Tap **NEXT** to proceed.



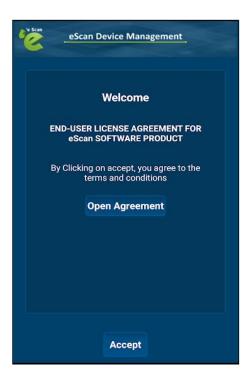
3. The application will get access to your call logs, text messages and USB storage. Tap **INSTALL**.







Welcome screen appears.



- 4. Tap **Open Agreement** and read the agreement completely.
- 5. After reading the agreement completely, tap **Accept**. Enrollment Details form appears.





eSca	n Device Mana	agement	
	rollment De tries through		
Mobile N	lumber *		
Server*			
2221			
Country			
Version : 7.2 * Field is man Default Por	ndatory		
	Enroll Devic	e	

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 and the enrolment process starts.





Beer Scar	eScan Device Management	-
	Enrollment Details Fill entries through QR code	
	90 (#1#1#1#1#1#1	
	emm.escanav.com,192.168.0.6/	
	2221	
	Country	
	Version : 7.2.0.49 * Field is mandatory Default Port is 2221	
	Enroll Device	

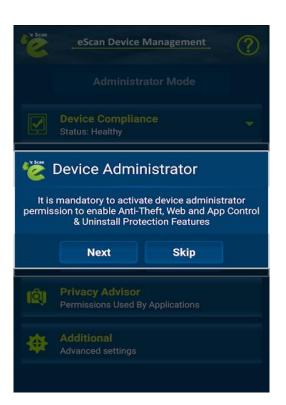
Device Enrollment begins. Wait till the device gets enrolled.



Device Administrator prompt appears.







It is recommended that you tap Next.
 Activate Device Administrator prompt appears.

Activate device administrator?
eScan Device Management
Activating this administrator will allow the app eScan Device Management to perform the following operations:
Erase all data Erase the phone's data without warning by performing a factory data reset.
Change the screen lock Change the screen lock.
Set password rules Control the length and the characters allowed in screen lock passwords and PINs.
Monitor screen-unlock attempts Monitor the number of incorrect passwords typed. when unlocking the screen, and lock the phone or erase all the phone's data if too many incorrect passwords are typed.
Lock the screen Control how and when the screen locks.
CANCEL ACTIVATE

8. Read about the permissions asked by the application completely and then tap **ACTIVATE**.

VPN Service Permission dialog box appears.





e Scan	eScan Device Management					
	Device Compliance 🗸					
Vpn service permission						
Tap 'Next' and allow eScan to enable Vpn Service. Do you want to continue?						
	*Vpri will not work if Skipped.					
	👽 Do not ask again					
	Next	Skip				
	Mode : Both					
8						
(Ê)						

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.

'e Scan	eScan Device Management ?						
	Device Complian Status: Healthy						
禭 AppLockActivity							
	By going further the Application Blocking will be disabled ,click on Next and Allow escan to read app usage. Do you want to continue?						
	Next	Skip					
20							

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.

() The Container application can be accessed only after the eScan MDM**NOTE** application is installed and enrolled on the managed device.

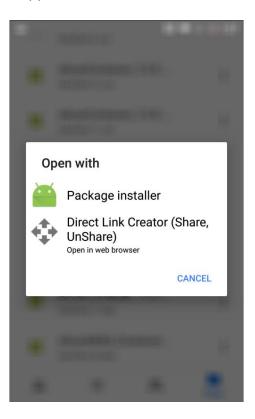




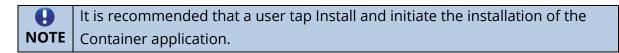
Installing eScan Container app

To install eScan Container app, follow the steps given below:

 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.

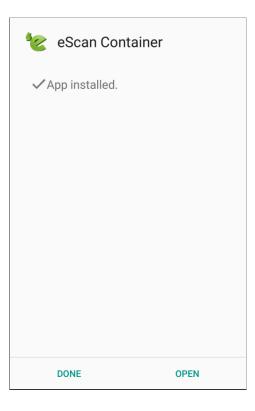






After tapping **INSTALL**, an installation prompt appears.

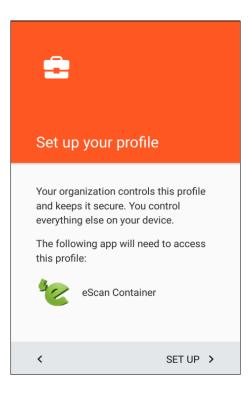
- 3. Tap **INSTALL**. The Container application will be successfully installed on the user's device.
- 4. Following screen appears after successful installation. Tap **OPEN**.



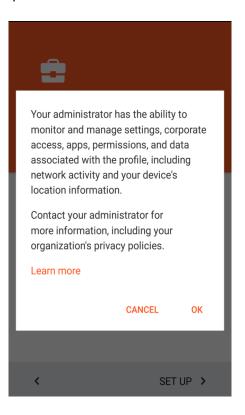




5. Launch the Container application. The application asks you to set up your profile. Tap **SET UP >**.



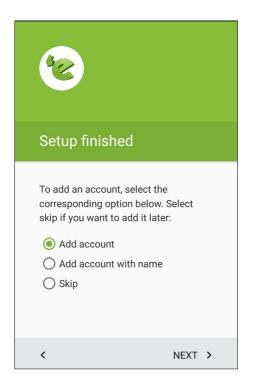
6. A message informing about device information access to administrator is displayed. Tap **OK** to proceed.



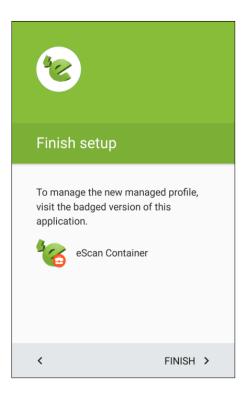




- 7. To create a work profile, select one of the following three options.
 - Add Account: Enter your Gmail account details and tap ACCEPT.
 - Add account with name: Enter your Gmail account details and name.
 - Skip: Select this option to skip entering your login details.
- 8. After selecting an option, tap **NEXT >**.



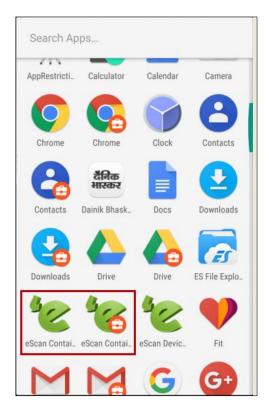
9. Finish setup screen appears, tap FINISH >.



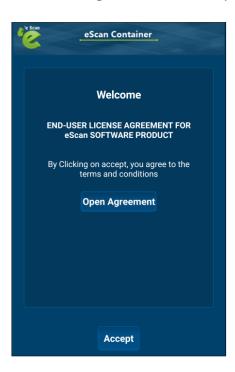




- 10. Launch eScan Container and then tap **ACCEPT**.
- 11. After the Container app is successfully installed, there will be two eScan containers displayed on the device as follows. Uninstall the eScan Container without the \bigcirc icon.



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.

eScan Container						
Enrollment Details						
Fill entries through QR code						
Mobile Number *						
Server *						
Port *						
Country						
Version : 7.2.0.3 * Field is mandatory Default Port is 2221						
Enroll Device						

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 Θ .

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.

Add New Device [Group Name: Managed Device	s] [Group Type: MDM]
Mobile Number*	
	Add Add More Close

2. Enter the details, select the OS Type as **iOS** and then click **Add**.





3. After clicking **Add**, the device will be added to the console as shown in the following screen.

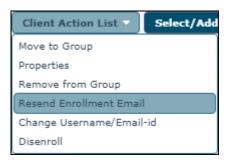
Action List 🔻 🛛 Client Acti	ion List 🔻	Select/Add Colu	ımns 🗌 🗅 Pol	icy Templ	ates		Total Devices: 2
. Managed Devices					1 - 2 of 2 🖂 (page	1 of 1 >>> Ro	ws per page: 10 🗸
Policy		Mobile Number	User's name	QR Code	Device Added Date	Enrollment Status	Enrollment Date
Client Devices		1. 78 8	afierre	<u>View</u>	04 Aug 2021 04:24 PM	Enrolled	04 Aug 2021 05:26 P
	0	é 84	Test_fadini_f	<u>View</u>	30 Jul 2021 03:10 PM	Not Enrolled	

4. Notice the icon ⁶ 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**.





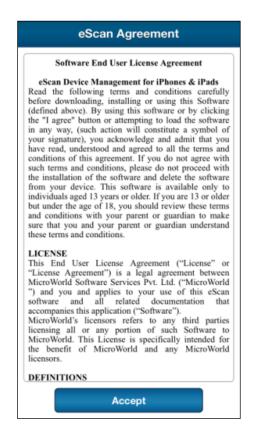


After you've received the enrollment email, perform the following steps:

1. Download and install the **eScan MDM** application from the App Store.



2. Read the eScan Agreement completely and then tap **Accept**.



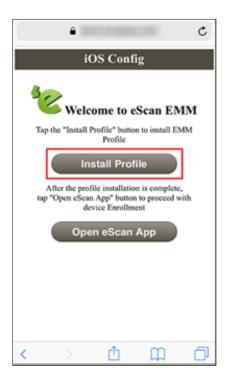




3. Launch the eScan MDM application and enter the details mentioned in the enrollment email, or fill in the details automatically via QR code by tapping **Read QR Code**. Doing so will turn on your device's camera. Match up the on-screen square with the QR code and hold your device steady till the application scans it. After the successful scan, the details will be automatically filled.

	Device Enrollment
_	009198xxxxx
_	
_	2221
Fie	elds are mandatory
	Read QR Code
	Enroll Device

4. After the enrollment details are filled, tap **Enroll Device**. iOS Config screen appears.







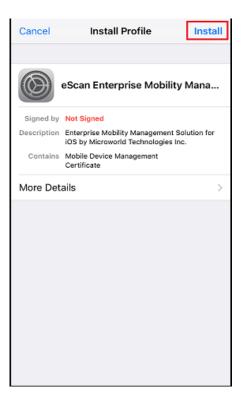
5. Tap Install Profile.

The application attempts to access your device's Settings. The following dialog box appears asking confirmation.

Q Se	arch or ente	r website	name	
to show	osite is trying you a config t to allow thi	uration p		

6. Tap **Allow**.

Install Profile settings appear.







7. Tap Install.

Enter Passcode screen appears.

	Enter Passcode C					
Enter your passcode						
00	000000					
1	2	3				
4	5	6 MN0				
7 PGRS	8	9 ****2				
	0	۲				

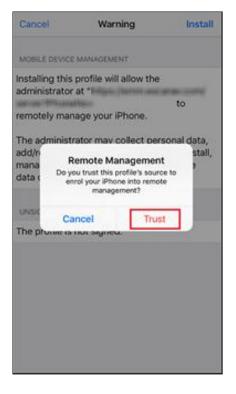
Enter the device's passcode to proceed with the installation.
 After entering the passcode, Warning message appears stating that the administrator will be able to remotely manage your device.

Cancel	Warning	Install
MOBILE DEVICE N	MANAGEMENT	
administrator a	orofile will allow th at * age your iPhone.	e /* to
add/remove ad	ntor may collect per counts and restric at apps, and remote Phone.	ctions, install,
UNSIGNED PROF	ILE	
The profile is n	ot signed.	

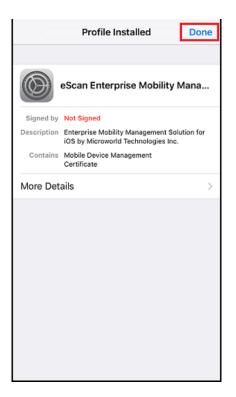




To proceed with the installation, tap **Install**.
 A pop-up message appears asking confirmation for remote management of your device.



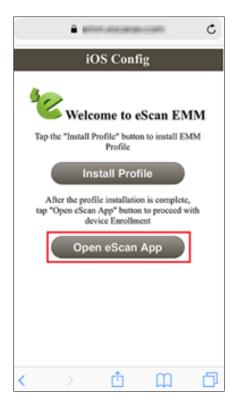
10. Tap **Trust**. The MDM profile will be installed on your device. To exit the installation process, tap **Done**.





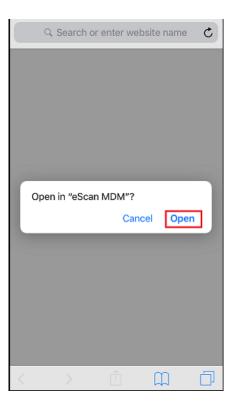


The iOS Config screen appears.



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.

Action List 🔻 Client Acti	on List 🔻 🛛 Se	elect/Add Colu	ımns 🛛 🕒 Pol	icy Templ	ates		Total Devices: 2
Managed Devices					1 - 2 of 2 ⊣∈ (page	1 of 1 >>> Ro	ws per page: 10 🗸 🗸
Policy	🔲 Mo	bile Number	User's name	QR Code	Device Added Date	Enrollment Status	Enrollment Date
Client Devices		78 8	afferne	<u>View</u>	04 Aug 2021 04:24 PM	Enrolled	04 Aug 2021 05:26 P
±	0 🧉	84 84 5	Teal_failmi_f	<u>View</u>	30 Jul 2021 03:10 PM	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	Web and Application	Web and Application
Control	Control	Control
App Specific Network	App Specific Network	App Specific Network
Blocking	Blocking 😑	Blocking 😑
Anti-Theft Policy	Anti-Theft Policy	Anti-Theft Policy
Additional Settings 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	Required Applications	Required Applications
Policy	Policy 😑	Policy 😑
Wi-Fi Settings Policy	Wi-Fi Settings Policy	Wi-Fi Settings Policy
Scheduled Backup	Scheduled Backup	Scheduled Backup
(Contacts & SMS)	(Contacts & SMS) 👘	(Contacts & SMS) 👘
Content Library Policy	Content Library Policy 😑	Content Library Policy 😑
Kiosk Mode Policy	Restriction Policy 😑	Restriction Policy 😑
		Location Fence 😑





Policies sporting icon are applicable for container version of the application for BYOD and COD groups.
 Policies sporting i 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
- Kiosk Mode 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.

Additional Settings	
Disable Screenshot	
Disable uninstalling applications	
Disable Cross Profile Copy-Paste	
Disable Install App (From all sources)	
Disable Incognito Mode	
Disable Install From Unknown Sources	

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 copypaste 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.

Enable Fencing				
Import Geo Fencing location(s)				
Geo Fencing				
± Import 🗍 🗑 Delete				
Custom Address	Latitude	Longitude	Radius(m)	
4				ŀ
				Þ
and Or				ł
and Or				Þ
AND OR UIFI Fencing Add				4
AND OR WIFI Fencing + Add Delete				¢
AND OR WIFI Fencing				•
AND OR WIFI Fencing + Add Delete				•
AND OR WIFI Fencing + Add Delete				•

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, <u>click here</u>.





Geo fencing: To enable Geo Fencing, check this check box.

1. Click Import.

Fencing Location(s) window appears.

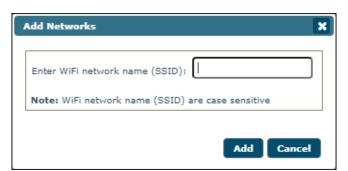
	Custom Address	Latitude	Longitude	Radius(m)	Address
)	но	19.11997	72.87334	100	80, 400 , India
)	Sitter	19.07428	72.85895	100	WING-G,
)	TEST1	19.07598	72.87766	200	b Mumbai, Maharashtra 400 🛛 , India
)	TEST2	19.08016	72.91079	200	2 M Mumbai, Maharashtra 400 , India

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.



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**.

1anage Backup					Ç'
			:		Backup Now
Managed Devices	📃 Mobile Number	User's name	Last backup	Backup Now	Manage Backup
	78 ************************************	ademe		<u>Backup Now</u>	<u>Manage Backup</u>
e-		Test_finding_fi		Backup Now	<u>Manage Backup</u>
78					
84 84 5					

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.

Manage Backup					¢ ?
					Backup Now
Hanaged Devices	Mobile Number	User's name	Last backup	Backup Now	Manage Backup
	🗭 78 - 8 - 8	ademe		Backup Now	<u>Manage Backup</u>
	👾 84 5	Tesl_tislini_ti		Backup Now	<u>Manage Backup</u>
78]= 1 = 1 84]== 5					





2. Select the desired backup and then click **Backup Now**.

Select Backup			×
SMS	÷		
Contacts	🖷 🗉		
		Backup Now Ca	incel

Backup window appears displaying the progress.

Backup	×
Parlans in announ	
Backup in progess	
Backup for 75 1996 15	
L	
Cle	ose

The report displays following fields.

Mobile Number, User's name, Last backup, Backup Now, Manage Backup.

Manage Backup					¢ ?
					Backup Now
	🔲 Mobile Number	User's name	Last backup	Backup Now	Manage Backup
	A 1 1 5 A	Test_failmi_fi		Backup Now	<u>Manage Backup</u>





Manage Backup: Clicking Manage Backup link displays following screen.

Mobile No.: 75	5 User's na	ame: Device_	18
SMS Backup	Contact Backup	Device Status	Refresh backup list
There is no info	rmation for this device		

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.

Anti-Theft								¢ ?
Wipe Data Block Device Unblock Devic	e 🏥 Scream	Send Message	Locate Device	Remove Work Profile	F			
€ Managed Devices	📕 Mobile Numbe	r User's name	Last Location	Wipe Status	Scream Status	Block Status	Message Status	Profile Remo
	🗆 🃫 75 💷 🖷	Device_						
	0 🔅 84 19 19 1	Test_fieldni_fi						

Selecting an added device enables following tabs:

- Wipe Data
- Block Device
- Unblock Device (Android)
- Scream
- Send Message
- Locate Device
- Remove Work Profile (Android)

Anti-Theft					¢ ?
Wipe Data Block Device Unblock Device	vice 👘 Scream Send Message Locate Device	Remove Work Profile			
- Managed Devices	Mobile Number User's name Last Location	Wipe Status	Scream Status	Block Status	Message Status Profile Remo
L C test Intim	✓ [♣] 75 5 Device_				
	□ [•] • 84_10010015 Test_1000011				

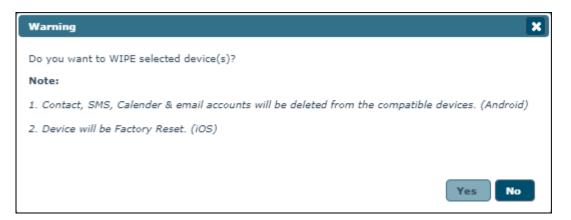




Wipe Data

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.

	×
Anti-Theft 3	2
Request in process]
Request WIPE for mobile number 75 5 was scheduled	
	_
Close	





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.

Warning	×
Lock device irrespective of policy set in "Wifi Settings Policy (Lock Device)"	*
Note : If unchecked, 1.The device(s) will not be locked if connected to Wifi SSID as per "Wifi Settings Policy (Lock Device)"	
The device(s) will be locked if "Wifi Settings Policy (Lock Device)" is not set.	-
OK Cancel	

This option can be used for both iOS and Android devices.

Click **OK**.

Anti-Theft window appears displaying the request in process.

	×
Anti-Theft ?)
Request in process Request LOCK for mobile number 75 5 was scheduled	
Close	

After the device is blocked, the device user will need the Admin Access Password to unlock the device.





Unblock Device 🗭

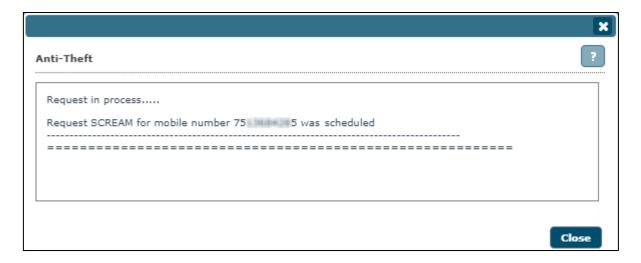
This option lets you unblock a device. To unblock a device, select the device from the list of managed devices and then click **Unblock Device**. Following window appears after clicking **Unblock Device**.

This feature works only for Android devices.

	×
Anti-Theft	?
Request in process	
Request for mobile number 75 1940 195 was scheduled	
	Close

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.

Message	×
Please call on 85	
	/
Max. 180 characters.	
Send	el

Type the message in the field and then click **Send**.

	×
Anti-Theft	?
Request in process	
Request SEND MESSAGE for mobile number 75 345 5 was scheduled	
	_
	Close





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.

	×
Anti-Theft	?
Request in process	
Request LOCATE for mobile number 75: 100 15 was scheduled	
	Close

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

lardware Inform	nation Appli	ication Info	rmation					
 Filter Criter Device Details 	ia			-	Export Option	page 1 of	1) > Rows per page:	10 🗸
Mobile Number	User's name	Group	Group Type	IP Address	1		Operating System	
	i Device	test MDM	MDM	192.000.000	35	History E	Android	6,81
75 5	Device_	const_month						

Viewing Hardware information

- 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.

 Filter Criteria 				Export Option			
Filter Criteria							
Mobile Number	*	Include 🗸	✓	Phone Memory (System Usable) (MB)	*		Include 🗸
IP Address	*	Include 🗸	~	External SD (MB)	*		Include 🗸
🗹 User's name	*	Include 🗸	~	Internal Memory (User Usable) (MB)	*		Include 🗸
IMEI Number	*	Include 🗸	✓	Network Type	Select	~	Include 🗸
Phone Model	*	Include 🗸	✓	Roaming Enabled	Select	~	Include 🗸
Operating System	*	Include 🗸	✓	Rooted	Select	~	Include 🗸
OS Version	*	Include 🗸	✓	Bluetooth	Select	~	Include 🗸
🗹 RAM (MB)	*	Include 🗸	✓	WI-FI	Select	~	(Include 🗸
Group	*	Include 🗸	~	GPS	Select	v)	Include 🗸

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				
Phone Number	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				
User's name	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)	Displays the phone memory of the device.				
(MB)					
External SD (MB)	Displays the external SD card's storage capacity (MB) of the				
	device.				
Internal Memory	Displays the internal memory of the device.				
(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

ardware Information Application Information	
Filter Criteria	 Export Option
pplication Details	1 - 10 of 72 I€ (page 1 of 8 ≯ N Rows per page: 10 ∨
Application Name	Device Count
Adobe Acrobat	1
Authenticator	1
Bitdefender Security	1
Calculator	2
Calendar	2
Camera	2
Chrome	2
Clock	2
Compass	1
Contacts	1

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	*	Include V Group By]
Mobile Number	*	Include Application Name Mobile Number	
PSearch 9 Reset	t		

- 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

Hardware Information	Application Information		
 Filter Criteria 		 Export Option 	
Export Option			
C Excel		ITML	Ľ ⁷ Export

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

 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.

🗅 New 📕 Edit 🍵 Delete 🛛 🕫	liew				
Template Name	Report Type	Date Filter	Sort By	Created On	Modified On
Application Control Report 🛱	Application Control Report	Last 7 days	Date	31 Jul 2021	31 Jul 2021
Device last connection report 👾 ≤	Device last connection report	Last 7 days	Devices	31 Jul 2021	31 Jul 2021
🗋 Enrollment Report 🖷 🛸	Enrollment Report	Last 7 days	Date	31 Jul 2021	31 Jul 2021
] Inventory Report 👾 🛸	Inventory Report	Last 7 days	Devices	31 Jul 2021	31 Jul 2021
Update Report 📫	Update Report	Last 7 days	Date	31 Jul 2021	31 Jul 2021
Virus Report 🛱	Virus Report	Last 7 days	Date	31 Jul 2021	31 Jul 2021
Web Control Report	Web Control Report	Last 7 days	Date	31 Jul 2021	31 Jul 2021

Creating a Report Template

1. In the Report Templates screen, click **New**. New Report Template window appears.

late Name :* New Tanging Tanging		
lected Template Type		
Virus Report	O Update Report	
🔿 Web Control Report	O Inventory Report	
O Application Control Report	O Enrollment Report	
O Device last connection report		
lect Filter Options		

2. Type a name for the new report template and select the required report type from the given options.





 In Select Filter Options section, select the appropriate Date Options and Sort By, then click Save.

New Report Template		×
Template Name :* New Tagent Tanglata	4	
▶ Selected Template Type)
Select Filter Options		
Date Options		
Today	🔿 Last 7 days	
C Last 30 days	C Last 365 days	
○ Since Installed	O Date Range	
Sort By		
 Date 	O Devices	
O Virus	O Action Taken	
Date	Device Type	
File Infected	Action Taken	
	Uirus count	
Custom columns	column2	
column3	Column2	
	Column	
		Save Cancel





Editing a Report Template

 Select a Report Template and then click Edit. Edit Report Template window appears.

t Report Template		
emplate Name :* New Tagent Tangin		
Selected Template Type		
 Select Filter Options 		
Date Options		^
Today	🔿 Last 7 days	
O Last 30 days	🔿 Last 365 days	
○ Since Installed	O Date Range	
-Sort By		
Date	O Devices	
O Virus	O Action Taken	
Sort column in report		
Date	Device Type	
File Infected	Action Taken	
Description	□ Virus count	
Custom columns	C column2	
Column3	🗌 column4	

2. Make the required changes and then click **Save**. The Report Template will be updated.





Deleting a Report Template

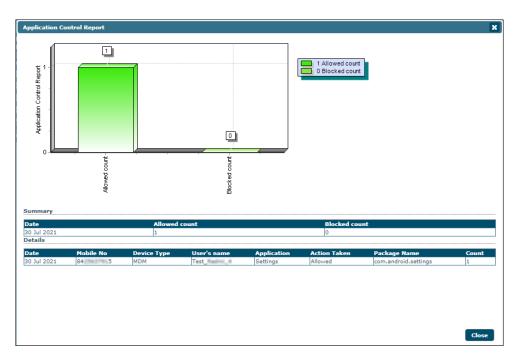
Select a Report Template and then click **Delete**.

Template Name	Report Type
Application Control Report	Application Control Report
Device last connection report 👾 🛋	Device last connection report
🗆 Enrollment Report 🛱 🗯	Enrollment Report
🗋 Inventory Report 🛱 🧯	Inventory Report
New Report Template_1	Virus Report
Update Report 🛱	Update Report
Virus Report 🖷	Virus Report
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.

🕒 New 📓 Edit 🗊 D	elete 🕨 Run 🛛 🗘	/iew 📋 Res	ults			
Schedule Name	Report Recipient	Format	Туре	Next Scheduled	Created On	Modified On

Under Report Scheduler, following options are available. Except **New**, all other options are enabled only after selecting a template.

Report Scheduler						¢ ?
🗅 New 📔 Edit 🝵 Delete	e ► Run 🛛 View) Results				
🗹 Schedule Name	Report Recipient	Format	Туре	Next Scheduled	Created On	Modified On
New Tannel Scheduler	excom	HTML	Scheduled	31 Jul 2021 08:30 PM	31 Jul 2021	31 Jul 2021

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
Results	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.

▼ Template Selection
Select a Template for creating a Report
± Application Control Report
🗄 🛛 Enrollment Report
🗓 🗌 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		
"Description of Devices," will each be		_
"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 Pare	ent 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

end Report by Email		
Report Sender*:	telles gamel.com	
Report Recipient*:	example@example.com Add	
	Delete	
Mail Server IP Addre	ss: smtp.gmail.com	
Mail Server Port:	465	
Auth. Username:	te .com	
Auth. Password:	•••••	

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

Scheduled			O Manual	
Daily				
O Weekly	Mon	🗌 Tue	Wed Sat	Thu Sun
O Monthly	1 🗸			

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.



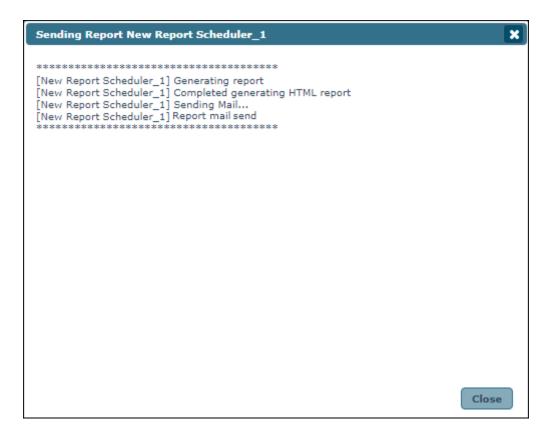


Running a schedule

To run a schedule, select a schedule and then click **Run**.

Report Scheduler						¢ ?
🗅 New 📔 Edit 🍵 Del	ete 🕨 Run 🛛 View	🔒 Results				
Schedule Name	Report Recipient	Format	Туре	Next Scheduled	Created On	Modified On
Vew Report Scheduler_L	example com	HTML	Scheduled	31 Jul 2021 08:30 PM	31 Jul 2021	31 Jul 2021

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.

Edit R	eport Scheduler	
New	Report Scheduler : New Farmer Education 1	
• T	emplate Selection	
S	elect a Template for creating a Report	
Г	🗄 🏹 Application Control Report	
	🗄 🔲 Device last connection report	
	🗄 🗸 Enrollment Report	
	··· 🔵 Date	
	🗄 🔲 Inventory Report	
	···· Update Report	
	🗄 🗇 Virus Report	
L		
→ s	election For Applied Groups/Clients	
► R	Report Send Options	
► R	Report Scheduling Settings	_
	Save Canc	21

Make the required changes and then click **Save**.

Deleting a Schedule

Select a schedule and then click **Delete**.

\$?	¢						port Scheduler	Rep
					🕽 Results	► Run 🛛 View	🗈 New 📲 Edit 💼 Delete	
l On	Modified On	Created On	Next Scheduled	Туре	Format	Report Recipient	Schedule Name	~
21	31 Jul 2021	31 Jul 2021	31 Jul 2021 08:30 PM	Scheduled	HTML	example com	New target Schullung	
0	31 Jul 2	31 Jul 2021	31 Jul 2021 08:30 PM	Scheduled	HIML	ex. com	New Taylor Schalter	

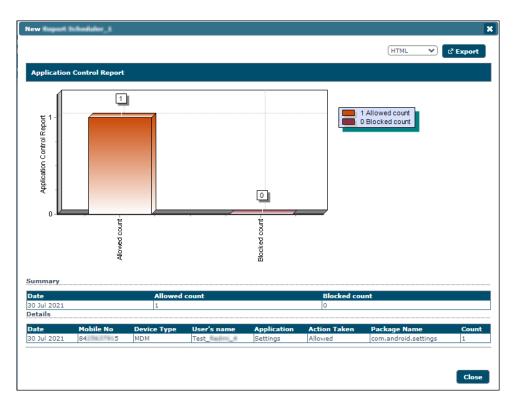
The selected schedule will be deleted.





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.

New Ingene Scheduler - Results					
Start	Finish	Туре	Status		
02 Aug 2021 10:59 AM	02 Aug 2021 11:01 AM	Scheduled	Report mail sent successfully		
02 Aug 2021 11:09 AM	02 Aug 2021 11:09 AM	Manual	Report mail send		





Events and Devices

Events and Devices module shows all events performed on the 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.

Edit Selection 🔻								MDM Container Filter
Events And Devices	Rec	ent					1 - 10 of 141	1 of 15 → H Rows per page: 10 →
Events Status		Date	Phone Number	Device Type	User's name	Event Id	Module Name	Description
- 🔝 Recent - 🔂 Critical	0	30 Jul 2021 05:06 PM	75	MDM	Device_Herme	7085	Anti-Theft (Android)	Anti-Theft Unlock
	0	30 Jul 2021 05:05 PM	75	MDM	Device_	7085	Anti-Theft (Android)	Anti-Theft Unlock
- E Device Selection	0	30 Jul 2021 05:05 PM	75	MDM	Device_	7085	Anti-Theft (Android)	Anti-Theft Unlock
E Application/Hardware Changes	0	30 Jul 2021 04:32 PM	75 1111 5	MDM	Device_	7033	Config(Android)	Auto sync status[07/30/2021 16:32:2
	0	30 Jul 2021 04:32 PM	75	MDM	Device_	7047	Android	Compliance
	0	30 Jul 2021 03:38 PM	75	MDM	Device_	7047	Android	Compliance
	0	30 Jul 2021 03:38 PM	75	MDM	Device_	7033	Config(Android)	Auto sync status[07/30/2021 15:38:1
	0	30 Jul 2021 03:23 PM	84 5	MDM	Test_failmi_f	7047	Android	Compliance
	0	30 Jul 2021 03:23 PM	84 5	MDM	Test_fieldmi_fi	6152	Config(Android)	Protection Status
	• 0	30 Jul 2021 03:23 PM	84 5	MDM	Test_Radmi_#	7009	Call & SMS Filter (Android)	Call/SMS Filter Status

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

vents And Devices	s Settings		(
Events Status	Device Selection	Application/Hardware Changes	
Events			
Events Name	Recent 🗸		
Number Of R	ecords	1000	
Save			

Select an event from the drop-down and enter the number of records you want to see.





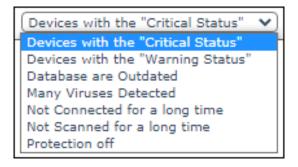
Device Selection

The following actions can be performed by selecting this tab.

ents Status Device Selection Application/Hardware Changes Devices Device Status Devices with the "Critical Status" Check for Monitor Status Check for Not Scanned	
Device Status Devices with the "Critical Status" 💙	
Check for Monitor Status	
Check for Not Scanned	
check for Not Scattled	
Check for Database Not Updated	
Check for Not Connected	
Database Not Updated from more than 7 Device Not Scanned for more than 7	days
Device Not Connected for more than 7	days
Number Of Records	j

Device Status

The Device Status drop-down consists 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
- Protection off





Option	Description
Check for Monitor	Select this check box to generate events related to eScan
Status	Monitor Protection.
Check for Not	Select this check box to view the list of devices which are
Scanned	not scanned.
Check for Database	Select this check box to view the list of devices on which
Not Updated	virus signature database is not updated.
Check for Not	Select this check box to view the list of devices that are not
Connected	connected with the eScan server.
Database Not	All the devices that are not updated from more than the
Updated from more	specified days will be added to the report.
than	specified days will be added to the report.
Device Not Scanned	All the devices that are not scanned for more than specified
for more than	days will be added to the report.
Device Not	All the devices that are not connected to the eScan server
Connected for more	for more than the specified days will be added to the report.
than	To 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.

ents And Devices	Settings		×
Events Status	Device Selection	Application/Hardware Changes	L
Updates			
Application/Han	dware Changes Applica	ation Changes 💙	
Number Of D	ays	1 days	
Number Of R	ecords	1000	
Save			





Field	Description			
Application/Hardware	Select from the drop-down to generate events related to			
Changes	Application changes, Hardware changes, and Existing			
Changes	Device Info.			
	Enter the number of days, to view changes made within			
	the specified days.			
Number of 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.

ertificate Management Email Notification Settings Data Purg	e Connection Sequence
+ Add	Certificate Detail
emm_escanav_com.crt	Domain : Issuer : Expiry Date : Oct 26 23:59:59 2021 GMT

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 <u>our website</u>, 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.

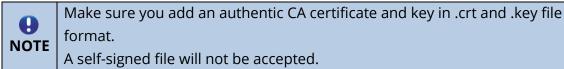




Importing an SSL certificate

- 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.



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.

Add Certificate	×
Select Certificate File	2
Certificate File (.crt):	Choose File No file chosen
Certificate Key File (.key):	Choose File No file chosen
Certificate Key File Password:	Enter password
	*Enter password in case your key file is password protected, else leave blank.
	Save Cancel





- 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.

	¢ ?
Certificate Management Email Notification Set	ings Data Purge Connection Sequence
Email Notification Settings	
From (Administrator Email Id)*:	teilinni jammi min
SMTP Server*:	sing gradient com
SMTP Port*:	465
Auth. Username:	te com
Auth. Password:	•••••
* Mandatory Field	
✓ Save ✓ Test	
lease and the second se	

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

rtificate Management Email Notification S	Settings	Data Purge	Connection Sequence	
Keep Location History for	60	Days	(0-365) 0=Unlimited	
Keep Data Usage data for	60	Days	(0-365) 0=Unlimited	
Keep Call logs data for	60	Days	(0-365) 0=Unlimited	
Keep Battery Status/Signal Strength History d	lata for 60	Days	(0-365) 0=Unlimited	
Keep Geo Fence History data for	60	Days	(0-365) 0=Unlimited	
Keep App Usage History data for	60	Days	(0-365) 0=Unlimited	

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 you are done making changes, click **Save**. The Data Purge changes will be saved.

Connection Sequence

				¢ [
Certificate Management	Email Notification Settings	Data Purge	Connection Sequence]
	ne server list ("Server" entry) to b cide which server is connected firs		ification email/QR code.	

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.





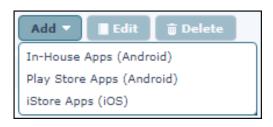
App Store

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.

App Store							
Applications listed below can be imported through "Policy >> Required Application Policy", for deployment to devices.							
Add 🔻 🔳 Edit 🗊 Delete							
In-House Apps (Android)	ay Store Apps (Android)	iStore Apps (iOS)					
Application Name Package Name Version Size Installed Added On							

Adding an Android application with In-House Apps (Android) option

1. Click Add > In-House Apps (Android).



Add App (In-House) window appears.

Add App (In-House)	×
Select Application source	
Select a file with .apk extension	
Choose File No file chosen	
Continue	cel

2. Click **Choose File** and browse your computer for the **.apk** file. After selecting the file, click **Continue**.





Add Application window appears.

Add App (In-House)		×
Application Name:	APKTime	
Application Icon:	Choose File No file chosen	
Application Id:	com. agiitime. agiitime	
Description:		
	Save	

3. Write a brief description about the application and then click **Save**. The application will be added to the App Store.

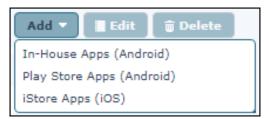
Click the numerical in the **Installed** column to view the list of devices on which the application is installed. Before the policy deployment the count will be 0. If the application with the same version number already exists on the devices, the installation count will be shown accordingly.





Adding an Android application with Play Store Apps (Android) option

1. Click Add > Play Store Apps (Android).



Add App (Play Store) window appears.

Add App (Play Store)		×
App Details		
Select Region	India 🗸	
App Name *	Enter app name	
Application Name:	[]	
Package Name:	[]	
Application Icon:		
* Mandatory Field		
L		
	Save Cance	

- 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**.

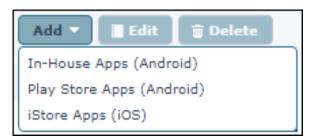
The application will be added to the App Store.





Adding an iOS application

1. Click Add > iStore Apps (iOS).



Add Apps (iOS) window appears.

Add Apps (iOS)	×
App Details	
Select Region	India 🗸
App Name *	Enter app name P Search
Application Icon	
 Mandatory Field 	
	Save Cancel

- 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.



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**.

Store	nported through "Policy >> Rec				
Add 🔻 📳 Edit 🍵 Dele	te				
In-House Apps (Android)	Play Store Apps (Android)) iStore App	s (iOS)	Installed	Added On
	com.aglittime aglittime	2.2	4868 Kb	0	20 Jul 2021 04:34 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.

Content Library			¢ ?
+ Add 📲 Edit 🝵 Delete			
🔲 File Name	Size	Updated On	Description

Adding a file

1. Click **Content Library** > **Add**.

Add File window appears.

Add File	×
Select File source	
Allowed file formats PDF, DOC, DOCX, XLS, XLSX, PPT, PPTX, JPG, JPEG, PNG, BMP Choose File No file chosen	IXT,
Conti	Cancel

- 2. Click **Choose File** and search your computer for the file.
- 3. After selecting the file, click **Continue**.





Add File window appears.

Add File		×
File Name:	Escalation Charl Companying .docx	
	important	
Description:		
	Save	icel

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**.

Content Library + Add Edit Delete						
✓ File Name	Size	Updated On	Description			
ED ED	2184 Kb	20 Jul 2021 12:58 PM	important			

Edit window appears.

Edit		×
File Name:	EDT_Tentilitert_Til.doc	
	important	
Description:		
		Save Cancel

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**.

Content Library			¢ ?
+ Add 📲 Edit 🗊 Delete			
✓ File Name	Size	Updated On	Description
ED Section States	2184 Kb	20 Jul 2021 12:58 PM	important

A confirmation prompt appears.

Del	ete File(s) X
0	Selected items will be permanently deleted. Are you sure?
	Note: If these Files/Documents are added to Policy Details>>Content Library Policy, make sure that you re-deploy the policy for that specific groups to update the Content Library on the device.
_	
	Delete Cancel

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.

all Logs						P (*
Check configuration under "F	Policy >> Device Oriented	Policy", if Call logs are not d	isplayed.			
Data Purge set to "60 days",	to configure <u>click here</u>					
						HTML V Export
- 📄 Managed Devices	All calls			1 - 10 of 20 🖂	(page 1 of 2) №	Rows per page: 10 🗸
Tell_MD	Mobile No	Name (As in Contact List)	Contact No	Type of Call	Call/Receive time	Call Duration (HH:MM:SS
	× 78	UNKNOWN	61-1111	Outgoing	08 Mar 2018 10:48 PM	00:45:00
🛨 💼 tes nom	✓ 781+11+18	B UNKNOWN	9	Outgoing	08 Mar 2018 10:21 PM	00:30:00
	✓ 78 8 8	UNKNOWN	+910030000	Missed	08 Mar 2018 10:16 PM	00:00:00
	✓ 781+11+18	UNKNOWN	961+114	Outgoing	08 Mar 2018 09:48 PM	00:28:00
	🖌 78 m 8	UNKNOWN	+9103636835	Missed	08 Mar 2018 09:16 PM	00:00:00
	✓ 78 ** 1 ** 8	B UNKNOWN	+91	Missed	08 Mar 2018 08:16 PM	00:00:00
	🖌 78 m 1 m 1	UNKNOWN	+91	Missed	08 Mar 2018 07:16 PM	00:00:00
	✓ 781+11+18	3 UNKNOWN	8 34 3 3 3 34	Outgoing	08 Mar 2018 06:48 PM	00:13:00
	↗ 78 ** 1 ** 8	UNKNOWN	76012-100	Outgoing	08 Mar 2018 06:48 PM	00:26:00
	✓ 78 - 1 = 18		+9100000000000	Missed	08 Mar 2018 06:16 PM	00:00:00

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.

ta Usage						P (*)
Data Purge set to "60 days",	to configure <u>click</u>	here				
					C	HTML 🗸 🗹 Export
- Carl Managed Devices	User's r	ame: adams	Mobile Number: 78	54123658	1 - 8 of 8 I∢ ∢ page 1 of 1 → H	Rows per page: 20 🗸
💼 Tell	Sr. No.	Date	Mobile No	User's name	Group	Data Usage
💼 Te#(68	1	27 Jul 2021	78 8	adams	test_mt:m	840.48 MB
	2	28 Jul 2021	78 8	adams	tein_mt:m	735.58 MB
🗄 🧫 te	3	29 Jul 2021	78 8	adams	te <u>st ntim</u>	630.68 MB
			and the same the last of the			
	4	30 Jul 2021	78 8	adams	tess_wtine	525.77 MB
	5	30 Jul 2021 31 Jul 2021	78 8	adams adams	te	420.87 MB
	4 5 6				te <u>stine</u>	
	4 5 6 7	31 Jul 2021	781+111B	adams	teas	420.87 MB

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.					
User's name	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.

Location History Battery Status/Sign	al Strength G	eo Fence Histo	гу Арр	Usage History		
Data Purge set to "60 days", to confi	gure <u>click here</u>				(HTML 🗸	් Export 🎾 අ ද
Hanaged Devices	Mobile Number	User's name	Groups	Last Location	Last Location Date and Time	Total Locations
	78 8 8	adams	test_MDM	<u>19.2301,72.8411</u>	03 Aug 2021 11:59 PM-04 Aug 2021 09:30 AM	<u>17</u>

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.
	This column displays the total number of the locations where the
Total Locations	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.

Location History Battery Status,	Signal Strength Geo Fence Hi	story App Usage History		
Data Purge set to "60 days", to	configure <u>click here</u>			
- Managed Devices	User's name: Tes	Mobile No: 84	(HTI	ML 💙 ピ Export 🔎 🗘 ?
🚰 Test_AD			1 - 1 of 1 🖂 page 🚺	of $1 \rightarrow H$ Rows per page: 20 \checkmark
	Date	Battery Status	WiFi Strength	SIM Signal Strength
84100015	30 Jul 2021 03:23 PM	45%	99%	No Network
781411118				

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	This column displays the available SIM signal strength of a device.			
Strength				

Filter

You can also view the details related to the Battery Status/Signal Strength as per the date range.

Geo Fence History

The Geo Fencing History displays the geo fencing history of the devices along with the details of date/time and location of the fence (inside or outside).

ocation History Battery Stat	tus/Signal Strength Geo Fence Hist	ory App Usage History		
Data Purge set to "60 days",	to configure <u>click here</u>			
- Managed Devices	User's name: a Mobile	e No: 78	(HTML 💙 🗗 Export 🔎 🕼 ?
(Test_100	Note: More accurate results	can be achieved for Geo-fence, if t	he device is in-use/action 1 - 3 of 3 K (page 1	ve. of 1 → >> Rows per page: 20 v
	Note: More accurate results Date			
Tes Ca			1 - 3 of 3 ।∢ (page 1	of 1 >>> Rows per page: 20 🔹
Tes 68	Date	Lat/Long From Device	1 - 3 of 3 K (page 1 Fence Name	of 1 +>> Rows per page: 20 V Inside/Outside Fence

Column	Description			
Date	DateThis column displays the date.			
Mobile Number	This column displays the mobile number of the device.			
User's name	This column displays the user name of the device			





Last Visited	This column displays the name of the last visited fence.
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 location visited lastly.

App Usage History

The App Usage History module displays the details of the apps along with its package name and total time usage of it.

cation History Battery Status/Signal Strength Geo Fence History App Usage History				
Data Purge set to "60 days", t Managed Devices		Mobile No: 78 8 Tot	al Usage: (Today 🗸 (HTML 🗸	් Export ይ අ ?
	Date	Application Name	Package Name	Total Usage (HH:MM:SS)
	07 Aug 2021 04:54 PM	eScan Device Management	com.eScan.mdm	01:05:28
	07 Aug 2021 04:54 PM	Google	com.google.android.googlequicksearchbox	00:05:08
	07 Aug 2021 04:54 PM	Chrome	com.android.chrome	00:02:28
	07 Aug 2021 04:54 PM	File Manager	com.itel.filemanager	00:00:49
	07 Aug 2021 04:54 PM	Drive	com.google.android.apps.docs	00:00:47
	07 Aug 2021 04:54 PM	Google Play Store	com.android.vending	00:00:38
	07 Aug 2021 04:54 PM	Docs	com.google.android.apps.docs.editors.docs	00:00:37
	07 Aug 2021 04:54 PM	Settings	com.android.settings	00:00:24
	07 Aug 2021 04:54 PM	Gmail	com.google.android.gm	00:00:18

Column	Description
Date	This column displays the date.
Application	This column displays the name of the application.
Name	
Package Name	This column displays the package name of the application.
Total Usage	This column display the total time the application was used
Time	





Fencing Location(s)

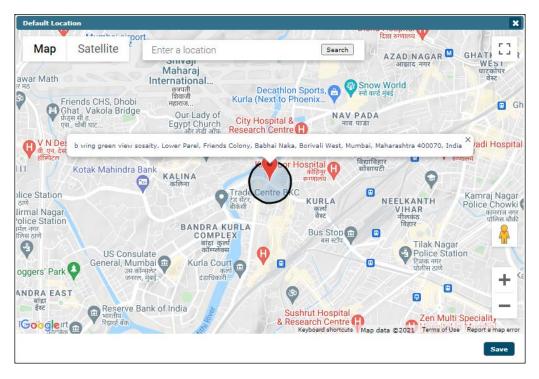
Geo-Fencing refers to drawing a virtual barrier around a location using a device's Global Positioning System (GPS) or Internet Protocol (IP) address. Technically, geo-fencing can be any size radius from a particular location, anywhere from 25m to 5000m in stretch. You can define an address on the map 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.

			¢
te 🛛 🛛 View On Map	🗅 Edit Default	Location ± 1	import Locations via file
	1 - 1 of 1 ⊣ (pa	ge 🚺 of 1	🕞 Rows per page: 20 💊
Latitude	Longitude	Radius(m)	Address
19.07598	72.87766	200	-
	Latitude	te 🛛 View On Map 🕒 Edit Default 1 - 1 of 1 📧 (pa Latitude Longitude	te View On Map Edit Default Location ± 1 1 - 1 of 1 K (page 1 of 1 Latitude Longitude Radius(m)

Creating a Fencing Location

To create a Fencing Location, it is necessary that a default location must be set first.

Click Fencing Location(s) and then click Set Default Location.
 Default Location window appears.



2. Enter the location and then click **Save**.





After setting the default location, click Add.
 Fencing Location(s) window appears.

Fencing Location(s)
्रणगश्चरा 🗸 Arte Coience and Mahakali Caves 🗃
C Map Satellite escan india Search owai Garden C I R
Ition Plot No 80, Rd Number 15, Marol MIDC Industry Estate, Andheri East, Mumbai, Maharashtra 400093, India
वर्षा नगर TY ANDHERIEAST अंधेरी इस्ट PNA Trouse PNA Trouse प्रिया हाउस PNA Trouse प्रिया हाउस Physical State (TUNGA) तुंग ICICI Bank Chandivali, State (TUNGA) तुंग ICICI Bank Chandivali, State (TUNGA) तुंग ICICI Bank Chandivali, State (TUNGA) तुंग ICICI Bank Chandivali, State (TUNGA) तुंग ICICI Bank Chandivali, State (TUNGA) तुंग
Andheri/ متعلقهم معلم المعلم المع معلم المعلم ا معلم المعلم المعلم المعلم المعلم ا
PARLE COLONY पार्ले कार्वानी Hanuman road bus stop
प बंसे थांबा JW Marriott (क्र Mumbai Sahar → Millat Hospital (न मिल्लत ऑस्पिटल → SERVE : CE
Google Sahar Airport Sahar Airport
Cocation Details
Latitude: 19.12000 Longitude: 72.87357
Radius(m): 200 ✔ Meters Set
Address: Plot No 80, Rd Number 15, Marol MIDC Industry Estate, Andheri East, Mur
Custom Address: Head Office
Save Cancel

- 4. Enter the location and select the appropriate one from suggestions.
- 5. Click the **Radius** drop-down to select the appropriate radius and then click **Set**.
- 6. In the **Custom Address** field, enter a name for your fencing location.
- 7. After entering all the details, click **Save**.

Editing a Fencing Location

1. Select a location and then click **Edit**.

Fencing Location(s)				¢ ?
+ Add 📲 Edit 🗑 Delete 🛛 V	/iew On Map 🛛 🕒 E		Import Locations via file of 1 4 (page 1 of 1	
	Ŧ	1-	I of I ((page []) of I	Fri Rows per page: 20 ▼
Custom Address	Latitude	Longitude	Radius(m)	Address
✓ office	19.07598	72.87766	200	-

2. After making the necessary changes, click **Save**.





Deleting a Fencing Location

1. Select a location and then click **Delete**.

enci	ing Location(s)				¢
+	Add 📲 Edit 🍵 Delete 🛛 🕫 Vie	ew On Map 🛛 🖪	Edit Default Location	± Import Locations via file	
			1 -	1 of 1 ⊣ (page 1 of 1	🕅 Rows per page: 20 🗸
<	Custom Address	Latitude	Longitude	Radius(m)	Address
	office	19.07598	72.87766	200	-

A confirmation prompt appears.

Delete L	ocation	X
	you sure you want to delete selected Geo ation(s)?	
	OK	

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.

Custom Add	dress: TEST1								×
7				/	Holy Cross	Church, Kur			ऑफ इं ि न न
Мар	Satellite					Elest shiel	44 -		123
JAF	SHIV NA			Researc	ospital & h Centre 🕀 सेटी हॉस्पिटल	171	Aren		KI
18	Road	State Bank	of India		व रिसर्च सेंटर		Fremier Road		
a Market	Our Lady o Egypt Church	f	AU		MHabib Ho	Kohinoor		VIDYAVIH SOCIET × विद्याविहार	
कलिना बाजार	Cbd Belap	ur - Near Bridge Ending,	Lower Parel, H	Kismat Naga	r, Kurla, Mumbai,	Maharashtra		सोसायटी	К
Cortes	KALINA कलिना		Mariya n	He tal यम हे सेटल	Kohinoo	r Hospital कोहिनूर रूग्णालय	₽		Som
	JEE.	CLR Bridge 🖽 स्कलर ब्रिज 🤁 R U	PA NAGA रुप नगर	R	Suraj Hospital सूरज हॉस्पिटल	Q ~	Kurla EMU Ca ईएमय	arshed कुर्ला 🔛 कारशेड	Gom
na Mumbai	Axis Bank का ऍक्सिस बँक	टेड सेंटर, बीकेसी	entre BKC	New Mill Rd	Pipe Line Rd	KURLA कर्ला वेस्ट			
ersity । मंबई सिंटी	Centrum Cap संट्रम हाउस	ital Limited		JRLA WI	FST	att			
	SW Centre - B	NDRA KURLA	2	कर्ला वेस्ट		al Rukmini I		okmanya Terminus	+
He	eadquarters	COMPLEX बांद्रा कुर्ला कॉम्प्लेक्स	ladur Shastri Rd ^{HP Keluskar Marg}	A Mill Rd		रुवि	मणी मंदिर मंड ठि	Terminús ई लोकमान्य ळक टर्मिनस	- Mar
Google			Iad(CLW A	Keyboard shortcut	s Map,data	©2021 Terms	of Use Report	a map error
Latitude: 1		e: 72.87766 Radius(r	n): 200						
	Longitud								
									ancel
									ancel





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					¢ ?
Create New Account		1 - 1 of 1	e page 1 of 1 🕅	Rows per page	: 10 🗸
User's name Full Name	Domain	Role	MDM Role	Session Log	<u>Status</u>
root Administrator account created during installation		Administrator	Administrator	<u>View</u>	
Create New Account		1 - 1 of 1	(page 1 of 1 ⊳∣	Rows per page	: 10 🗸





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	2
User Accounts > Create User	
Account Type and Information	
Username*:	
Full Name*:	
Password*:	
Confirm Password*:	
Email Address:*	
	For Example: user@yourcompany.com
Account Role	
Role*: Administrator	✓
MDM Role*: Administrator	►
Save Cancel	(*) Mandatory Fields

After filling all the details, click **Save**.
 The user will be added to the User Accounts list.





Adding a User from Active Directory

 In the User Accounts screen, click Add from Active Directory. Add Active Directory Users form appears.

Add Active Directory Users	2
<u>User Accounts</u> > Add Active Directory U	sers
Search Criteria	
User's name*:	
	For Example: user or user*
Domain*:	
AD IP Address*:	
AD Admin User name*:	
	For Active Directory account: domain\username
AD Admin Password*:	
Use SSL Auth.:	
AdsPort*:	389
Search	
Search Results	
Users	Selected Users
Account Role	
Role*: Administrator	~
MDM Role*: Administrator	▼
Save	(*) 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.

		E
User Accounts		
Do you want to delete the selected user acc	ount(s) ?	
	Ok	Cancel

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 Mobility Management Console and the networked Devices. 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 on network devices or define Policies and tasks for the devices.

User Roles	¢ ?
New Role Properties 🗊 Delete	
Role Name	Description
Administrator	





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 :	IT_kémin	
Select Group :		
Select subgroups on	selecting Parent group	
	Jevices	
OK Cancel		
Cancel		

- 2. Enter name and description for the role.
- 3. Click **Managed Devices** 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 all the modules and configuration permissions.

ils			
excription :			
Select Group			
Main Tree Menu Client Tre	Vi	ew Configu	re
Dash Board			
Managed Mobile Devices			
Manage Backup			
Anti Theft	(
Asset Management			
Report Templates			
Report Scheduler			
Events And Devices			
App Store			
Content Library			





The Client Tree Menu consists of selected groups on which permissions the user is allowed to take further.

ole		
etails		
New Role Name :*	IT_Admin	
Description :	viewer	
Select Group		
Main Tree Menu	Client Tree Menu	
⊕ ि Managed Do	vices Please Select a Group to set Permission	
	1	
e Cancel		

- 6. Select the check boxes that will allow the role to view/configure the settings.
- 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	¢ ?
New Role Properties 🗊 Delete	
Role Name	Description
Administrator	
Viewer	

2. Click Properties.

Properties screen appears. Main Tree Menu lets you modify role description, permissions for accessing and configuring all the 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**