

# eScan Enterprise Mobility Management (Android Enterprise)

GB

## User Guide

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

24x7 FREE Online Technical Support

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

An ISO 27001 Certified Company

www.escanav.com





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: Current Software Version: Technical Support: Sales: Forums: eScan Wiki: Live Chat: Printed By: Date: 5BUG/04.10.2021/22.x 22.0.xxxx.xxx support@escanav.com sales@escanav.com http://forums.escanav.com/ https://www.escanav.com/wiki http://www.escanav.com/english/livechat.asp MicroWorld October, 2021





## Table of Content

Introduction	8
System Requirements	9
Getting Started	9
Dashboard	10
Deployment Status	10
Functional Status	11
eScan Status	11
eScan Version (Android - MDM App)	12
eScan Version (Android - eScan EMM App)	12
eScan Version (iOS - MDM App)	13
Android Version	13
iOS Version	14
Device Sync Status (Successful)	14
Kiosk Status	15
Protection Status	16
Update Status	16
Scan Status	17
Anti-Virus	17
Web Control	18
Application Control	18
Call and SMS Filter	19
Protection Statistics	20
Anti-Virus	21
Web Control	21
Application Control	22
Call Statistics	22
SMS Statistics	23
Settings	23
Managed Mobile Devices	24
Action List	24
Group Type	25
Creating a New Group	26
Adding a New Device	26
Adding Multiple Devices	27
Change Server IP	29
Properties	30
Client Action List	31
Moving Device from one group to the other group	31
Checking a Device Properties	33
Removing a device from group	34
Resending Enrollment Email	34
Changing a User's Name/Email ID	34
Disenrolling a device	35
Select/Add Columns	36
Policy Templates	37
Steps for defining Policies for the Group	37



Creating New Template	
Common QR Code Scan	
Refresh Scan Devices	
Window Buttons	
Android Templates	
Anti-Virus Policy	
Call & SMS Filter Policy	
Call and SMS Filter Mode set to Off	
Call and SMS Filter Mode set to Blacklist	
Call and SMS Filter Mode set to Whitelist	
Call and SMS Filter Mode set to Both List	51
Call Filter (Outgoing) Mode set to Off	51
Call Filter (Outgoing) Mode set to Whitelist	51
Web and Application Control	54
Control Mode	54
App Specific Network Blocking	60
Anti-Theft Policy	61
Additional Settings Policy	63
Password Policy	64
Device Oriented Policy	65
Required Applications Policy	
Importing an application	
Deleting an application from Required Applications Policy	67
Wi-Fi Settings Policy	68
Enable Wi-Fi Restrictions (For devices with Android version below 6.0)	
Adding a Wi-Fi SSID	69
Deleting a Wi-Fi network SSID	69
Lock/Sound alarm	70
Scheduled Backup (Contacts & SMS)	71
Creating a schedule	71
Modifying a schedule	72
Deleting a schedule	
Content Library Policy	
Import a file	
Klosk Mode Policy	
Application(s) to be added to Kiosk	
Whitelist for apps	
Allow User to Turn ON/OFE	
Installation of eScan Kiosk Lockdown Application	
Location Fence	
iOS Templates	93
Device Passcode Policy	94
Petrictions Policy	
Device Europeitre	
Weh Clin Policy	
Adding a Wah Clin	
Deleting a Web Clip	
Email Policy	
Adding Email policy	101
- $        -$	





Deleting an Email Policy	105
WiFi Settings Policy	106
Adding a WiFi Settings Policy	106
Deleting a WiFi Settings Policy	107
Content Library Policy	108
Importing a file	108
Deleting a file	108
Importing on application	109
Deleting an application	110
Group Tasks	111
Creating a New Group Task	111
Common OR Code Scan	
COD/BYOD Enrollment on Android Device(s)	
Installation and Enrollment of Android device in MDM Group	114
Adding a device to the console	114
Enrolling the added device to MDM group	115
Differences between COD and BYOD group	123
Installation and Enrollment of Android device to BYOD Group	124
Installation and Enrollment of Android device to COD Group	134
Installation and Enrollment of iOS Device	143
Adding a device to the console	143
Enrolling the added device	144
Policy comparison of MDM, COD and BYOD Group Types	153
Restriction Policy	154
WiFi Configuration	156
System Updates	158
Manage Backup	160
Taking a backup from devices to the server	160
App Store	162
Adding an Android application with In-House Apps (Android) option	162
Adding an Android application with Play Store Apps (Android) option	163
Adding an iOS application from iStore Apps	164
Deleting an application from the App Store	165
Anti-Thett	166
Wipe Data	166
Block Device	167
Unblock Device	168
Scream	168
Send Message	168
	169
Remove Work Profile	170
Factory Reset	170
Lock Device	170
Asset Management	171
Hardware Information	171
Viewing Hardware information	171
Application information	1/5





Export Options for the Generated Reports	
Exporting a Report	
Report Templates	
Creating a Report Template	
Editing a Report Template	
Deleting a Report Template	
Viewing a Report	
Report Scheduler	
Adding a Scheduler	
Template Selection	
Selection For Applied Groups/Clients	
Report Send Options	
Report Scheduling Settings	
Running a schedule	
Editing a Schedule	
Deleting a Schedule	
Viewing the report	
Viewing results of a report	
Events and Devices	
Viewing Events	
Event Status	
Device Selection	
Application/Hardware Changes	
Events and Devices settings	
Settings	
Enterprise Configuration	190
Certificate Management	
Email Notification Settings	
Data Purge	
Server Configuration	
Console Settings	
Two-Factor Authentication	196
Enabling 2FA login	197
Disabling 2FA login	
Adding Users for 2FA	
Event Alert	
UnLicense Alert	
Content Library	
Adding a file	
Editing a file description	
Deleting a file	
Call Logs 🛄	
Filter Call Logs	
Exporting Call Logs	
Data Usage 🔢	
Filter Data Usage logs	





Exporting Data Usage logs	
History 💼	211
Location History	
Battery Status/Signal Strength	
Geo Fence History	
App Usage History	
Fencing Location(s)	
Creating a Fencing Location	
Editing a Fencing Location	
Deleting a Fencing Location	
View On Map	
Import Locations via file	
Administration	
User Accounts	
Creating a User Account	
Adding a User from Active Directory	
Deleting a User Account	
User Roles	
Adding a User Role	
Role Properties	
Deleting a User Role	
Export & Import	
Export Settings	
Import Settings	
Scheduling	
License	
Adding and Activating a License	
Moving licensed devices to Non-Licensed Devices section	
Moving non-licensed devices to Licensed Devices section	
Contact Us	
Forums	
Chat Support	
Email Support	





## Introduction

eScan Enterprise Mobility Management (EMM) introduces a comprehensive mobile security solution helps organizations to maintain compliance while minimizing IT intervention and efforts. EMM introduces a single centralized platform to secure data from diverse range of mobile devices. From the same platform, it allows you to enforce the security policies for mobile devices connected to organizations network.With policy-based controls and sophisticated threat protection; it allows you to proactively enable mobile productivity without compromising security.

EMM's Backup module keeps the backup of all data from the enrolled devices to mitigate the risk of data loss in case of device has been formatted, upgraded or reset. It also allows restoring the backed up data through the management console as per requirement. User can keep track on all hardware as well as software resources available on devices connected within network using an Asset Management module of eScan EMM, additionally it allows to filter and export the captured information of hardware as per need.

It will allow an administrator to 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 locked automatically or raised an alarm, if it is not connected to any of the listed Wi-Fi network connections. An administrator can restrict web and application access on the device within the office perimeter by restricting personal browser and personal apps through ADP deployment and geo fencing policy.

Through Anti-Theft module of it has chances of recovering device or data in case of lost that prevents the misuse of it. To recover the data or device admin can remotely execute commands such as Data Wipe, Block, Scream, Locate and Send Message to the stolen device.

Following are the benefits of MDM (Mobile Device Management):

- Deploy, manage, and protect Company-Owned Devices (COD) and Bring Your Own Devices (BYOD).
- Implement various device controls on user's device without handling it physically.
- Secure data and resources, enhance user productivity, reduce costs, and maintain communications.
- 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.
- User will be able to access only the whitelisted applications, while all other third-party applications will be blocked.
- Facilitate call and SMS filtering for enrolled devices.





## **System Requirements**

#### For Android

#### (Android Endpoints) Platforms Supported:

- Android version: 7.0 and above
- Storage: 50-60 MB

#### For iOS

#### (iOS Endpoints) Platforms Supported:

- iOS version: 12.0 and above
- Storage: 50-60 MB

**OVE** Rooted and Jailbroken devices are not supported.

## **Getting Started**

• Click **eScan Mobility Management** in the Navigation Panel. Select Platform prompt appears.

Select Platform		
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, click **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, click **Email Notification Settings** tab. These settings should be configured at start as they help administrator receive notifications.

Learn more about Email Notification Settings, click here.





## Dashboard

The Dashboard displays eScan EMM application's real-time Deployment Status, Protection Status and Protection Statistics for managed devices.



### **Deployment Status**

This tab displays detailed pie chart view and statistics of the following:

- Enrollment Status
- eScan Status
- eScan Version (Android MDM App)
- eScan Version (Android eScan EMM App)
- eScan Version (iOS MDM App)
- Android Version
- iOS Version
- Device Sync Status (Successful)
- Device Compliance
- Kiosk Status





#### **Enrollment Status**



Enrolled – It displays the number of devices that are enrolled.
Not Enrolled - It displays the number of devices that are not enrolled.
Container – It displays the number of devices on which Container application is not enrolled.

#### 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.

#### eScan Version (Android - eScan EMM App)



**Version Numbers** – It displays the eScan EMM application's version number installed on devices. **Unknown** – It displays the number of devices on which the eScan EMM 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 on 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.





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



#### 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 signature update status is Unknown.







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.



### 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.





#### 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.





### **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

Deployment Status	Protection Status	Protection Statistics	]		
			Since L	ast 7 Days	
	Anti-Vi	us			Web Control
		Skipped Deleted Total	1 1 2		Allowed <u>1</u> Blocked <u>1</u> Total <u>2</u>
	Application	Control			Call Statistics
		Allowed Blocked	<u>10</u> 0 <u>10</u>		Incoming (Allowed) 0 Incoming (Blocked) 0 Outgoing (Allowed) 0 Outgoing (Blocked) 0 Total 0
	SMS Stati	stics			
		Received Sent Total	0 0 0		





Anti-Virus

Anti-Virus	
Skipped Deleted Total	1 1 2

**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.

#### 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.

#### **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.



### of DIGITAL WORLD

### **SMS Statistics**



**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 in all tabs.

1. Click Settings icon

Configure Dashboard Display window appears.

Care Chatra	
escan Status	<ul> <li>eScan Version (Android - MDM App)</li> </ul>
eScan Version (Android - eScan EMM pp)	eScan Version (iOS - MDM App)
Android Version	✓ iOS Version
Device Sync Status (Successful)	Device Compliance
Kiosk Status	
Protection Status	
Update Status	Scan Status
🗹 Anti-Virus	Web Control
Application Control	Call & SMS Filter
rotection Statistics	
Anti-Virus	Web 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 options available in this module:

- Action List
- Client Action List
- Select/Add Columns
- Policy Templates
- Common QR Code Scan
- Refresh Scan Devices

Managed Mobile Devices		P 🕼 ?		
Action List  Client Action List	Select/Add Columns 🗋 Policy Templates Common QR Code Scan	)		
E. Managed Devices	Group Information			
🛄 Policy	LDAP/Active Directory Sync	Not Configured		
Group Tasks	Total Subgroups	0		
Client Devices	Total Devices	0		
Gienc Devices	Group Type	MDM		
	Name			
	Assigned Policy Template: Managed Devices_Policy  View Policy Templa	te		
	Group Tasks			
	Client Devices			

#### Action List

This drop-down lets you take following actions for a group.



Options	Description		
New Group	This option lets you create a new group for categorizing/adding devices.		
Add New Device	This option lets you add new devices to the selected groups.		
Add Multiple Devices	This option lets you import (*.txt, *.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 <b>Note</b> : Do not put space before or after comma in the above format.		





Remove Group	This option lets you remove a group from the Managed Devices.
Change Server IP	This option lets you change the server IP address on the managed device. The new server IP can be allotted to a particular group or list of devices.
Synchronize with LDAP/Active Directory	This option lets you synchronize the managed devices with the source active Directory Organization unit, the minimum sync interval is five minutes and you can also exclude ADS source 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. The Web-blocking, Application Control and many more 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 moves 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

To create a new group, follow the below steps:

- 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 :*			
L			
Group Type:	🔘 мдм		O BYOD
Select Template			
Default_Policy MDM	~		
* Mandatory Field			
		Sav	/e Cancel

- 3. Enter a name for group.
- 4. Select a preferred group type.
- 5. Select Policy Template from drop down list.
- 6. 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.
- Click Action List > Add New Device. Add New Device window appears.





Add New Device [Group Name: Managed Devices]	[Group Type: MDM]
Mobile Number*	Scan above QR code for MDM/iOS enrollment
	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 Add More option will enabled after you add a device. Click **Add More** to add another device in the same group.



#### Adding Multiple Devices

By using Add Multiple Devices option, you can add multiple devices simultaneously to a group by importing details from a .csv or .txt file in the given 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.





d Mu	ltiple Devices
lect	File source
	Select file for import (*.txt,*.csv):
	Choose File No file chosen Upload
	Eg: 9821000000,xyx,xyz@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

- 3. Click **Choose File** and select the **.txt** and **.csv** file consisting required details.
- 4. Click **Upload** and then **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	Cancel

#### 5. Click OK.

	•	Ensure there is no space before or after comma in the above format.
	•	Use a line break to separate each device's information.
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.

After the successful addition, the following window will be displayed.

Add Multiple D	evices	×
**************************************	**************************************	
Total devices Device added Not added	: 1 : 1 : 0	
		Close

All devices from the **.txt** and **.csv** file will be added to the group.





#### Change Server IP

The Change Server IP option allows you to change server IP address of the managed device. The new server IP can be allotted to a particular group or list of devices as configured. To change the Server IP address, follow the below steps:

- 1. Select a group.
- 2. Click Action List > Change Server IP.

Change Server IP Address on device window appears. The IP Address field displays the current IP address of a group.

Change Server IP Address on device(	5)	×
IP Address: 192.1	Change To	]
Apply To	O List of Devices	
Select Group(s)		
	Apply Cancel	

- 3. Select the Change To checkbox 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.
- 6. After you are done making changes, click **Apply**.





Change Server IP Address on device(s)	×
IP Address: 192. Change To 192	
Apply To     Groups     C List of Devices	
Select Group(s)	
Apply Cancel	

The group's or device's IP address will be changed.

#### Properties

The Properties option displays the general information of selected group. It shows the count of groups and devices are present in the particular group.

Properties		×
Properties (Managed Devices)		
General		
Name :	(Managed Devices	
Parent Group :		
Contains :	Groups , Devices	
Group Type:	MDM	
Ok Cancel		
Cancer		





### **Client Action List**

This drop-down lets you take action for the devices added in the console.

Client Action List 🔻
Move to Group
Properties
Remove from Group
Resend Enrollment Email
Change User's name/Email-id
Disenroll

Select a device or devices and take the action of your preference.

#### Moving Device from one group to the other group

After adding devices in a group, you can move a device or devices from one group to other as per your requirement.

To move device(s) from one group to other, follow the steps given below:

1. Select the group in which the device(s) is already added and then click **Client Devices**.



2. Select the device you want to move to another group and then click **Client Action List** > **Move to Group**.

Mobile Number	User's name	QR Code
75 75 5	Device_	<u>View</u>
84 14 17 15	Test_fieldmi_#	<u>View</u>







Select Group window appears.

Select Group	×
⊡ 🔄 Managed Devices	
tent M	
	New Group Ok Cancel

3. Select the group to which you wish to move the device(s) and then click **OK**.

•	You can create a new group by clicking <b>New Group</b> and move the device(s) to that
NOTE	group.





#### Checking a Device Properties

The Properties option lets you check a device's general properties, anti-virus settings, protection status and miscellaneous properties and also policies.

- 1. Select a device.
- Click Client Action List > Properties. The Properties window for the selected device appears.

Properties- User's name: moto Mo	bile No.: 6
General	
Mobile Number	614.111
User's name	milli
Column1	-
Column2	-
Column3	-
Column4	-
Mac Number	84. (B) (B) (m) (cm) (cm) (1)
Email Id	s com
Enrollment Date	2
AV Setting	
eScan Install	Installed
eScan Version	7
Last Connection	20 Aug 2021 06:22 PM
Last Update	20 Aug 2021 04:49 PM
Last Scanned	22 Aug 2021 02:35 PM
Destantion	
Anti-Virus	Enabled
Web Control	Disabled
Application Control	Disabled
Call & SMS Filter	Enabled
Miscellaneous	
Battery Status	81%
WiFi Strength	79%
CIM Cianal Strength	No Network





#### Removing a device from group

The Remove from Group option lets you remove selected device from a group. To remove the device from a group, follow the steps below:

- 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.

e	If a device is removed, all details related to that device are also deleted from the
NOTE	database.

#### **Resending Enrollment Email**

The Resend Enrollment Email option lets you resend an enrollment email to the user who didn't receive it at the time of adding the device.

To send the enrollment email again,

- 1. Select the specific device.
- 2. Click **Client Action List** > **Resend Enrollment Email**. A new enrollment email will be sent to the user.

#### Changing a User's Name/Email ID

The Change User's Name/Email ID option lets you change the name/email ID of a user as per need. To make changes in user's name or email ID,

- 1. Select the specific device.
- 2. Click Client Action List > Change User's name/Email ID.





Change Details window appears.

Change Details	×
Mobile Number	_
75	
User's name*	
Device_	
Email Id*	
ne e com	
OS Type O Android O 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 allow to disenroll a selected device. To disenroll the specific device,

- 1. Select a device.
- 2. 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.

Mobile Number	Anti-Virus	
🕼 User's name	Veb Control	
	Network Block Status	
	Application Control	
	Call & SMS Filter	
	Last Connection	
QR Code	Last Update	
Device Added Date	Last Scanned	
Enrollment Status	Update Server	
C Enrollment Date	Client OS	
Mac Number	Policy Applied Date	
C Email Id	GPS Status	
Kiosk Status	eScan Status	
Battery Status	eScan Version	
WiFi Strength	Emm Version	
SIM Signal Strength		
Last Policy Applied		
IMEI Number		
Carrier		

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

After selecting options as per requirement, click Save.




# **Policy Templates**

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

# Steps for defining Policies for the Group

To define policies for a group, select a group and under selected group, click **Policy**. Group Policy pane appears on the right side.

Managed Mobile Devices				P (\$ ?
Action List 🔻 Client Acti	on List 🔻	Select/Add Columns	Policy Templates	Common QR Code Scan
Managed Devices     Managed Devices     Monaged Devices     Group Tasks     Group Tasks	Group Policy			?
	Assign	ied Template	Date And Time of Assign	ned Template
	Manag	ed Devices_Policy	19 Jul 2021 03:12 PM	

• Click Select Template, it displays a list of available templates.

Select P	olicy Ten	plate		×
Group	Name:	Managed Devices		
Group	Type:	MDM		
Default	_Policy B	/OD		
Default	_Policy C	DD		
Default	_Policy M	DM		
Manag	ed Device	s_Policy		
			 	-
			Select	Cancel

• Click **Policy Templates**, it displays Policy Template screen and lets you create, copy, and assign template to specific group or devices.

licy Template					
New Template     Propertie	s 🗊 Delete 🛛 A	ssign to Group(s)	sign 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	-
Managed Devices_Policy	MDM	19 Jul 2021 03:12 PM	19 Jul 2021 03:12 PM	Managed Devices	-





### Creating New Template

To create a new policy template, follow the steps given below:

- 1. Click **Policy Templates**.
- Policy Template window appears.
   Click New Template.

Create Policy Template window appears.

reate Policy Template	×
Policy Template Name:	
ielect Group Type:	l
Android Template 0S 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	

- 3. Enter a name for policy template.
- 4. Select appropriate group type.
- 5. Configure the policy template module-wise.
- 6. Click **Save**.

The new policy template will be created.

# Common QR Code Scan

This option displays the QR code to enroll the device on the management console. To learn more about it, <u>click here</u>.





# **Refresh Scan Devices**

This option allows you to add COD/BYOD device(s) on EMM web console whenever a new user attempts to add and enroll the device using Common QR Code.

•	The added devices will be displayed under the AutoAdded groups with their respective
NOTE	group types.

# Window Buttons

The Managed Mobile Devices window has following buttons:

- Filter
- Refresh
- Help

**Filter** This button allows you to search the managed device(s). Additionally you can export the list of filtered device(s). It also allows you to take necessary actions on the filtered device(s) using **Anti Theft Action List** and **Client Action List**.

rch Device(s)	
Anti Theft Action List 🔻 📔 Client Actio	m List *
Filter Criteria	- Export Options
Mobile Number User's name QR Co	de Device Added Date Enrollment Status Enrollment Date Group IMEI/Android ID Mac Number
Mobile Number User's name QR Co	de Device Added Date Enrollment Status Enrollment Date Group IMEI/Android ID Mac Number
Mobile Number User's name QR Correct and the second	de Device Added Date Enrollment Status Enrollment Date Group IMEI/Android ID Mac Number
Mobile Number User's name QR Co are are no items to show in this view.	de Device Added Date Enrollment Status Enrollment Date Group IMEI/Android ID Mac Number
Mobile Number User's name QR Co are are no items to show in this view.	de Device Added Date Enrollment Status Enrollment Date Group IMEI/Android ID Mac Number
Mobile Number User's name QR Co	ode Device Added Date Enrollment Status Enrollment Date Group IMEI/Android ID Mac Number
Mobile Number User's name QR Co	ode Device Added Date Enrollment Status Enrollment Date Group IMEI/Android ID Mac Number

You can use this option in three methods as below:

#### Method 1: Using User's name/Mobile Number:

1. In the Search Devices window, click on **Filter Criteria** drop-down. The Search Devices window expands with Filter Criteria options.





Filter Criteria	
User's name/Mobile Number:	Find Now
Note:	
1. Blank search will display result for all dev	vices.
Search Groupwise	
Select subgroups on selecting Parent g	roup
Custom Column Check	
All O Enrolled O Not Enrolled	

- 2. Enter User's name/Mobile Number in the provided field.
- 3. Click on **Find Now** button. The device will be displayed in the list in same window.

#### Method 2: Using the checkbox Search Groupwise to search the device(s):

- 1. In the Filter Criteria options, select the checkbox **Search Groupwise** to search the device(s) from particular group(s) or subgroup(s). The group tree appears.
- 2. Select the group(s)/subgroup(s).
- 3. Click on **Find Now** button. The device(s) will be displayed in the list in same window.

# **Method 3:** Using the checkbox **Search subgroups on selecting Parent group** to search the device(s):

- 1. In the Filter Criteria options, select the checkbox **Search subgroups on selecting Parent group** to search the device(s) from parent group(s).
- 2. Select the Parent group(s). All the subgroup(s) will be selected automatically wherein you can deselect particular subgroup.
- 3. Click on **Find Now** button. The device(s) will be displayed in the list in same window.

Method 4: Using the checkbox Custom Column Check to search the device(s):

- 1. In the Filter Criteria options, select the checkbox **Custom Column Check** to search the device(s) based on their enrolment status.
- 2. Select the group(s)/subgroup(s).
- 3. Click on **Find Now** button. The device(s) will be displayed in the list in same window.

This option allows you to export the list of filtered device(s). Follow the steps mentioned below to export the list of device(s):

1. After filtering the device(s), click on **Export Options** drop-down. The Search Devices window expands with Export Options and the list of filtered device(s).





F	ilte	r Criteria Options				<ul> <li>Export Options</li> </ul>			
0	Ex	cel	C	PDF		HTML			Export
				and the set of the		<b>1 - 10</b> of 13	H   page 1 of 2	▶ H Rows per page	: (10 🗸
4	Mo	bile Number	User's name	QR Code	Device Added Date	Enrollment Status	Enrollment Date	Group	IMEI/Andr
2	-	6444	()	<u>View</u>	16 Feb 2021 05:00 PM	Enrolled	16 Feb 2021 05:15 PM	Merrie	A) Internet
2		1343434343	elicar Tax Drift	<u>View</u>	18 Jan 2021 08:44 AM	Not Enrolled		eSian (DH) dama	•
2	-	1234067788	Bandiat	View	21 Aug 2021 05:03 PM	Enrolled	26 Aug 2021 05:14 PM	Managed Designation	
2		121436.9888	White HE	<u>View</u>	05 Apr 2022 12:32 PM	Enrolled	05 Apr 2022 12:42 PM	Summer	864-141-0
3	-	8454255478	NAME ADDRESS	View	30 Jan 2023 10:36 AM	Not Enrolled		xya_letter	-
2		912442344733	Back Hots	View	05 Apr 2022 02:01 PM	Enrolled	05 Apr 2022 02:19 PM	contactorization	35

- 2. Select the preferred export format from Excel, PDF, or HTML.
- 3. Select the device(s).
- 4. Click on **Export**. The list will be exported in the selected format.

**Refresh :** This button refreshes the entire window.

**Help** This button redirects you to the eScan Help page in a browser.





# **Android Templates**

olicy Template Name:		5
elect Group Type:	(MDM V)	
Android Template iOS Te	mplate	
Anti-Virus Policy		
Call & SMS Filter Policy		
• Web and Application Co	itrol	
App specific network blo	cking	
Anti-Theft Policy		
Additional Settings Police	y	
Password Policy		
Device Oriented Policy		
• Required Applications P	licy	
• WiFi Settings Policy		
Scheduled Backup (Cont	acts & SMS)	
Content Library Policy		
Kiosk Mode Policy		)
Location Fence		

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

0

NOTE

The features/options in each policy may vary depending upon the group type selected.





# Anti-Virus Policy

Anti-Virus Policy lets you scan the device, schedule a scan and update the virus signature database as per your requirement.

nti-Virus Policy			
S C			
- Scan Settings			
Protection	Enabled 🗸		
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 💙		
Update Day	Sunday 🗸		
Update Time	13:00		
✓ Update from Internet server			
Update only if Wi-Fi is available			
Note: These option are not applicable for MDM apk version 7.0.2.2	4 and above. Container apk version 7.0.2.3 and above.		

Configuration options of Anti-Virus policy are as follows:

Options	Description
Scan Settings	Using this option, administrator can define settings for enabling or disabling virus protection on devices along with settings of file types to be scanned on managed devices.
Protection Scanning for files on installation is enabled	Select <b>Enabled</b> or <b>Disabled</b> to enable or disable protection on managed devices in the group.
Scan Type	Select the appropriate scanning option either <b>All Files</b> or <b>Executable Only</b> .
Automatic Scan	Use this option to scan devices on startup or schedule the scan as per requirement.
Startup Scan	Select from drop-down to enable or disable scanning on device startup, as per your requirement.
Schedule Scan	Select a schedule to scan managed devices. You can conduct a weekly or daily scan as required or even disable the scan schedules.





Scan Day	Select a particular day of the week to scan the managed devices present in the group. This checkbox will be activated only if you select weekly scan option.
Select Scan Time	Set time for scanning the managed devices in the group.
Schedule Update Settings	Define settings for updating eScan on managed devices.
Schedule Update	Define a schedule to update virus signature database on a daily or weekly basis or disable the update schedule.
Update Day	Select a particular day of the week to update the managed devices present in the group. This checkbox will be activated only if you select weekly update.
Update Time	Set time for the devices to take virus signature database update from the server. It will be helpful in saving network congestion where large numbers of devices are added in the MDM Server.
Update from Internet server	Select this checkbox to update the virus signature database from the Internet server.
Update only if Wi-Fi is available	Select this checkbox to update virus signature database only if the Wi-Fi connection is available.





# Call & SMS Filter Policy

The Call & SMS Filter Policy lets you to set filter incoming calls, text messages and outgoing calls on managed devices.

▼ Call & SMS Filter Policy
Call & SMS Filter (Incoming)
Call & SMS Filter Mode Both List 🗸
Allow Contacts Allow incoming calls and SMS from numbers in Contacts
Block Non Numeric SMS and Calls SMS and Calls from Non Numeric numbers are blocked
Blacklist Whitelist
Call Filter (Outgoing)
Call Filter Mode Off 🗸
Whitelist
Send Call Details to Server, including Call/SMS filter events

### Call and SMS Filter Mode set to Off



If the Call and SMS Filter Mode is set to **Off**, all calls and text messages will be allowed.





# Call and SMS Filter Mode set to Blacklist

Call & SMS Filter (Incoming)					
Call & SMS Filter Mode Blacklist 🗸					
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					

- Select **Block Non-Numeric SMS and Calls** checkbox 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		X
Add Delete Remove Al		
Blocked Phone Number	Filter Forbidden Text	-
		-
	-	
		lose

• Click Add.





Block Incoming window appears.

- Select whether to block SMS, Calls or both Calls & SMS.
- Enter the blocked phone number and forbidden text in the respective fields and then click **Add**.

Call & SMS Blacklist			X	
Add Delete Remove All				
Blocked Phone Number	Filter	Forbidden Text	-	
981.1154.141	Calls & SMS	-		
86 86 86 86 8	Calls	-		
74 14 14	SMS	dear-		
			-	
			Close	

• To delete a specific number from the Blacklist, select the number and click **Delete**.





ilter	Fashidan Tast
	Forbidden Text
alls & SMS	-
alls	
MS	dear
	alls MS

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



• Select Allow Contacts checkbox and then click Whitelist.





Call and SMS Whitelist window appears.

Call & SMS Whitelist			×
Add Delete Remove All			
Allowed Phone Number	Filter	Allowed Text	•
			-
			Close

• Click Add.

Allow Incoming window appears.

Allow Incoming	I	X	3
● SMS	Calls	Calls & SMS	
Allowed Phone	Number		
Allowed Text			
Noto: Wildowd @	6 will be recented in	"Allowed Phone Number" field	
Note: Wildcard 9	o will be accepted il	Allowed Phone Number Tiela.	
		Add Close	

• Select whether to allow SMS, Calls or both Calls & SMS.





• Enter the allowed phone number and forbidden text in the respective fields and then click **Add**.

Il & SMS Whitelist Add Delete Remove	All		
Allowed Phone Number	Filter	Allowed Text	*
97#1110#1	SMS	hell+	
78 - 1	Calls	-	
87et 11.1et	Calls & SMS	-	
			-
			Clos

• To delete a specific number from whitelist, select the number and click **Delete**.

l & SMS Whitelist			
Add Delete Remove A	All		
Allowed Phone Number	Filter	Allowed Text	-
97	SMS	heli	
78	Calls	-	
87411111	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

Call & SMS Filter (Incoming)
Call & SMS Filter Mode Both List 🗸
Allow Contacts Allow incoming calls and SMS from numbers in Contacts
Block Non Numeric SMS and Calls SMS and Calls from Non Numeric numbers are blocked
Blacklist Whitelist

Select **Allow Contacts** and **Block Non-Numeric SMS and Calls** checkboxes, you will be able to access both Blacklist's and Whitelist's features simultaneously.

### Call Filter (Outgoing) Mode set to Off

Call Filter (Outgoing)	
Call Filter Mode Off 🛛 🗸	
Whitelist	

If Call Filter Mode is set to Off, all outgoing calls will be allowed.

# Call Filter (Outgoing) Mode set to Whitelist

Call Filter (Outgoing)
Call Filter Mode Whitelist 🗸
Whitelist

If Call Filter Mode is set to Whitelist, a user can make outgoing calls only to whitelisted numbers.





#### • Click Whitelist.

Outgoing calls window appears.

Outgoing calls	×
Add Delete Remove All	
Allowed Phone Number	-
	_
	Close

• Click **Add**.

Allow Outgoing window appears.

Allow Outgoing	×
[	
Allowed Phone Number	_
Note: Wildcard % will be accepted in "Allowed Phone Number" field.	
Add	Close

• Enter the allowed phone number and then click **Add**.

0	lutgoing c	alls	×
	Add	Delete Remove All	
		Allowed Phone Number	<b>^</b>
		98	
			*
			Close

The number will be added to the Whitelist.





• To delete a specific number, select a number and then click **Delete**.

Outgoing	calls	×
Add	Delete Remove All	
	Allowed Phone Number	·
	98-413-411	
		~
		Close

The number will be deleted.

• To delete all the numbers at a time, click **Remove All**.

Send Call Details to Server, including Call/SMS filter events

**Send Call Details to Server, including Call/SMS filter events**: Select this checkbox to send information of the call details to the server with both filter events.





# Web and Application Control

Web and Application Control policy lets you allow and block applications and websites on managed devices as per requirement.

ntrol Mode (Website V)			
Illow / Block Website categories			
Category Name	Allow	Block	-
Select All			
Advertisements and Popups	۲	0	
Alcohol and Tobacco	0		
Anonymizers	0		
Arts	۲	0	-
Botnets	0	0	-

#### **Control Mode**

Allow or Block Applications/Website or Both or disable based on your requirement and Policies.

#### **Control Mode set to Off**



If the Control Mode is set to Off, you cannot allow/block websites and applications.





#### **Control Mode set to Website**

Setting the control mode as a Website, lets you allow and block website categories.

ntrol Mode Website V			
llow / Block Website categories			
Filter Categories			
Category Name	Allow	Block	<u> </u>
Select All			
Advertisements and Popups	۲	0	
Alcohol and Tobacco	0	0	
Anonymizers	0	0	
Arts	۲	0	
Botnets	0	0	-

Allow List: Websites added to this list can be accessed in browser. You can modify and delete websites from the list as per need.

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	
	<b>.</b>
Clos	e

• Click Add.





Add in allow list window appears.

Add in allow list	×
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 can be blocked in browser. You can modify and delete websites from the list as per need.

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	
	*
	Ψ
Clos	ie i

• 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.

▼ Web and Application Control		
Control Mode Application 🗸		
Allow / Block Application List		

• Click Allow/Block Application List.





Allow/Block Application List window appears.

Allow / Block Application List				×
Note :				
<ol> <li>Apps added to the below list will be Allowed/Blocked as per action specified.</li> <li>System apps will be Allowed by default unless explicitly added to "Block" action.</li> <li>User Installed apps will be Blocked by default unless explicitly added to "Allow" action.</li> <li>If action is set to "Ask Uninstall" the device will prompt the User to uninstall the App and will App is uninstalled.</li> <li>If "Ask Uninstall" action is set for System App, the app will be Blocked and will have no effect</li> </ol>	l remain "N t on Device	Ion-Compli e Complian	ant" until the	
Select Applications	+ 4	dd	Select All	
Delete			Count: 0	
Application Name	Allow	Block	Ask Uninstall	
Select All				
<b>Note:</b> If Application is NOT in the "Available Applications" list, you can add the package name wit Enter Package Name:	h the "Ente	er Package	Name" option.	
	+	Add	I	
			Clos	e

- Select an applications from the drop-down menu and click Add.
- Click on **Select All**, to select an available application in one click.
- To delete a particular application, select an 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 an application and will remain "**Non-Compliant**" until an application is uninstalled.
- 5. If "**Ask Uninstall**" action is set for the system applications, applications will be blocked and will have no effect on the device compliance.

Ð	If Application is NOT in the "Available Applications" list you can add the package
NOTE	name with the "Enter Package Name" option.

- Enter an 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**

Allow	Block	<b>A</b>
۲	0	
0	0	
0	0	
۲	0	
	Allow	Allow Block

Setting the control mode to **Both**, lets you allow/block website categories and applications.





# 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:	
Delete Remove All	
Package Name	
	-

• In the Enter Package Name field, enter 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.

<b>OVEN</b> VPN permission is necessary to work this functionality.	
---	--

To delete a package from the list, select the specific package and then click **Delete**.

A

To remove all packages at a time, click **Remove All**.





# Anti-Theft Policy

Anti-Theft Policy lets you keep track of a device's location history, block a device and sends alert about SIM card change in case of lost or stolen.

Anti-Ti	Theft Policy	
🗸 En:	nable Anti-Theft	
Loca	cation History	
	) Enable Location History	Interval 30 Mins 💙
	Capture location details - Time based	
	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.
Unir	install Protection	
	Block Device	
	Ask "Admin Access Password" (Do not block device)	
Anu	ti-Theft WIPE Settings	
✓	Delete all configured email accounts	
	) Delete specific domain account	
	Enter domain names:	
Not	the Add domain name in comma constant format	
eg.	. yourcompany.com, gmail.com, yahoo.com	
- Sim	n watch eattinge	
0	) and and entities as CTM and shares	
	) Send SMS notification on SIM card change	
	To Mobile No.:	
	Send Email potification on SIM card change	
	joena emaintación on osis euro enange	
	Administrator Email Id:	
	U Custom Email Id:	

Options	Description
Enable Anti-Theft	Select this checkbox to enable Anti-Theft feature. By default, this checkbox is selected.
Enable Location History	Select this checkbox to track the location history. <b>NOTE</b> : Location coordinates will be captured by the device only during the selected time slots.
Interval in Minutes	Track the location history in a defined interval. You can set the interval using <b>Interval</b> field between 15 minutes to 24 hours.
Configure	Select the time slot to capture the location coordinates as per requirement.





Show GPS alert block screen	Select this checkbox to show the GPS alert and lock the screen. <b>NOTE</b> : "Screen Overlay" permission should be enabled on the device in order to work this option.
Block Device	Select this option if you want the device to be blocked, if a user tries to uninstall the MDM application.
Ask "Admin Access Password" (Do not block device)	Select this option if you don't want the device to be blocked, if a user tries to uninstall the MDM application. The application will ask user to enter an Admin Access Password to uninstall the application.
Delete all configured email accounts	Select this checkbox to delete all email accounts configured on the managed device.
Delete specific domain account	Select this checkbox to delete email accounts of specific domain. After selecting this checkbox, enter the domain name in <b>Enter</b> <b>domain names</b> field. <b>NOTE</b> : Domain Names are separated by comma.
Send SMS notification on SIM card change	Select this checkbox to receive a text message informing about SIM card change. The text message will be sent to the number added by you. Add the desired number in <b>To Mobile No.</b> text box.
Send Email notification on SIM card change	Select this checkbox to receive an email informing about SIM card change. The notification email will be sent to the administrator's email ID or custom email ID that the administrator has specified in <b>Custom Email Id</b> field.





# **Additional Settings Policy**

Additional Settings policy lets you configure the notification and sync settings.

Additional Settings Policy		
Show Notification	Notifications will be shown	
Sound	Sound notifications for application events	
□ Write Logs ┌ Sync Settings	Write user actions to the eScan Log File	
Sync at Device Reboot	Sync Everytime When Device Reboots	
Sync Frequency 60 Mins 💙	Policy Data Collection Frequency	

Use below options to configure Additional Settings policy.

Options	Description
Show Notification	Selecting this checkbox will display all notifications on devices.
Sound	Selecting this checkbox will play notification sound for eScan MDM application events.
Write Logs	Selecting this checkbox will enable MDM application to write extensive logs to the eScan log file.
Sync at Device Reboot	Selecting this checkbox will sync the device with the eScan server after it reboots.
Sync Frequency	You can set the Sync Frequency in minutes and let the device sync with the eScan server. Allow to set the sync frequency between 15 minutes to 24 hours.





# **Password Policy**

The Password Policy lets you define Administrator Access Password that allows an authorized user to configure settings of eScan modules on respective managed devices. It also has the option to set password on a device as well as on the Work profile created on a device.

	- 02
Admin Access Password	••••
Show Password	
Note: Password has to be numeric and n	ninimum 4 digits are required.
Note: Password has to be numeric and m Device Password Policy	ninimum 4 digits are required.
Note: Password has to be numeric and m Device Password Policy Select Password type:	ninimum 4 digits are required. None
Note: Password has to be numeric and m Device Password Policy Select Password type: Work Profile Password Policy	ninimum 4 digits are required. None

#### **Admin Access Password**

Enter the password in Admin Access Password field.

• Show Password: Select this checkbox to see the entered Admin Access Password in plain text format for confirmation purpose.

#### **Device Password Policy**

Select and define the device password based on below available password types:

- 1. Any
- 2. Numeric
- 3. Numeric Strong
- 4. Alphabetic
- 5. Alphanumeric
- 6. Complex

#### Work Profile Password Policy

Select and define the device password based on below available password types:

- 1. Any
- 2. Numeric
- 3. Numeric Strong
- 4. Alphabetic
- 5. Alphanumeric
- 6. Complex

**NOTE** 

The password should be numeric and minimum of four digits in length.





# **Device Oriented Policy**

Device Oriented Policy lets you enable GPS and disable Camera, Bluetooth, and USB Connectivity on a device.

▼ 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 USB Connectivity (For devices with Android version below 4.0)	
Set Device Block : Days : 0 🗘 Hours : 0 🗘	

Options	Description		
Enable GPS (For devices with Android version below 4.0)	Select this checkbox to enable GPS service.		
Disable Device Settings	Select this checkbox to block the access to Android Settings. <b>NOTE</b> : 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 checkbox to disable the use of camera.		
Disable USB Connectivity (For devices with Android version below 4.0)	Select this checkbox to disable USB Connectivity.		
Set Device Block	Select the days and time to block the device between specified time period.		





# **Required Applications Policy**

The Required Applications Policy lets you import applications from the App Store module to install it on devices in the group through policy deployment.

Required Applications Policy					
± Import 🗊 Delete					
Application Name	Application Id	Арр Туре	Version	Added On	
4					÷

# Importing an application

To import the application, follow the below steps:

1. Click Import.

Import Application window appears.

🛓 Import 🗊 Delete					
Application Name	Package Name	Арр Туре	Version	Added On	1
eScan Device Management	com.eScan	In-House	7.2 0 22	25 mm 2022 01:55 PM	
4					- F -

- 2. Select an application(s) from the Available applications list.
- 3. Click Save.

The selected application will be imported.

A pop-up message appears.







#### 4. Click **OK** to exit.

<b>Provide a provide a provi</b>	<b>9</b> NOTE	If the device is not connected to Internet, the policy changes will be applied on the next sync with the server. By default, the device(s) sync with the server every 60 minutes. If an application is deployed via the Required Application Policy, the device(s) in the group receive a notification to install the application. The user will be provided with the option to start an 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:

1. Select an application and then click **Delete**.

Required Applications Policy	1				
🛓 Import 🗊 Delete					
Application Name	Application Id	Арр Туре	Version	Added On	-
🗹 eScan Mobile Security	com.eScan	Play Store	-	04 Jan 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 checkbox to allow device to connect only to the listed WiFi network name (SSIDs). This option is available only for devices with Android version below 6.0.

WiFi Settings Policy		
Disable WLAN / WiFi		
WiFi Restrictions		
Enable WiFi Restrictions (For devices	with Android version below 6.0)	
Note: Device(s) will be allowed to conn	ect 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 alarn	n when NOT connected to either of the listed WiFi network name (SSIDs)	
+ Add 🗊 Delete		
WiFi Network Name (SSIDs)		-
		-





### Adding a Wi-Fi SSID

#### To add Wi-Fi SSID:

1. Select the checkbox **Enable Wi-Fi Restrictions** and then click **Add**. Add window appears.

Add	×
Enter WiFi network name (SSIDs):	
Note: WiFi network name (SSID) are case sensitive	
Add	incel

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.

Wi-Fi network name are case sensitive.NOTEThe devices will be allowed to connect only to the added Wi-Fi network SSID.

### Deleting a Wi-Fi network SSID

To delete the added Wi-Fi network SSID:

1. Select a particular Wi-Fi network SSID and then click Delete.

+ Add 🗊 Delete
✔ WiFi Network Name (SSIDs)
V automatic

A confirmation prompt appears.



#### 2. Click OK.

The Wi-Fi network SSID will be deleted.





### Lock/Sound alarm

Select the appropriate option to give alert of device is not connected to the listed Wi-Fi networks.

1. Select the checkboxes **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)	·
automatio	
	-
4	•
	Save 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.





# Scheduled Backup (Contacts & SMS)

The Schedule Backup (Contacts & SMS) policy lets you take a backup of all the contacts from a device as per your requirements. The backup can be scheduled on daily/weekly basis.

•	Scheduled Backup (Contact	ts & SMS)		
	+ Add 🔳 Modify	jj Delete		
	🔲 Job Name	Schedule Type	Schedule Time	<b>*</b>
				· ·
	4			•

### Creating a schedule

To create a new schedule:

1. Click Add.

Add new job window appears.

ob Name:	
▼ Job Settings	
– Select Backup	
□ sms	
Contacts	1
Job Scheduler Settings	

- 2. Enter a job name.
- 3. In **Job Settings** section, select the preferred backup(s) option.





Add new job	×
	1
Job Name:	
Job Settings	
▼ Job Scheduler Settings	
Opaily	
O Weekly Mon Tue Wed Thu	
Fri Sat Sun	
Disable Schedule	
At 05:30	
Save Cancel	

- 4. In **Job Scheduler Settings** section, select whether you want to take a backup Daily, Weekly or want to disable schedule.
- 5. Set the specific time at which you want to take the backup and then click **Save**. The schedule will be created as per the configuration.

# Modifying a schedule

To modify a schedule:

1. Select the specific schedule and then click **Modify**.

+ Add 📗 Modify 🗊 Delete						
<b>~</b>	Job Name	Schedule Type	Schedule Time		*	
<ul> <li>Image: A set of the s</li></ul>	demm	Daily	05:30			
					Υ.	
				×.		




Modify backup job window appears.

Job Settings	
Job Scheduler Sett	ings
Daily	
O Weekly	Mon Tue Wed Thu
O Disable Sched	ule
At 05:30	•

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	-
✓ d====	Daily	05:30	
4			F T

A confirmation prompt appears.



2. Click OK.

The schedule will be deleted.





# **Content Library Policy**

The 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:

- 1. Click Import.
- 2. Select the file and then click **Save**.

Import Files		×
Available Files	Total: 1	
File Name	Added On	
ED#_familierarif_fil.doc	20 Jul 2021 12:58 PM	
		Save Cancel

The file will be imported.

3. 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

The Kiosk Mode policy, allows admin to control the usage of devices within organizations by limiting the device functionalities that keep employees focused on work. It lets you run a device in Single App Mode even if multiple apps are installed. Furthermore, admin can restrict the hardware key controls such as volume and power buttons on the enrolled devices to the kiosk mode.

Kiosk Mode Policy			
Enable Kiosk Mode			
Application(s) to be added to Kiosk			
Use Single App Mode			
	~		
		Count: 0	
Application Name			-
4			
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 checkbox.

## Application(s) to be added to Kiosk

This section allows an application to be accessed in Kiosk mode.

### **Use Single App Mode**

Select this checkbox to use kiosk in single app mode. The Kiosk Mode Policy lets you run a device in Single App Mode wherein the only one app will run even if multiple apps are installed on device. The device user will be unable to exit the application or perform other device activities.

It also provides another option wherein the dropdown menu displays a list of installed applications.

- 1. Select an application and then click **Add**. The application will be added.
- 2. To delete the added application(s) from Kiosk mode, select the application(s) and then click **Delete**. The application will be deleted.

User can only add a single application, if Use Single App Mode checkbox is selected.
 NOTE This option is not enabled if Geo fence checkbox is selected in Location Fence policy.

### 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 required apps.

	+ Add	
ote: .Package names added to the list will be allowed i .These apps will not be visible in Kiosk mode.	f launched from within any other apps added to kiosk mode.	
Delete		
Package Name		
4		

#### **Enter Package Name**

Enter the name of the package and click **Add** to whitelist the particular app. To delete the added application, select application and click **Delete** button.

#### Allow all non-launchable system apps

Select this checkbox if you want to allow the non-launchable system apps to launch from within any other app added to Kiosk mode.



### Hardware Key Control

Kiosk mode also lets you disable a device's hardware keys.

Hardware Key Control Disable Power button Disable Volume buttons

**Disable Power button** – Selecting this checkbox disables a device's Power button. **Disable Volume buttons** – Selecting this checkbox disables a device's Volume buttons.





## Allow User to Turn ON/OFF

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.		

**WiFi** – Selecting this checkbox allows user to turn device's Wi-Fi ON/OFF through Kiosk application.

**Bluetooth** – Selecting this checkbox allows user to turn device's Bluetooth ON/OFF through Kiosk application.

**Volume** – Selecting this checkbox allows user to increase/decrease the device's volume through Kiosk application.

**Brightness** – Selecting this checkbox allows user to adjust the device's brightness through Kiosk application.



Allow Wi-Fi setting	Allow device setting
---------------------	----------------------

### Allow Wi-Fi setting

Selecting this checkbox allows user to access and configure the Wi-Fi settings in the Kiosk mode.

#### Allow device setting

Selecting this checkbox allows user to access and configure the device settings in the Kiosk mode.





## Installation of 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**.



2. After an application gets installed, tap **OPEN**.





After opening the app, Welcome screen appears with End User License Agreement.



3. Tap **OPEN AGREEMENT**. Read it carefully and then tap **ACCEPT**. You will have to grant permissions to the app manually.

•	To run this application, you need to install the eScan Device Management application
NOTE	on the device.





4. 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 applica	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.



 $\bigcirc$  = Toggle disabled

= Toggle enabled



The app permissions may vary depending upon the android version and device manufacturer.





5. Tap 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	>
Please allow all above permissions for this applica	ation to
function properly and a better experience.	
PROCEED	





7. Tap eScan Kiosk Lockdown.



8. Tap **Permit usage access** toggle and then go back.





The option **Permit usage access** maybe **Allow usage tracking** in your device. This option may vary depending upon the device manufacturer and 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	>
eSan	
Please allow all above permissions for this app function properly and a better experience	blication to ce.
PROCEED	

10. Tap **Allow modifying system settings** toggle and then go back.







### 11. Tap Allow to write DND setting.

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
PROCEED	
PROCEED	





12. Tap eScan Kiosk Lockdown.



13. Tap Allow Do Not Disturb toggle.







A prompt appears. 14. Tap **ALLOW** and then go back.

> 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.

#### 15. Tap Device Admin Permission.

Permit Drawing Over Other Apps  App Usage Access  Write Setting Permission  Allow to write DND setting  Device Admin Permission  Allow app installation permission  Second	eScan Kiosk Lockdown	
App Usage Access <ul> <li>Write Setting Permission</li> <li>Allow to write DND setting</li> <li>Device Admin Permission</li> <li>Allow app installation permission</li> <li>Allow app installation permission</li> </ul> Please allow all above permissions for this application to function properly and a better experience.	Permit Drawing Over Other Apps	~
Write Setting Permission  Allow to write DND setting Device Admin Permission Allow app installation permission	App Usage Access	~
Allow to write DND setting  Device Admin Permission  Allow app installation permission	Write Setting Permission	~
Device Admin Permission       >         Allow app installation permission       >         ESean       *         Please allow all above permissions for this application to function properly and a better experience.       *	Allow to write DND setting	~
Allow app installation permission	Device Admin Permission	>
Please allow all above permissions for this application to function properly and a better experience.	Allow app installation permission	>
function properly and a better experience.	Please allow all above permissions for this at	polication to
	function properly and a better experie	nce.





#### 16. Tap Activate this device admin app option and then go back.



Uninstall app





17. Tap Allow app installation 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 applic function properly and a better experience.	ation to

18. Tap **Allow from this source** toggle and then go back.







	eSean	
	Kiosk Lockdown	
Sele	ect eScan Kiosk Lockdown as your Home	арр
Select	a Home app	
1	eScan Kiosk Lockdown	1
\$	Default Launcher	
	JUST ONCE ALWAYS	2
1	Select eScan Kiosk Lockdown	
2	Tap on ALWAYS	
ote: You	n may not be able to make an emer	gency
	OK, GOT IT!	

After all permissions are granted, an instructional image appears.

- 19. Read the instructions in the image and then tap **OK**, **GOT IT!** The application asks you to use eScan Kiosk Lockdown as a Home App.
- 20. Tap ALWAYS.







The device now runs in Kiosk mode and only the apps deployed via Kiosk Mode Policy are visible.





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 Store and install updates manually.

Tapping the menu icon  $\equiv$  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 or 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 an Admin Password.





## Location Fence

The Location Fencing policy allows to define an address on the map and to 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 here</u>.

Import Geo Fencing location(s)				
Geo Fencing				
🛓 Import 📗 🗊 Delete				
Custom Address	Latitude	Longitude	Radius(m)	
				÷
4				

- 1. To configure Location Fencing policy, select Geo **Fencing** checkbox. After enabling this option, you can import and delete the fencing locations.
- 2. Click Import option to select the address and click Save.
- 3. To delete the added address, select the address and click **Delete**.

### Block device when outside of the set fence

1. Select this checkbox to block the device when it is outside the defined fencing location.

If Block device when outside of the set fence is unchecked then device will not be blocked, but only events will be sent to the server.





# **iOS** Templates

Create Policy Template
Policy Template Name:
Select Group Type: (MDM v)
Android Template iOS Template
Device Passcode Policy
Restrictions Policy
Web Clip Policy
Email Policy
WiFi Settings Policy
Content Library Policy
Required Applications
Save Cancel

The iOS Template consists following policies:

- Device Passcode Policy
- Restrictions Policy
- Web Clip Policy
- Email Policy
- WiFi Settings Policy
- Content Library Policy
- Required Applications





## **Device Passcode Policy**

The Device Passcode Policy lets you configure the passcode, auto-lock duration, device lock grace period and data wipe in case of maximum passcode fail attempts.

Select the Enable checkbox to enable all the fields in this section.

▼ Device Passcode Policy		
└ □ Enable		
Allow Simple Value	🔍 Yes 🔘 No	
Require Alphanumeric Value	🔾 Yes 🔍 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 🗸	•

**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 passcode length 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. It can be set between 1 to 50 or can be blank.

**Grace Period for Device Lock**: Grace period is a time duration that ensures the device stays locked until the next passcode entry. This option lets you set the grace period for a device from 1 Minute to 4 Hours.

Maximum Number of Failed Attempts (Before all data is erased): This option lets you set the maximum number of failed attempts allowed for unlocking a device before all data on the device is erased.





## **Restrictions Policy**

The Restrictions Policy lets you apply restrictions on a device.

- Device Functionality
- Application
- Safari Settings
- iCloud
- Security and Privacy
- Content Ratings
- Ratings by Region

### **Device Functionality**

Device Functionality	
Allow Installing Apps	● Yes ○ No
Allow Use of Camera	● Yes ○ No
Allow FaceTime	● Yes ○ No
Allow Screen Capture	● Yes ○ No
Allow Automatic Sync While Roaming	● Yes ○ No
Allow Siri	● Yes ○ No
Allow Siri while device locked	● Yes O 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 ○ No
Allow Voice Dialing	● Yes ○ No
Allow In App Purchase	● Yes ○ No
Force User to enter iTunes Store password	🔿 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 function.

Allow Screen Capture: Set this option to Yes, to allow users to take a screenshot or record their screen.





Allow Automatic Sync While Roaming: Set this option to Yes, to allow users to sync automatically while roaming.

Allow Siri: Set this option to Yes, to allow users to use Siri.

Allow Siri while the device 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 Passbook while the device is locked (iOS 6 and above): Set this option to Yes, to allow the use of Passbook while the device is locked. Learn more about Passbook 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



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 application.





### Safari Settings

Safari Settings	
Enable Autofill	● Yes ○ No
Force Fraud Warning	🔾 Yes 🔘 No
Enable JavaScript	● Yes ○ No
Allow Pop-ups	● Yes ○ No
Accept Cookies	Always 🗸

**Enable Autofill**: Set this option to **Yes**, if you want Safari to remember the information of users entered in the web forms previously.

**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**

- Se	- Security and Privacy-				
00	becancy and Privacy				
Al (i	llow Diagnostic Data to be sent to Apple OS 6 and above)	● Yes ○ No			
A	llow User to accept untrusted TLS Certificates	● Yes ○ No			
Al (i	llow automatic updates to certificate trust settings OS 7 and above)	● Yes ○ No			
Fo	orce Encrypted Backups	🔾 Yes 🔘 No			
Fo (i	orce limited ad tracking OS 7 and above)	⊖ <sub>Yes</sub> ● <sub>No</sub>			
Al (i	llow documents from managed apps in unmanaged apps OS 7 and above)	● Yes ○ No			
A (i	llow documents from unmanaged apps in managed apps OS 7 and above)	● 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**



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.





# Web Clip Policy

The Web Clip policy lets you get important websites on a device's home screen to let users access it quickly.

Select **Enable** checkbox to enable the configuration of Web Clip Policy.

▼ Web Clip Policy	
+ Add 🗊 Delete	
Webclip Policy Name	<b>^</b>
4	

## Adding a Web Clip

To add a web clip policy:

• Check **Enable** and then click **Add**. Web Clip Policy window appears.

Web Clip Policy	×
Web Clip Label *	
URL to be Linked *	
Removal of Web Clip	● Enable ○ Disable
Allow Full Screen	⊖ Yes  ●No
	Save Cancel

- Web Clip Label: Enter a name for the Web Clip.
- **URL to be Linked:** Enter the website URL.
- **Removal of Web Clip**: Set the Web Clip status as either **Enable** or **Disable**. If enabled, the user can remove the Web Clip 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 Web Clip

To delete the existing web clip:

• Select a Web Clip and then click **Delete**.

Enable	
+ Add 🗊 Delete	
Vebclip Policy Name	▲
	-
(	⊢ ⊢ I

The Web Clip policy will be deleted.





# **Email Policy**

The Email Policy lets you set up an email account for the managed devices and define the settings for incoming and outgoing emails.

Check **Enable** to configure the Email Policy

▼ Email Policy		
ſ □ Enable		
+ Add 🗊 Delete		
Email Policy Names		<b>A</b>
		-
(	⊢ F	

## Adding Email policy

To add Email Policy, follow below steps:

1. Check **Enable** and then click **Add**. Email Policy window appears.

Account Name *			
Account Type	IMAP		~
Path Prefix			
User Display Name			
	Note : " "%email appropri mapped	%usemame%" %" will fetch th ate Username/l to the device	or e Email
Email Address			
	Note : " appropria mapped	%email%" will ate Email Addre to the device	fetch the ess
Allow Move	● Yes	O No	
Disable recent mail address sync (iOS 6 and above)	Oyes	No No	

2. Fill the following appropriate details:





#### Account Name: Enter an account name.

Account Type: Set an Account Type as IMAP or POP.

- If choose POP
  - You need constant access to your email, regardless of the Internet availability.
  - You have limited server storage.
- If choose IMAP
  - 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. This field is available only when you select Account Type as IMAP.

**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 Moving. 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.

- 3. Enter the Incoming Mail and Outgoing Mail details.
  - To learn more about Incoming Mail, <u>click here</u>.
  - To learn more about Outgoing Mail, click here.
- 4. After filling the details, click **Save**.





### **Incoming Mail**

- Incoming Mail	
Mail Server *	
Port *	143
Username	
	<b>Note :</b> "%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 an 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 V
Password	
Use Outgoing Password Same as Incoming	⊖ <sub>Yes</sub> ● <sub>No</sub>
Use Only in Mail	⊖Yes ◉No
Use SSL	🔾 Yes 🖲 No

Mail Server: Enter the hostname for Outgoing Mail Server.

**Port**: Enter the outgoing 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 an 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 defined 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.

After making all the configuration, click **Save**.





## Deleting an Email Policy

To delete an email policy, follow the steps below:

1. Select the particular Email Policy from the list.

+ Add 🗑 Delete	
🖌 Email Policy Names	

2. Click **Delete**.

The Email Policy will be deleted.





## WiFi Settings Policy

The WiFi Settings Policy lets you manage how a user connects their devices to a Wi-Fi network. Check **Enable** to configure the WiFi Setting Policy.

▼ WiFi Settings Policy		
Fnable frable framework for the second secon		
Wifi Policy Name		<b>.</b>
		-
4	•	

## Adding a WiFi Settings Policy

To add a WiFi Settings Policy, follow the below steps:

 Click Enable and then click Add. WiFi Settings Policy window appears.

ViFi Settings Policy	×
Wireless Network Identification *	
Automatically Join Network	● Yes ○ No
Hidden Network	🔿 Yes 🖲 No
Security Type	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.

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.



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>.

Select Enable checkbox to configure the Content Library Policy.

✓ Content Library Policy		
Г 🗍 Enable		
± Import 🗑 Delete		
File Name	Updated On	· · · · · · · · · · · · · · · · · · ·
		-
4		

### Importing a file

To import a file from Content Library:

1. Select **Enable** checkbox and then click **Import**. Import Files window appears.

Import Files	×
Available Files	Total: 1
🗹 File Name	Added On
EDIdoc	20 Jul 2021 12:58 PM
	Save Cancel

2. Select a file and then click **Save**. The selected file will be imported.

### Deleting a file

To delete a file from Content Library:

1. Select a file and then click **Delete**.

± Import 👔 Delete	
📝 File Name	Updated On
C ED*_Sectioner#_S*.doc	20 Jul 2021 12:58 PM

2. 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** checkbox and then click **Import**.

▼ Required Applications						
Enable						
± Import 🗊 Delete						
File Name	Updated On	· · · · · · · · · · · · · · · · · · ·				
4						

Import Application window appears.

± Import 🗊 Delete						
Application Name	Package Name	Арр Туре	Version	Added On		*
eScan Device Management	com.eScar	In-House	7.2 0 22	25 mm 2022 01:55 PM		
4					- F.	

2. Select an application(s) to be installed on users' devices and then click **Save**. The application(s) will be imported.





## Deleting an application

1. Select an application and then click **Delete**.

Required Applications		
Enable		
± Import 🗊 Delete		
✓ File Name	Updated On	·
eScan Mobile Security	04 Aug 2021 04:33 PM	
	04 Aby 2021 04.55 PM	
4		
•		

2. The selected application will be deleted.





## **Group Tasks**

The Group Tasks option lets you create and schedule tasks for the devices in a group.

Managed Mobile Devices			P († ?
Action List - Client Action	List 🔻 🛛 Select/Add (	Columns 🛛 🕒 Policy Template	5
Managed Devices	Group Tasks 🖷		?
Group Tasks	🗅 New Task 🕨	Start Task #Properties	🛱 Results 🛛 🥡 Delete Task
	Task Name	Task Performed	Schedule Type

### Creating a New Group Task

To create new group task, follow the below steps:

 Select a group and then click Group Tasks > New Task. The New Task window appears.

ew Tas	c .	
Task N	lame:	
<b>•</b> T	ask Settings	
П	Scan	
	Full Scan	
	Memory / Services	
	_	
	Update	
Т	ask Scheduling Settings	ĭ I
	Save	ancel

- 2. Enter a task name.
- 3. In **Task Settings** section, select the scan type to be run on a device.
- 4. By checking the Update, you can also let the application update its virus signature database.





5. In **Task Scheduling Settings** section, schedule the created task by selecting the appropriate options.

[ask	Scheduling Settings
0	Enable Scheduler O Manual Start
• •	Daily Weekly Mon Tue Wed Thu Fri Sat Sun Monthly 1 V
At	8 30 AM V

6. Click Save.

The task will be created instantly as per configuration.

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 <b>Start Task</b> , to run the selected task for the specific group.					
Properties	Click <b>Properties</b> , to view properties and change settings of the selected task.					
Results	Click <b>Results</b> , to view detailed results of the selected task.					
Delete Task	Click <b>Delete Task</b> , to delete the selected task from the list of tasks.					





## Common QR Code Scan

Use this QR Code to enroll your device into the console. As per the scanning method, it automatically identifies the type of device either COD or BYOD. After scanning, the device will be added to the respective AutoAdded group in the console. Select the group and click on **Refresh Scan Devices** to refresh the list of devices. A User can move device to another group as per need.



**NOTE** 

Do not scan the above QR code as this is for reference purpose.

### COD/BYOD Enrollment on Android Device(s)

To know more about the device enrollment process using Common QR Code, click here.





# **Installation and Enrollment of Android device in MDM Group**

The enrollment procedure for an Android device consists of two main steps:

- Adding a device to the console
- Enrolling an 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.
- 3. Select the group type as **MDM** and then click **Save**.

Create New Group			×
New Group Name :*			
Group Type:	<ul> <li>мдм</li> </ul>	O cod	O BYOD
Select Template			
Default_Policy MDM	~		
* Mandatory Field			
		Sav	e Cancel

Group will be created.

To add the new device in created group, follow the given steps below:

- 1. Select the created group.
- 2. Click Action List > Add New Device.





Add New Device window appears.

Add New Device [Group Name: Managed Devices	] [Group Type: MDM]
Mobile Number*	
	Scan above QR code for MDM/iOS enrollment

3. Enter the mandatory details, select an appropriate OS Type and then click **Add**. The device will be added to the MDM group as shown in the following screen.

Managed Mobile Devices									۹ ¢	?
Action List  Client Action List  Select,	/Add Columns	Policy Templates						т	otal Devices: 1	
Hanaged Devices						<b>1 - 1</b> of 1	page 1 of	1 >> Rows pe	r page: 10 🗸	•
Policy	📕 Mobile Nur	nber User's name	QR Code	Device Added Date	Enrollment Status	Enrollment Date	IMEI/Android ID	Mac Number	Email Id	eS
Client Devices (1)	78 # 78 # 1	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  $\mathbf{P}$  icon next to the checkbox. This icon indicates that the added device is not enrolled.

## Enrolling the added device to MDM group

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.



### 2. Tap DOWNLOAD.

Tap the downloaded file and read thoroughly about the permissions asked by the application.





3. To proceed, tap **NEXT**.



4. After reading the application's access permissions, tap INSTALL.



Open the "eScan EMM" app, after the installation is completed.





Welcome screen appears.

- 5. Tap **Open Agreement** and read the agreement completely.
- 6. After reading the agreement, tap **Accept**.



Enrollment Details form appears.

<b>.</b> 8				🗸 🗋 11:29
Se Sca	eSc	an Device	Managemen	t.
	Er	nrollme	ent Details	
	Fill e	ntries th	rough QR co	de
	Mobile	Numbe	r *	
	Server*			
	-			
	Country	/		
	1	2	3	-
4	4	5	6	<u> </u>
-	7	8	9	$\langle \times \rangle$
	,	0		$\rightarrow$
	$\bigtriangledown$	(	0	





- 7. Enter the enrollment details mentioned in the email. To fetch the details automatically by scanning QR code, tap **Fill entries through QR Code**.
- 8. 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.

🖬 💿 💆 🎽 🎽		🔻 🖌 🛑 12:07
eScan	n Device Manage	ment
Eni	rollment Deta	ails
Fill en	tries through QI	R code
9000000	DID	
emm.ess	canax com, 792	2,168.0.6/
2221		
Country		
Version : 6. * Field is mai Default Port	ndatory t is	
	Enroll Device	
$\bigtriangledown$	0	

9. Device Enrollment begins. Wait till the device gets enrolled.







Device Administrator prompt appears.



10. It is recommended that you tap **Next**. Activate device administrator prompt appears.



11. Read about the permissions completely and then tap ACTIVATE.





The Vpn service permission dialog box appears.

12:15	⊑ 'e 'e •	¥{ 🛼 🔐 🛔
e Scan	eScan Device Management	
~ <u>@</u>	Call And SMS Filter	
Ve Scan	Vpn service permission	
Тар '	Next' and allow eScan to enable Vpn S you want to continue?	Service. Do
	📀 Do not ask again	
	Next Skip	
*	Advanced settings	

12. 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.



13. It is recommended that you tap Next.





The application enrollment is completed after this step.







## **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.

Image: Note installed and enrolled on the managed device.The Container application is accessed only after the eScan MDM application is





# **Installation and Enrollment of Android device to BYOD Group**

To add and enroll a device in the eScan Mobility Management (EMM), perform the following steps:

1. Click Managed Mobile Devices > Common QR Code Scan The Common QR code is displayed.



Connect the device to your WiFi network and perform the following steps:







2. Open device settings.



3. Tap on Google







4. Tap on **Set up & restore** 



5. Tap on Set up your work profile







### 6. Tap on Next







7. Scan the **Common QR Code** displayed on the web console.



8. Tap on Accept & continue







### 9. Tap on Next

A Work Profile has been created on a device and the device has been added in EMM under 'AutoAdded\_BYOD' group.

≡ (	eScan			eScan Mobility	🗈 🕲 🕩 Management
::	Managed Mobile Devices				<b>A</b> († ?
C <sup>a</sup>	Action List  Client Action List	Select/Add Columns	Policy Templates	Common QR Code Scan	Refresh Scan Devices
	🖻 🚞 Managed Devices	Mobile Number User's	name IMEI/Android ID	Device Added Date En	rollment Status Enrollment Date 📤
•	- 🛄 Policy 🎲 Group Tasks	There are no items to show in the	his view.		
A	Client Devices		C₂		
×.	🚺 Policy 🍘 Group Tasks				
*	Client Devices				
P					
8					
\$					
					*
		🗯 👘 Enrol	led	💼 🛊 Not Enrolled	

10. On a console, click on **Refresh Scan Devices** in the AutoAdded\_BYOD group.

As shown in the below image, the added device will appear with  $\stackrel{\bullet}{\P}$  logo. This indicates that the device is added but not yet enrolled.

≡ (	eScan			eScan Mo	bility Management	•
	Managed Mobile Devices				٩	¢ ?
ľ	Action List  Client Action List	Select/Add Columns	Policy Templates	Common QR Coo	le Scan Refresh Scan Devices Total Devi	ces: 1
		1		1 - 1 of 1 ⊣( ( page	1 of 1 ) ⊨ Rows per page: 500 N	
(U)	- Group Tasks	Mobile Number	User's name	IMEI/Android ID	Device Added Date Enrollment Sta	itus
A	Client Devices	3346453789433468	3390+52709625+03	-	07 Aug 2023 02:20 PM Not Enrolled	
Å	AutoAdded_BYOD     Group Tasks				G	
*	Client Devices (1)					
1	⊕ <b>`</b>					111
ß						
						111
<b>\$</b>						
		i 🧯 👘 Enrolle	:d	🥌 🏟 No	t Enrolled	, • •

11. On a device, Go to Work profile and open Play Store





2:20 🌣 👬 🖾	Ċ 8	• # ♥ ∡	
Q Search App	os & Games	Ŷ	
eScan EMM Bi Installed			
٩	•		

12. Open eScan EMM application



13. Allow Camera permission







14. Tap on Accept and allow Location permission



15. Grant necessary permissions







#### 16. Tap on Next

The Enrollment details will be displayed as shown in below image:







#### 17. Tap on **Enroll Device**



The device has been enrolled successfully.

18. On a console, click on Client Devices under AutoAdded\_BYOD group



As shown in the above image, the added device will appear with 🗭 logo that indicates the device is now enrolled successfully.





# **Installation and Enrollment of Android device to COD Group**

#### Prerequisites

- Perform Factory Reset on a device
- Have a WiFi network to be connected to the device

To add and enroll a device in the eScan Mobility Management (EMM), perform the following steps:

1. On a console, click Managed Mobile Devices > Common QR Code Scan



On a device, perform following steps:







2. Tap 7 times on a screen to open QR Scanner



3. Scan the Common QR Code displayed on a console





	•	17 A A B
	(;	
	Connect to Wi-Fi	
ID address		
Unavailable		
AAAC antidese		

4. After scanning the QR code, connect the device to your WiFi network



5. Tap on Next







6. Tap on Accept & continue



7. Tap on Accept & continue to accept Privacy policy and Software policy







8. Tap on **More** and then tap on **Accept** 



9. Tap on Done





Managed Mobile Devices				P Ø ?
Action List * Client Action List *	Select/Add Columns	Common QR Code Scan	Refresh Scan Devices	Total Devices: 0
Managed Devices	Hobile Number User's name IHEI/Andro There are no items to show in this view.	oid ID Device Added Dat	e Enrollment Status Enrollment (	Date Last Policy Applie ▲
	e 👘 Enrolled	<b>é</b> (	Not Enrolled	

10. On a console, click on **Refresh Scan Devices** in 'AutoAdded\_COD' group. As shown in the below image, the added device will appear with in logo. This indicates that the device is added but not yet enrolled.

Managed Mobile Devices						ρφ?
Action List * Client Action List *	Select/Add Columns	cy Templates	Common QR Code	Scan Refresh Sca	in Devices	Total Devices: 0
Anaged Devices				1 - 1 of 1      page	1 of 1 + H Rows p	er page: (500 💙
- Policy	Mobile Number	User's name	IMEI/Android ID	Device Added Date	Enrollment Status	Enrollment Date
- Elient Devices	🗆 🍁 3757545an bie 5 Mie	329764040304199	3554982425905625	04 Aug 2023 12:13 PM	Not Enrolled	•
E AutoAdded_BYOD						
AutoAdded_COD						
- Policy						
Client Devices (14)						
⊞ <b>```</b> X_!						
	<b>*</b> • •			📫 👜 National Second		
	- π en	rolled		Not Enrolled		

11. On a device, open eScan EMM application







12. Tap on Accept



13. Allow necessary permissions







#### 14. Tap on Next

The Enrollment details will be displayed as show in below image:



15. Tap on Enroll Device







The device has been successfully enrolled.

16. On a console, click on Client Devices under 'AutoAdded\_COD' group

Managed Mobile Devices						P (\$ ?
Action List * Client Action List *	Select/Add Columns	icy Templates	Common QR Code	Scan Refresh Sc	an Devices	Total Devices: 1
Anaged Devices				1 - 1 of 1 He ( page (	1 of 1 + H Rows	per page: (500 💙
- Policy	Mobile Number	User's name	IMEI/Android ID	Device Added Date	Enrollment Status	s Enrollment Date
- 🔚 Client Devices	🗌 🍁 3398/9645an 3de 186	3387645ac3de535	358464242590433	04 Aug 2023 12:13 P	M Enrolled	04 Aug 2023 12:18
AutoAdded_BYOD  AutoAdded_COD  AutoAdded_COD  Group Tasks  Client Devices (1)  Client X_		La				
	é 🛊 E	nrolled		🗯 🌞 Not Enrolled		

As shown in the above image, the added device will appear with  $\frac{1}{2}$  logo that indicates the device is now successfully enrolled.





## **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 Devices]	[Group Type: MDM]
Mobile Number*	
	Add Add More Close

2. Enter the details; select an 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.

Managed Mobile Devices							P (\$ ?
Action List 🔻 Client Action Lis	i 🔻 🛛 S	elect/Add Colu	ımns 🛛 🕒 Pol	icy Templ	ates		Total Devices: 2
- Managed Devices					1 - 2 of 2 🖂 ( page	1 of 1 $\rightarrow$ H Ro	ws per page: 10 🛛 💙
Policy	🔲 Ма	bile Number	User's name	QR Code	Device Added Date	Enrollment Status	Enrollment Date
Client Devices	0	78 8	atiene	<u>View</u>	04 Aug 2021 04:24 PM	Enrolled	04 Aug 2021 05:26 PM
	0 🧉	84 5	Tell_failmi_f	<u>View</u>	30 Jul 2021 03:10 PM	Not Enrolled	

Notice the icon **≤** in the **Mobile Number** column; it denotes that the device is not enrolled.

## Enrolling the added device

After a device is added to the console, an email containing the enrollment procedure will be sent to the specified email ID. This email will contain steps to download MDM application and details such as Mobile No, Server, and Port. In addition to this, it will also contain the QR code that will fetch the above mentioned details by scanning it from the device. In case a user didn't receive the enrollment email at the time of adding the device, you can resend the enrollment email.

Select the specific device and then click **Client Action List** > **Resend Enrollment Email**.



**Enterprise Security**




After you have 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.

009198xxxxxx
2221
elds are mandatory
Read QR Code

4. After the enrollment details are filled, tap **Enroll Device**. The 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 9	Search or e	enter web	osite name	
This w	ebsite is ti w you a co	rying to o	pen Settir	ngs
you wa	ant to allow	v this?	on promo.	00
you wa	ant to allow	v this?	ore Allo	w
you wa	ant to allow	v this?	ore Allo	w
you wa	ant to allow	w this?	ore Allo	w
you wa	ant to allow	Igno	ore Allo	w
you wa	ant to allow	Igno	ore Allo	w

6. Tap Allow.

Install Profile settings appear.



7. Tap Install.





Enter Passcode screen appears.

	Enter Passcode	Cancel
	Enter your passcode	'
0 0	0000	0 0
1	2	3
4	5	6
0HI	. Jac	MNO
PORS	8	9
	0	۲

8. Enter the device's passcode to proceed with the installation.

After entering the passcode, Warning message appears stating that an administrator will be able to remotely manage your device.

Cancel	Warning	Install
MOBILE DEVIC	E MANAGEMENT	
Installing this administrato remotely ma	s profile will allow the r at " nage your iPhone.	i" to
The administ add/remove manage and data on your	trator may collect pe accounts and restric list apps, and remot iPhone.	rsonal data, tions, install, tely erase
UNSIGNED PR	DFILE	
The profile is	not signed.	
-		

9. To proceed with the installation, tap **Install**.





A pop-up message appears asking confirmation for remote management of your device.



10. Tap **Trust**.

The MDM profile will be installed on your device.

11. To exit the installation process, tap **Done**.







The iOS Config screen appears.



12. Tap Open eScan App.

A pop-up appears.



#### 13. 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 **s** and the enrollment status change to **Enrolled** from **Not Enrolled**.

Managed Mobile Devices						P ¢ ?
Action List 🔻 Client Action Lis	it 🔻 Select/Add Col	umns 🗋 Po	licy Templ	ates		Total Devices: 2
- Managed Devices				1 - 2 of 2 ⊨ ( page	1 of 1 $\rightarrow$ H Ro	ws per page: 10 🗸
Policy	🔲 Mobile Number	User's name	QR Code	Device Added Date	Enrollment Status	Enrollment Date
Client Devices	78 8	afiene	<u>View</u>	04 Aug 2021 04:24 PM	Enrolled	04 Aug 2021 05:26 PM
	6 84 14 17 5	Tell_failm_f	<u>View</u>	30 Jul 2021 03:10 PM	Enrolled	
🛨 · 📷 teer_msam						





# 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	Application Control 😑	Application Control 😑
Web and Application Control	Additional Settings Policy 😑	Anti-Theft Policy 😑
App specific network	Password Policy	Additional Settings Policy
blocking		G
Anti-Theft Policy	Required Applications Policy	Password Policy 😑
Additional Settings Policy	Scheduled Backup (Contacts &	Required Applications
Additional Settings Foncy	SMS) 😑	Policy
Password Policy	Content Library Policy 😑	Content Library Policy 😑
Device Oriented Policy	Restriction Policy 😑	Restriction Policy 😑
Required Applications	Wi Fi Configuration	Location Fance
Policy		
WiFi Settings Policy	System Updates 😑	Wi-Fi Configuration 😑
Scheduled Backup (Contacts		
& SMS)		
Content Library Policy		
Kiosk Mode Policy		
Location Fence		

Policies sportingicon are applicable for container version of the application forNOTEBYOD and COD groups.

For detailed policy description for following policies, refer **<u>Policies section under Managed Mobile</u> <u>Device</u>**.

- Anti-Virus Policy
- Call Filter Policy
- Application Control
- Additional Settings Policy
- Password Policy
- Required Applications Policy
- Scheduled Backup (Contacts & SMS)
- Content Library Policy

More additional policies for COD and BYOD are **Restriction Policy**, **Wi-Fi Configuration** and **System Updates**.





#### **Restriction Policy**

The Restriction Policy lets you apply certain restrictions on a device that prevents the user from getting access to certain device features.

Restriction Policy	
Additional Settings	
Disallow camera	Disallow Volume Control
Disallow "USB Tethering and Portable Hotspots"	Disable Cell Broadcast
Disable Microphone	Disallow Outgoing Phone Calls
Disallow Screen Capture	Disallow Send/Receive SMS
✓ Disable Developer Options	Disallow Adding and Removing of Accounts
✓ Disallow usb file transfer	Disallow Adding Users
Disable Bluetooth	Disable Removing Users
Disallow Bluetooth Configuration	Disallow User Icon Change
Disallow Keyguard	Disallow Wallpaper Change
Disallow "Factory Reset"	Disallow App Installation Manually
Disallow "Reset Network Settings"	Disallow Multi Window
Disallow "Data Roaming" services	Disable Using NFC Beam
Disallow "Mobile Networks" configuration	Disable bluetooth contact sharing

Following are the Additional Settings that can be disabled from being configured on managed device(s):

- Disallow camera Select this checkbox to disallow a device from using camera.
- **Disallow "USB Tethering and Portable Hotspots"** Select this checkbox to disallow a device from using USB Tethering and Portable Hotspots.
- **Disable Microphone** Select this checkbox to disable a device from using microphone.
- **Disallow Screen Capture** Select this checkbox to disallow a device from taking screen capture.
- **Disable Developer Options** Select this checkbox to disable the Developer Options. By default this option is selected.
- **Disallow USB file transfer** Select this checkbox to disallow a device from transferring files via USB. By default this option is selected.
- Disable Bluetooth Select this checkbox to disable Bluetooth feature on a device.
- **Disallow Bluetooth Configuration** Select this checkbox to disallow Bluetooth configuration from the device.
- Disallow Keyguard Select this checkbox to disallow Keyguard option on a device.
- Disallow "Factory Reset" Select this checkbox to disallow a device from factory reset.
- **Disallow "Reset Network Settings"** Select this checkbox to disallow a device from resetting network settings.
- **Disallow "Reset Network Settings"** Select this checkbox to disallow a device from resetting network settings.
- **Disallow "Data Roaming" services** Select this checkbox to disallow a data roaming services from device.
- **Disallow "Mobile Networks" configuration** Select this checkbox to disallow configuration of mobile networks.





- **Disallow Volume Control** Select this checkbox to disallow volume controls on a device.
- Disable Cell Broadcast Select this checkbox to disable a device from cell broadcasting.
- **Disallow Outgoing Phone Calls** Select this checkbox to disallow outgoing phone calls from the device.
- **Disallow Send/Receive SMS** Select this checkbox to disallow send and receive SMS service on a device.
- **Disallow Adding and Removing of Accounts** Select this checkbox to disallow a device from adding and removing of accounts.
- **Disallow Adding Users** Select this checkbox to disallow a device from adding users.
- **Disable Removing Users** Select this checkbox to disable removing users function from a device.
- **Disallow User Icon Change** Select this checkbox to disallow a device from change user icon.
- **Disallow Wallpaper Change** Select this checkbox to disallow a device from changing its wallpaper.
- **Disallow App Installation Manually** Select this checkbox to disallow a device from manually installing application.
- **Disallow Multi Window** Select this checkbox to disallow multi window option on a device.
- **Disable Using NFC Beam** Select this checkbox to disable NFC (Near-field communication) from a device.
- **Disable Bluetooth contact sharing** Select this checkbox to disable a device from sharing contacts through Bluetooth.

Following are the Escan settings that can be disabled from being configured on managed device(s):

- **Disable WiFi Settings** Select this checkbox to disable WiFi settings from being configured on a device.
- Disable GPS Setting Select this checkbox to disable GPS settings.
- **Disallow Incoming Calls** Select this checkbox to disallow incoming calls on a device.
- **Disable Bluetooth Setting** Select this checkbox to disable Bluetooth settings.
- Disable Mobile-Network Setting Select this checkbox to disable mobile-network settings.

Following are the Administrator settings that can be disabled on the managed devices:

- **Disable Mount Physical Data Setting** Select this checkbox to disable settings for mounting physical data from being configured.
- Ensure Verify Apps Setting Select this checkbox to disable Ensure Verify Apps setting.





#### WiFi Configuration

The WiFi configuration 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.

Wifi Configuration	
Prevent user from manually configuring Wi-Fi settings on the device	
+ Import 🗊 Delete	
WiFi Network Name (SSIDs)	<b>*</b>
	-
4	

**Prevent user from manually configuring Wi-Fi settings on the device:** Select this checkbox to disallow users to configure Wi-Fi settings manually.

#### **Importing a WiFi SSID**

To import the Wi-Fi SSID:

1. Click Import.

Add window appears.

Add	1
Enter WiFi network name (SS	IDs):
Select authentication:	None 🗸
Password:	
	Show Password
Note: WiFi network name (SS	SID) are case sensitive
	Add Cancel
	Aud

- 2. Enter the Wi-Fi network name (SSID) in the field.
- 3. Select authentication type.
- 4. Enter a password 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.





#### **Deleting a Wi-Fi network SSID**

To delete the Wi-Fi SSID:

1. Select a Wi-Fi network SSID and then click **Delete**.

+ Import Delete
✔ WiFi Network Name (SSIDs)
✓ automatic

A confirmation prompt appears.

Delete	×
Do you really want to Delete?	
	OK Cancel

#### 2. Click OK.

The Wi-Fi network SSID will be deleted.





#### System Updates

The System Update policy allows admin to configure system update settings on a device. By enabling the freeze time admin can freeze the system updates of a particular device for defined time period.

NOTE : The system update policy controls h applied between given time interval. NOTE : The system updates will be applied	iow OS updates are applied. If only outside given Freeze time	if the update type is "Windowed", the updates will be automatically ne period(s).
System Updates	Unspecified	~
Start Time	00:00	Ð
End Time	00:00	•
Enable Freeze Time		
Start	Date	End Date
	No entries	s added

System Updates: Select the system update type from the drop-down list.

- **Unspecified**: Select this option to update the system at no specified time.
- Automatic: Select this option to update the system automatically, whenever update is available.
- **Postponed**: Select this option to postpone the system update for 30 days. After 30 days, the system will get updated immediately.
- **Windowed**: Select this option to specify the time interval for system update. As you select update type as a windowed following field will be enabled.
  - Start Time: Specify the start time for system update.
  - End Time: Specify the end time for system update.

System will be get automatically updated between specified time interval, when youNOTEselect update type as "Windowed".

**Enable Freeze Time:** Select this checkbox to enable the freezing of system update for defined time period.

To add the freeze time:

1. Click Add.

Set Freeze time period prompt appears.

2. Select Start Date and End Date.





3. Click Add.

The freeze time will be added.

Add Delete	
Start Date	End Date
06-24-2022	06-25-2022

To delete the added freeze time, Select the freeze time you wish to delete, click **Delete** option. The freeze time will be deleted.





# **Manage Backup**

The 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 the list of all devices in it along with their details such as **Mobile Number**, **User's Name, Last Backup, Backup Now** and **Manage Backup**.

Manage Backup					¢ ?
					Backup Now
Managed Devices	📕 Mobile Number	User's name	Last backup	Backup Now	Manage Backup
Tell_mb	P 78     P 7	ademe		<u>Backup Now</u>	<u>Manage Backup</u>
	# 84 84 5	Test_failm_fi		Backup Now	<u>Manage Backup</u>
78 <b>**</b> 1 <b>**</b> 8 <b>**</b> 84 <b>**</b> 5					

Clicking on a device shows information about its last SMS Backup, Contact Backup, and Device Status.

Mobile No : User's name : to t				
	SMS Backup	Contact Backup	Device Status	Refresh backup list
	There is no information for this device.			

# Taking a backup from devices to the server

To take a backup of device:

- 1. Click **Manage Backup** and select the specific group or devices of your wish to take a backup to the MDM server.
- 2. 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
Tell_mb	78 - 8	ademe		<u>Backup Now</u>	<u>Manage Backup</u>
	0 📫 84 10 5	Test_tellni_#		Backup Now	<u>Manage Backup</u>
84 5					

3. Select the desired backup option and then click **Backup Now**.





elect Backup			X
SMS	÷		
Contacts	÷ ć		
		Backup Now	Cancel

Backup window appears displaying the progress.

Backup	×
Backup in progess	
Backup for 75	
(	Close

The report displays following fields:

Mobile Number, User's name, Last backup, Backup Now, Manage Backup.

Manage Backup					¢ ?
					Backup Now
• Managed Devices	Mobile Number	User's name	Last backup	Backup Now	Manage Backup
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Test_fieldmi_fi		<u>Backup Now</u>	<u>Manage Backup</u>

Manage Backup: Clicking Manage Backup link displays following screen.

Í	Mobile No :	User's n	ame : 🛲 t	
	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 were requested by the server.
    - **Description:** displays whether the Contacts or SMS backup was requested from the server.
- Refresh backup list: Clicking Refresh backup list, refreshes the existing backup list.





# **App Store**

The App Store module lets you push applications on a device by policy deployment. The user will receive a notification to install an 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	r deployme	nt to device	25.	
In-House Apps (Andro	id) Applicable only for MDM group type.				
Add 💌 🔳 Edit 🗊	Delete 🛛 Policy Templates				
In-House Apps (Android) Play Store Apps (Android) iStore Apps (iOS)					
Application Name	Package Name	Version	Size	Installed	Added On
C Reader	com pdf viewer pdftoxi meder document	<b>II</b> .3	Kb	0	21 2022 04:43 PM
O Anage	on and and and of nanageonfiguration angeog	1.0	ны жь	0	17 🕅 2022 11:54 AM

# Adding an Android application with In-House Apps (Android) option

To add an application, follow the below steps:

1. Click Add > In-House Apps (Android).



Add App (In-House) window appears.

Add App (In-House)	×
Select Application source	
Select a file with any extension	
Choose File No file chosen	
	Continue Cancel

2. Click Choose File and browse your computer for the .apk file.





3. 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. again again ag	
Description:		
	Save	

4. Write a brief description about an 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

To add an application, follow the below steps:

1. Click Add > Play Store Apps (Android).



Add App (Play Store) window appears.





Add App (Play	y Store)							×
Þ G	oogle Play	Search	Q			20	0	*
>	Featured App	DS				See n	nore	
S			**	کے	in			L
	Google Chrome: F Google LLC ****	WhatsApp Messen WhatsApp LLC ****	Dropbox: Cloud & Dropbox, Inc. * * * * *	Adobe Acrobat Rea Adobe	LinkedIn: Jobs & B LinkedIn ****			
	Slack	Evernote - Note Or	TeamViewer Quick	Firefox Fast & Priv	Rescue + Mobile fo			• •
		21 						Close

- 2. Search for required application.
- 3. Select appropriate application from list and approve it.
- 4. Click Close.

The application will be added to the App Store.

#### Adding an iOS application from iStore Apps

To add an application, follow the below steps:

1. Click Add > iStore Apps (iOS).







Add Apps (iOS) window appears.

Add Apps (iOS)		×
App Details		1
Select Region	India 🗸	
App Name *	Enter app name Psearch	
Application Icon		
* Mandatory Field		
	Save Cancel	

- 2. Select a region.
- 3. In the App Name field, enter an application name and select an appropriate application from the suggestions.
- 4. Click Save.

0

The application will be added to the App Store.

The description can be edited only for In-House Apps (Android) applications. NOTE

#### Deleting an application from the App Store

To delete an application, follow the below steps:

Select an application and then click **Delete**.

				<u> </u>			
Applications listed below can be imported through "Policy >> Required Application Policy", for deployment to devices.							
In-House Apps (Android) Play Store Apps (Android) iStore Apps (iOS)							
Package Name	Version	Size	Installed	Added On			
com.aglitime aglitime	2.2	4868 Kb	0	20 Jul 2021 04:34 PM			
	Play Store Apps (Android) Package Name com.;	Play Store Apps (Android) iStore App Package Name Version com.: 2.2	Play Store Apps (Android)     iStore Apps (iOS)       Package Name     Version     Size       com.;     2.2     4868 Kb	Play Store Apps (Android)       iStore Apps (iOS)         Package Name       Version       Size         com.       2.2       4868 Kb       0			

The selected application will be deleted.





# **Anti-Theft**

The Anti-Theft module lets you remotely locate and block a device, in case of loss of device. This module also lets you wipe data available on a device and also allow scream an alarm. It allows to unblock the device using Admin Access code.

Anti-Theft								¢	?
Wipe Data Block Device Unblock Device 🏥 S	cream Send Message	Locate De	vice						
- Managed Devices	Mobile Number	User's name	Last Location	Wipe Status	Scream Status	Block Status	Message Status	Profile Remove sta	tus Fa
factory reset		MERR	13 May 2022 03:46 PM(Failed)						-
GeoStrata	🗆 🌞 estetues	rhour							-
Sangram_MDM		Tab etti							-
TEST BYOD									
TEST COD									

Selecting an added device enables following options:

- Wipe Data
- Block Device
- Unblock Device 闸
- Scream
- Send Message
- Locate Device
- Remove Work Profile 💮
- Factory Reset
- Lock Device

# Wipe Data

With this option you can delete entire data from the device if it gets lost or stolen. To wipe the data:

- 1. Select the specific device and then click **Wipe Data**.
  - A confirmation prompt appears.



2. Click Yes, to confirm data wipe on a device.





A window appears displaying the request in progress.

	×
Anti-Theft	?
Request in process Request WIPE for mobile number 75 was scheduled	=
	Close

Wipe Data option will delete contacts, SMS, calendar data & email accounts from an Android device whereas, an iOS device it will be factory reset.

### **Block Device**

This option lets you block a device remotely. This option can be used for both iOS and Android based devices. To block a device that has been lost or stolen:

1. Select the device from the list of managed devices and then click **Block Device**. A confirmation prompt appears.



#### 2. Click OK.

Anti-Theft window appears displaying the request in process.

	×
Anti-Theft	?
Request in process Request LOCK for mobile number 75 19 5 was scheduled	
Clos	e

After the device is blocked, the device user will need Admin Access Password to unlock the device.





## Unblock Device

This option lets you unblock a device. This feature works only for Android based devices. To unblock a device:

1. Select the device from the list of managed devices and then click **Unblock Device**. Following window appears showing request in process:

5	•
Anti-Theft ?	
Request in process Request for mobile number 75 5 was scheduled	
Close	

#### Scream

The Scream lets you raise a loud alarm on a device will help the user to locate their device if it is in the vicinity. This option can be used for both iOS and Android based devices. To raise a loud alarm on a device:

1. Select the specific device and then click **Scream**. Following window will be displayed on screen:

	×
Anti-Theft	?
Request in process	
Request SCREAM for mobile number 75 19 19 5 was scheduled	
	Close

## Send Message

The Send Message lets you send a message to the device. This option can be used for both iOS and Android based devices. To send a message (notification message):

1. Select the specific device and then click Send Message.





Message window appears.

Message	×
Please call on 85	
Max. 180 characters.	
	_1
Send Canc	el

2. Type the message in the field and then click **Send**.

ti-Thaft		
Request in process		
Request SEND MESSAGE	for mobile number 75	
		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 location on Google Maps. This option can be used for both iOS and Android based devices. To locate a device:

1. Select the specific device and click **Locate Device**. Anti-Theft window appears displaying process.

	×
Anti-Theft	?
Request in process	
Request LOCATE for mobile number was scheduled	
Note : Location details of the device will also be sent to the Administrator's Email-id on receipt of this request by the device.	
	_
	Close





### Remove Work Profile

The Remove Work Profile lets you remove the container work profile from a device. This feature is available for only Android based devices. 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:

	×
Anti-Theft	?
Request in process	
Request for mobile number enables was scheduled	
	Close

### Factory Reset

The Factory Reset option allows you Reset the device, in case of lost or stolen. This option can be used for both iOS and Android based devices. To Reset a device:

1. Select the specific device and click **Factory Reset**. Anti-Theft window appears displaying process.

### Lock Device

The Lock Device option lets you lock the device, in case of lost or stolen. This option can be used for both iOS and Android based devices. To lock a device:

1. Select the specific device and click **Lock Device**. The command will be executed on the device.

	×
Anti-Theft	?
Request in process	
Request PROFILE_LOCK for mobile number 100 106 was scheduled	
	Close





# **Asset Management**

The Asset Management module displays detailed description of all the hardware configuration and applications installed on the managed devices.

# Hardware Information

lardware Inforn	nation Appli	cation Info	rmation					
• Filter Criter	ia			-	Export Option			
Device Details 1 - 2 of 2 H ( page 1 of 1 + H Rows per page: 10 -					10 🗸			
Mobile Number	User's name	Group	Group Type	IP Address	IMEI Number	Phone Model	Operating System	OS Versio
75 5	Device_	test_MDM	MDM	192.000.000	35 2	Neure 5	Android	6.8.8
84 10 5	Test Balloi #	test MDM	MDM	192.	86	Badmi #	Android	7.

### Viewing Hardware information

- 1. Click **Asset Management** and then click **Hardware Information** to view all the hardware related information and all the information captured by the eScan Server can be filtered.
- 2. To filter the hardware information, click Filter Criteria drop-down.

<ul> <li>Filter Criteria</li> </ul>				Export Option				
Filter Criteria								-
Mobile Number	*	Include 🗸	✓	Phone Memory (System Usable) (MB)	*		Include 1	×
IP Address	*	Include 🗸	✓	External SD (MB)	*		Include 1	¥
🗹 User's name	*	Include 🗸	✓	Internal Memory (User Usable) (MB)	*		Include 1	×
IMEI Number	*	Include 🗸	✓	Network Type	Select	~	Include 1	¥
Phone Model	*	Include 🗸	✓	Roaming Enabled	(Select	~	Include 1	¥
Operating System	*	Include 🗸	✓	Rooted	Select	~	Include 1	¥
OS Version	*	Include 🗸	✓	Bluetooth	Select	~	Include 1	¥
🗹 RAM (MB)	*	Include 🗸	✓	WI-FI	Select	~	Include 1	×
Group	*	Include 🗸	✓	GPS	Select	~	Include 1	Y

- 3. Select the checkbox next to each criterion and select **Include/Exclude** to include/exclude that particular criterion in the filtered report.
- 4. Select the desired criteria drop-down and then click **Search**. Details will be filtered in the table instantly.
- 5. Click **Reset** to set the default values.





Following Hardware information is captured from Managed Devices.

Options	Description
Mobile Number	Displays the mobile number that is assigned to the device during adding a device/enrollment.
User's name	Displays the username with which the device is registered on the MDM Server.
Group	Displays the group to which the device belongs.
Group Type	Displays the type of a group.
IP Address	Displays the IP address of the device.
IMEI Number	Displays the device IMEI number.
Phone Model	Displays the device model details.
Operating System	Displays the device operating system details.
OS Version	Displays the device operating system version.
RAM (MB)	Displays the device RAM in MB.
Phone Memory (System Usable) (MB)	Displays the phone memory of the device.
Internal Memory (User Usable) (MB)	Displays the internal memory of the device in MB.
External SD (MB)	Displays the external SD card storage capacity (MB) of the device.
Network Type	Displays the network type used by the device.
Rooted	Displays if the device is whether rooted or not.
Roaming Enabled	Displays the roaming status of the device.
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.
Applications	Displays the list of applications installed on device.
Kiosk Application	Displays the list of applications installed on device in kiosk mode.





# **Application Information**

Hardware Information Application Information	
← Filter Criteria ←	Export Option
Application Details	1 - 10 of 72 H ( page 1 of 8 → H 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

- 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	
Application Name Mobile Number	*	Group By Include V Include V Mobile Number	
PSearch 9 Rese			

- 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.
- Select the desired criteria drop-down and then click Search. 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.
- 5. Click **Reset** to set the default values.





# Export Options for the Generated Reports

Hardware Information	Application Information		
Filter Criteria		<ul> <li>Export Option</li> </ul>	
	O PDF	HTML	년 <sup>7</sup> Export

You can export reports generated for the hardware as well as software inventory in **Excel**, **PDF** or **HTML** formats, as per requirement.

#### Exporting a Report

1. Select an export option of your preference and then click **Export**. A message appears informing about successful export.



2. Click the link in the prompt to open/download the report.





# **Report Templates**

The Report Templates module lets you generate/edit (Customize) any pre-defined report template for any eScan module. You can also create your own customized report template as per your requirements.

Report Templates					¢ ?
🗅 New 📓 Edit 🍵 Delete 🕞 View					
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
	1 .				1

# Creating a Report Template

To create a new Report Template:

1. In the Report Templates screen, click **New**. New Report Template window appears.

lected remplate Type		
Virus Report	O Update Report	
O Web Control Report	O Inventory Report	
O Application Control Report	O Enrollment Report	
O Device last connection report		

2. Type a name for the report template and select the required report type from the given options.





	elected Template Type				
elect Filter Options					
Date Options					
Today	O Last 7 days				
🔿 Last 30 days	🔿 Last 365 days				
$\bigcirc$ Since Installed	O Date Range				
Sort By					
Date	O Devices				
~	Action Takan				

3. In Select Filter Options section, select an appropriate Date Options and Sort By, then click Save.

A Report Template will be added.





# Editing a Report Template

To edit an existing Report Template:

1. Select a Report Template and then click **Edit**. Edit Report Template window appears.

Select Filter Options		
Date Options	O Last 7 days	
C Last 30 days	C Last 7 65,5	
O Since Installed	O Date Range	
Sort By		
O Date	Devices	

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**.

🕒 New 📗 Edit 🗑 Delete 🛛 🖓 View				
📕 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.

Report Scheduler						¢ ?
🕒 New 📕 Edit 🍵 Delete 🕨 Run 🕼 View	📋 Results					
Schedule Name	Report Recipient	Format	Туре	Next Scheduled	Created On	Modified On
New Report Echellular_1	turn g 122.com	HTML	Manual	-	22 Apr 2022	22 Apr 2022
New Tesport Edhadular_1		HTML	Manual	-	22 Apr 2022	22 Apr 2022
New Taport Scheduler_3	head grin, com	HTML	Manual	-	22 Apr 2022	22 Apr 2022
New Tesport Scheduler_1	eee jee.com	PDF	Manual	-	22 Apr 2022	22 Apr 2022
New Terror Scheduler_1	fuel greet.com	HTML	Manual	-	29 Apr 2022	29 Apr 2022

Under Report Scheduler, following options are available. Except **New**, all other options are enabled only after selecting a template.

Select a Particular Schedule name to enable all the options.

Report Scheduler						¢ ?
🗅 New 📔 Edit 🍵 Delete	e ► Run 🛛 View	Ĵ Results				
🗹 Schedule Name	Report Recipient	Format	Туре	Next Scheduled	Created On	Modified On
New tapart Schallular_1	example com	HTML	Scheduled	31 Jul 2021 08:30 PM	31 Jul 2021	31 Jul 2021

Options	Description
New	This option lets you create a new report schedule.
Edit	This option lets you edit an existing report schedule.
Delete	This option lets you delete a report schedule.
Run	This option lets you run a report schedule.
View	This option lets you view a report schedule.
Results	This option lets you view the results of previously deployed report schedule.

# Adding a Scheduler

To create a new Report Scheduler:

- 1. After clicking New, New Report Scheduler window appears.
- 2. 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 an appropriate template for generating a report according to your preferences of Date, Devices, and Action taken.

÷. 🔾	Application Control Report[Type: Application Control Report]
÷.	Device last connection report[Type: Device last connection report]
ė. 🗋	Enrollment Report[Type: Enrollment Report]
ė. 🗋	File new firewall[Type: Virus Report]
÷.	Inventory Report[Type: Inventory Report]
÷- 🗆	New Updates[Type: Virus Report]
	Update Report[Type: Update Report]
÷ 🔾	Virus Report[Type: Virus Report]
÷. 🗋	Web Control Report[Type: Web Control Report]

Under the Template Selection we have following templates:

- Application Control Report
- Device last connection report
- Enrollment Report
- File new firewall
- Inventory Report
- New Updates
- Update Report
- Virus Report
- Web Control Report

Select an appropriate template to create 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/Clier	nts
"Report for a List of Devices" will no	t be applicable for "Enrollment Report"
Report for Groups	O Report for a List of Devices
Select subgroups on selecting F	Parent group
🗄 🗌 📄 Managed Devices	

### **Report Send Options**

Configure the options for sending the report on email using Report Send Options. Select an appropriate format for sending the report on email.

end Report by Email		
Report Sender*:	te	
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:

#### 1. 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**. To delete the recipient email, select the specific email id and click **Delete**.

#### 2. 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
O Monthly	1 🗸			

There are two options to schedule a report, either Scheduled or 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.

After making all the configuration, click **Save**. The Report Scheduler will be added.

## Running a schedule

To run a schedule:

• Select a schedule and then click **Run**. After clicking **Run**, the console runs the schedule, generates a report and sends it to the recipient mail address.

Sending Report New Report Scheduler_3	×
**************************************	
	Close





# Editing a Schedule

To edit a schedule:

• Select a schedule and then click **Edit**. Edit Report Scheduler window appears.

Edit Report Scheduler	×
New Report Scheduler : New Report Scheduler	
▼ Template Selection	)
Select a Template for creating a Report	
🗄 🗸 🖌 Application Control Report	
🗄 🛛 🗋 Device last connection report	
🗄 🗸 🖌 Enrollment Report	
··· 🔵 Date	
± Inventory Report	
···· Update Report	
🗄 🗇 Web Control Report	
Selection For Applied Groups/Clients	
Report Send Options	)
Report Scheduling Settings	)
Save	

• Make the required changes and then click **Save**. The schedule will be updated.

# Deleting a Schedule

To delete a schedule:

• Select a schedule and then click **Delete**.

I	Report Scheduler						¢ ?
	🕒 New 📳 Edit 🗊 Delete	e ► Run 🛛 View	Ĵ Results				
	Schedule Name	Report Recipient	Format	Туре	Next Scheduled	Created On	Modified On
	New Taylor Schallung	example com	HTML	Scheduled	31 Jul 2021 08:30 PM	31 Jul 2021	31 Jul 2021

The selected schedule will be deleted.





# Viewing the report

To view 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 former to have a results					
	Status	Туре	Finish	Start		
ccessfully	Report mail sent successfully	Scheduled	02 Aug 2021 11:01 AM	02 Aug 2021 10:59 AM		
	Report mail send	Manual	02 Aug 2021 11:09 AM	02 Aug 2021 11:09 AM		
1	Report mail sent su Report mail send	Scheduled Manual	02 Aug 2021 11:01 AM 02 Aug 2021 11:09 AM	02 Aug 2021 10:59 AM 02 Aug 2021 11:09 AM		





# **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.

Events And Devices									¢ ?
								И мом	Filter
Events And Devices	Rec	ent					1 - 10 of 879 10	page 1 of 88 ) H Rows per page:	10 🗸
Events Status		Date	Phone Number	Device Type	User's name	Event Id	Module Name	Description	Action T
- L Recent	0	26 May 2023 05:44 PM	4.68	MDM	Realimations	7047	Android	Compliance	
	0	26 May 2023 05:44 PM	466	MDM	Resimentati	7033	[C]Config(Android)	Auto sync status[05/26/2023 17:44:37]	Sync suc
Device Selection	0	26 May 2023 05:19 PM	3 Hild a territika tike6	MDM	30mDite herrither Whe6	7013	[W]Anti-Theft (Android)	Anti-Theft Locate	successfu
🗄 🔝 Application/Hardware Changes	0	26 May 2023 05:13 PM	3 Mut 19 Me De Davier	Work Profile	3) That the "He per parties	7047	[W]Android	Compliance	
	0	26 May 2023 05:05 PM	3 million million he 6	Work Profile	3(m)tahantilaithe6	7033	[W]Config(Android)	Auto sync status[05/26/2023 17:05:40]	Sync suc
	0	26 May 2023 04:33 PM	3 342547549 ++/101750	Work Profile	3)(()()()))))))))))))))))))))))))))))))	7047	[W]Android	Compliance	
	0	26 May 2023 04:33 PM	300000000000000000000000000000000000000	Work Profile	300500000000000000000000000000000000000	7047	[W]Android	Compliance	

The **Filter** button allows you to filter data based on device type i.e. MDM or Container. Select appropriate checkboxes and click **Filter**.

### **Event Status**

Events are categorized into three types based on their severity.

- **Recent**: It displays both critical and informational 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

It captures events on the basis of Application Change, Hardware Change 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 on 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**

ents And Devices	Settings		(
Events Status	Device Selection	Application/Hardware Changes	
Events			
Events Name R	lecent 🗸		
Number Of R	ecords	1000	
Save			
_			

Select an event from the drop-down and enter the number of records as per requirement and click **Save**.





### **Device Selection**

The following actions can be performed by selecting this tab.

ts And Device	s Settings		
vents Status	Device Selection	Application/Hardware	Changes
Devices ——			
Device Status (	Devices with the "Critic	:al Status" 💉	
Check for Mo	nitor Status		
Check for No	t Scanned		
Check for Da	tabase Not Updated		
Check for No	t Connected		
Database No	t Updated from more th	ian	7 days
Device Not S	canned for more than		7 days
Device Not C	onnected for more than	1	7 days
	ocordo		1000

#### **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 Status	Select this checkbox to generate events related to eScan Monitor Protection.
Check for Web Control	Select this checkbox if you want to view the list of client systems on which protection of Web Control module is inactive.
Check for Not Scanned	Select this checkbox to view the list of devices which are not scanned.
Check for Database Not Updated	Select this checkbox to view the list of devices on which virus signature database is not updated.
Check for Not Connected	Select this checkbox to view the list of devices that are not connected to the eScan server.
Check for Protection off	Select this checkbox to view the list of client systems on which protection for any module is inactive.
Database Not Updated from more than	All the devices that are not updated from more than the specified days will be added to the report.
Device Not Scanned for more than	All the devices that are not scanned for more than specified days will be added to the report.
Device Not Connected for more than	All the devices that are not connected to the eScan server for more than the specified days will be added to the report.
Number of Virus	Enter the number of viruses detected on client system.
Number of Records	Enter the count and the number of records will be displayed.

After doing necessary configuration, click Save.





## **Application/Hardware changes**

The following actions can be performed using this option.

Events And Devices	Settings		3
Events Status	Device Selection	Application/Hardware Changes	
Updates			
Application/Har	dware Changes Applic	ation Changes 🗸	
Number Of D	ays	1 days	
Number Of R	ecords	1000	
Save			

Field	Description
Application/Hardwar e Changes	Select from the drop-down to generate events related to Application Changes, Hardware Changes, and Existing Device Info.
Number of Days	Enter the number of days, to view changes made within the specified days. For example, if you have typed 2 days, then you can view the list of devices on which any software/hardware changes have been made in the last 2 days.
Number of Records	Enter the number of records to be displayed in the list.

After doing necessary configuration, click Save.





# Settings

The Settings module allows you to configure settings in following sub-modules:

- Enterprise Configuration
- Console Settings
- Two-Factor Authentication
- Event Alert
- UnLicense Alert

# **Enterprise Configuration**

The Enterprise Configuration allows you to 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. Apart from these settings, you can configure Data purge, Connection sequence, and Server configuration settings.

				ؿ
Certificate Management	Email Notification Settings	Data Purge	Server Configuration	
+ Add 🗑 Delete				
Credential Name				Certificate Detail
emm_seconds_settion	0			Domain : emm.escanav.com Issuer : Sectigo RSA Domain Validation Secure Server CA

### **Certificate Management**

The eScan EMM requires a SSL certificate to manage your iOS devices from the EMM console. This section gives you information of 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**

To import 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.
- 4. Search for the files in your local drive. Save the files. After saving files, a confirmation message appears.

Make sure you add an authentic CA certificate and key in .crt and .key file format.NOTE A self-signed file will not be accepted.

### To add the CA certificate if

You had selected to proceed with "Start with Android (without iOS)" earlier

OR

You have deleted the previous certificate, follow the steps given below:

- 1. On the navigation panel, click **Settings**.
- 2. Select Certificate Management tab.
- 3. Click Add.

Add Certificate window appears.

Add Certificate		×
Select Certificate File		?
Certificate File (.crt): Certificate Key File (.key): Certificate Key File Password:	Choose File No file chosen Choose File No file chosen Enter password	
	*Enter password in case your key file is password protected, else leave blank.	
	Save	icel

- 4. Click **Choose File** and select the .crt and .key files.
- 5. Enter the password in Certificate Key File Password, if your key file is password protected.
- 6. After selecting the files (and entering password), click Save.

A confirmation message appears "Certificate added successfully".

### To delete the CA certificate

To delete the CA certificate:

- 1. Select the Credential name from the list you want to delete.
- 2. Click Delete.

It will delete the selected certificate.





# **Email Notification Settings**

Set up an email account to receive notifications.

Certificate Management	Email Notification Settings	Data Purge	Connection Sequence	Server Configuration
Email Notification Sett	ings			
				[]
SMTP Server*:	10)*:			.com
SMTP Port*:				(#11.5
Auth. Username:				Nullian gynal.com
Auth. Password:				
* Mandatory Field				
✓ Save ✓ Test				

- From (Administrator Email Id): Enter an Administrator email ID.
- SMTP Server: Enter the SMTP server IP address.
- **SMTP Port**: Enter the SMTP Port number.
- Auth. Username: Enter an authorized username.
- Auth. Password: Enter the password.

After you are done filling the details, click **Save**. To run a test for the configured settings, click **Test**. A test email will be sent to the entered email ID.

### **Data Purge**

This setting lets you define the number of days for storing data in tables. The old data will be purged automatically after it reaches number of specified days.

ificate Management Email Notifi	cation Settings Data	Purge Connecti	on Seque	nce	Server Co	onfiguration
ep Location History for			60	Days	(0-365)	0=Unlimited
ep Data Usage data for			60 🗘	Days	(0-365)	0=Unlimited
ep Call logs data for			60 🗘	Days	(0-365)	0=Unlimited
ep Battery Status/Signal Strength H	listory data for		60 🗘	Days	(0-365)	0=Unlimited
p Geo Fence History data for			60 🗘	Days	(0-365)	0=Unlimited
ep App Usage History data for			60 🗘	Days	(0-365)	0=Unlimited
Save						

The data purge can be set for following data tables:

- Location History
- Data Usage data
- Call logs data
- Battery Status/Signal Strength History data
- Geo Fence History data
- App Usage History data





After making necessary changes, click **Save**. The Data Purge changes will be saved.

### **Connection Sequence**

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.

					¢
ertificate Management	Email Notification Settings	Data Purge	Connection Sequence	Server Configuration	
Arrange the sequence for	the server list ("Server" entry) to	be seen in the Not	ification email/QR code.		
Server list sequence will d	ecide which server is connected f	first by the device.			
(emm.escanav.com	•				

## **Server Configuration**

This setting displays the information of application server.

rtificate Management	Email Notification Settings	Data Purge	Connection Sequence	Server Configuration	ן
)evice(s) that can b	e managed:				
	(Android Enterprise) + iOS day	ices			
Android devices with AE	(Android Enterprise) + 103 dev	luca			
Android devices with AE Enterprise Name	(Android Enterprise) + 103 dev	etian	)		
Android devices with AE Enterprise Name Creation Time	(Android Enterprise) + 103 dev	(1 2022	2 07: PM		
Android devices with AE Enterprise Name Creation Time Enterprise Email	(Analoid Enterprise) + 103 dev	e	2 07: PM		

- Enterprise Name: It displays an enterprise name.
- Creation Time: It displays creation time of an enterprise ID.
- Enterprise Email: It displays an enterprise email ID.
- Enterprise Id: It displays an enterprise Id which is unique identifier.





# **Console Settings**

Web Console Settings sub-module lets you configure web console Timeout, Dashboard, Login Page, SQL Server Connection, SQL Database compression, and Password Policy Settings.

Web Console Settings			👔 Help
Web Console Timeout Setting			
Enable Timeout Setting			
Automatically log out the Web Console after	0 🗸 minutes		
DashBoard Setting			
Show Status for Last 7 days (1 - 365)			
Login Page Setting			
Show Client Setup Link			
Show eScan AV Report Link			
Logo Settings			
Logo : eSaan The logo needs to have the size 300 and needs to be in .png or .jpg (RG Change Default	) x 100px, B Color) format.		
Sql Server Connection Setting			
O Microsoft Windows Authentication Mode			
SQL Server Authentication Mode			
Server instance:	etiandiji.tarian	Browse	
Host Name/IP Address:	With edulation and acts of		
Login name	Si		
Password	•••••	Test Connection	
SQL Database Purge Settings			
Enable Database Purge			
Database Size threshold in (MB)	1024 (500 - 7168)		
Purge data older than specified days, if above threshold is met	7 days (7 - 365)		
Password Policy Settings			
Password Age :	90 days (30-180 days)	0 = Password Never Expires	
Password History :	3 (3-10 Passwords)	0 = No password history is maintained	
Maximum Failed login attempts :	3 (3-10 times)	0 = Unlimited failed attempts allowed	
Note: The above restrictions are not applicable	to "Root" login.		
Delete log settings			
Delete Uploaded log files (Forensics\Debug\Scre	enshots) after 7 days (1	- 365)	
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.

#### **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.

**U** NOTE

This setting will not be applicable for the root login.

After making the necessary changes, click Save. The web console Settings will be updated.





#### **Delete log settings**

This settings allows you to delete the uploaded log files (forensics/debug/screenshots) from eScan server. You can use the provided drop-down list to define number of days after which this action to be performed. The default value is 7.

# **Two-Factor Authentication**

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</u> <u>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.

actor Authentication	
2FA Settings Manage Othe	r User's Settings Users For 2FA
Scan QR Code	
Download eScan Authenticator fr	<u>om:</u> 🕨 🗯
Or Use below key	
Barrier and the second E	
Disable Two-Factor Authentication	(
Note: Ensure that the smart o	levice's date-time matches with the system's date-time else 1-01Ps generated by the app won't get validated.

0	Ensure that the smart device's date and time matches with the system's date and time or
NOTE	else TOTPs generated by app won't get validated.

•	We recommend that you save/store the Account Key in offline storage or a
IMPORTANT	paperback copy, in case you lose the account access.





## Enabling 2FA login

#### To enable 2FA login:

- 1. Go to Settings > Two-Factor Authentication.
- 2. Open the Authenticator app.
  - After basic configuration following screen appears on smart device.

÷		0 0 0
Add	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.

	×
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 Authentication

 2FA Settings
 Users For 2FA

 User's name
 2FA Status
 User Specific QR Code

 2a
 Image
 View
 Image
 NA

- To enable 2FA login for an added user, click the button to check icon. The 2FA login for added users gets enabled. After enabling the 2FA login for users, whenever they log in to eScan web console Verify TOTP window appears.
- 8. To view QR code of added user, click on **View** option under the column User Specific QR Code.

### Disabling 2FA login

To disable 2FA login:

- 1. Go to Settings > Two Factor Authentication.
- 2. Click **Disable Two-Factor Authentication**.





wo-Factor Authentication	🝸 Help
2FA Settings Manage Other User's Settings Users For 2FA	
Scan QR Code	
「自然は然於「同	
1. Sec. 200 12	
E1623-3-22	
Download eScan Authenticator from : 👂 🗯	
Or Use below key	
Bintinte Jahrensen E	
Disable Two-Factor Authentication	
Note: Ensure that the smart device's date-time matches with the system's date-time else T-OTP	s generated by the app won't get validated.
	· 2

Verify TOTP window appears.

11.15.01	
11:45:34 AM	
Enter T-OTP Verify T-OTP	

3. Enter the TOTP and then click **Verify TOTP**. The 2FA feature gets disabled.







## Adding Users for 2FA

To Add users for Two-Factor Authentication, follow the steps mentioned below:

A Settings Manag	e Other User's Settings	Users For 2FA		
Add User 💽 Add fro	om Active Directory	ort Users 🧋 Delete		
			destand the last transition	United and the second s

### 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	<u>?</u> 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
	<b>•</b>
Ok Cancel	(*) Mandatory Fields

- 3. Enter the required information.
- 4. Click Ok.

The Active Directory Users will be added.

### **Method 3: Importing Users**

To import the users, follow the below steps:

- 1. Go to Settings > Two-Factor Authentication > Users For 2FA.
- 2. Click Import Users.

Import Users window appears.





		E
Impo	ort Users	
2	<u>Users</u>	
	A Creation to a comparison	
Imp	port	

3. Select users and click on **Import**. The users will be imported.

## **Event Alert**

The Event Alert subtab allows you to configure settings to send an event alerts to specific email ID. Administrator has an option to select device(s) of which the events need to be sent

	Enable emai	l alert Notification	Configure SMTP Settings
	5 Send Inform	ation only in subject line	
elect Even	nt Ids	email alert is required	
	Event Id	Description	
	100	ESCAN_Builder_putplet	
	1	MWAV_POUND_mnuMmht	
	2	MWAV_ROUND_HINUE_HID_DIG.2700	
	501	SCHED_MMMM_POUND_MM_MMM	
	502	SCHED_MWWW_POUND_VIMUE_MID_DELET	Ð
	503	SCHED_HWAR_PDUND_stitute_and_class	10 E
	504	SCHED_WWWW_FOUND_ADWARE	
All Devi	ices d Devices		
elect Con	nputers		
±	Managed De	vices	

To configure Event alerts, follow the steps given below:

1. Go to **Settings** > **Event Alert**.

An Event Notification window appears as shown above.

- 2. Select the checkbox **Enable email alert Notification**.
- 3. Click on **Configure SMTP Settings** to set the SMTP settings for email alerts.





- 4. Click on **Send Information only in subject line** to let eScan send alert details only in the subject line of the mail.
- 5. From Select Event Ids section, select the activities for which the alerts are required.
- 6. Select the device(s) using the provided options All Devices or Selected Devices.
- 7. Click on **Save**. The Event Alerts have been configured.

### **UnLicense Alert**

The UnLicense Alert option allows you to configure settings to send an alert to specific email ID when any licensed device(s) moved to the unlicensed category.

Send notification for unlicensed computers.	Configure SMTP Settings	
27400 201		

To configure Unlicense alerts, follow the steps given below:

1. Go to **Settings** > **UnLicense Alert**.

An Unlicense Move Notification window appears as shown above.

- 2. Select the checkbox Send notification for unlicensed computers.
- 3. Click on **Configure SMTP Settings** to set the SMTP settings for email alerts.
- 4. Click on Save.

The Unlicense Alerts have been configured.





# **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, .bmp, .mp4, .mpeg-4, .mov, .avi, and .wmv. 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
	Kb	2 1 04:3 PM	TEST TEXT FILE
elsen Multile Security utt Dil.pdf	22000 КЬ	2	TEST PDF FILE UPLOADED
ob.et.an. Communite Dit Law Shuffer and an and a constant	2	Jul 2 04: PM	TEST WORD FILE
	<u>10 кь</u>	27 1 21 CM:33 PM	TEST EXCEL SHEET
	141 Kb	27 347 2021 04:3m PM	TEST IMAGE PNG FILE

# Adding a file

To add a file in Content Library:

1. Click **Content Library** > **Add**. Add File window appears.

Allowed file forma PNG, BMP, MP4, M	ts PDF, DOC, DOCX, XLS, XLSX, PPT, PPTX, TXT, JPG, J IPEG-4, MOV, AVI, WMV
Choose File No	file chosen

- 2. If file size is less than 200 MB, click **Choose File** and search for the file. If file size is more than 200 MB, enter the path of the file in textbox.
- 3. After selecting the file, click **Continue**.





Add File window appears.

Add File		×
File Name:	Computer Shortford Rays.docx	
	file with important instructions.	
Description:		
		Save Cancel

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:

1. Select a file and then click **Edit**.

Content Library						
+ Add 🔳 Edit 🗊 Delete						
File Name Size Updated On Description						
ED	2184 КЬ	20 Jul 2021 12:58 PM	important			

Edit window appears.

an	
File Name:	Computer Sterfoul fags.docx
	file with important
Description:	

2. Edit the description and then click **Save**. The file description will be updated.





# Deleting a file

To delete a file:

1. Select a file and then click **Delete**.

Con	Content Library 🕴 ?							
+ Add 🔳 Edit 🗊 Delete								
	Description							
	ED	2184 Kb	20 Jul 2021 12:58 PM	important				

A confirmation prompt appears.

Delete File(s)	×
Selected items will be permanently deleted. Are you sure? Note: If these Files/Documents are added to Policy Details>>Content Library Policy, make s that you re-deploy the policy for that specific groups to update the Content Library on the d	sure evice.
Delete	ancel

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.

<ul> <li>Check configuration under "P</li> <li>Data Purge set to "60 days",</li> </ul>	olicy >> Device Oriented	l Policy", if Call logs are not d	isplayed.			
						(HTML V) 2 <sup>a</sup> Export
] 📄 Managed Devices	All calls			1 - 10 of 20 14	(page 1 of 2 ) H	Rows per page: 10 🗸
- Ella Hall	Mobile No	Name (As in Contact List)	Contact No	Type of Call	Call/Receive time	Call Duration (HH:MM:S
Telf.,198		8 UNKNOWN	610433454	Outgoing	08 Mar 2018 10:48 PM	00:45:00
🕀 🔚 tea jatan		8 UNKNOWN	9	Outgoing	08 Mar 2018 10:21 PM	00:30:00
	✓ 78541348	8 UNKNOWN	+9104214044	Missed	08 Mar 2018 10:16 PM	00:00:00
	✓ 785+1145	8 UNKNOWN	9614134	Outgoing	08 Mar 2018 09:48 PM	00:28:00
	✓ 78561368	8 UNKNOWN	+9100030003	Missed	08 Mar 2018 09:16 PM	00:00:00
	✓ 78 ***1 ***	8 UNKNOWN	+9177856393	Missed	08 Mar 2018 08:16 PM	00:00:00
	✓ 78 54 2 34 5	8 UNKNOWN	+91	Missed	08 Mar 2018 07:16 PM	00:00:00
	▶ 785+1144	8 UNKNOWN	81430734	Outgoing	08 Mar 2018 06:48 PM	00:13:00
		8 UNKNOWN	76531758	Outgoing	08 Mar 2018 06:48 PM	00:26:00
	4 70 hard hard	8 UNKNOWN	+91	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.





# Filter Call Logs

To filter the Call Log information:

1. Click Filter Criteria icon.

Mobile No	(*	Include 🗸
Name (As in Contact List)	*	Include 🗸
Contact No	*	Include 🗸
Type of Call	All calls 🗸	Include 💙
From Date		
To Date		

- 2. Select the checkbox next to each criterion and select **Include/Exclude** to include/exclude that particular criterion in the filtered report and date.
- 3. Click **Filter**.
- 4. Click **Reset**, to set default values.

# **Exporting Call Logs**

You can export reports generated for Call Logs in **Excel**, **PDF** or **HTML** formats, as per requirement. To export the generated report:

1. Select the export option of your preference and then click **Export**. A message appears informing about successful export.



2. Click the link in the prompt to open/download the report.





# Data Usage 🖲

The Data Usage module lets you keep a track of cellular data usage of a device.

Data Usage						P (¢ )
Data Purge set to "60 days",	to configure <u>click</u>	here				
						HTML V C' Export
🗄 🚰 Managed Devices	User's I	name: adams	Mobile Number: 78	54123658	1 - 8 of 8 14 (page 1 of 1 ) )	Rows per page: 20 🗸
···· 🚰 Teiri, 👘	Sr. No.	Date	Mobile No	User's name	Group	Data Usage
	1	27 Jul 2021	78 18 8	adams	tere_ndim	840,48 MB
tem_tute	2	28 Jul 2021	78 8	adams	tess_million	735.58 MB
+ Call Internet	3	29 Jul 2021	78 8 8	adams	tegilintow	630.68 MB
	4	30 Jul 2021	78 8	adams	tess. MARAN	525.77 MB
	5	31 Jul 2021	78 8	adams	tega Mallana	420.87 MB
	6	01 Aug 2021	78 8	adams	team	106.15 MB
		International Association and a second s	70		to a strength	244 OC MD
	7	02 Aug 2021	/8 8	duantis		1211.00 MD

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.				

# Filter Data Usage logs

To filter the Data Usage information:

1. Click **Filter Criteria** icon.

Filter Criteria	X
Filter Settings	
🔘 User Name/Mobile No.	O Groupwise
Note: Blank search will display resu	It for all enrolled devices.
	Filter Reset

2. Select the checkbox next to each criterion and select **Include/Exclude** to include/exclude that particular criterion in the filtered report and date.





- 3. Click Filter.
- 4. Click **Reset**, to set default values.

# Exporting Data Usage logs

You can export reports generated for Data Usage logs in **Excel**, **PDF** or **HTML** formats, as per requirement.

1. Select the export option of your preference and then click **Export**.

A message appears informing about successful export.



2. Click the link in the prompt to open/download the report.





# History 通

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/Signal	Strength Ge	o Fence Histo	гу Арр	Usage History		
<ol> <li>Data Purge set to "60 days", to configu</li> <li>Applicable only for MDM group type.</li> </ol>	re <u>click here</u>				(HTML V)	Export 🔎 🖗 ?
. Managed Devices	Mobile Number	User's name	Groups	Last Location	Last Location Date and Time	Total Locations
	7814111418	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				
Mobile Number	This column displays the mobile number of the managed device.				
User's Name	This column displays the user's name 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.				
Last Location Date and Time	This column displays the last location date and time.				
Total Locations	This column displays the total number of the locations where the managed device was active. By clicking the numbers, you can view a detailed device location history recorded on the map along with the Date, Time, Latitude and Longitude. You can also export these details in PDF, XLS, and HTML formats.				





# Battery Status/Signal Strength

This tab displays the status of battery, Wi-Fi, and SIM signal strength of a device.

Data Purge set to 59 days, to con	ingure <u>click here</u>			
Managed Devices	User's name: 341 = 10+141 + b27	Mobile No: 341-11-11-11-12		<u>e</u> (
AutoAdded_COD			1 - 3 of 3 H + page 🤇	1) of 1 → H Rows per page: 20
AutoAdded_COD	Date	Battery Status	1 - 3 of 3 10 ( page ( WiFi Strength	1 of 1 + H Rows per page: 20 SIM Signal Strength
AutoAdded_COD	Date 26 May 2023 11:30 AM	Battery Status	1 - 3 of 3 K + page ( WiFi Strength 99%	1 of 1 + H Rows per page: 20 SIM Signal Strength No Network%
AutoAdded_COD	Date 26 May 2023 11:30 AM 26 May 2023 11:18 AM	Battery Status	1 - 3 of 3 K ( page ( WiFi Strength 99% 99%	1 of 1 + H Rows per page: 20 SIM Signal Strength No Network% No Network%

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.		
<b>SIM Signal Strength</b> This column displays the available SIM signal strength of a dev			

# Geo Fence History

The Geo Fence History displays the geo fencing history of the devices along with the details of date/time and location of the fence (inside or outside).

Location History Battery Status/Signa	al Strength Geo Fence Histo	ory App Usage History					
Data Purge set to "60 days", to configure <u>click here</u>							
Applicable only for MDM group type.							
🗄 🔚 Managed Devices	User's name: a Mobile	No: 78 8	(1	HTML 💙 🖻 Export 🔎 💠 ?			
🚍 Test_#3	Note: More accurate results can be achieved for Geo-fence, if the device is in-use/active.						
🚰 Test 66		1 - 3 of 3 H (page 1 of 1 ) H Rows per page: 20 ♥					
🗄 🧫 test_ntim	Date	Lat/Long From Device	Fence Name	Inside/Outside Fence			
	04 Aug 2021 06:57 PM	19.12004,72.87364	SU	Outside Geo Fence			
	04 Aug 2021 06:51 PM	19.12003,72.87364	H	Inside Geo Fence			
	04 Aug 2021 06:50 PM	19.12003,72.87365	H	Entered Geo Fence			

Column	Description			
Date	This 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 Fence	This column displays the name of the last visited fence.			
Status	This column displays the fencing status of a device.			





Last Lat/Long	This column displays the coordinates of latitude and longitude of the
	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.

Location History Battery Status/Signa	al Strength Geo Fence	History App Usage Histo	ry				
Data Purge set to "60 days", to configure <u>click hara</u>							
Applicable only for MDM group type.							
⊕	User's name: a M	obile No: 78 Tota	al Usage: Today 🔹 🖌 HTML 🗸	ピ Export 🔎 🔅 ?			
	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 Name	This column displays the name of the application.				
Package Name	This column displays the package name of an application.				
Total Usage Time         This column displays the total time period the application has					





# 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.

ncing Location(s)							
+ Add 🛛 📲 Edit 🗍 🤠 Delete 🖉 Viev	v On Map	🗈 Import Locat	ions via file				
				1 - 4 of 4 H + Fage 1 of 1 → H Rows per page: 20 🗸			
Custom Address	Latitude	Longitude	Radius(m)	Address			
] a.	18.95424	72.81383	2000	Mala della Cheveratta, Cirgano, Rumba, Maharashtra 400007, India			
a######	19.07598	72.87766	200	Kamat Sagar, Lawar Sana, Manda Calang, Karla Madi, Karla, Mumbai, Maharashtra 400070, India			
] не	17.44877	78.39173	100	; Telangana 500081, India			
Office	19.12000	72.87357	400	bil. Ad Rumber 15. Hand With Industry Educe. Andher East, Mumbai, Maharashtra 400069, India			

# Creating a Fencing Location

To create a Fencing Location, it is necessary that a default location must be set first.

1. Click **Fencing Location**(**s**) and then click **Set Default Location**. Default Location window appears.



2. Enter the location and then click Save.





3. After setting the default location, click **Add**. Fencing Location(s) window appears.

Fencing Location(s)
जागश्रय Arto Science and Mahakali Caves 🕤
c Map Satellite escan india Search owai Garden کو الک
MC X
ition Plot No 80, Rd Number 15, Marol MIDC Industry Estate, Andheri East, Mumbai, Maharashtra 400093, India Pot
वर्मा नगर
TY Rendra, Andheri अधेरी इंस्ट Powal Police प्रवर प्रतिस्त and प्रवर प्रतिस्त and प्रति स्त क्र स्त क्र प्रति स्त क्र स्त क्र क्र स्त क्र स्त क्र क्र स्त क्र क्र क्र स्त क्र स्त क्र क्र क्र क्र क्र स्त क्र स्त क्र क्र क्र क्र क्र क्र क्र क्र क्र क्र
una Tara Andheri अधेरी Garada agara Garada agara
PARLE COLONY कॉलरेनी कॉलनी कॉलनी Axon Hospital & Dialysis Center कॉलरेनी Millat Hospital Willight of the server
Google Sahar Airport Keyboard shortcute Map data @2021 Terms of Use Report # map er
Location Details
Latitude: 19 Longitude: 72.
Radius(m): 200 V Meters Set
Address: Plot No 🔄, Rd Number 📑, 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 an 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**. The default location will be saved.

## Editing a Fencing Location

To edit a fencing location:

1. Select a location and then click **Edit**.

Fencing Location(s)				¢ ?
+ Add 📱 Edit 🗑 De	lete 🛛 🛛 View On Map	Edit Default Location	± Import Locations via fi	e
		1 -	1 of 1 ⊣ ( page 1 of 1	Nows per page: 20 ♥
		:	:	:
Custom Address	Latitude	Longitude	Radius(m)	Address
Custom Address	Latitude	Longitude	Radius(m)	Address

2. After making the necessary changes, click **Save**. The fencing location will be modified.





# Deleting a Fencing Location

To delete a fencing location:

1. Select a location and then click **Delete**.

Fencing Location(s)				¢ ?
🕇 Add 📲 Edit 🇊 Delete 🛛	7 View On Map 🕒 I	Edit Default Location	± Import Locations via file	> → Rows per page: 20 V
Custom Address	Latitude	Longitude	Radius(m)	Address
office	19.07598	72.87766	200	-

A confirmation prompt appears.

Delete Location	×
Are you sure you want to delete selected Geo Location(s)?	
OK Cance	

2. Click OK.

The fencing location will be deleted.

## View On Map

Clicking View On Map lets you view the selected location on the Google Maps.

Custom Ad	ldress: TEST1					×
Мар	Satellite			Holy Cross Church, होली	Kurla	ऑफ ई ि न ट ज
J.S.	SHIV NAGAR ज्ञिव नगर		City Hosp Research C सिटी ह	ital & entre ऑस्पेट्ल	Kirol Premier o	<b>KI</b>
a Market इतिना बाजार	Our Lady of Egynt Church + Cbd Belapur - Near	State Bank of India भारतीय स्टेट बॅक Bridge Ending, Lower Parel,	Kismat Nagar, Ki	Habib Hospital urla, Mumbai, Maharash	Nonra 400070, India	YAVIHAR DCIETY Vi वेद्याविहार सोसायटी K
CS- Red	KALINA कलिना SCLR Brid स्कल्प	Mariya म ब्रिज RUPA NA रुप नगर	A R	Kohinoor Hospi को रूग्ण प्रावा Hospital सि सरज हॉस्पिटल	tal केन्द्र Kurla EMU Carshe कुल्	d र्ग छ
ha Mumbai ersity । मंबई	Axis Bank कि ऐक्सिस बँक Centrum Capital Lim	र् Trade Centre BKC हेद संदर, बीकेसी	Paline Wes	RURL कुर्ला वेस्ट T	ईएमयू कार्रहोः A	
<b>Q</b> J Google	SW Centre - leadquarters BANDR A COM aign aign	KURLA PLEX कुर्ला लेक्स	कला वेस्ट श्रि	Vithal Rukm	ini Mandir Lokma विव्रल Tilak Term रुक्मिणी मंदिर मुंबई लोव टिळक टो ata ©2021 Terms of Use	anya inus मान्य मेनस Report a map error
Location D	etails 19.07598 Longitude: 72.87	766 Radius(m): 200				Cancel




## Import Locations via file

The Import Locations via file option allows you to import locations through a (\*.txt, \*.csv) file and user location details in the following format for adding multiple locations at once with latitude, longitude, radius (m), and custom address. For example, 19.46523, 58.69659, 100, Head Office. To import multiple locations, follow the steps mentioned below:

1. Click **Import Locations via file** option.

Add Multiple Locations window appears.

Colored Electron and 18 and 8 and 1
Select file for import (",txt,",csv)i
Choose File No file chosen Upload
Latitude,Longitude,Radius(m),Custom Address
Eg: 19.46523,58.69659,100,Head Office
Note:
Latitude: Enter the latitude (Will be truncated upto 5 decimal places)
Radius(m): Enter radius for the geolocation
(Allowed values: 100,200,300,400,500,600,700,800,900,1000,
Custom Address: Add custom address for the Lat./Long.
(Allowed values: 100,200,300,400,500,600,700,800,900,1000, 1200,1400,1600,1800,2000,2500,3000,3500,4000,4500,5000) Custom Address: Add custom address for the Lat./Long.

- 2. Click on **Choose File** to browse file.
- 3. Click Upload.
- 4. After uploading click **OK**. The locations will be imported.





# 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 sub modules:

- User Accounts
- User Roles

### User Accounts

With User Accounts sub module, you can assign Administrator role to added users and reduce the workload. This sub module displays a list of users and their details such as Domain, Role, Session Log and Status and many more. You can create new user accounts and also add them from Active Directory.

Use	r Accounts						¢ ?
	Create New Accou	Int Add from Active Directory		<b>1 - 1</b> of 1	(page 1 of 1 ⊳)	Rows per page:	10 🗸
	<u>User's name</u>	Full Name	<u>Domain</u>	Role	MDM Role	Session Log	<u>Status</u>
	root	Administrator account created during installation		Administrator	Administrator	View	<b>V</b> .0
	Create New Accou	Int Add from Active Directory		<b>1 - 1</b> of 1	( page 1 of 1 ⊳	Rows per page:	10 🗸

#### Creating a User Account

To create User Account, follow the steps given below:

1. In the User Accounts screen, click **Create New Account**. Create User form appears.

Create User	•	?
User Account	ts > Create User	
Account T	ype and Information	
Userna	me*:	
Full Na	me*:	
Passwo	ord*:	
Confirm	n Password*:	
Email A	Address:*	
		For Example: user@yourcompany.com
Account R	ole	
Role*:	Administrator	<b>v</b>
MDM Role*:	Administrator	<b>v</b> ]
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

To add a user from Active Directory:

1. In the User Accounts screen, click **Add from Active Directory**. Add Active Directory Users form appears.

Add Active Directory Users		?
<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*:		
Al-D+*.		
	307	
Search		
Search Results		
Users	Selected Users	
Account Role		
Role*: Administrator	<b>v</b>	
MDM Role*: Administrator	<b>v</b>	
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  $\leq$ .
- 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.





User Accounts		
Do you want to delete the selected user acc	count(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 new user role, follow the steps given below:

 In the User Roles screen, click New Role. New Role form appears.

New Role		¢ ?
Role Details		
New Role Name :*		
Description :		
Role Details         New Role Name :*         Description :         Select Group :         Select subgroups on selecting Parent group		
Select subgroups on sele	cting Parent group ces	
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. Select the checkbox **Select subgroups on selecting parent group**, if you want to select subgroups by default after selecting parent group.
- 6. Click OK.

The new user role will be added and the Permissions section appears displaying Main Tree Menu and Client Tree Menu tabs.





iils			
w Role Name :*	IT_minin		
escription :	winever-		
Select Group			
Main Tree Menu	Client Tree Menu	Winner	Configure
	Menu		
Dash Board			
Managed Mobile Devi	ces		
Manage Backup			
Anti Theft			
Asset Management			
Report Templates			
Report Scheduler			
Events And Devices			
App Store			
Content Library			
C-111			

The Main Tree Menu consists of all the modules and configuration permissions.

The Client Tree Menu consists of selected groups on which permissions the user is allowed to take further.

New Role			¢	?
Role Details				
New Role Name :*	9930			
Description :	fyliayiayiayia			
Select Group	Client Tree Menu	Please Select a Group to set Permission		
Save Cancel				

- 7. Select the checkboxes that will allow the role to view/configure the settings.
- 8. After selecting the necessary checkboxes, 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:

In the User Roles screen, select a role.
 It enables **Properties** and **Delete** buttons.

User Roles	¢ ?
New Role Properties 🗊 Delete	
Role Name	Description
Administrator	
Viewer	

2. Click Properties.

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.

## 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.



<b>F</b>	
Choice	

Export Settings	Import Settings Scheduling	9	
WMC Setting Database	s and Policies		
Export			
View Exported Fil	es		
Export files path:		Change Path	
1. Select required 2. Click on "Expor	settings t" to export eScan Management Conso	ole settings	

- To backup WMC Settings and Policies and Database, select both the checkboxes. The backup file will be exported to the path shown in Export files path field. To change the file path, click Change Path. In the Add Folder window, enter the file path and click Add.
- 3. Click Export.

The backup file will be exported to the destination path. A success message appears at the top displaying date, time, and a download link for the exported file.



#### **Import Settings**

This tab lets you import the eScan Server Settings, Policies, and Database. To import the eScan Server settings, follow the steps given below:

1. In the Export Import Settings screen, click Import Settings tab.

Export Settings Import Settings Scheduling	
File Name Choose File No file chosen	
WMC Settings and Policies	
Database	
Import	
View Exported Files	
<ol> <li>Select file to import (EservConf_[YYYYMMDDhhmm][_SCHD].zip)</li> <li>Select required settings</li> <li>Click on "import" button to import the saved settings</li> </ol>	

- 2. Click Choose File.
- 3. To import WMC Settings and Policies and Database, select both the checkboxes.
- 4. Click Import.
- 5. 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.
NOTE • The Import Settings tab lets you import only Settings and Policies or Database.

#### Scheduling

This tab lets you schedule auto-backing up of Settings, Policies, and Database.

Enable Export Sche	duler			
WMC Settings a	nd Policies			abase
Daily     Weekly     Monthly	Mon Fri	💭 Tue 💭 Sat	Wed	🗆 Thu
e At	12:00 pm	0 <b>-</b>		
Sender: Recipient: SMTP Server: SMTP Port:				
Use SMTP Au User name: Password:	thentication			
Enable Optional Select how many ba Create the backup o	Settings ckup files to store nly if drive space is great	er than or equal to :	2 V 500	(MB <b>v</b> )

To create a Schedule for export, follow the steps given below:

- 1. Select Enable Export Scheduler checkbox.
- 2. Select the checkboxes whether to back up both Settings and Policies and/or Database.
- 3. Schedule the backup for a **Daily**, **Weekly** (Select a day) or **Monthly** (Select a date) basis.
- 4. For the At field, click the drop-down and select a time for backing up data. If you want to receive email notifications about the procedure, select Enable Notifications Settings checkbox and fill in the necessary details. If the SMTP server requires authentication, select the Use SMTP Authentication checkbox and enter the credentials. To check if the SMTP settings are correct, click Test. A test email will be sent to recipient email ID.

To configure additional settings for backup file, select the checkbox **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.





# License

The License module lets you manage user licenses. You can add, activate, and view the total number of licenses available for deployment, previously deployed licenses and remaining licenses with their corresponding values. The module also lets you move the licensed devices to non-licensed devices and vice versa. Here you can also view the number of Add-On licenses along with the names.

cense					💲 Refr	esh <u>थ</u> Hel
egister Information				6		-
<u>icense Key(30 char)</u>	Activation Code(60 char)	Registration Status	Contract Period Ends on	No. of Users	Add On License	<u>Refresh</u>
ни адо пран эких алех ваас-оцин вл	Activate Now	Activate before 02-Sep-2023	-	20		\$
Add Licence Click Have						
Add License <u>Click Here</u>	(	Alexandra and a second				
		License	== 🙉 🔛			
			25.0%			
		75.0%				
	• 1	license in Use - 5 🛛 😑 License Rem	aining - 15			
	•	License in Use - 5 🛛 😑 License Rem	aining - 15			

# Adding and Activating a License

To add and activate a license:

1. In the License screen, click the **Click Here** link.



Add License Key dialog box appears.

		X
Add 30 Character Lice	nse Key.	
	(	
	OK	Conservation of the second sec

2. Enter the license key and then click **OK**.

The license key will be added and displayed in the **Register Information** table.





# Moving licensed devices to Non-Licensed Devices section

To move licensed devices to Non-Licensed Devices section:

1. In the License statistics box, click **Manage License**. Manage License window appears.

censed Computers ()	Di Move t	o Non-Licens
Machine Name	Group	
] 🛄 1=	Managed Devices	
12048	Managed Devices	
] 📕 1##	Managed Devices	
3 A S President (P S intendis)	Managed Devices\AutoAdded_COD	
] 🔜 1==33	Managed Devices	
30mmetrika en aktor	Managed Devices\AutoAdded_COD	
on-Licensed Computers ()	<b>節</b> M	ove to Licens
	No Record Found	

- 2. Under the Licensed Devices section, select the device(s) that you want to move to Non-Licensed Devices section.
- 3. Click Move to Non-License.
- 4. The selected device(s) will be moved to Non-Licensed Devices section.

# Moving non-licensed devices to Licensed Devices section

To move non-licensed devices to Licensed Devices section, follow the steps given below:

1. In the License statistics box, click **Manage License**. Manage License window appears.





Manage License					
Licensed Computers / Devices	(2) Filter Licer	nse All 🗸	🚡 Move to Non-License		
Machine Name		Group	·		
🗆 🛄 uaunmu 🙇		Managed Computers			
		Managed Computers			
			<b>v</b>		
Non-Licensed Computers / Devices (1) Filter License All 🗸					
Machine Name	Group	<u>Unlicense Date Time</u>	Description		
🗆 📕 qakatan 🚅	Managed Computers	05/08/2021 16:43:00			
		·			
			-		
Close					

- 2. Under the Non-Licensed Devices section, select the device(s) that you want to move to Licensed Devices section.
- 3. Click Move to License.
- 4. The selected device(s) will be moved to Licensed Devices section.





# **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**