eScan™
Enterprise Security

eScan Enterprise Mobility Management (Android Enterprise)

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

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

Table of Content

Introduction 8
System Requirements 9
Getting Started 9
Dashboard 10
Deployment Status 10
Enrollment 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 38
Common QR Code Scan 38
Refresh Scan Devices 39
Window Buttons 39
Android Templates 42
Anti-Virus Policy 43
Call & SMS Filter Policy 45
Call and SMS Filter Mode set to Off 45
Call and SMS Filter Mode set to Blacklist 46
Call and SMS Filter Mode set to Whitelist 48
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 66
Importing an application 66
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) 68
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 73
Content Library Policy 74
Import a file 74
Kiosk Mode Policy 75
Application(s) to be added to Kiosk 75
Whitelist for apps 76
Hardware Key Control 76
Allow User to Turn ON/OFF 77
Installation of eScan Kiosk Lockdown Application 78
Location Fence 92
iOS Templates 93
Device Passcode Policy 94
Restrictions Policy 95
Device Functionality 95
Web Clip Policy 99
Adding a Web Clip 99
Deleting a Web Clip 100
Email Policy 101
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
Required Applications Policy 109
Importing an application 109
Deleting an application 110
Group Tasks 111
Creating a New Group Task 111
Common QR Code Scan 113
COD/BYOD Enrollment on Android Device(s) 113
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-Theft 166
Wipe Data 166
Block Device 167
Unblock Device 168
Scream 168
Send Message 168
Locate Device 169
Remove Work Profile 170
Factory Reset 170
Lock Device 170
Asset Management 171
Hardware Information 171
Viewing Hardware information 171
Application Information 173

Export Options for the Generated Reports 174
Exporting a Report 174
Report Templates 175
Creating a Report Template 175
Editing a Report Template 177
Deleting a Report Template 177
Viewing a Report 178
Report Scheduler 179
Adding a Scheduler 179
Template Selection 180
Selection For Applied Groups/Clients 180
Report Send Options 181
Report Scheduling Settings 182
Running a schedule 182
Editing a Schedule 183
Deleting a Schedule 183
Viewing the report 184
Viewing results of a report 184
Events and Devices 185
Viewing Events 185
Event Status 185
Device Selection 185
Application/Hardware Changes 186
Events and Devices settings 186
Settings 190
Enterprise Configuration 190
Certificate Management 190
Email Notification Settings 192
Data Purge 192
Connection Sequence 193
Server Configuration 193
Console Settings 194
Two-Factor Authentication 196
Enabling 2FA login 197
Disabling 2FA login 198
Adding Users for 2FA 200
Event Alert 202
UnLicense Alert 203
Content Library 204
Adding a file 204
Editing a file description 205
Deleting a file 206
Call Logs 207
Filter Call Logs 208
Exporting Call Logs 208
Data Usage 209
Filter Data Usage logs 209

Exporting Data Usage logs 210
History 211
Location History 211
Battery Status/Signal Strength 212
Geo Fence History 212
App Usage History 213
Fencing Location(s) 214
Creating a Fencing Location 214
Editing a Fencing Location 215
Deleting a Fencing Location 216
View On Map 216
Import Locations via file 217
Administration 218
User Accounts 218
Creating a User Account 218
Adding a User from Active Directory 219
Deleting a User Account 219
User Roles 220
Adding a User Role 221
Role Properties 223
Deleting a User Role 223
Export & Import 223
Export Settings 223
Import Settings 224
Scheduling 225
License 226
Adding and Activating a License 226
Moving licensed devices to Non-Licensed Devices section 227
Moving non-licensed devices to Licensed Devices section 227
Contact Us 229
Forums 229
Chat Support 229
Email Support 229

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 and software 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

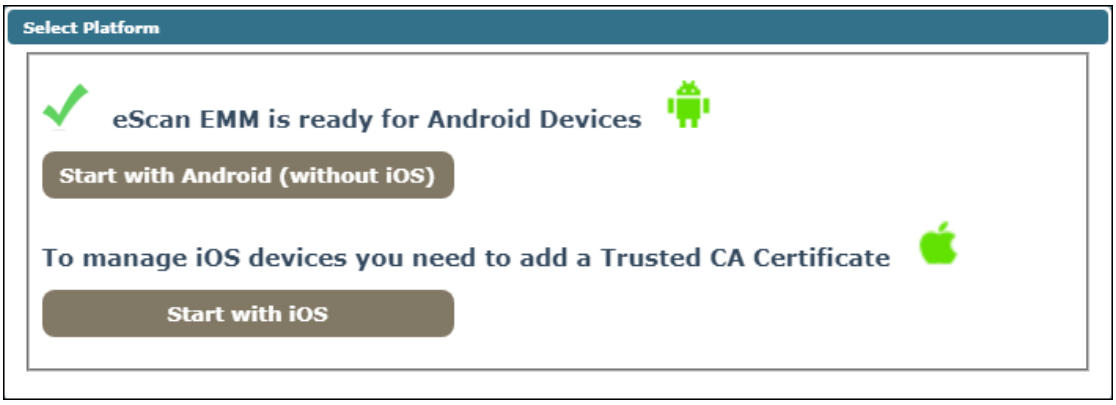
For iOS
(iOS Endpoints) Platforms Supported:

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

NOTE	Rooted and Jailbroken devices are not supported.

Getting Started

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

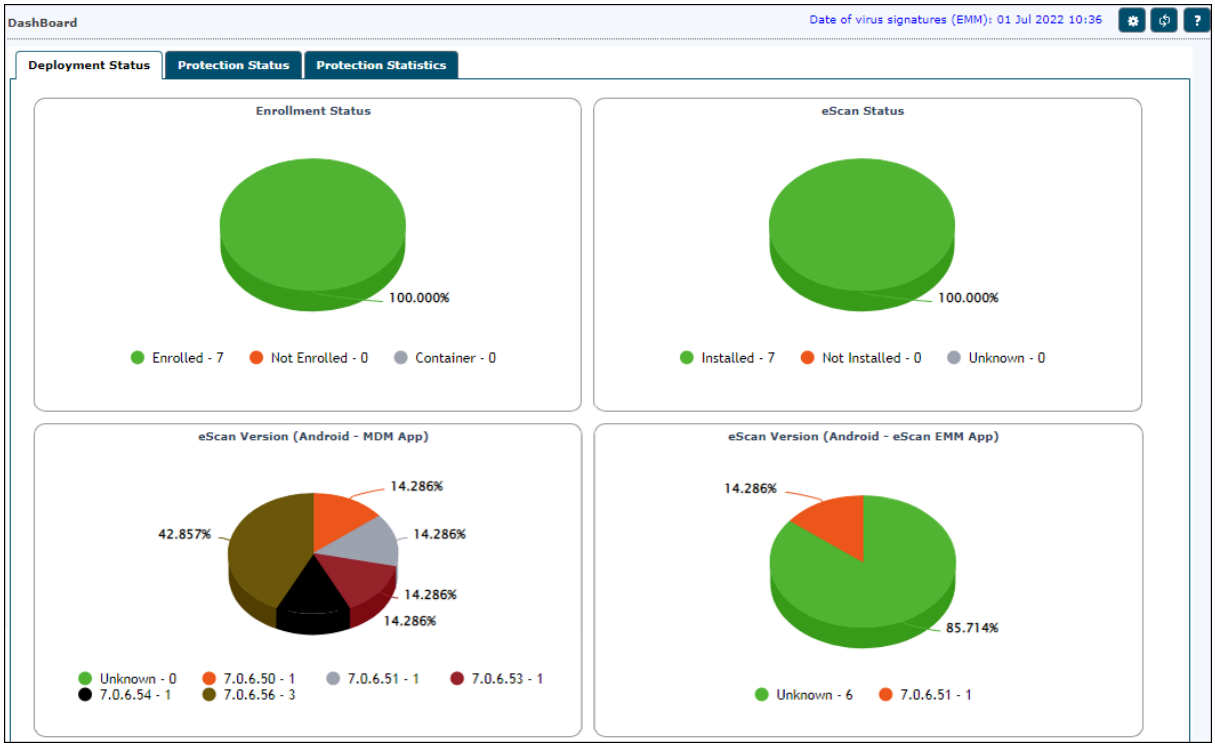


- Clicking **Start with iOS** takes you to the **Settings** module, click **Certificate Management** tab. To learn more about it, **click here**.
- Clicking **Start with Android (without iOS)** displays the **eScan Mobility Management Console**.
- If you clicked **Start with Android (without iOS)**,
  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.

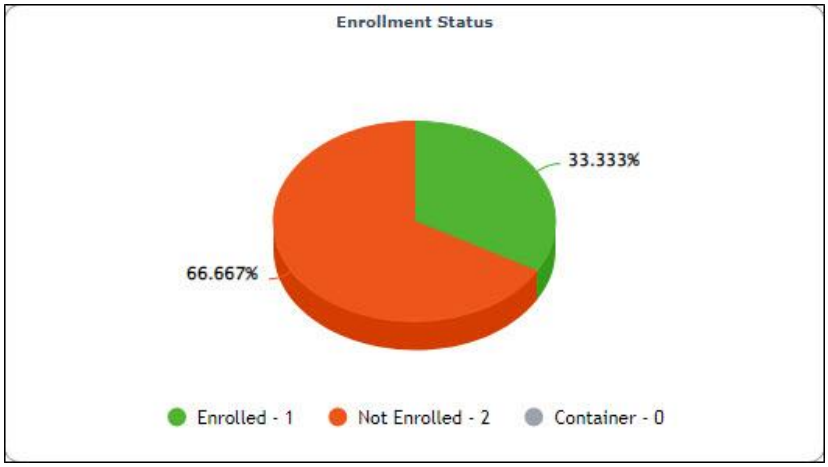


Deployment Status

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

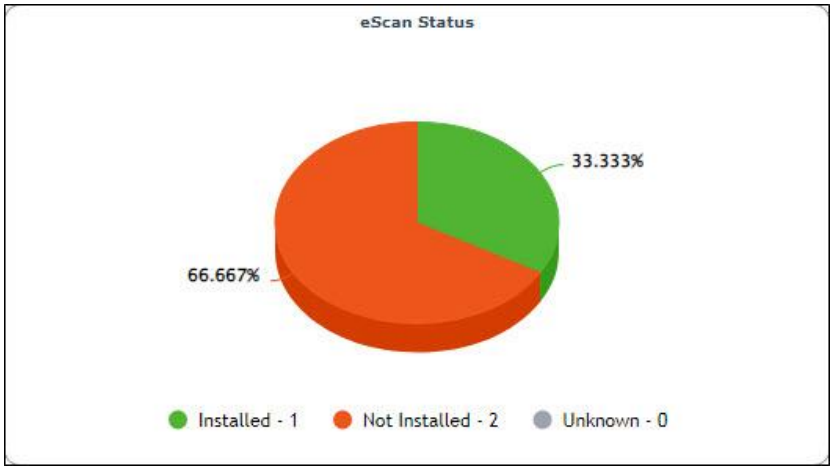
- Enrollment Status
- eScan Status
- eScan Version (Android - MDM App)
- eScan Version (Android – eScan EMM App)
- eScan Version (iOS - MDM App)
- Android Version
- iOS Version
- Device Sync Status (Successful)
- Device Compliance
- Kiosk Status

Enrollment Status



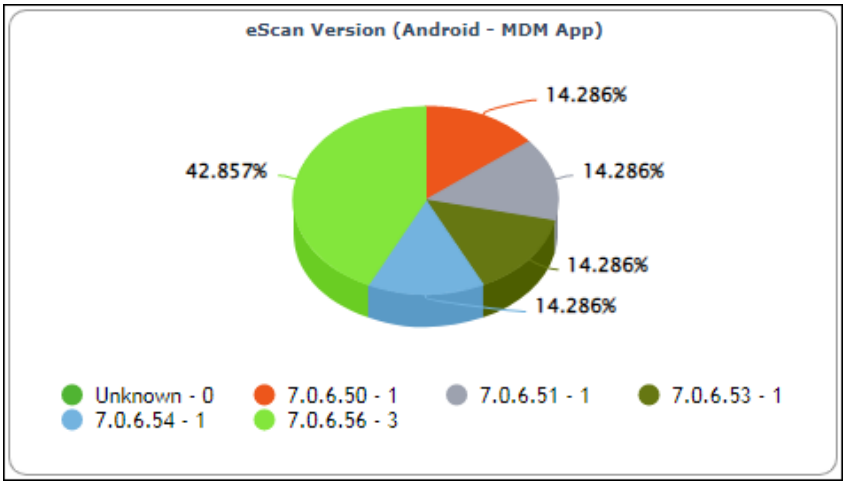
Enrolled – It displays the number of devices that are enrolled.
Not Enrolled - It displays the number of devices that are not enrolled.
Container – It displays the number of devices on which Container application is not enrolled.

eScan Status



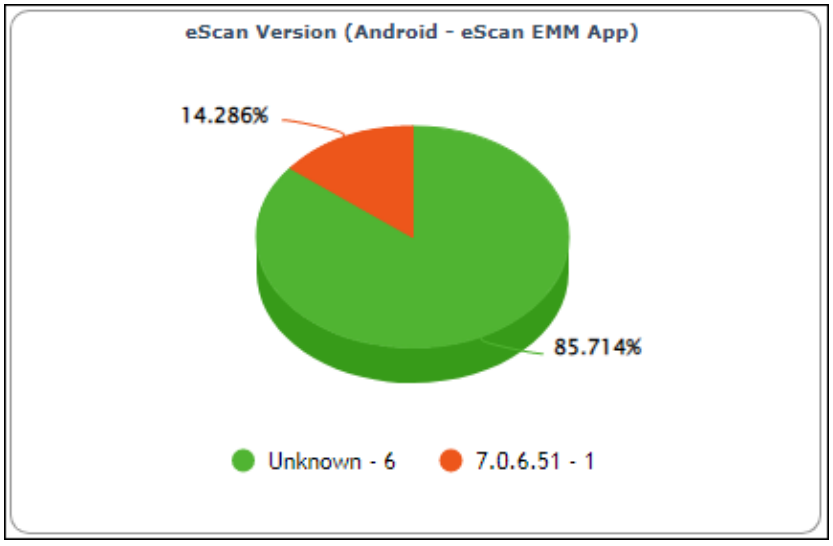
Installed – It displays the number of devices on which eScan MDM application is installed.
Not Installed – It displays the number of devices on which eScan MDM application is not installed.
Unknown – It displays the number of devices on which the eScan MDM application installation status is Unknown.

eScan Version (Android - MDM App)



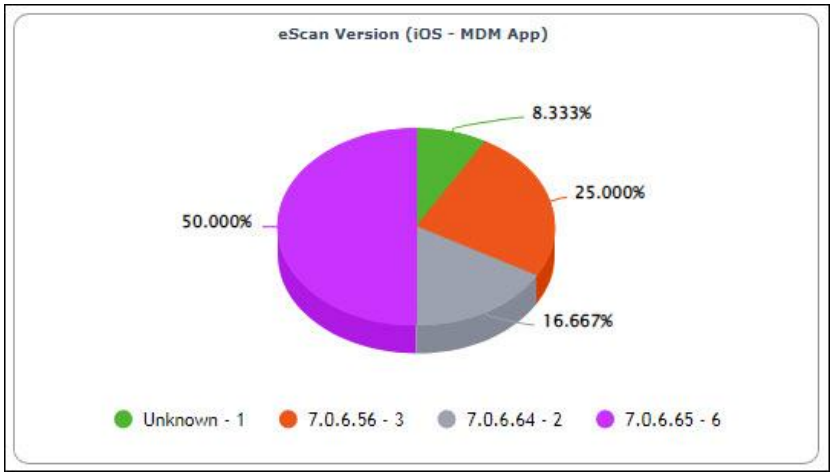
Version Numbers – It displays the Android MDM application's version number installed on devices.
Unknown – It displays the number of devices on which the Android MDM application's version number is unknown.

eScan Version (Android - eScan EMM App)



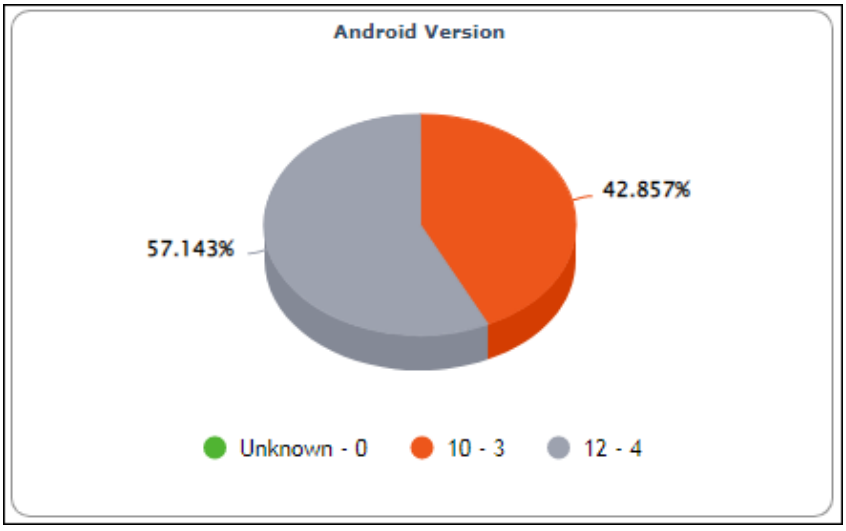
Version Numbers – It displays the eScan EMM application's version number installed on devices.
Unknown – It displays the number of devices on which the eScan EMM application's version number is unknown.

eScan Version (iOS - MDM App)



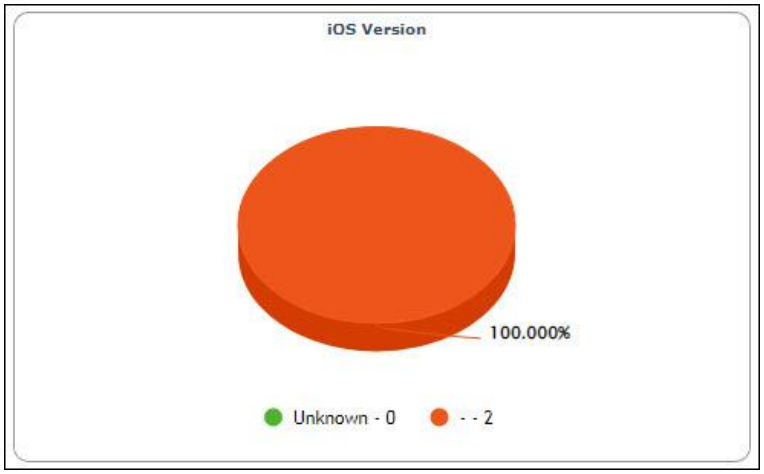
Version Numbers – It displays the iOS MDM application's version number installed on devices.
Unknown – It displays the number of devices on which the iOS MDM application's version number is unknown.
Total – It displays the total number of devices.

Android Version



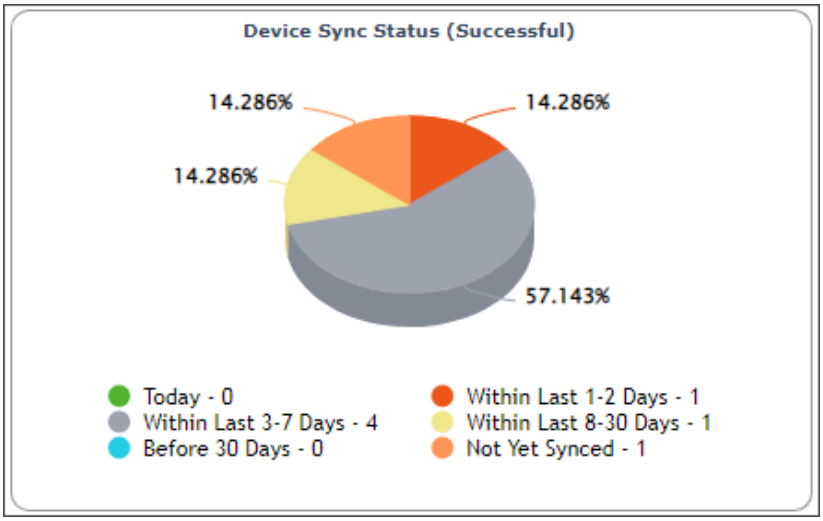
Version Numbers – It displays the Android OS version numbers and the number of devices which are running it.
Unknown – It displays the number of devices on which the Android OS version is unknown.

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.

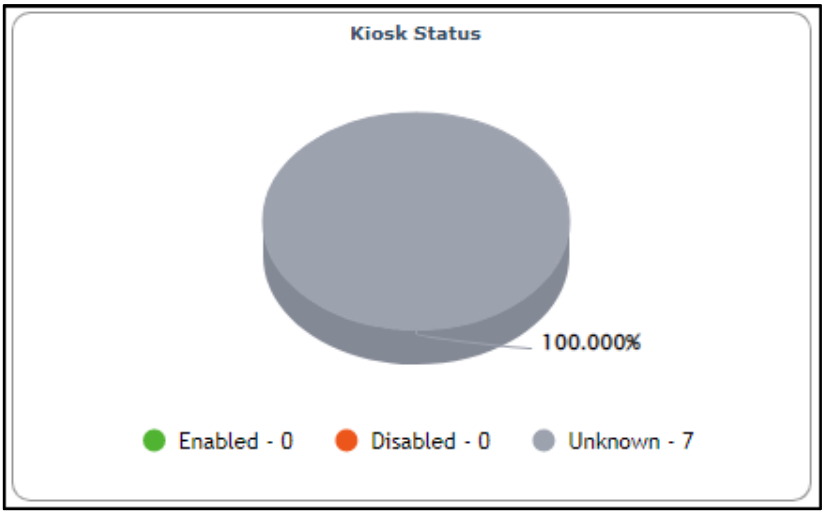
Device Sync Status (Successful)



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.

Kiosk Status

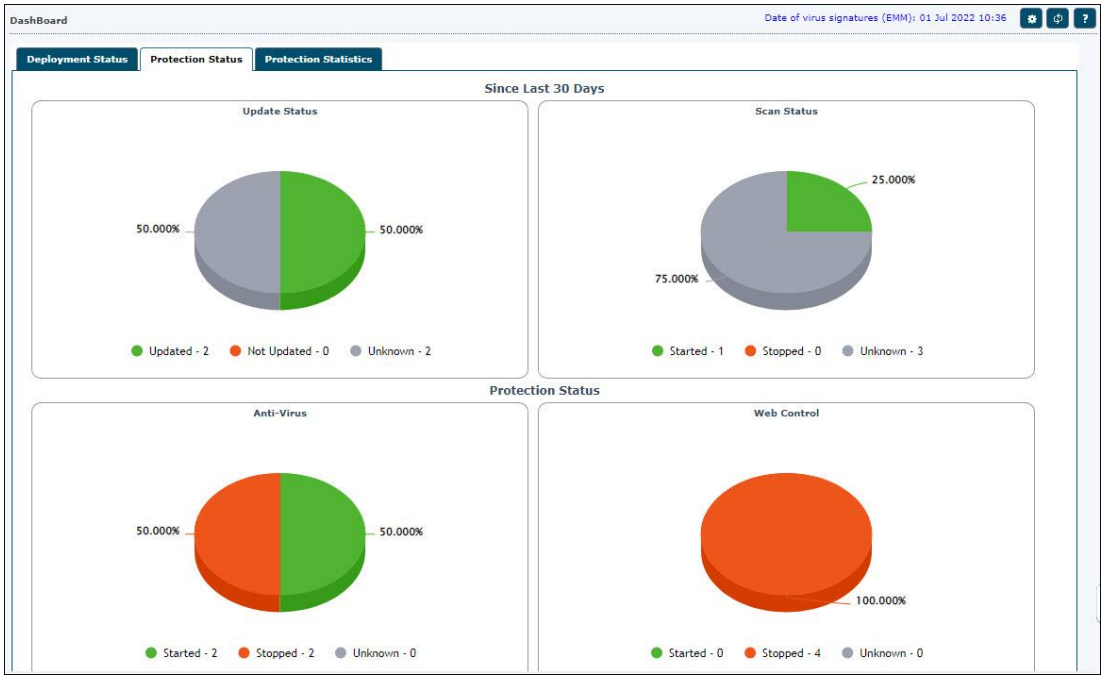


Enabled – It displays the number of devices on which the Kiosk mode is enabled.
Disabled – It displays the number of devices on which the Kiosk mode is disabled.
Unknown – It displays the number of devices on which the Kiosk mode status is Unknown.

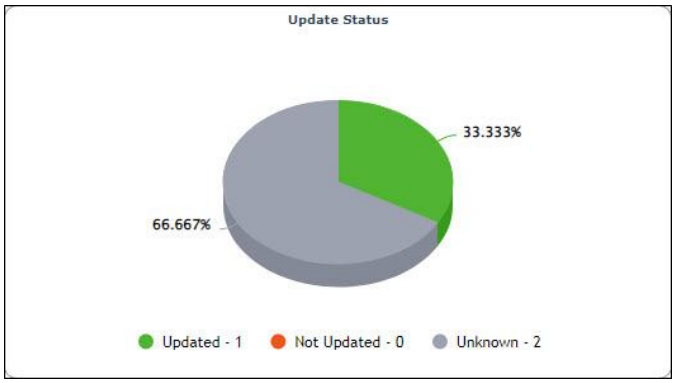
Protection Status

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

- Update Status
- Scan Status
- Anti-Virus
- Web Control
- Application Control
- Call & SMS Filter

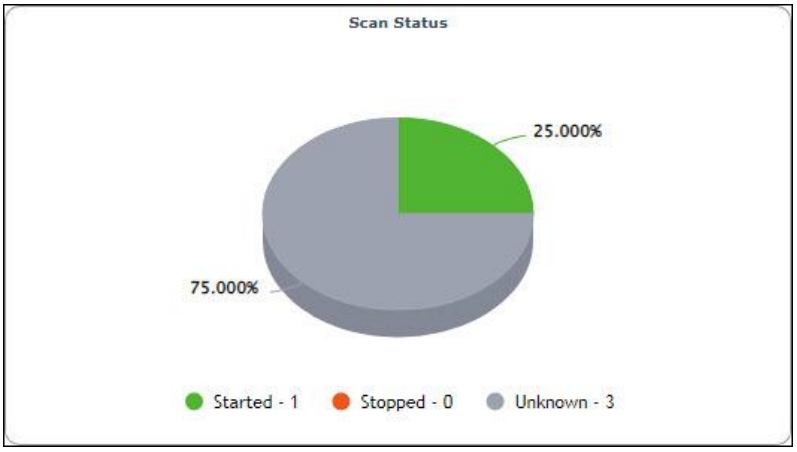


Update Status



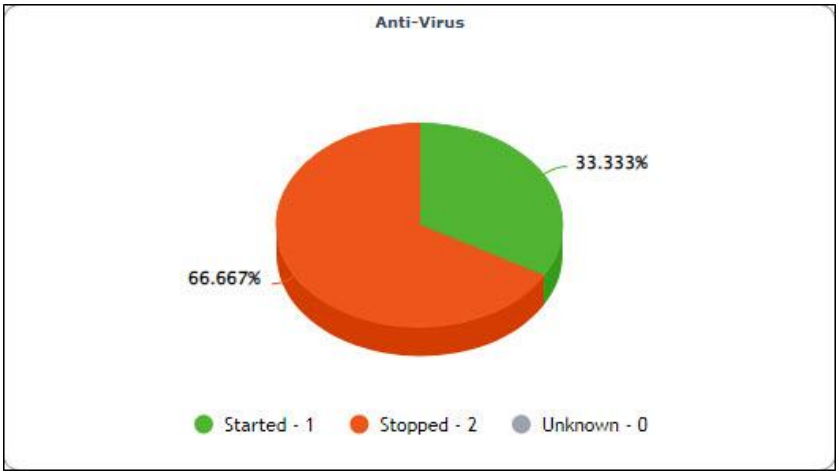
Updated – It displays the number of devices on which the Anti-Virus signatures are updated.
Not Updated – It displays the number of devices on which the Anti-Virus signatures are not updated.
Unknown – It displays the number of devices on which the Anti-Virus signature update status is Unknown.

Scan Status



Scanned – It displays the number of devices which are scanned.
Not Scanned – It displays the number of devices which are not scanned.
Unknown – It displays the number of devices on which the scan status is Unknown.

Anti-Virus

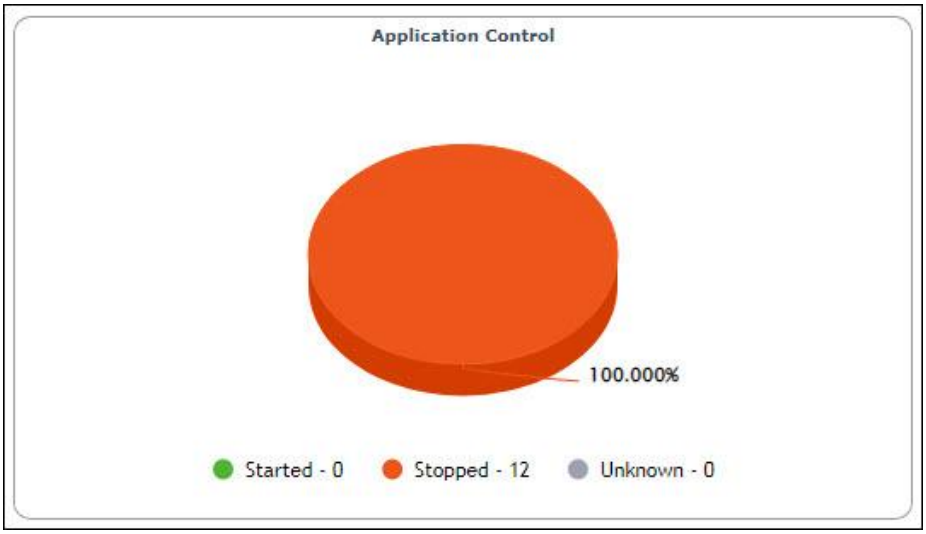


Started – It displays the number of devices on which the Anti-Virus module is started.
Stopped – It displays the number of devices on which the Anti-Virus module is stopped.
Unknown – It displays the number of devices on which the Anti-Virus module status is Unknown.

Web Control

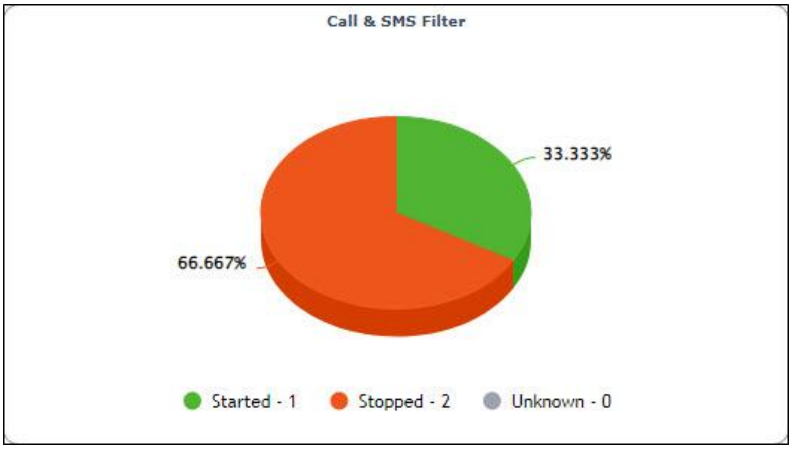
Started – It displays the number of devices on which the Web Control module is started.
Stopped – It displays the number of devices on which the Web Control module is stopped.
Unknown – It displays the number of devices on which the Web Control module status is Unknown.

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

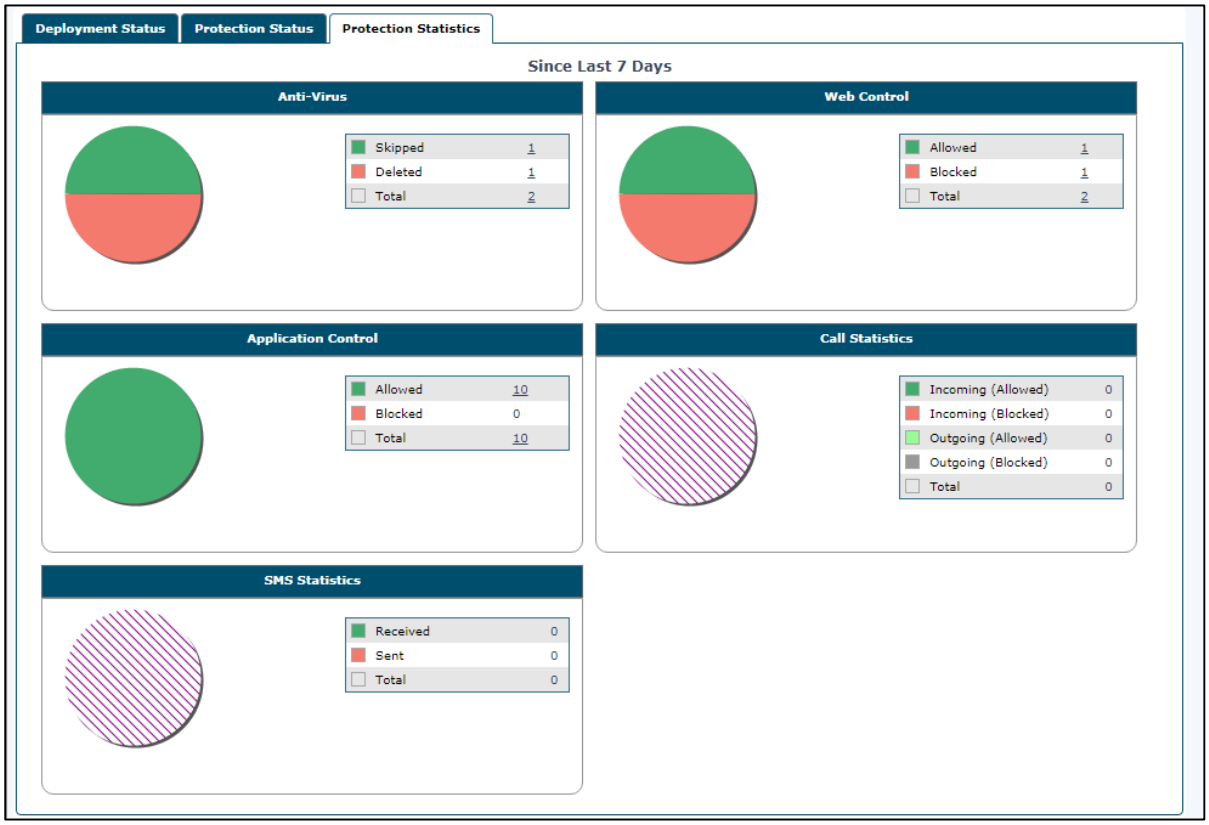


Started – It displays the number of devices on which the Call and SMS filter is started.
Stopped – It displays the number of devices on which the Call and SMS filter is stopped.
Unknown – It displays the number of devices on which the Call and SMS filter status is Unknown.

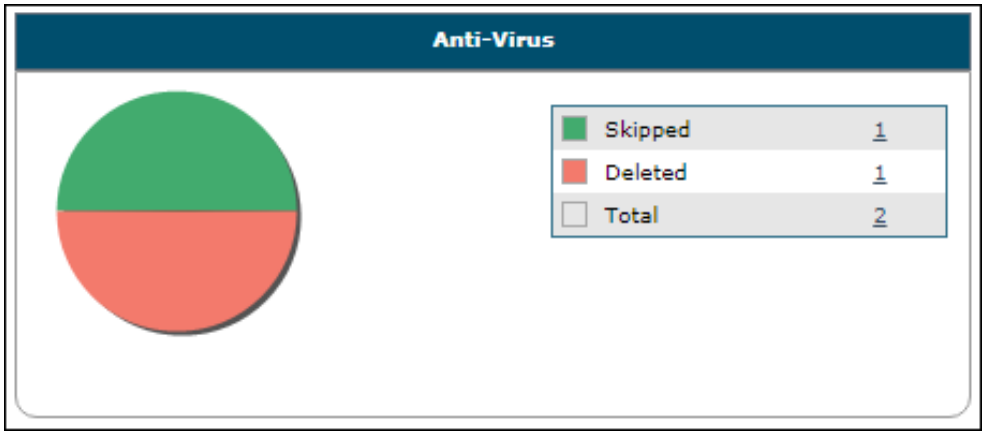
Protection Statistics

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

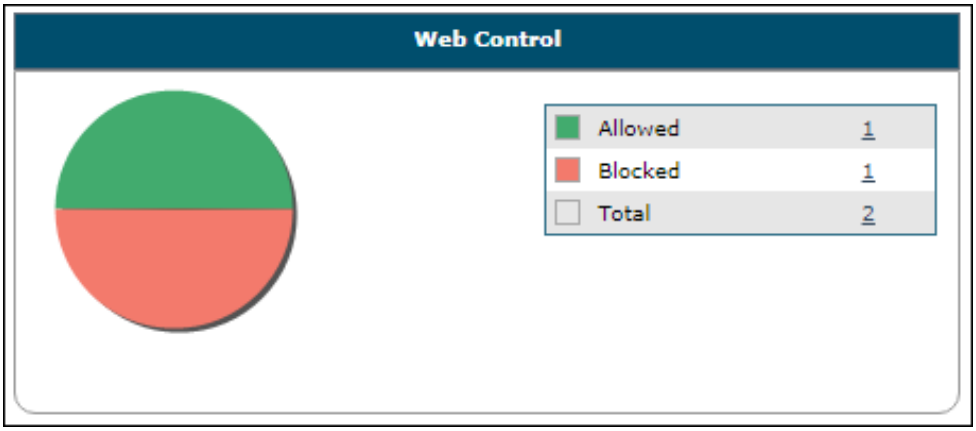


Anti-Virus



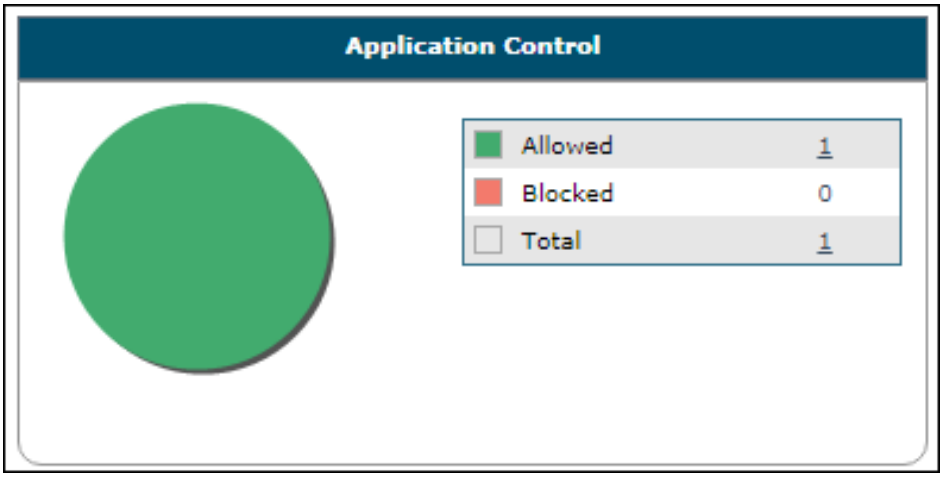
Skipped – It displays the number of files skipped during a scan on a device.
Deleted – It displays the number of files deleted during a scan on a device.

Web Control



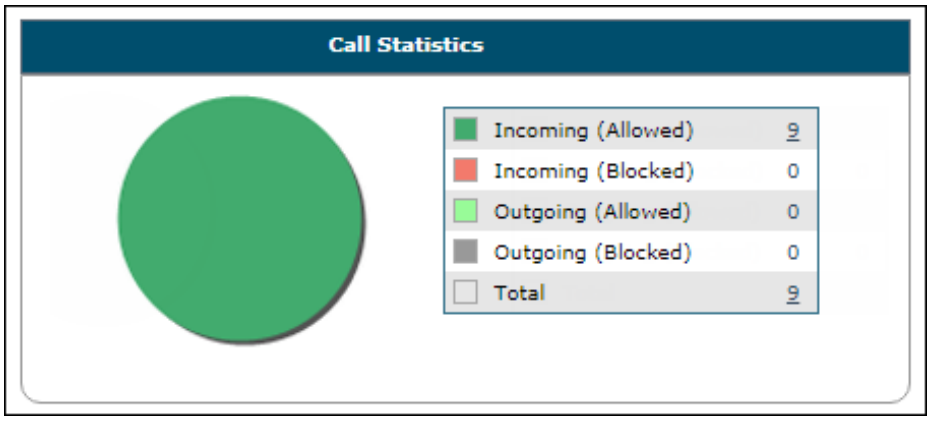
Allowed – It displays the number of websites allowed on a device.
Blocked – It displays the number of websites blocked on a device.

Application Control



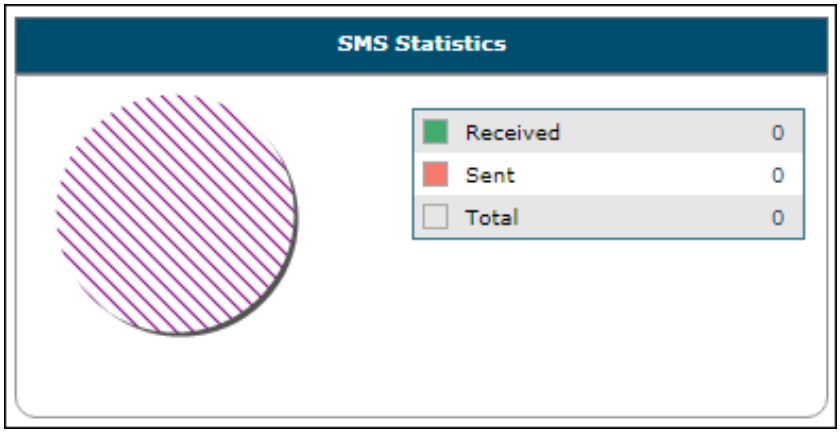
Allowed – It displays the number of applications allowed on a device.
Blocked – It displays the number of applications blocked on a device.

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.

SMS Statistics

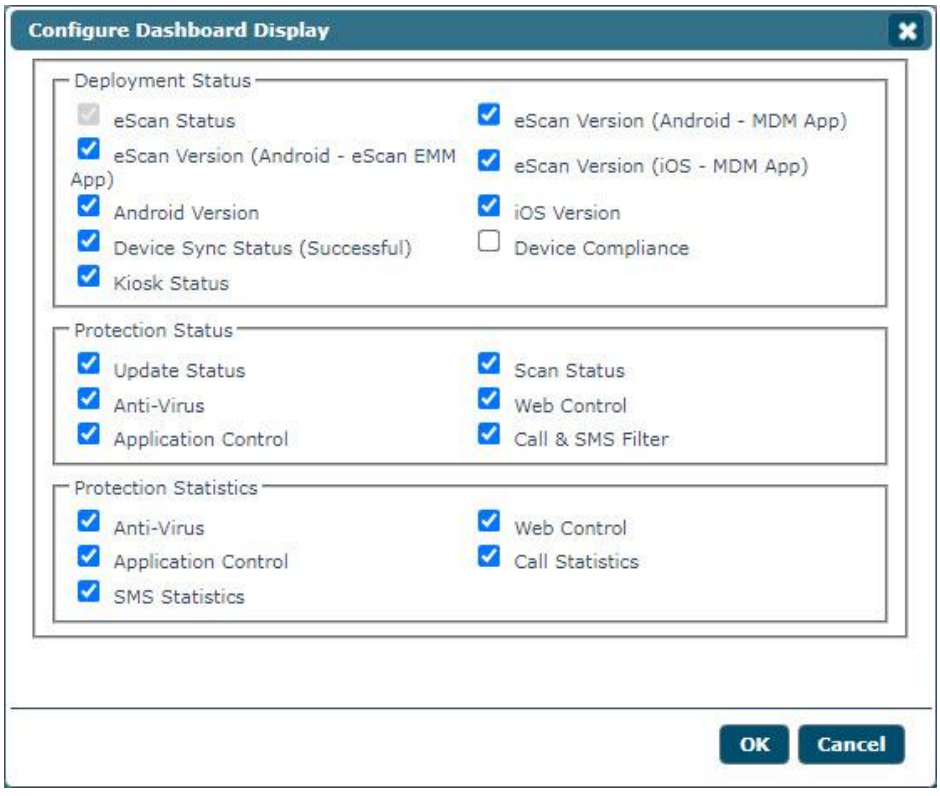


Received – It displays the number of messages received on a device.
Sent - It displays the number of messages sent from a device.

Settings

The Settings let you configure the modules to be displayed in all tabs.

1. Click **Settings** icon
   Configure Dashboard Display window appears.

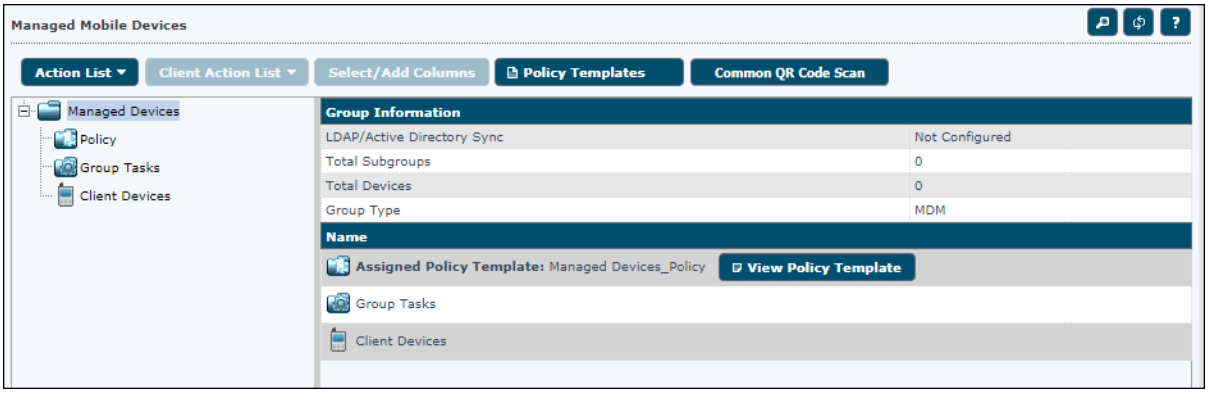


2. Select the module(s) to be displayed in the tabs and then click **OK**.

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



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 **Note**: Do not put space before or after comma in the above format.

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

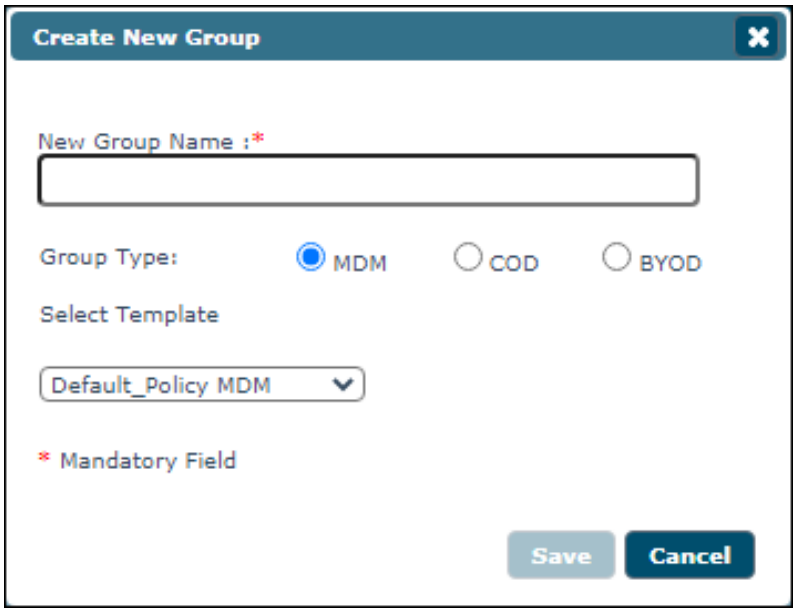
In case the users are allowed to bring their own devices to company for work/task purposes, select the group type as BYOD (Bring Your Own Device). In this group type, user installed apps in the Personal profile will be restricted within the set Geo/Wi-Fi location. This restrictions will be removed once 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, **click here**.

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.

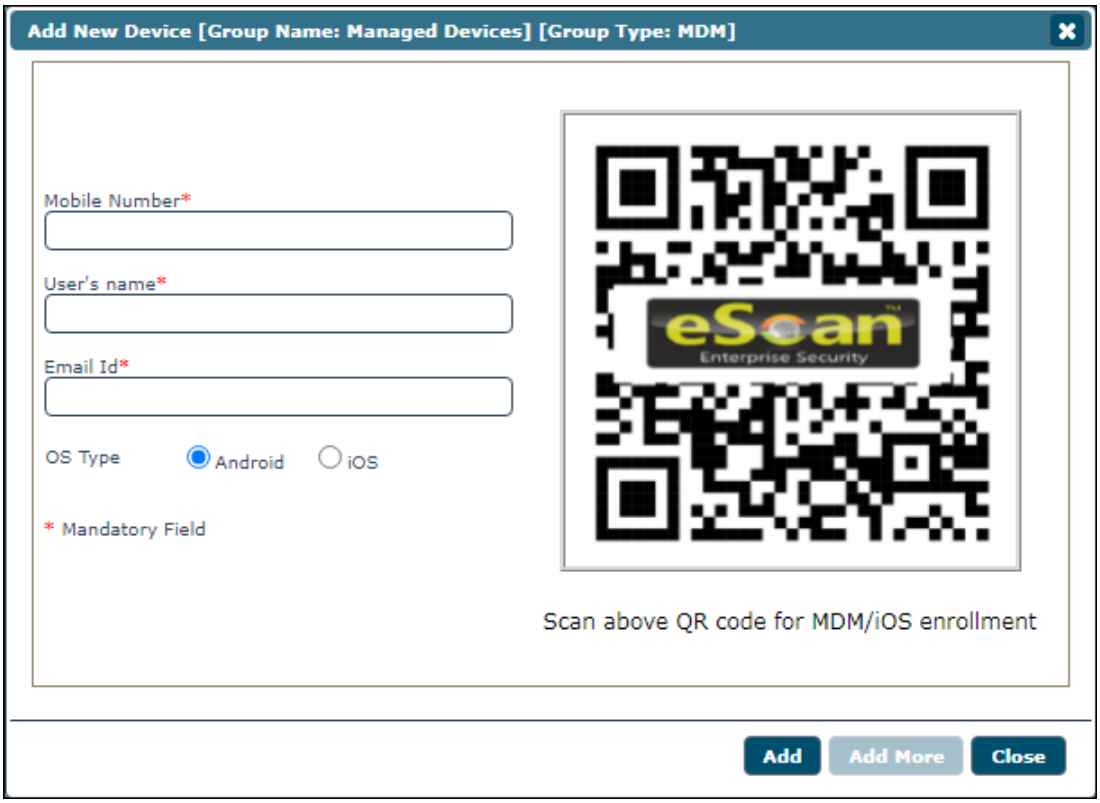


3. Enter a name for group.
4. Select a preferred group type.
5. Select Policy Template from drop down list.
6. Click **Save**.
   A new group will be created.

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.
2. Click **Action List** > **Add New Device**.
   Add New Device window appears.



3. Enter the mandatory details.
4. Select the appropriate OS type.
5. Click **Add**.

An enrollment email with a link to download and install eScan Device Management (client) will be sent to the specified email address.

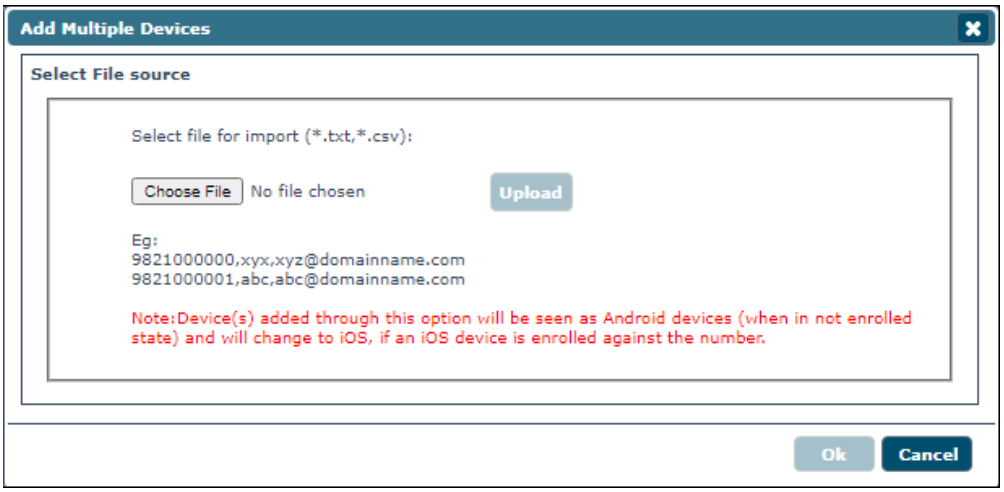
The Add More option will enabled after you add a device. Click **Add More** to add another device in the same group.

NOTE	The mobile number required here, only for indicative purpose and it need not be an actual mobile number.

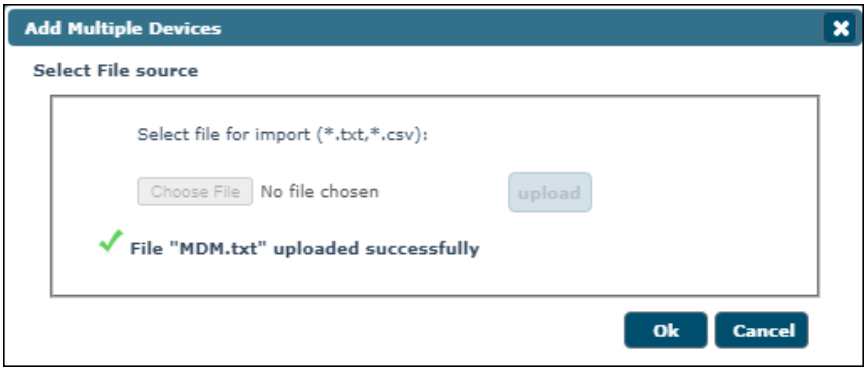
Adding Multiple Devices

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.



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.



5. Click **OK**.

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

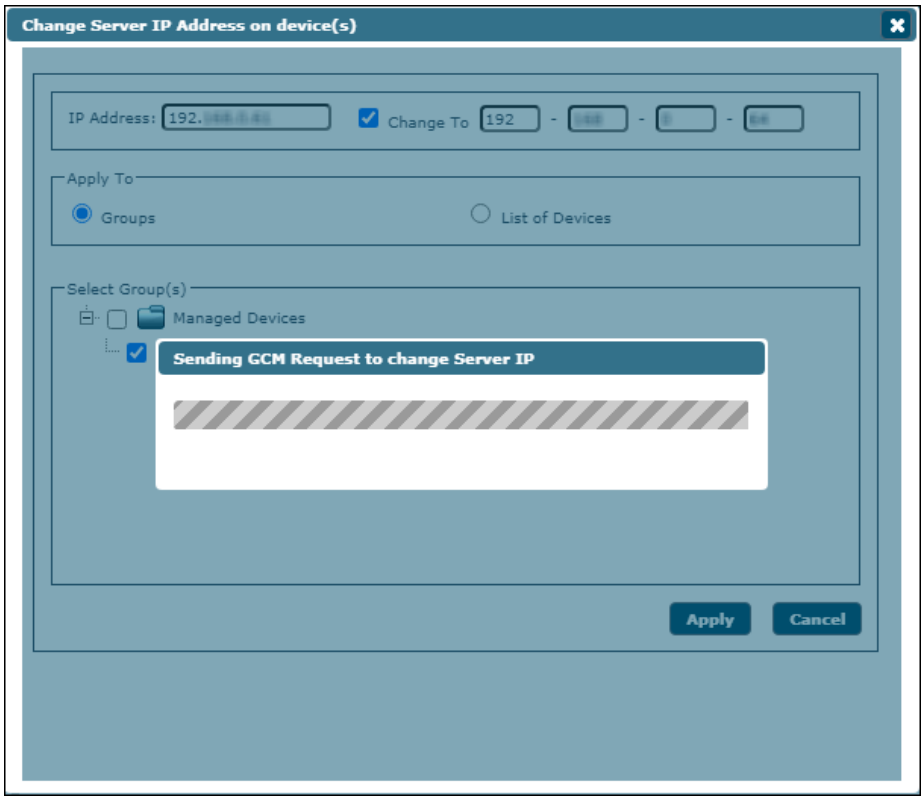
All devices from the **.txt** and **.csv** file will be added to the group.

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.

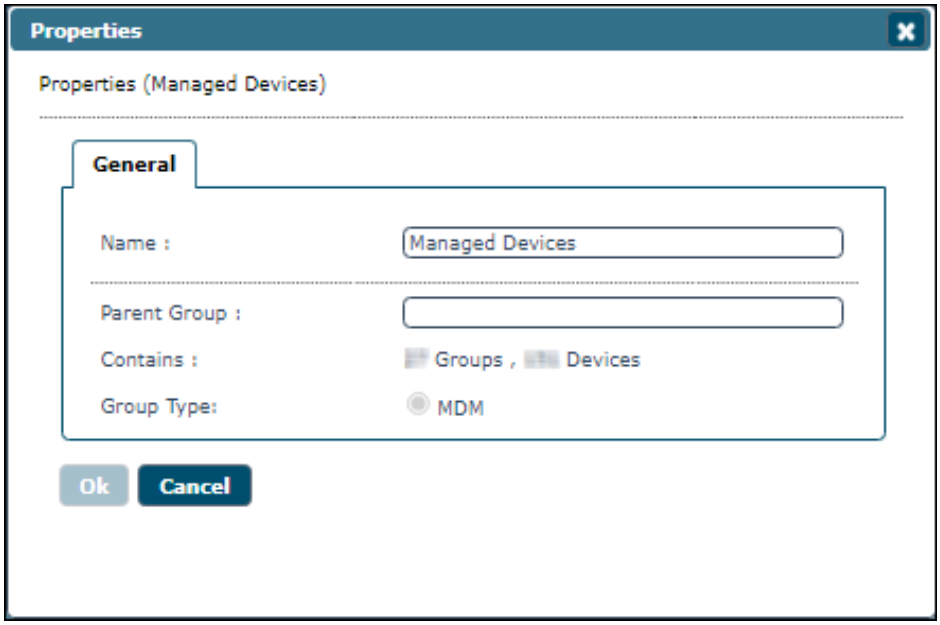
3. Select the **Change To** checkbox and enter the new server IP address.
4. In the **Apply To** section, select whether IP address change is for **Groups** or **List of Devices**.
5. Select the group or devices in below section.
6. After you are done making changes, click **Apply**.



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.



Client Action List

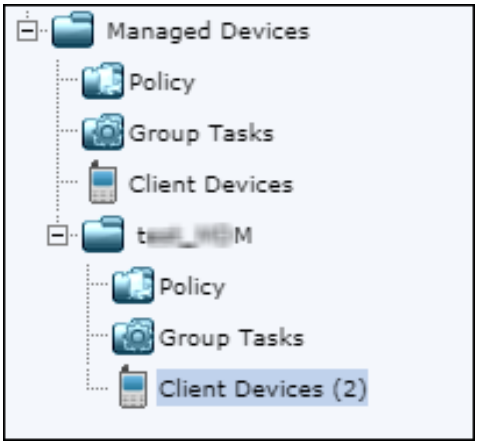
This drop-down lets you take action for the devices added in the console.

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

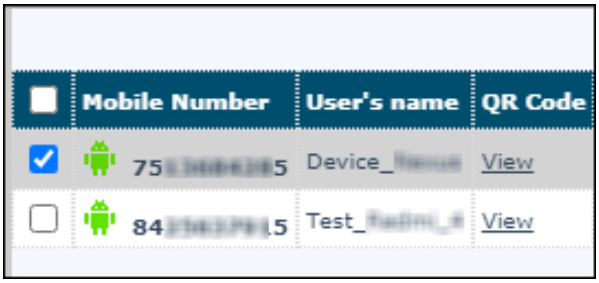
Moving Device from one group to the other group

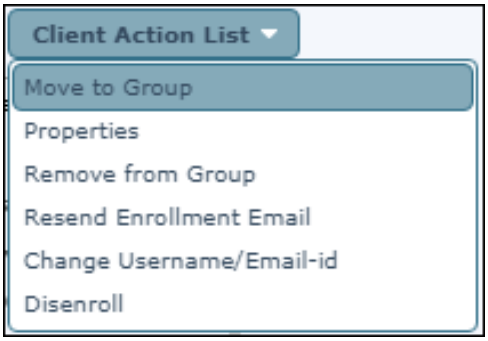
After adding devices in a group, you can move a device or devices from one group to other as per your requirement.
To move device(s) from one group to other, follow the steps given below:

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

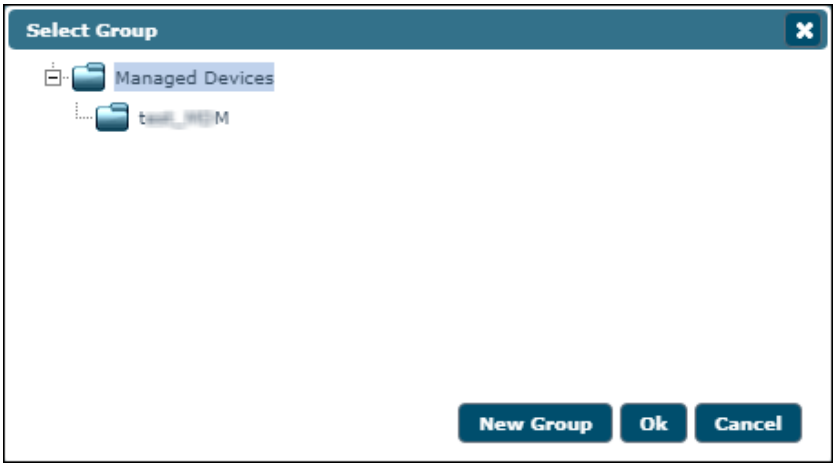


2. Select the device you want to move to another group and then click **Client Action List** > **Move to Group**.





Select Group window appears.



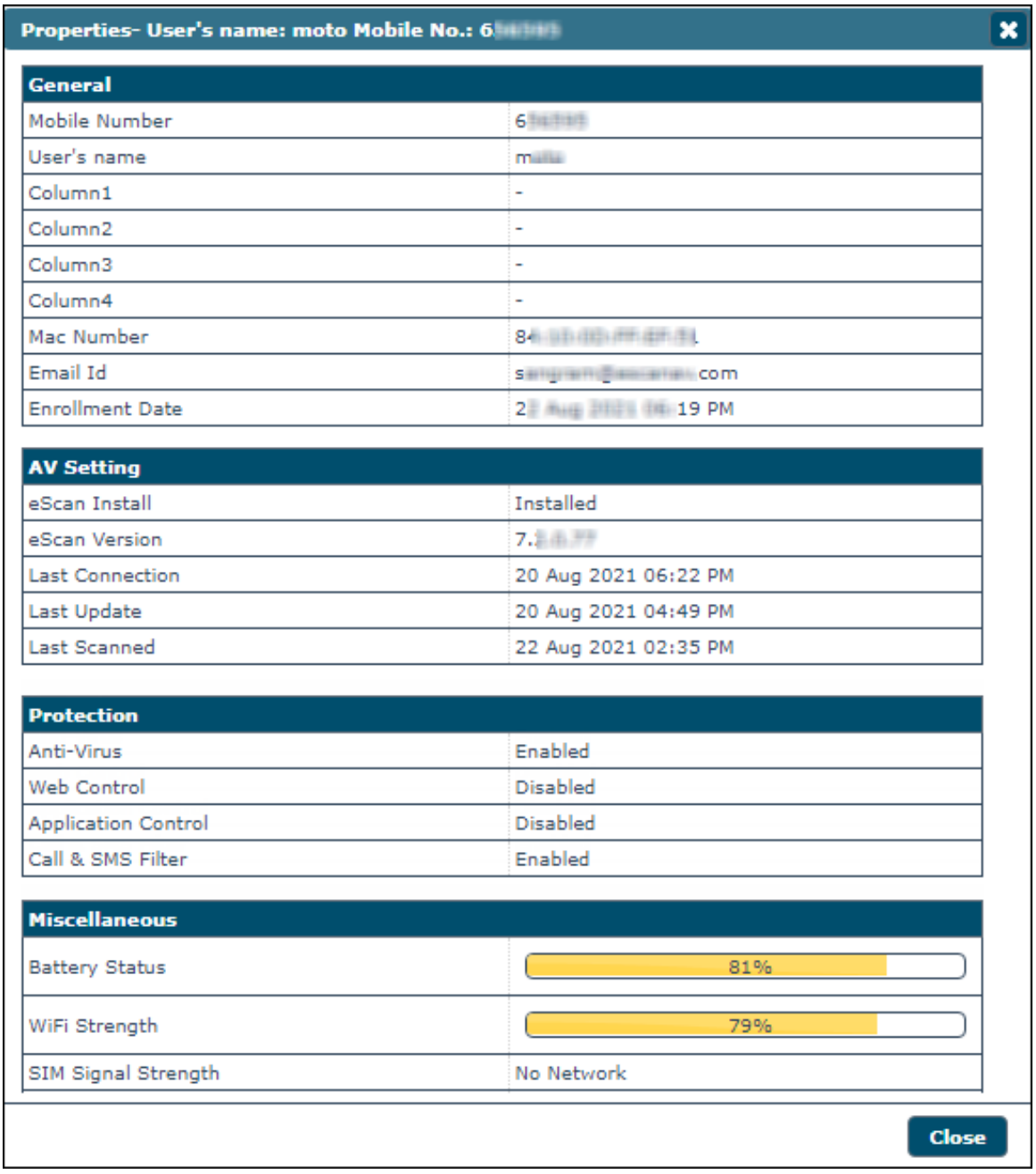
3. Select the group to which you wish to move the device(s) and then click **OK**.

NOTE	You can create a new group by clicking **New Group** and move the device(s) to that group.

Checking a Device Properties

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

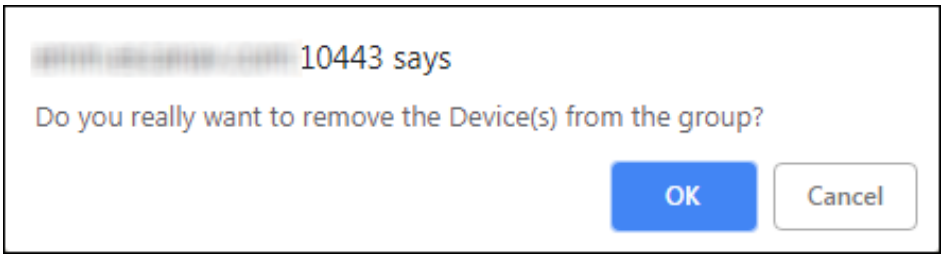
1. Select a device.
2. Click **Client Action List** > **Properties**.
   The Properties window for the selected device appears.



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.

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

Resending Enrollment Email

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

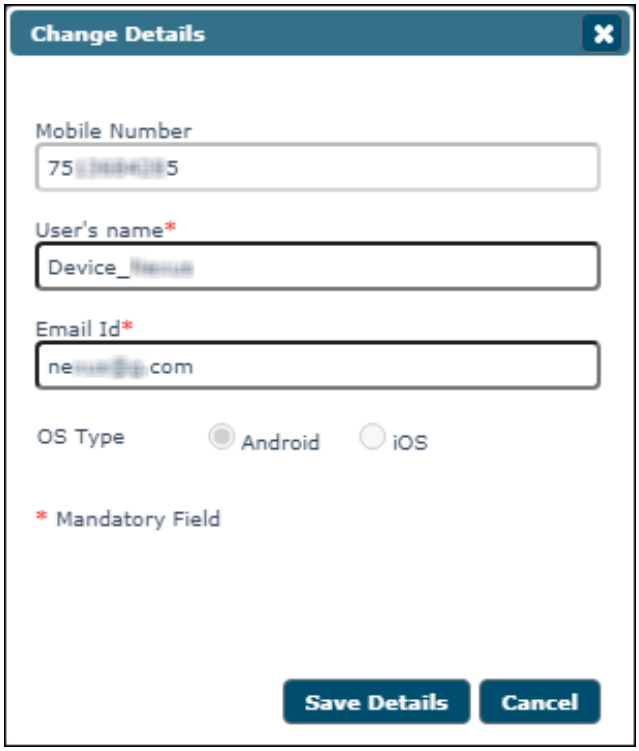
1. Select the specific device.
2. Click **Client Action List** > **Resend Enrollment Email**.
   A new enrollment email will be sent to the user.

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.



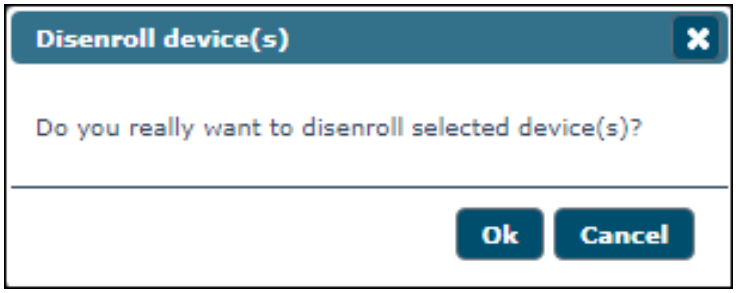
3. Make the required changes and then click **Save Details**.
   The User details will be updated.

NOTE	The Mobile Number and OS Type cannot be changed.

Disenrolling a device

The Disenroll option lets you allow to disenroll a selected device.
To disenroll the specific device,

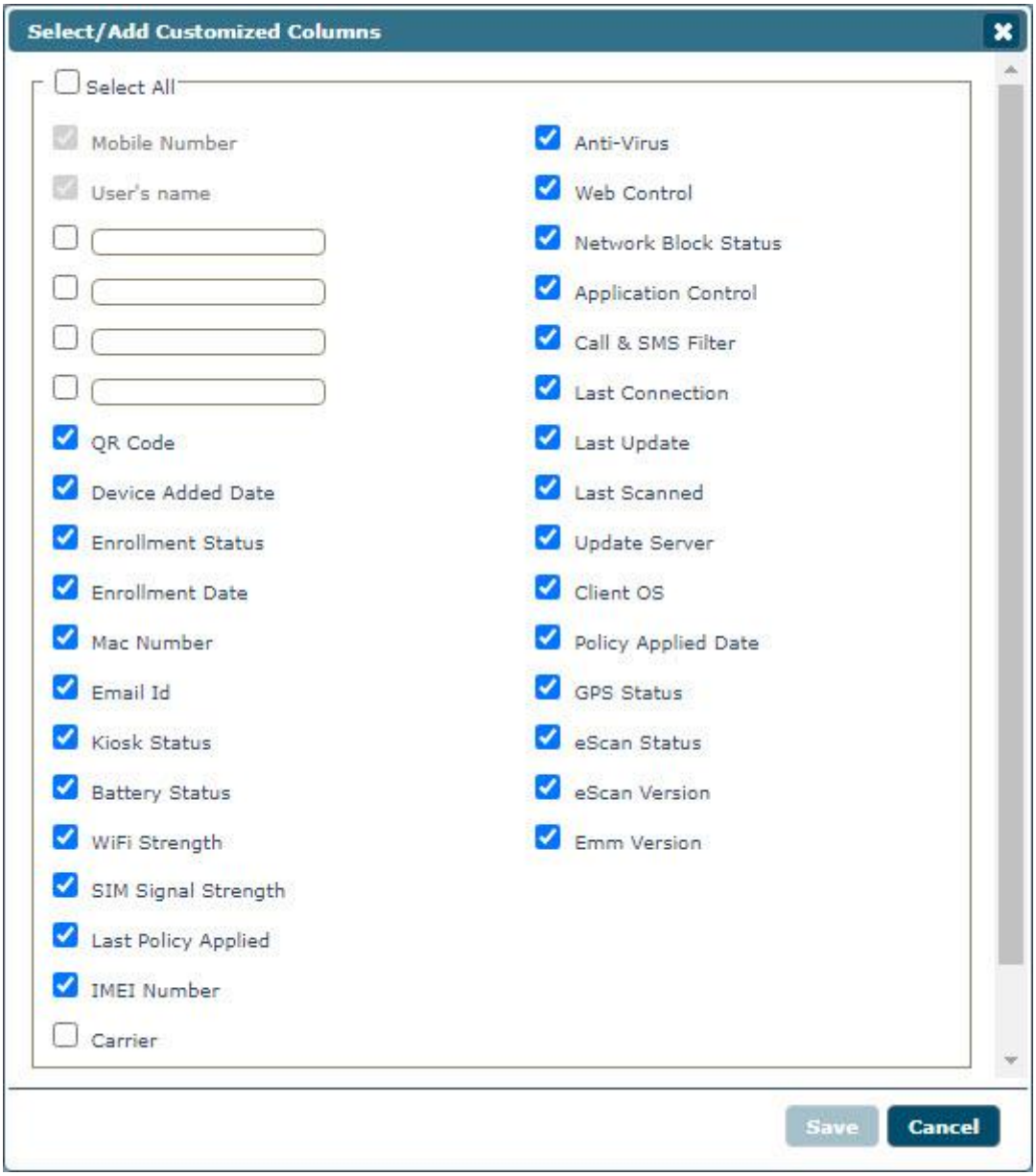
1. Select a device.
2. Click **Client Action List** > **Disenroll**.
   A confirmation prompt appears.



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.



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

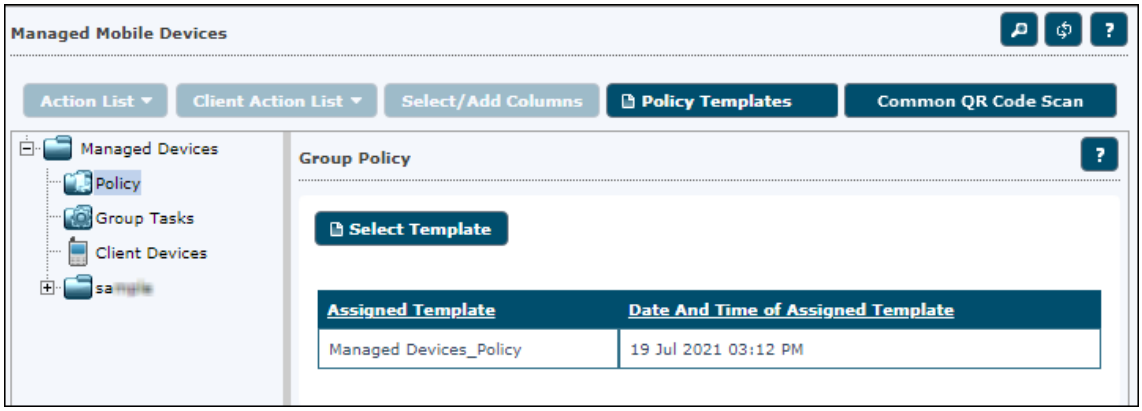
After selecting options as per requirement, click **Save**.

Policy Templates

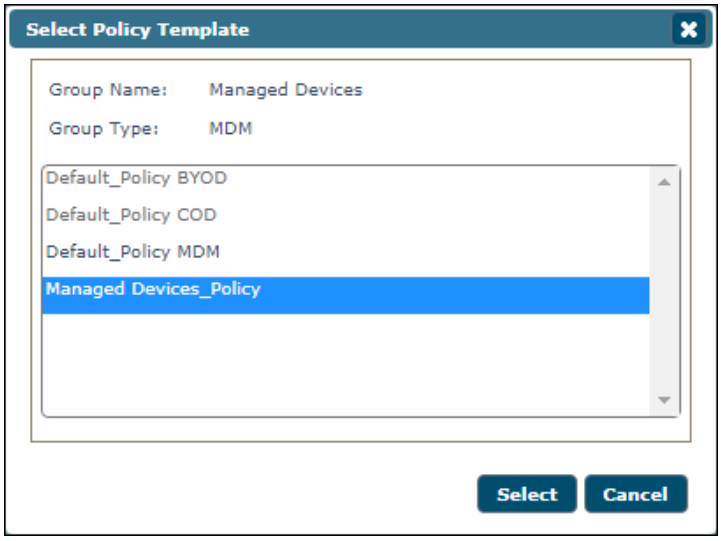
This button allows you to add different security baseline policies for specific computer or group.

Steps for defining Policies for the Group

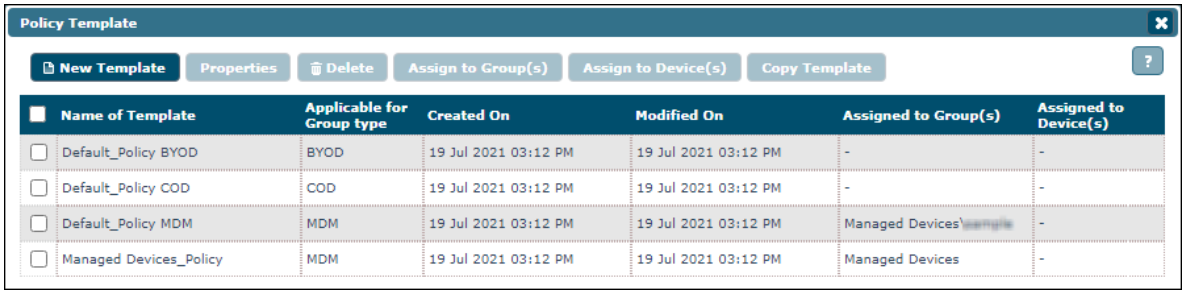
To define policies for a group, select a group and under selected group, click **Policy**.
Group Policy pane appears on the right side.



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



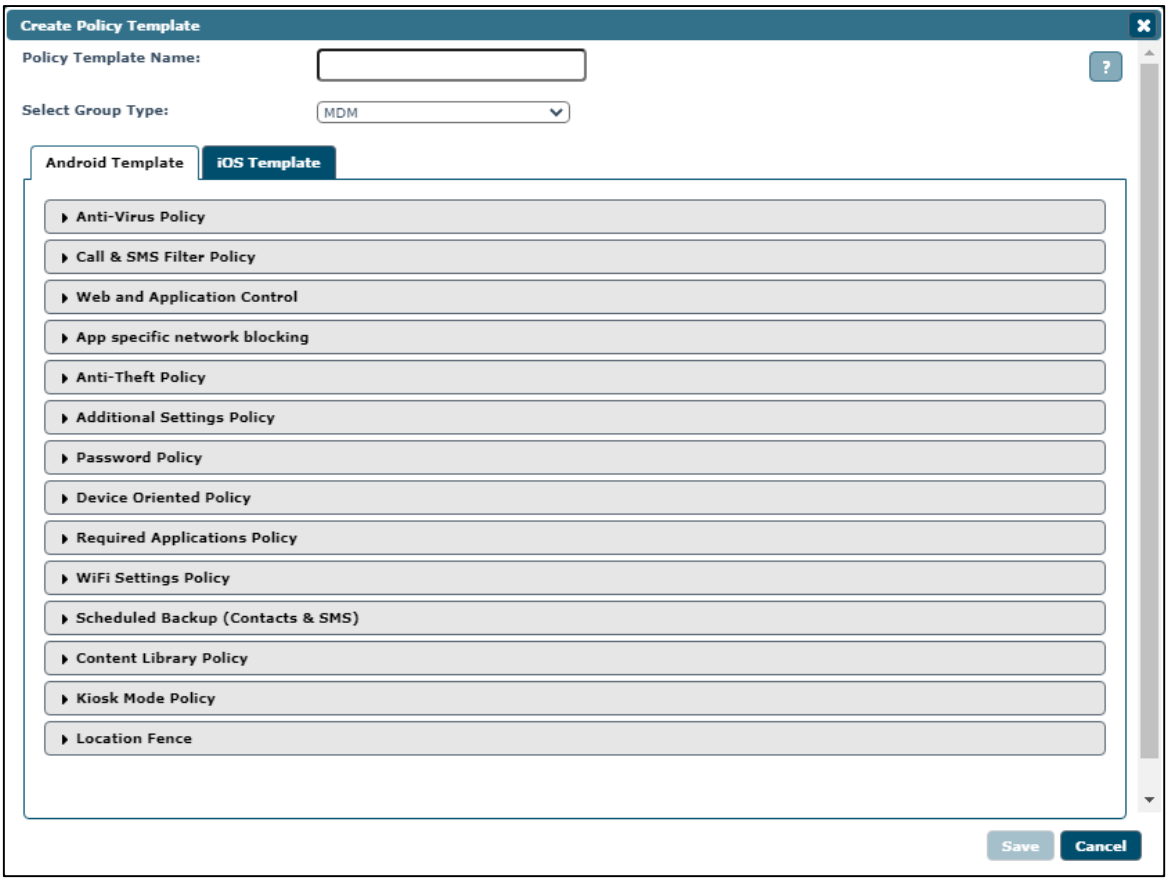
- Click **Policy Templates**, it displays Policy Template screen and lets you create, copy, and assign template to specific group or devices.



Creating New Template

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

1. Click **Policy Templates**.
   Policy Template window appears.
2. Click **New Template**.
   Create Policy Template window appears.



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, **click here**.

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.

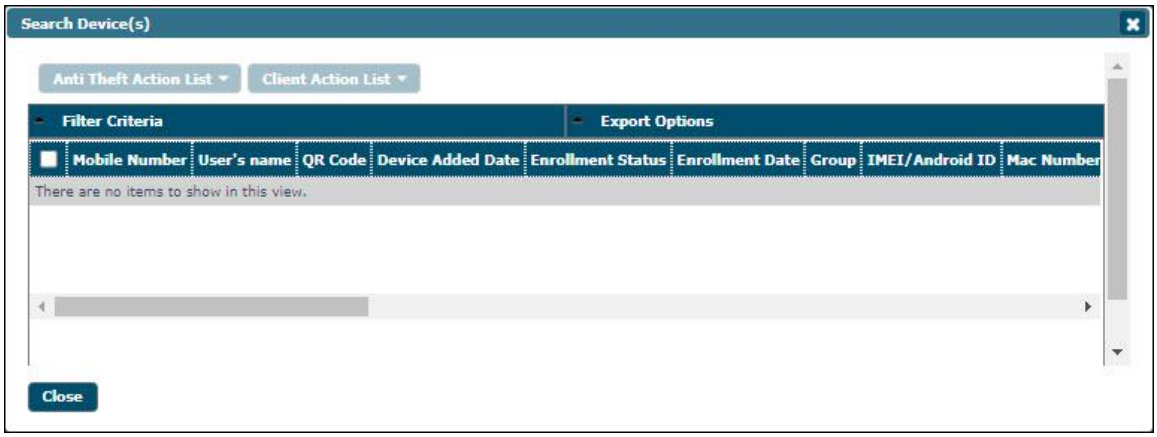
NOTE	The added devices will be displayed under the AutoAdded groups with their respective group types.

Window Buttons

The Managed Mobile Devices window has following buttons:

- **Filter**
- **Refresh**
- **Help**

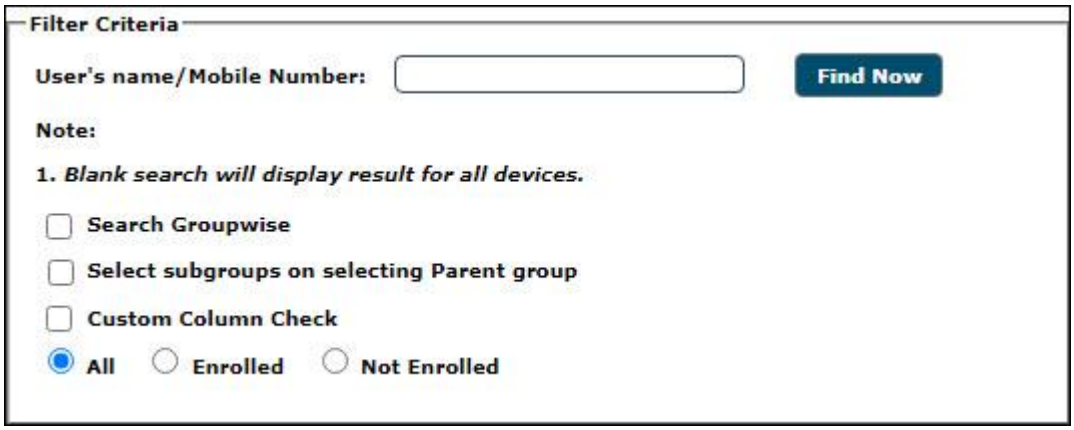
Filter : This button allows you to search the managed device(s). Additionally you can export the list of filtered device(s). It also allows you to take necessary actions on the filtered device(s) using **Anti Theft Action List** and **Client Action List**.



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.



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):

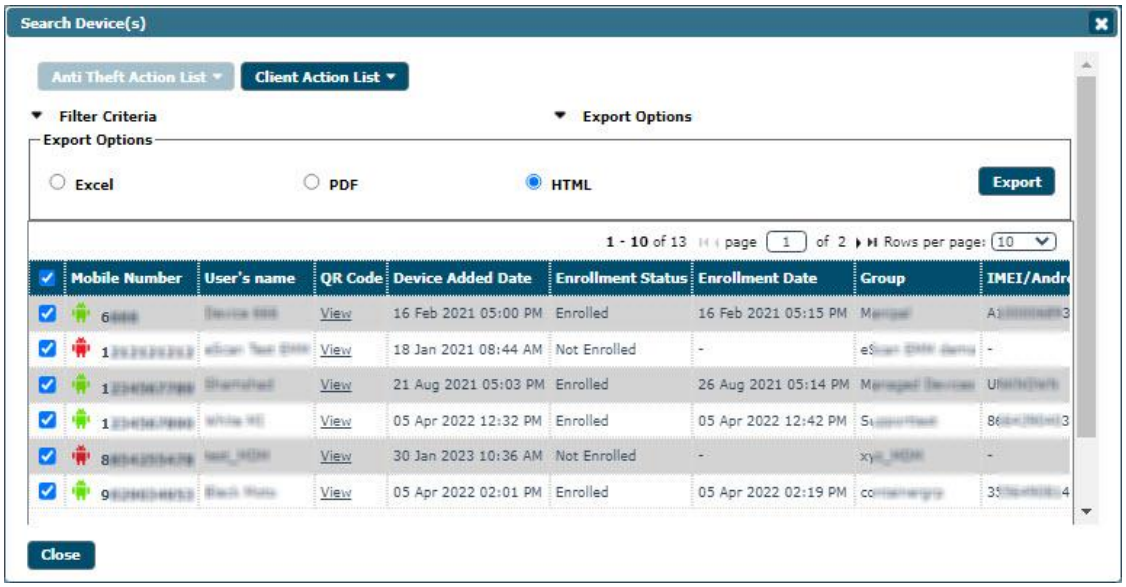
1. In the Filter Criteria options, select the checkbox **Search subgroups on selecting Parent group** to search the device(s) from parent group(s).
2. Select the Parent group(s). All the subgroup(s) will be selected automatically wherein you can deselect particular subgroup.
3. Click on **Find Now**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

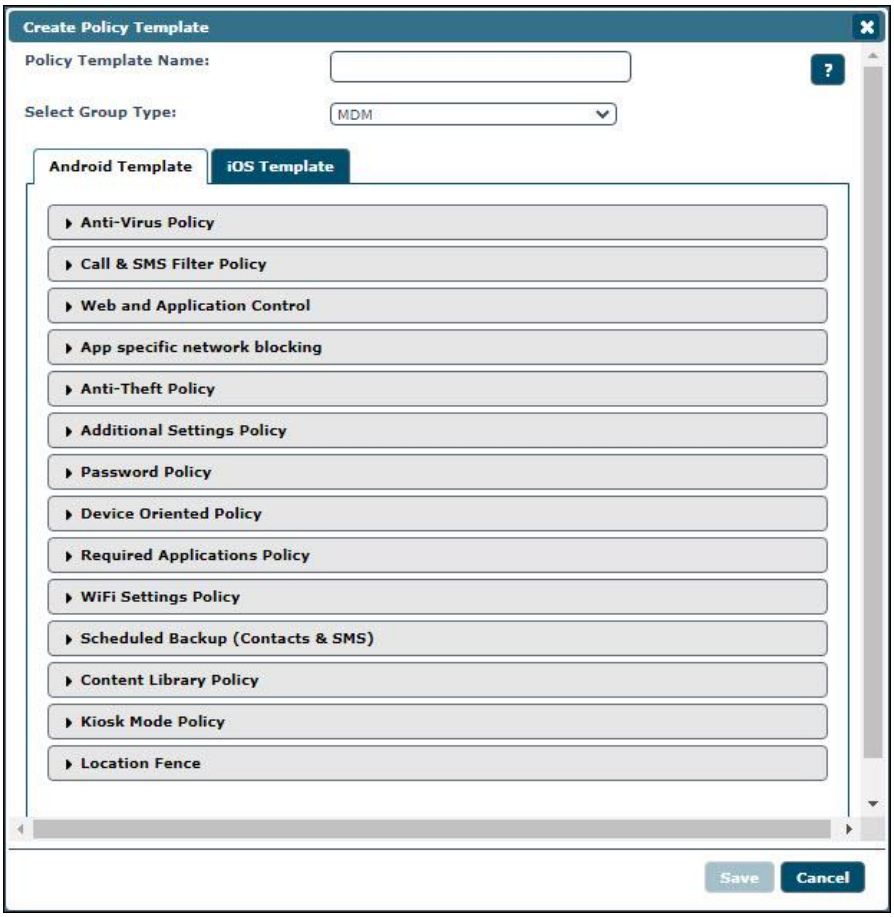


2. Select the preferred export format from Excel, PDF, or HTML.
3. Select the device(s).
4. Click on **Export**. The list will be exported in the selected format.

Refresh : This button refreshes the entire window.

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

Android Templates



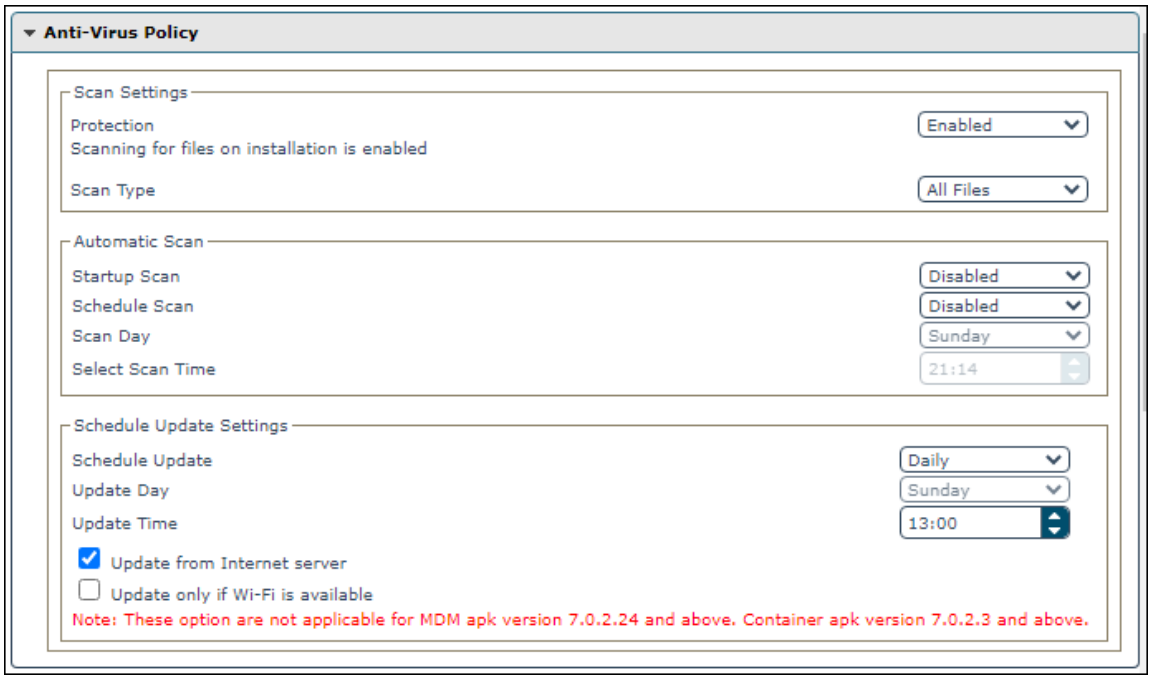
The Android Template consists following policies:

- 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

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.



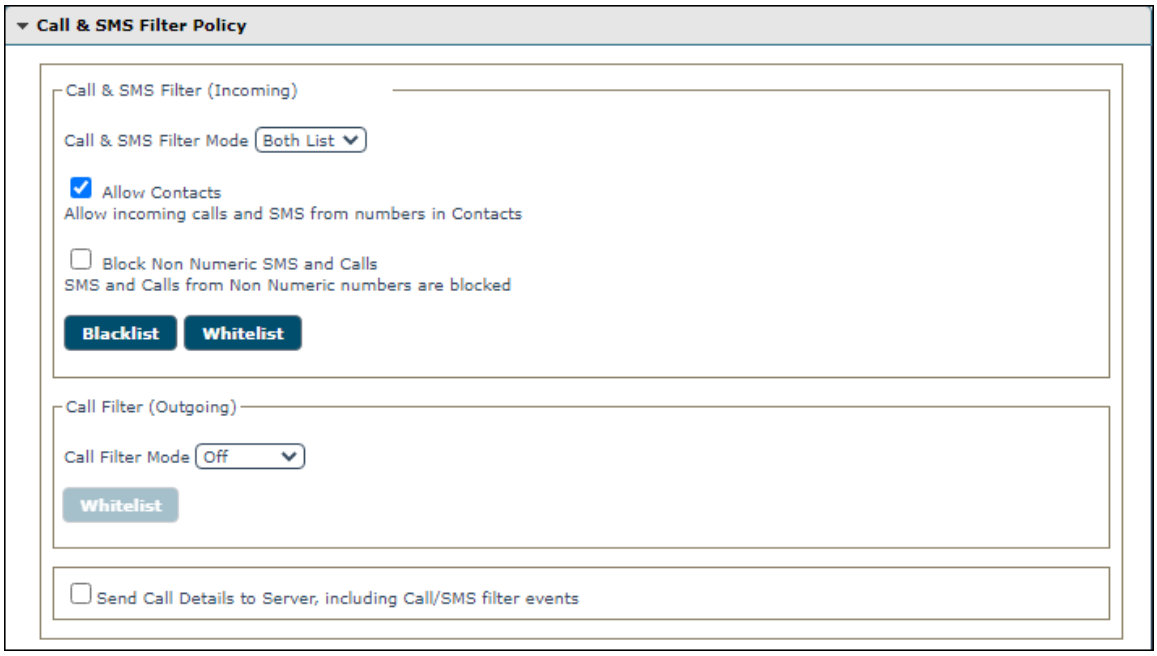
Configuration options of Anti-Virus policy are as follows:

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 **Enabled** or **Disabled** to enable or disable protection on managed devices in the group.
Scan Type	Select the appropriate scanning option either **All Files** or **Executable Only**.
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.

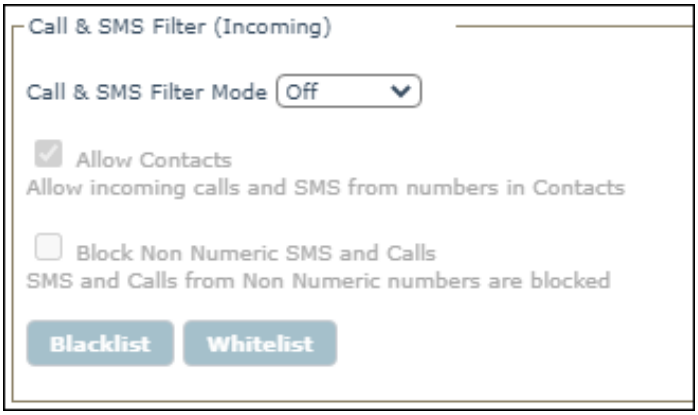
Scan Day	Select a particular day of the week to scan the managed devices present in the group. This checkbox will be activated only if you select weekly scan option.
Select Scan Time	Set time for scanning the managed devices in the group.
Schedule Update Settings	Define settings for updating eScan on 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.

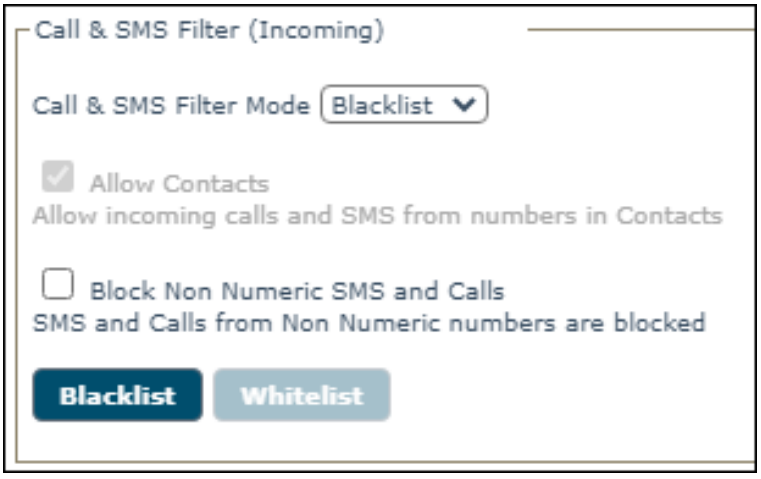


Call and SMS Filter Mode set to Off

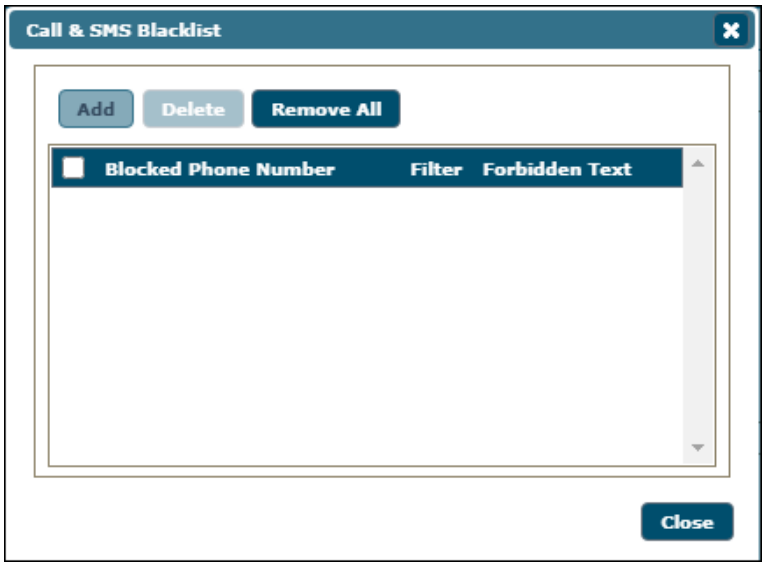


If the Call and SMS Filter Mode is set to **Off**, all calls and text messages will be allowed.

Call and SMS Filter Mode set to Blacklist

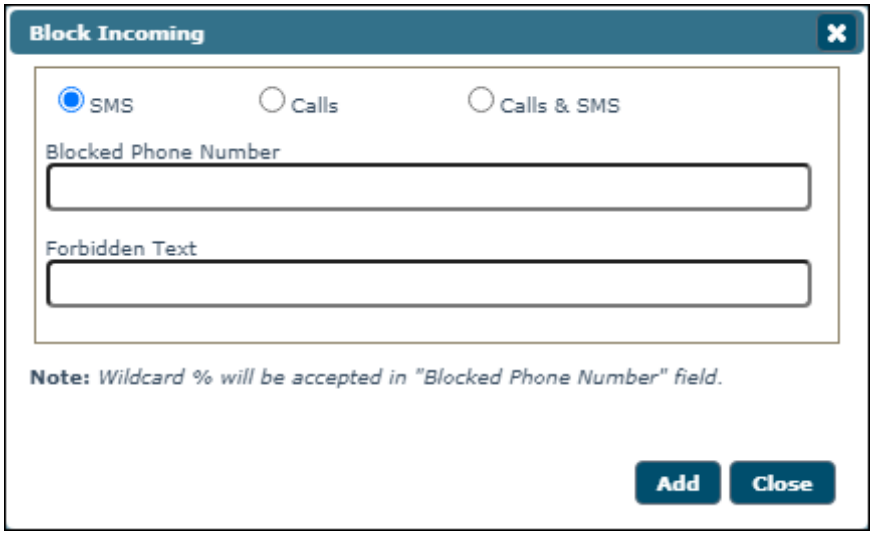


- Select **Block Non-Numeric SMS and Calls** checkbox to block SMS and calls from non-numeric numbers.
- To block incoming calls from known numbers and SMS consisting specific keywords, click **Blacklist**.
  Call and SMS Blacklist window appears.

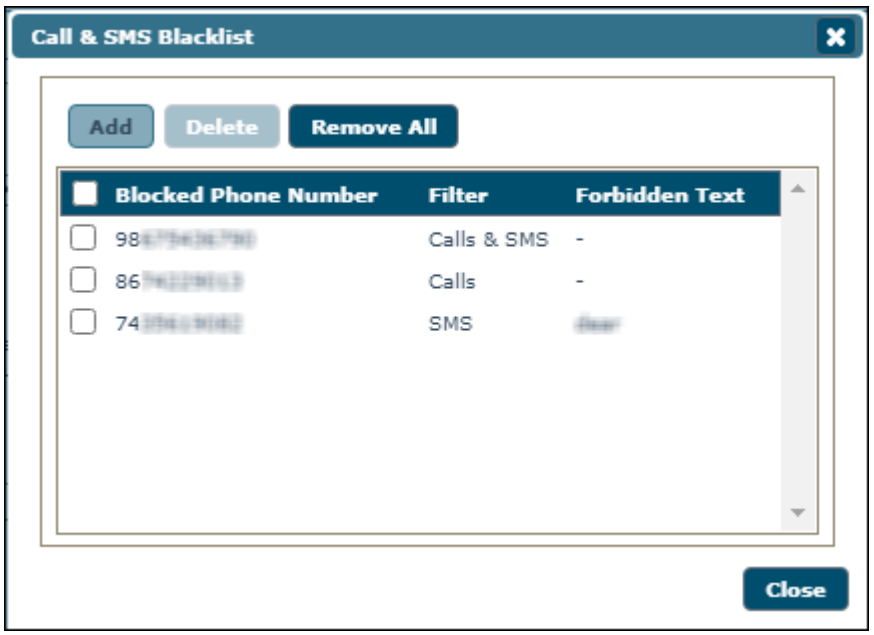


- Click **Add**.

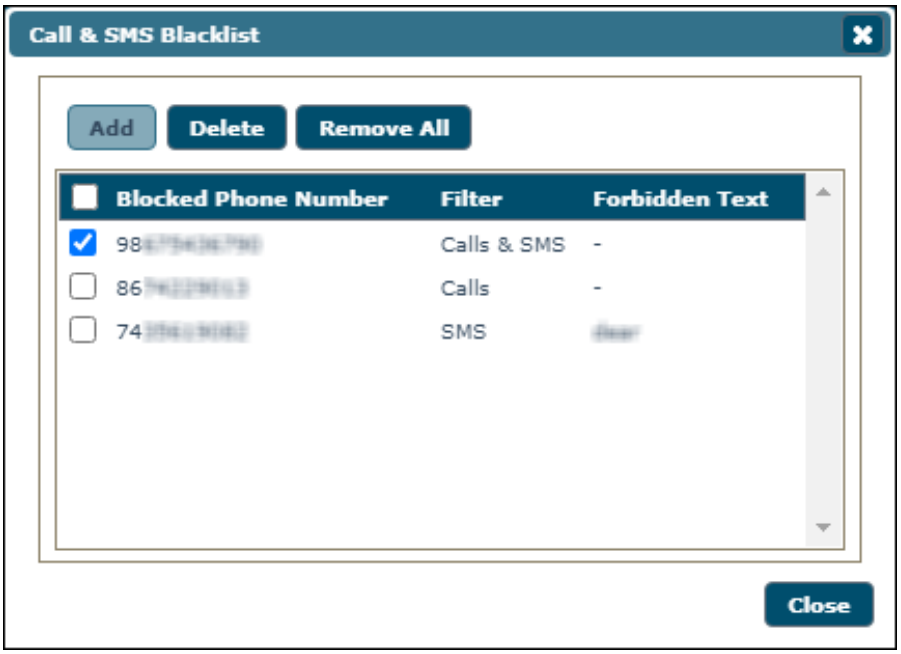
Block Incoming window appears.



- 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**.



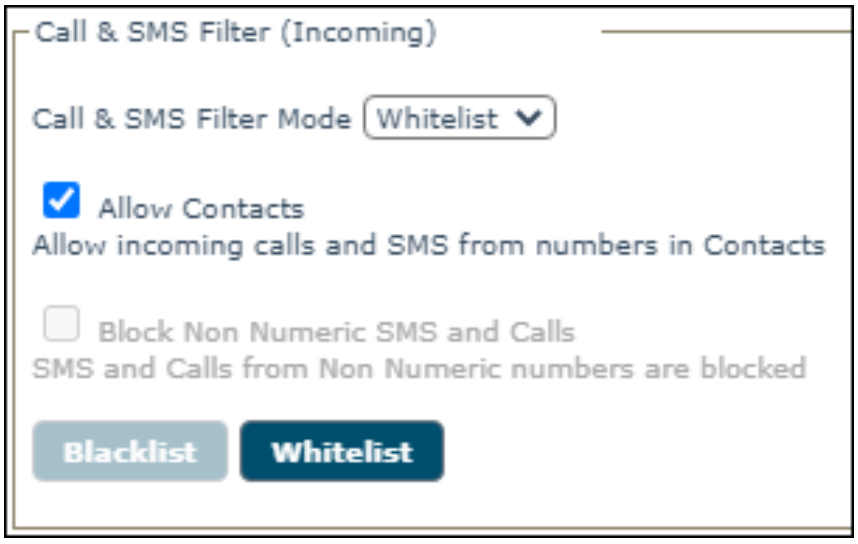
- To delete a specific number from the Blacklist, select the number and click **Delete**.



The selected number will be deleted.

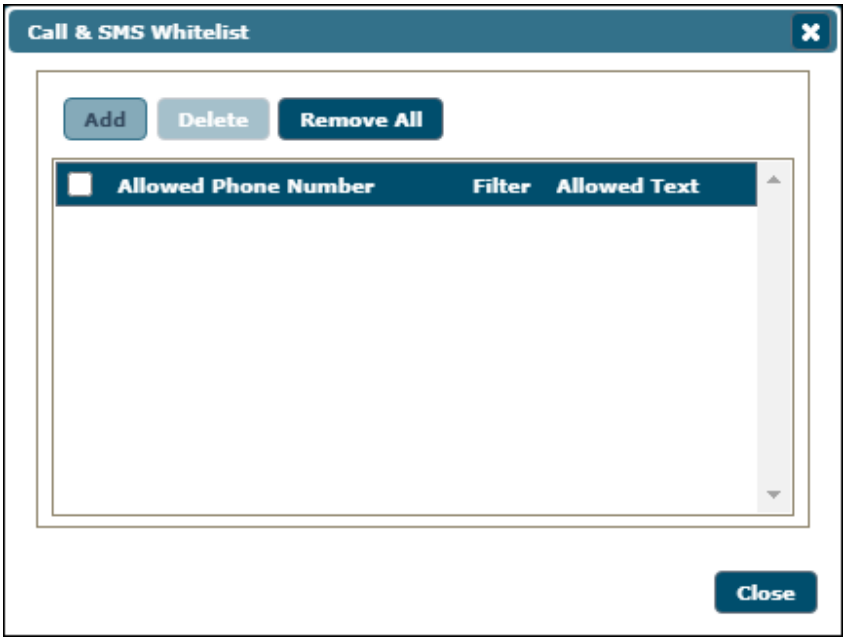
- To remove all the added numbers in a single-click, click **Remove All**.

Call and SMS Filter Mode set to Whitelist

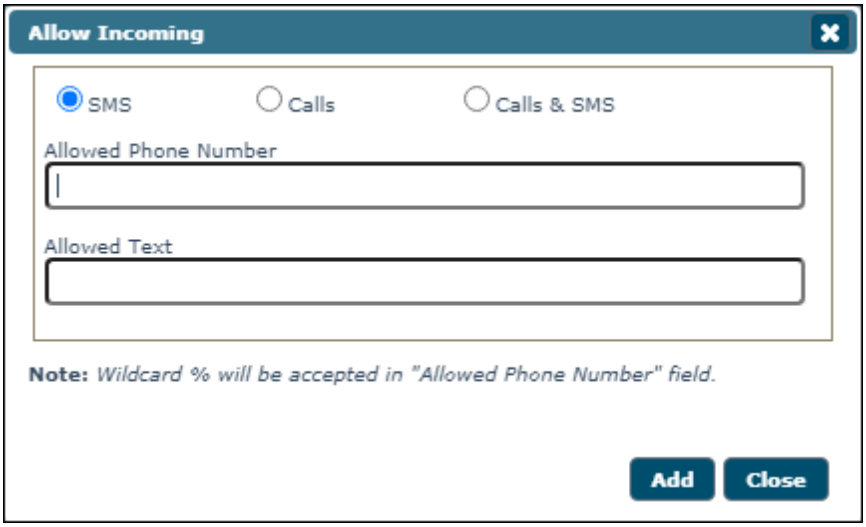


- Select **Allow Contacts** checkbox and then click **Whitelist**.

Call and SMS Whitelist window appears.

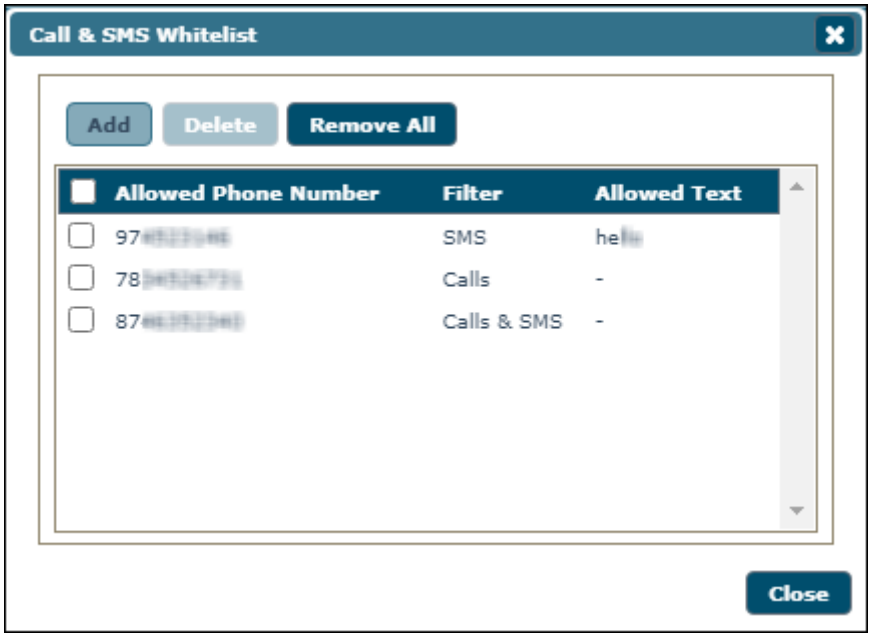


- Click **Add**.
  Allow Incoming window appears.

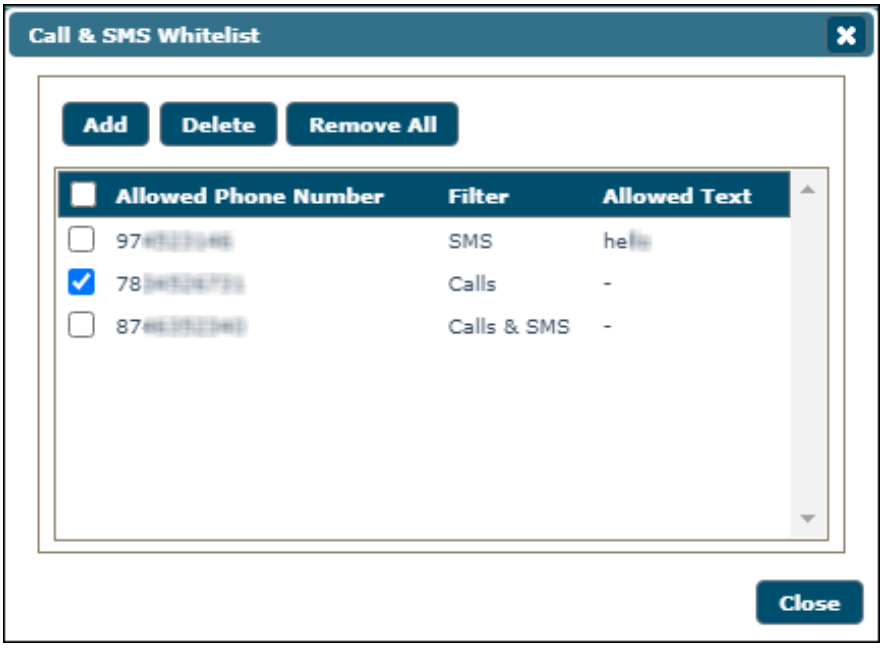


- Select whether to allow **SMS**, **Calls** or both **Calls & SMS**.

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



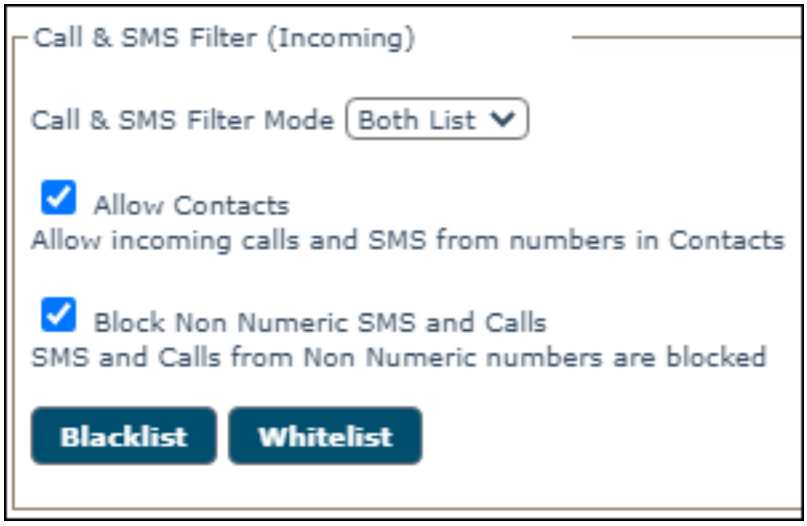
- To delete a specific number from whitelist, select the number and click **Delete**.



The number will be deleted.

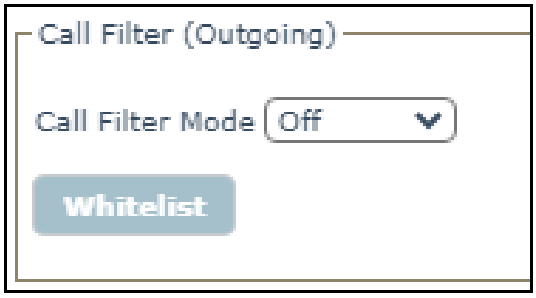
- To remove all numbers in a single-click, click **Remove All**.

Call and SMS Filter Mode set to Both List



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

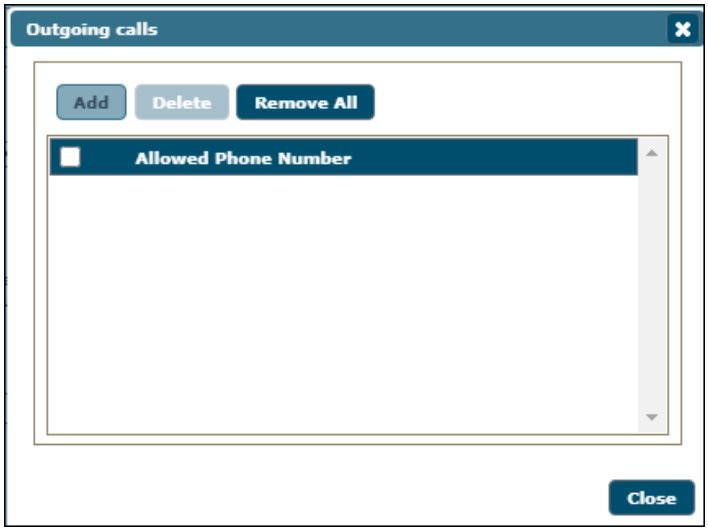


If Call Filter Mode is set to **Off**, all outgoing calls will be allowed.

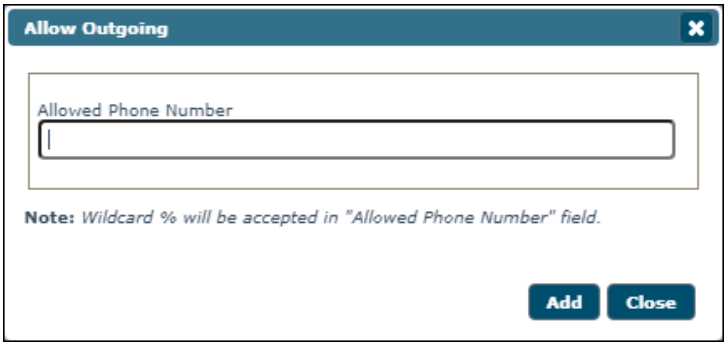
Call Filter (Outgoing) Mode set to Whitelist

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

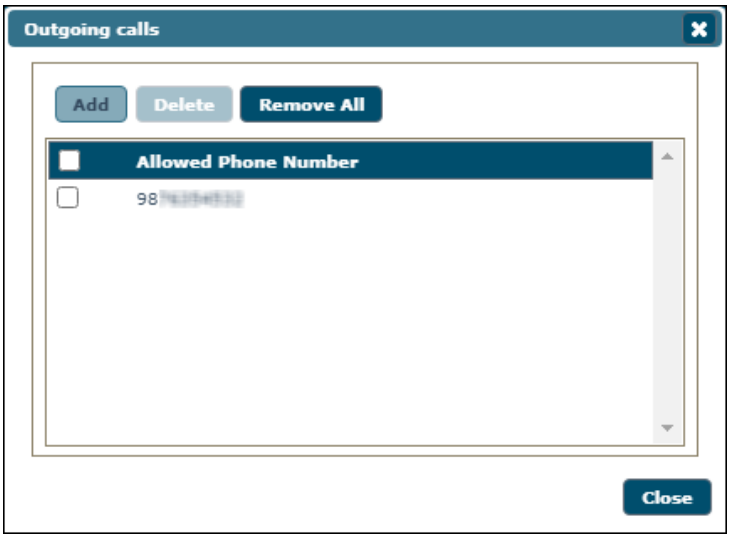
- Click **Whitelist**.
  Outgoing calls window appears.



- Click **Add**.
  Allow Outgoing window appears.

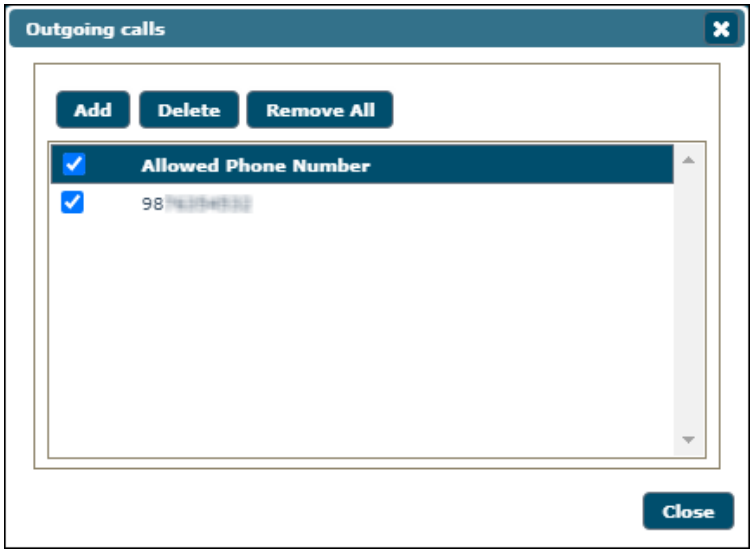


- Enter the allowed phone number and then click **Add**.



The number will be added to the Whitelist.

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



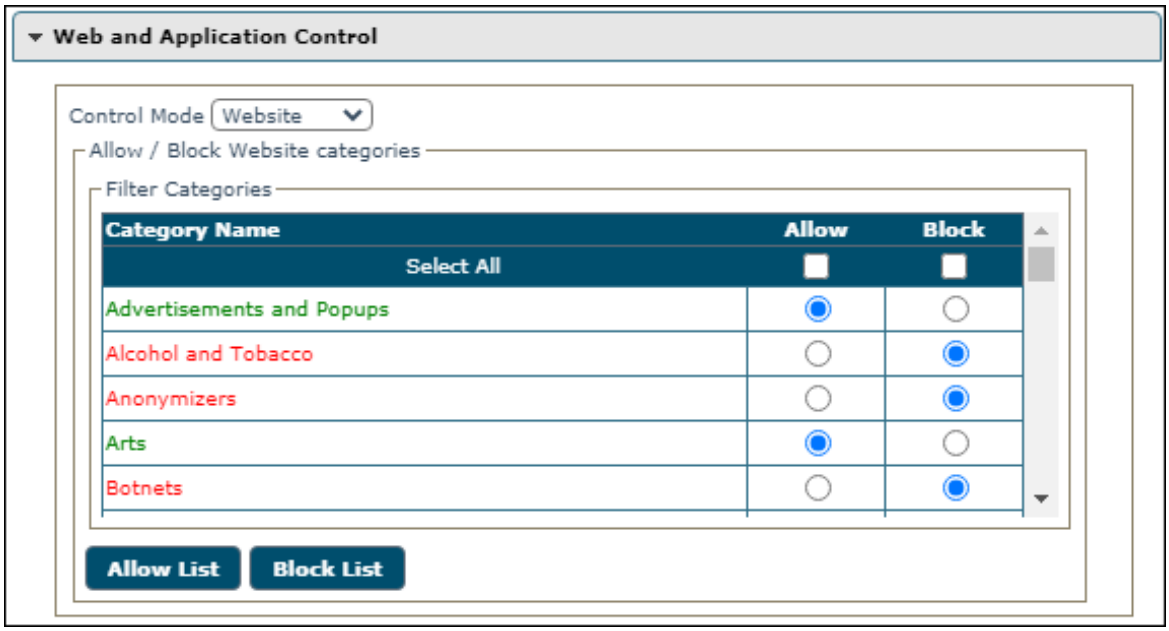
The number will be deleted.

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

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

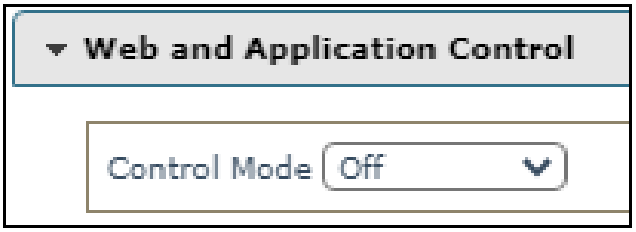
Web and Application Control policy lets you allow and block applications and websites on managed devices as per requirement.



Control Mode

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

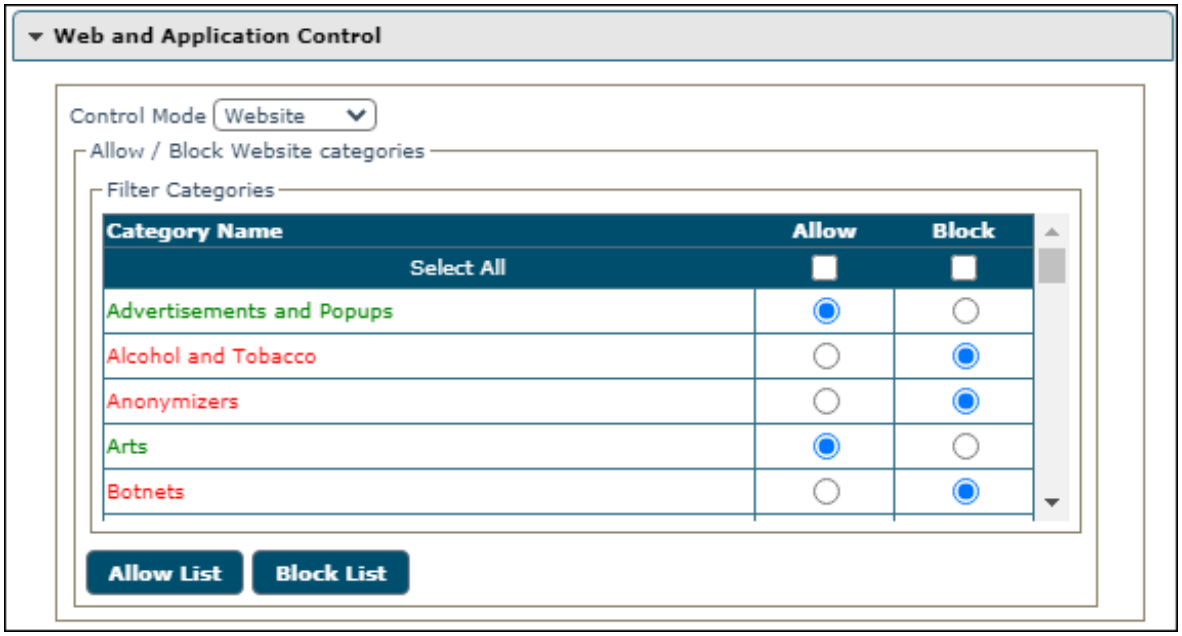
Control Mode set to Off



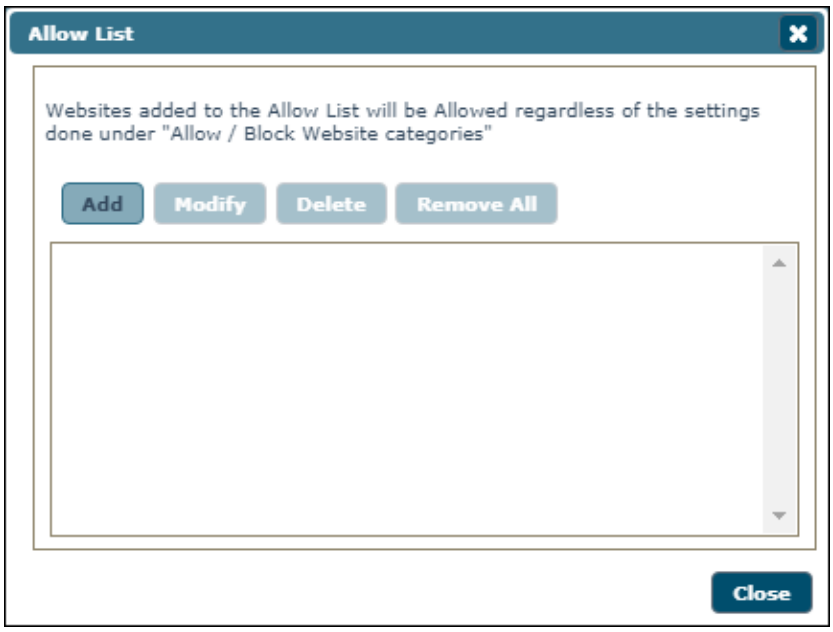
If the Control Mode is set to **Off**, you cannot allow/block websites and applications.

Control Mode set to Website

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

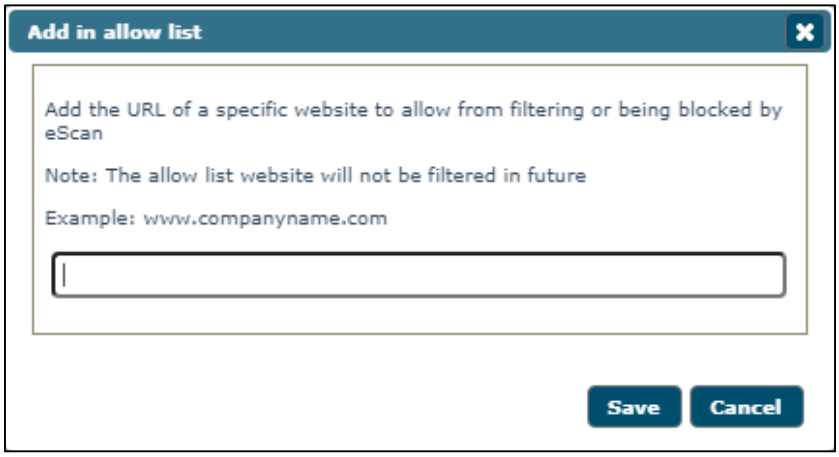


Allow List: Websites added to this list can be accessed in browser. You can modify and delete websites from the list as per need.



- Click **Add**.

Add in allow list window appears.



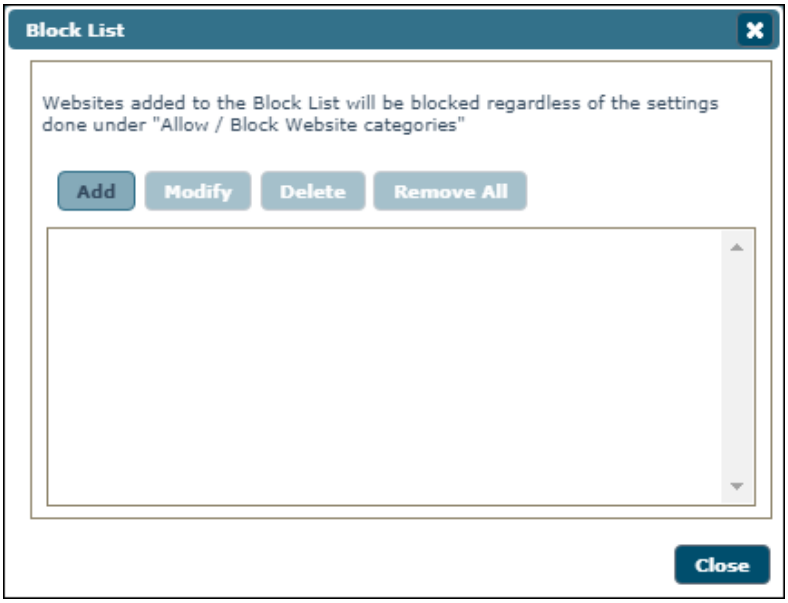
- Enter the URL in the field and then click **Save**.

To edit the existing allowed website, select the particular website and click **Modify**.

To delete a particular website, select the website and click **Delete**.

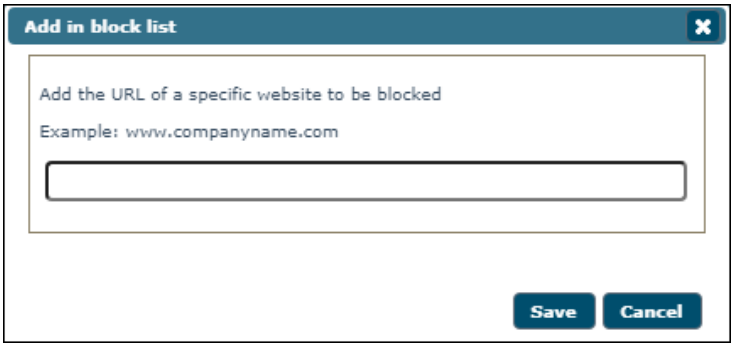
To remove all the website from the list in a single-click, click **Remove All**.

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



- Click **Add**.

Add in block list window appears.



- Enter the URL and then click **Save**.

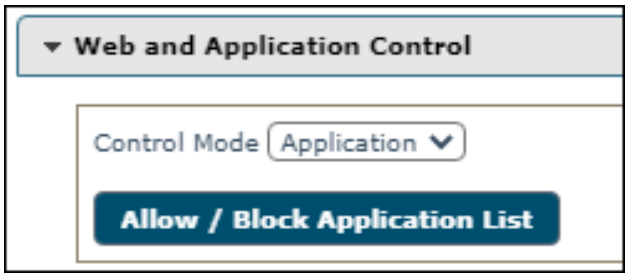
To edit the existing blocked website, select the particular website and click **Modify**.

To delete a particular website, select the website and click **Delete**.

To remove all the website from the list in a single-click, click **Remove All**.

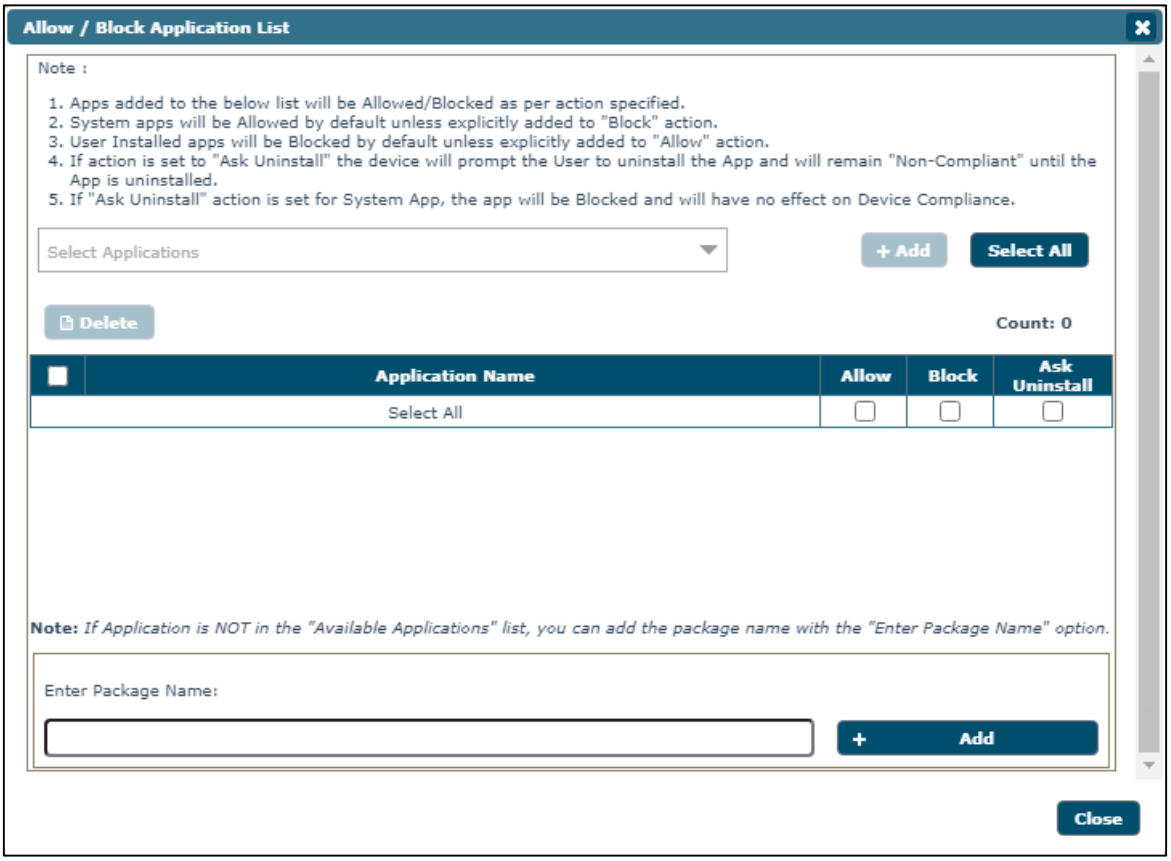
Control Mode set to Application

Setting the control mode to **Application**, lets you allow or block an application.



- Click **Allow/Block Application List**.

Allow/Block Application List window appears.



- 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**.

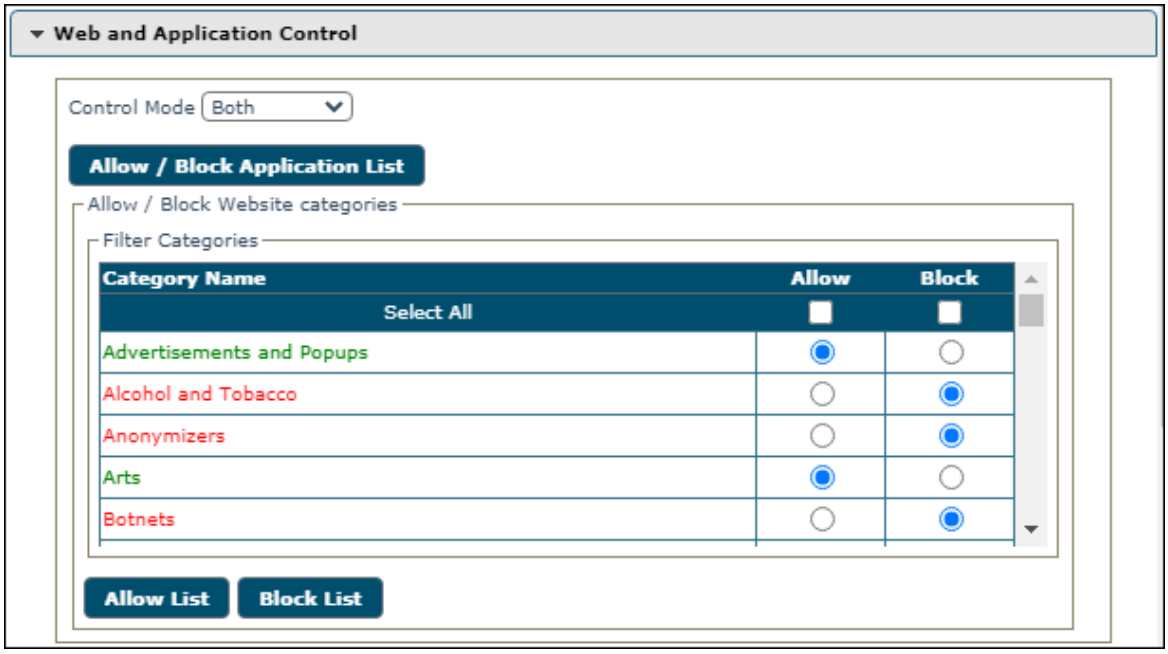
Application List

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.

NOTE	If Application is NOT in the "**Available Applications**" list you can add the package 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.

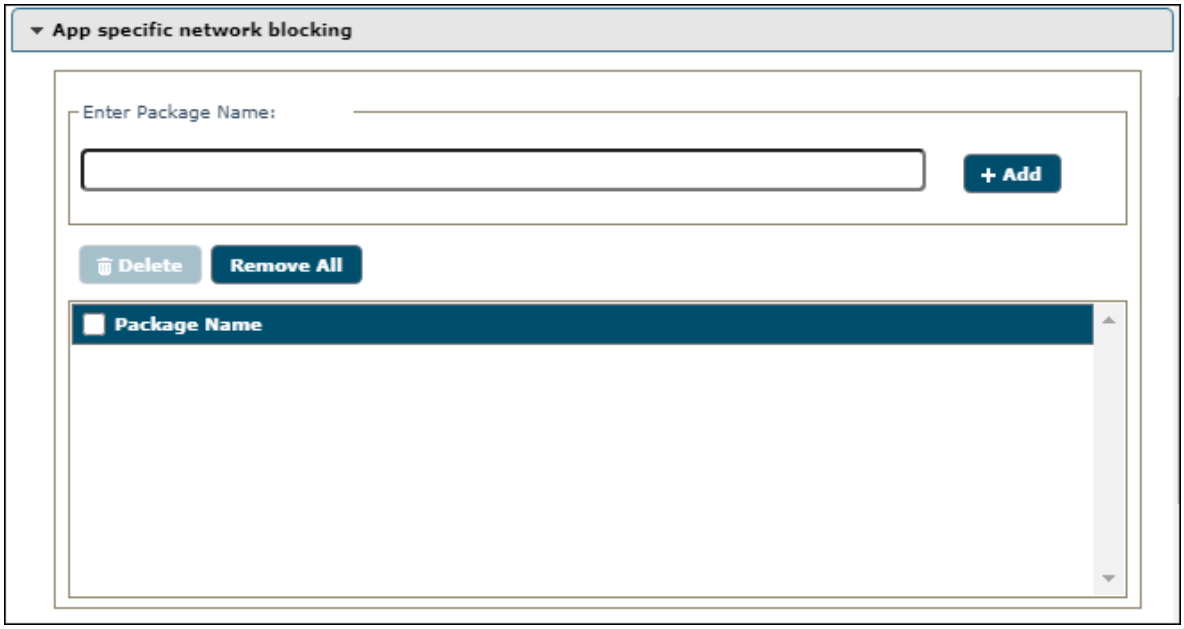
Control Mode set to Both



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.

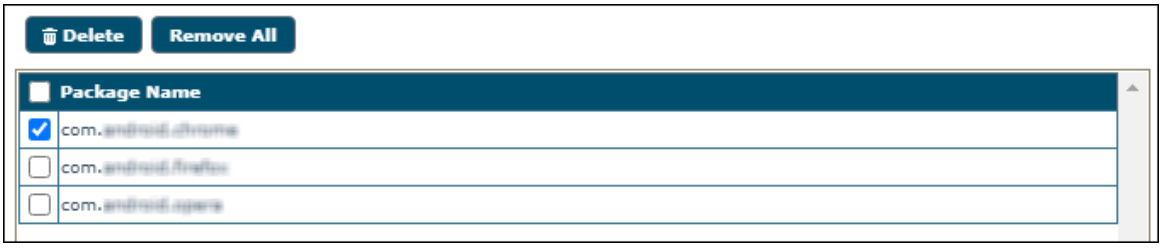


- In the **Enter Package Name** field, enter the application's package name and then click **Add**.
- The package will be added and displayed in **Package Name** section below.

After a package is added, the respective application will be unable to access the Internet.

NOTE	VPN permission is necessary to work this functionality.

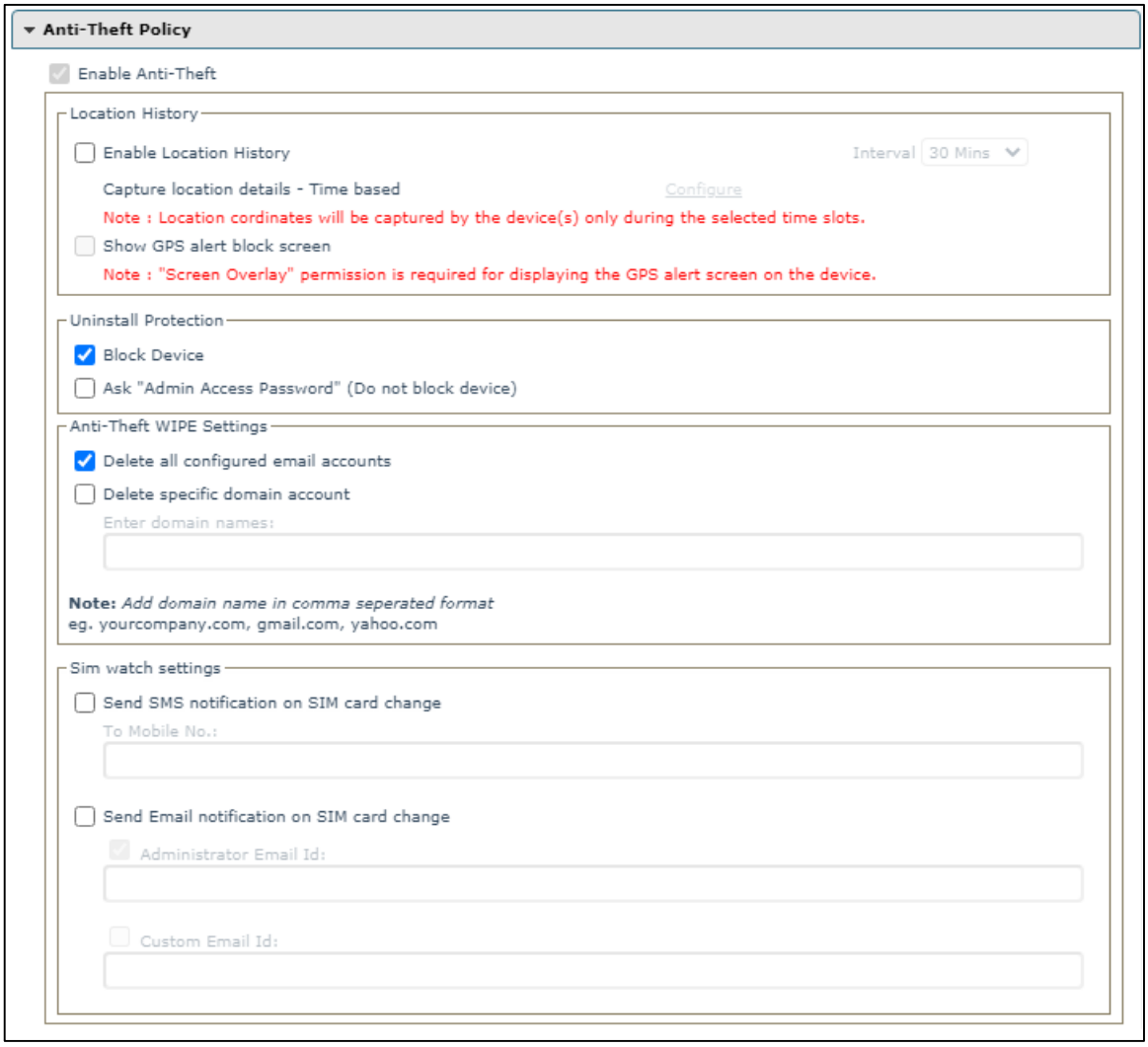
To delete a package from the list, select the specific package and then click **Delete**.



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.

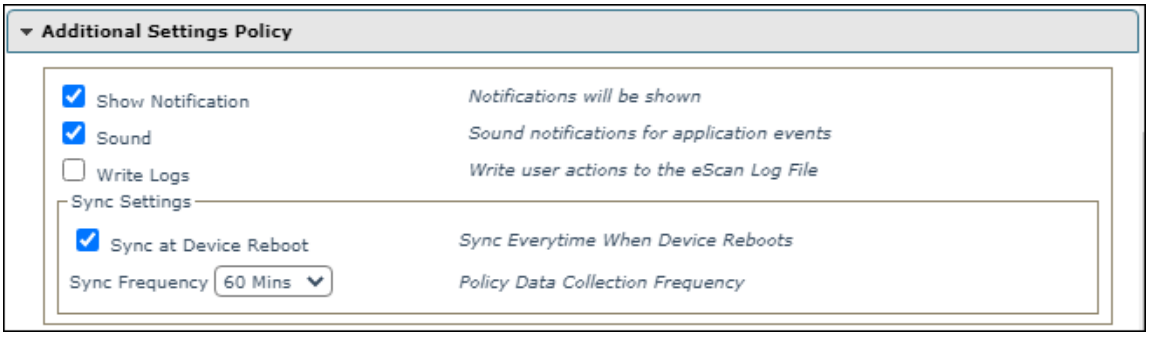


Options	Description
Enable Anti-Theft	Select this checkbox to enable Anti-Theft feature. By default, this checkbox is selected.
Enable Location History	Select this checkbox to track the location history. **NOTE**: Location coordinates will be captured by the device only during the selected time slots.
Interval in Minutes	Track the location history in a defined interval. You can set the interval using **Interval** 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. **NOTE**: "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 **Enter domain names** field. **NOTE**: 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 **To Mobile No.** 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 **Custom Email Id** field.

Additional Settings Policy

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



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.

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

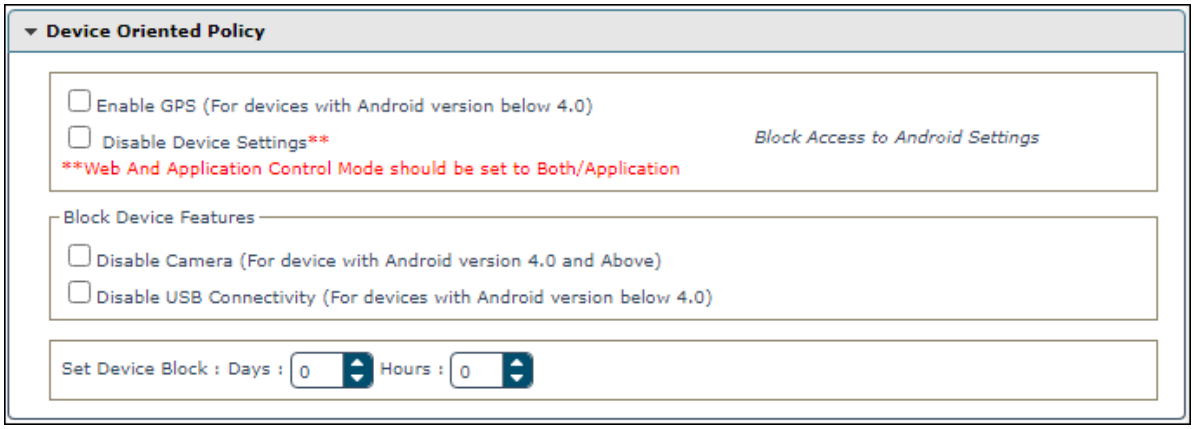
Select and define the device password based on below available password types:

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

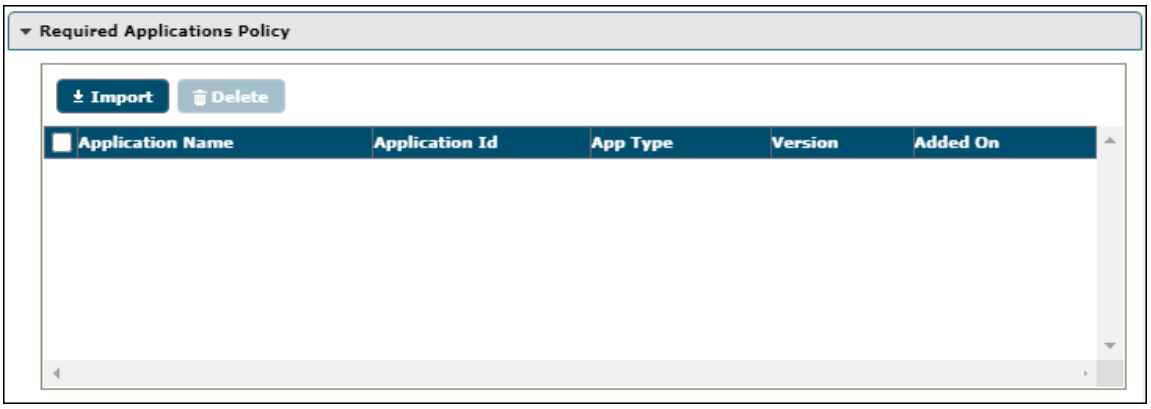
Device Oriented Policy lets you enable GPS and disable Camera, Bluetooth, and USB Connectivity on a device.



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. **NOTE**: This option to work, Web and Application Control Mode should be set to Both/Application.
Disable Camera (For device with Android version 4.0 and Above)	Select this 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

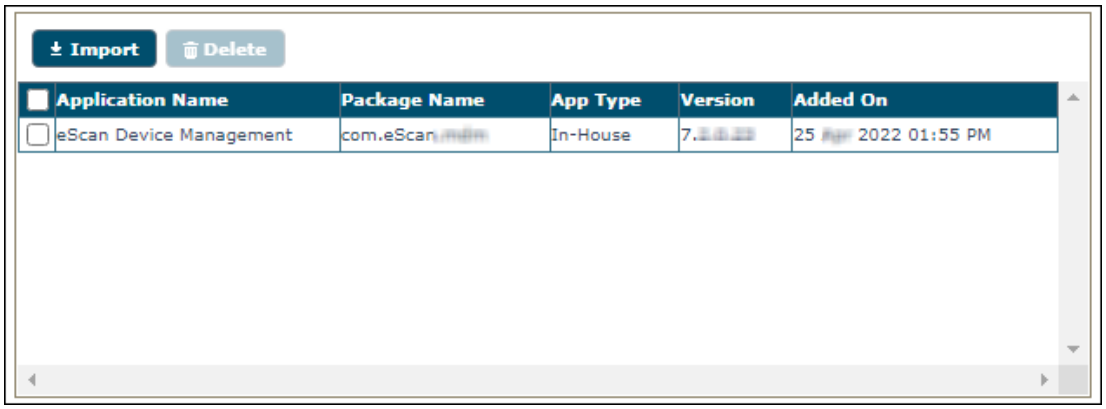
The Required Applications Policy lets you import applications from the App Store module to install it on devices in the group through policy deployment.



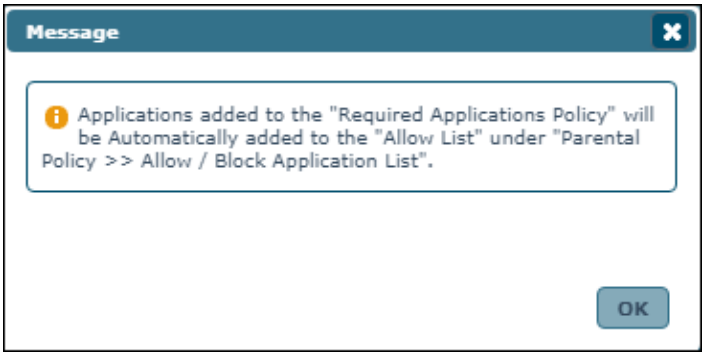
Importing an application

To import the application, follow the below steps:

1. Click **Import**.
   Import Application window appears.



2. Select an application(s) from the Available applications list.
3. Click **Save**.
   The selected application will be imported.
   A pop-up message appears.



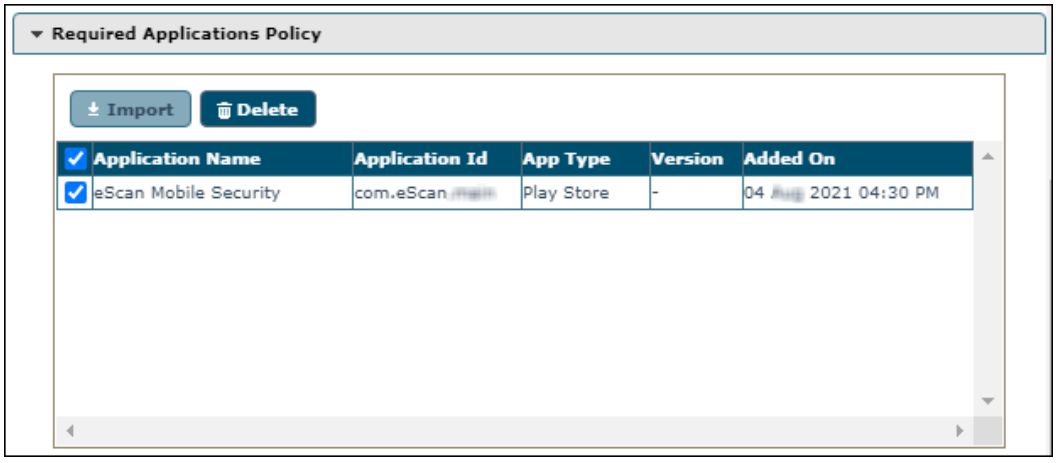
4. Click **OK** to exit.

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**.



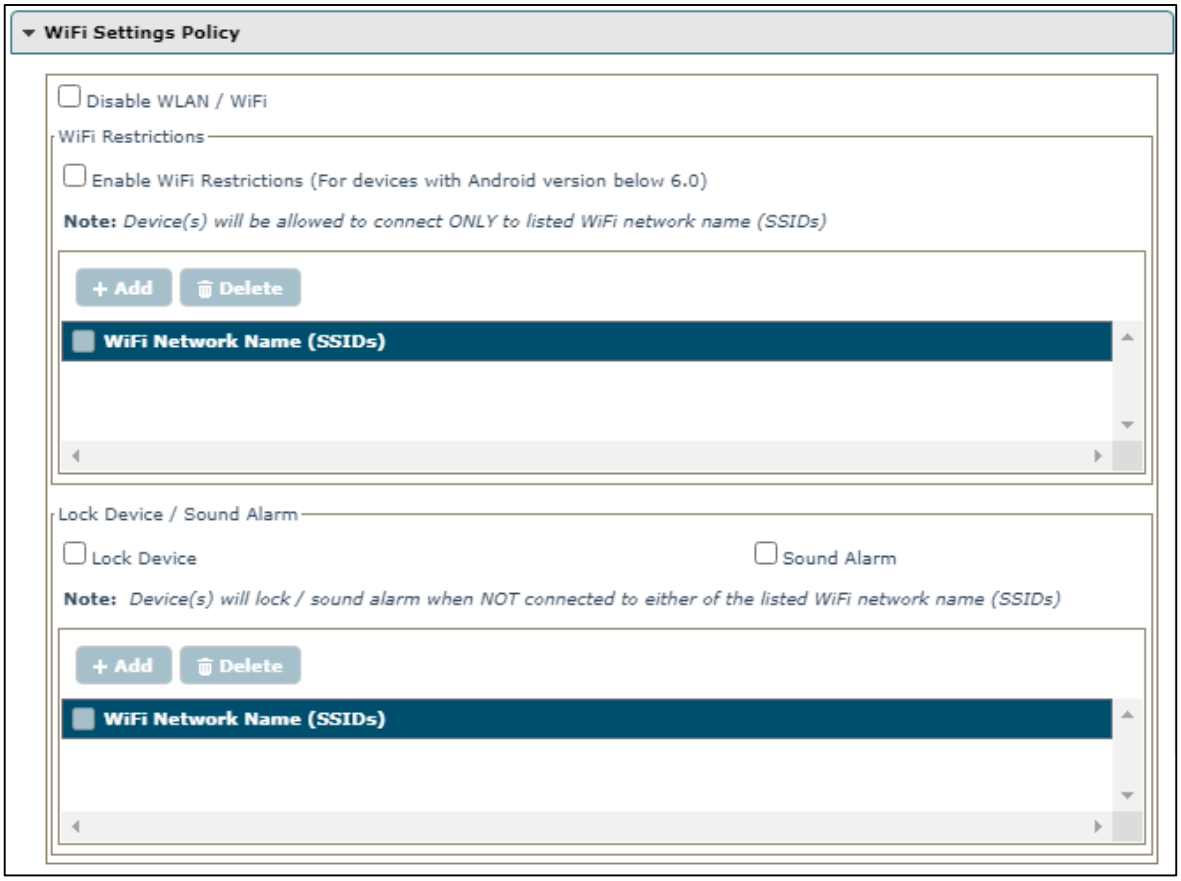
The selected application will be deleted.

Wi-Fi Settings Policy

The Wi-Fi Settings policy lets you define the settings for your Wi-Fi connections. You can disable WLAN/Wi-Fi or restrict the usage of Wi-Fi by allowing the device to connect only to the listed Wi-Fi networks. The device can be automatically locked or raise a sound alarm if it is not connected to any of the listed Wi-Fi connections.

Enable Wi-Fi Restrictions (For devices with Android version below 6.0)

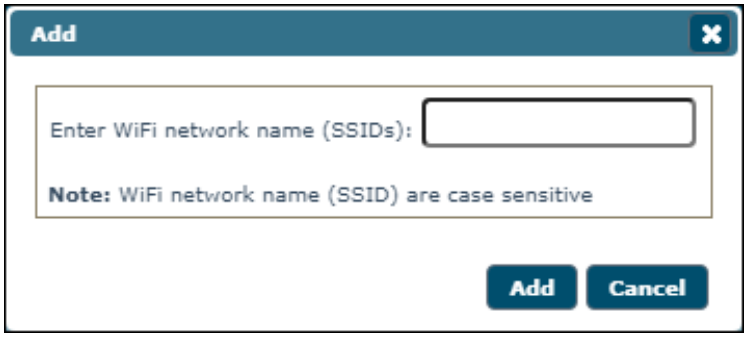
Select this checkbox to allow device to connect only to the listed WiFi network name (SSIDs). This option is available only for devices with Android version below 6.0.



Adding a Wi-Fi SSID

To add Wi-Fi SSID:

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



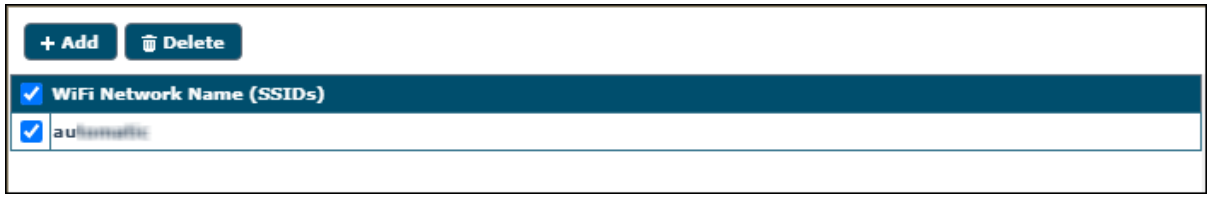
2. Enter the Wi-Fi network name (SSID) in the field and then click **Add**.
   The Wi-Fi network will be added to the console.

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

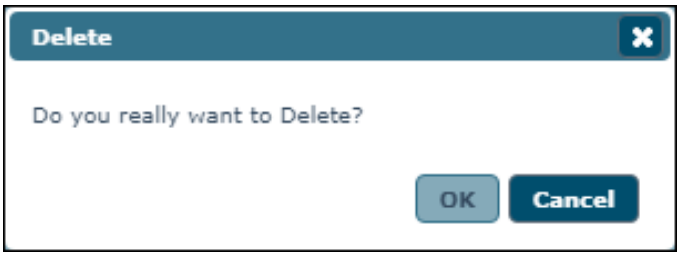
Deleting a Wi-Fi network SSID

To delete the added Wi-Fi network SSID:

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



   A confirmation prompt appears.

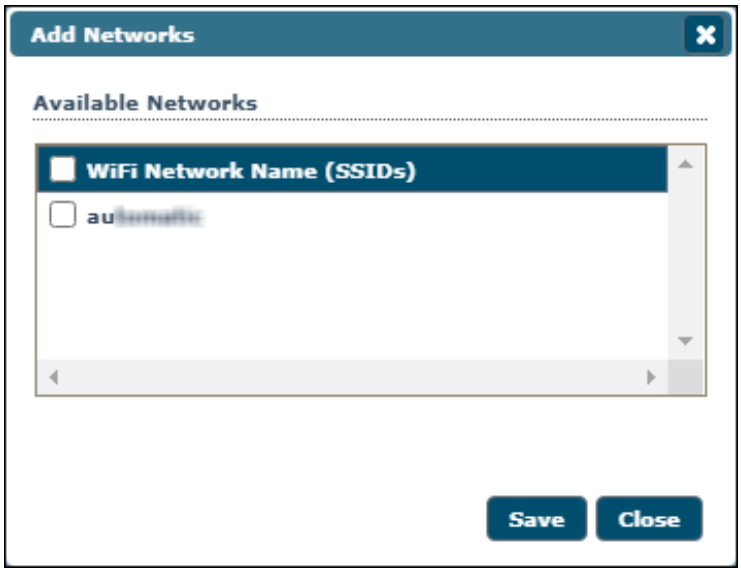


2. Click **OK**.
   The Wi-Fi network SSID will be deleted.

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.

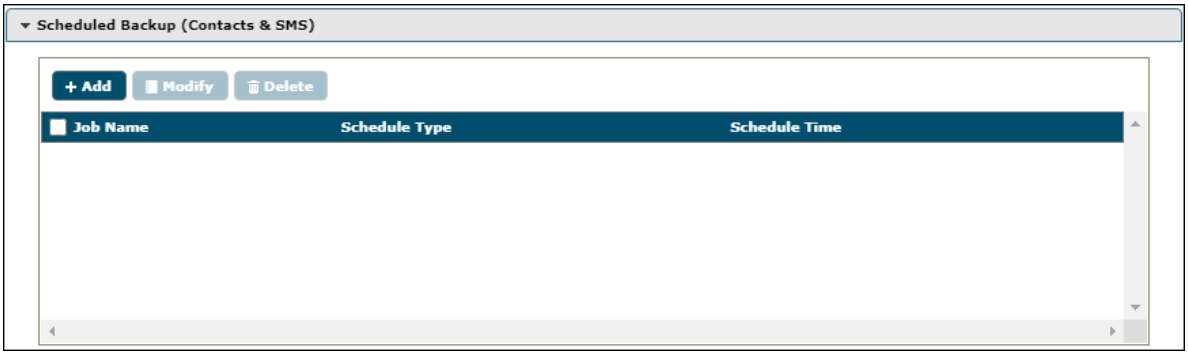


2. Select the Wi-Fi networks you want the device to always be connected to and then click **Save**.

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)

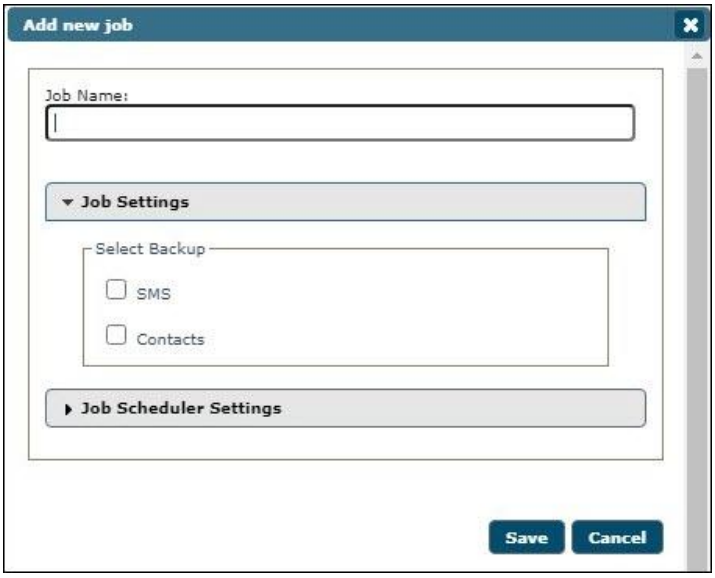
The Schedule Backup (Contacts & SMS) policy lets you take a backup of all the contacts from a device as per your requirements. The backup can be scheduled on daily/weekly basis.



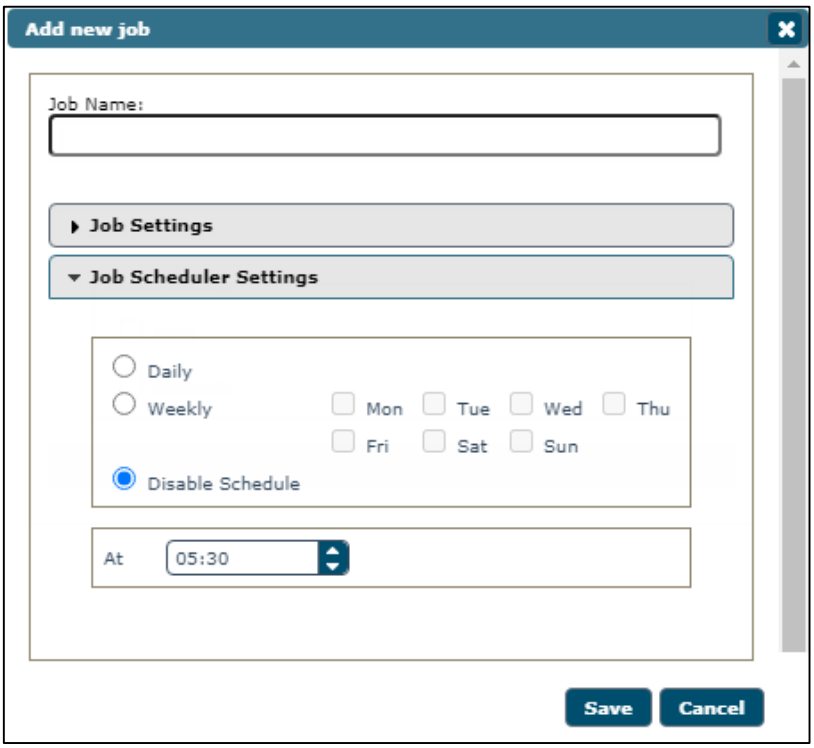
Creating a schedule

To create a new schedule:

1. Click **Add**.
   Add new job window appears.



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

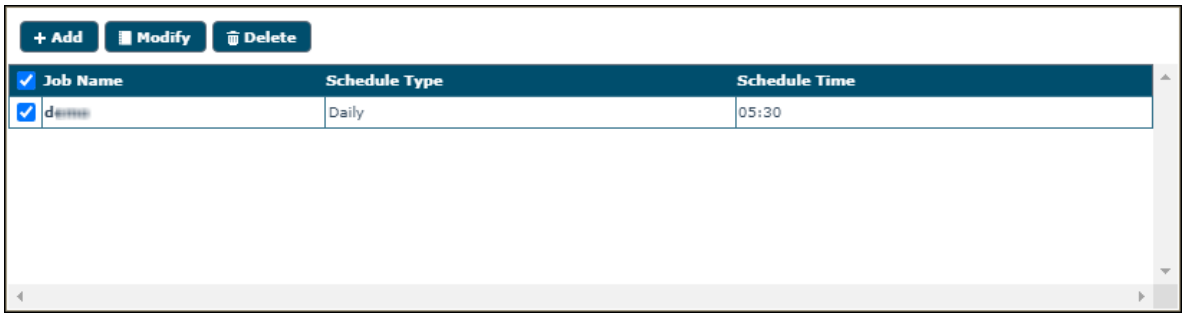


4. In **Job Scheduler Settings** section, select whether you want to take a backup Daily, Weekly or want to disable schedule.
5. Set the specific time at which you want to take the backup and then click **Save**.
   The schedule will be created as per the configuration.

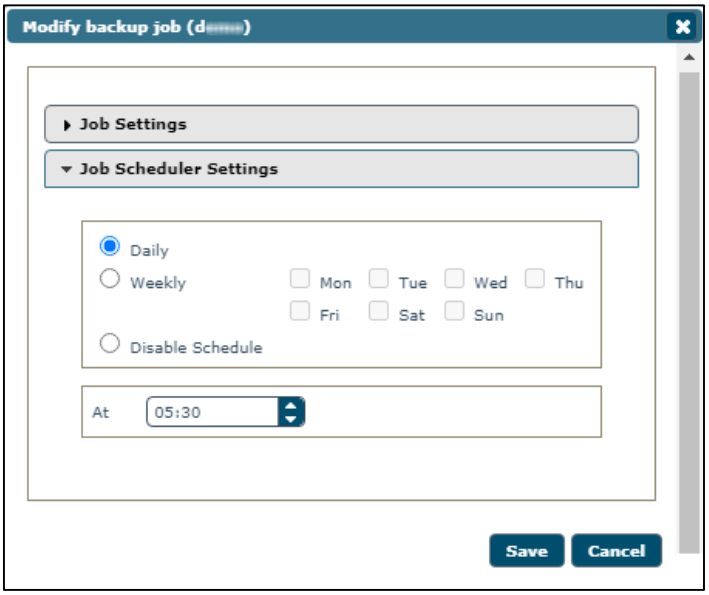
Modifying a schedule

To modify a schedule:

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



Modify backup job window appears.



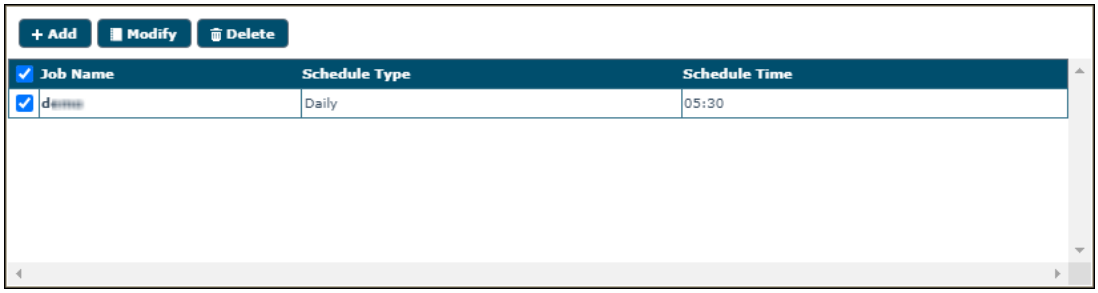
2. Make the required changes and then click **Save**.
   The schedule will be modified.

As an Administrator, you can even disable a scheduled backup by selecting the option **Disable schedule** > **Save**.

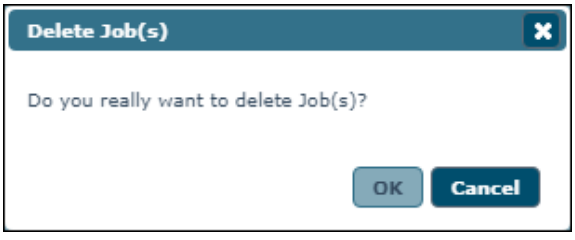
Deleting a schedule

To delete a schedule, follow the steps given below:

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



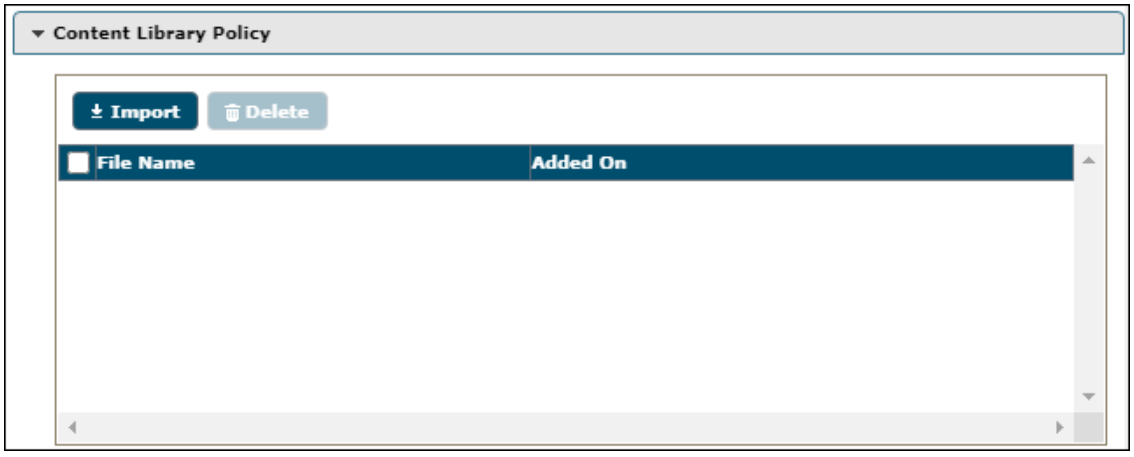
A confirmation prompt appears.



2. Click **OK**.
   The schedule will be deleted.

Content Library Policy

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, **click here**.



Import a file

To import a file from Content Library:

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

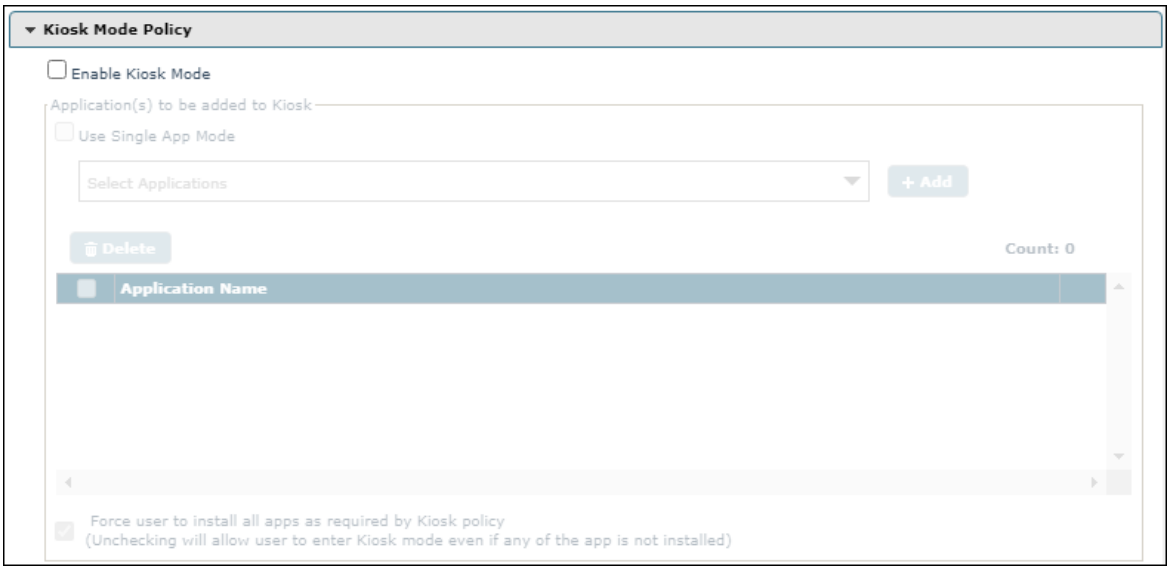
The file will be imported.

3. To delete a file, select the specific file and then click **Delete**.

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.



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.

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

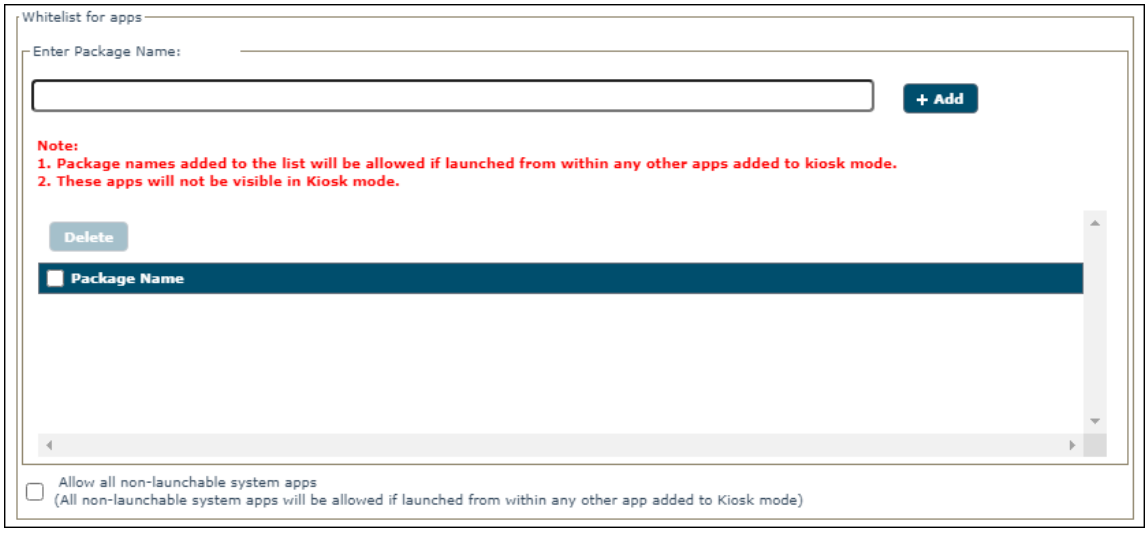
Force user to install all apps as required by Kiosk policy

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.

NOTE	Unchecking **Force user to install all apps as required by Kiosk policy** option will allow user to enter Kiosk mode even if any of the app is not installed.

Whitelist for apps

This section lets you to whitelist the required apps.



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.

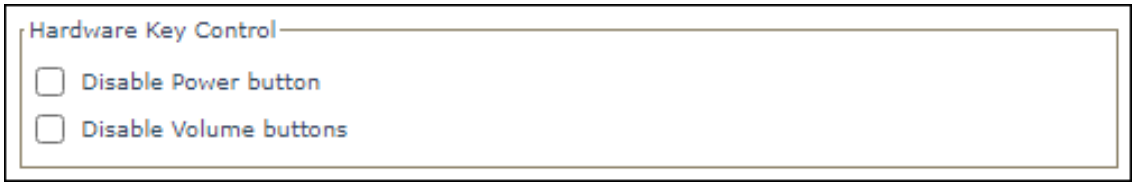
Allow all non-launchable system apps

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

NOTE	All non-launchable system apps will be allowed if launched from within any other app added to Kiosk mode.

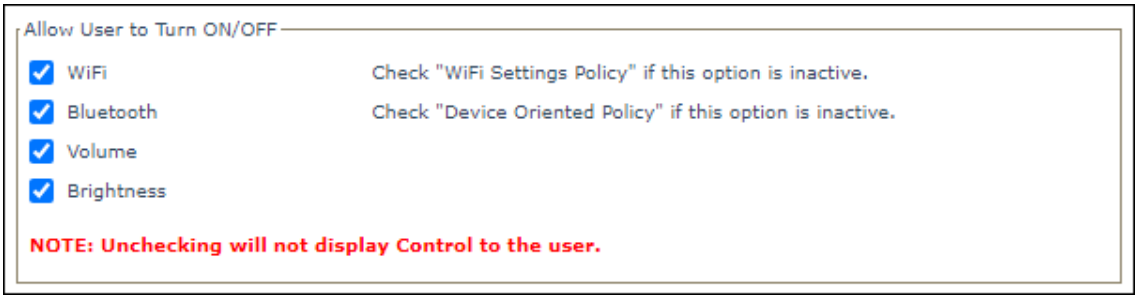
Hardware Key Control

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



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



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.

NOTE	Unchecking options won't display Control to the user on the Kiosk application.

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

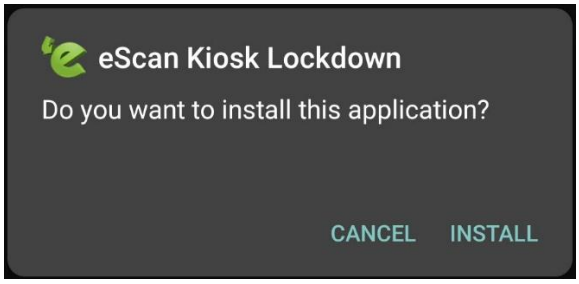
Allow device setting
Selecting this checkbox allows user to access and configure the device settings in the Kiosk mode.

Installation of eScan Kiosk Lockdown Application

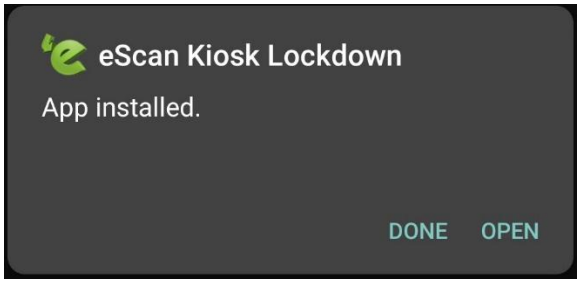
To run the eScan Kiosk Lockdown application in your device, it is necessary that you have installed eScan Device Management application and your device is enrolled in eScan Mobility Management console. Also, ensure that the Kiosk Mode policy is deployed to the device via the console.

NOTE	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**.



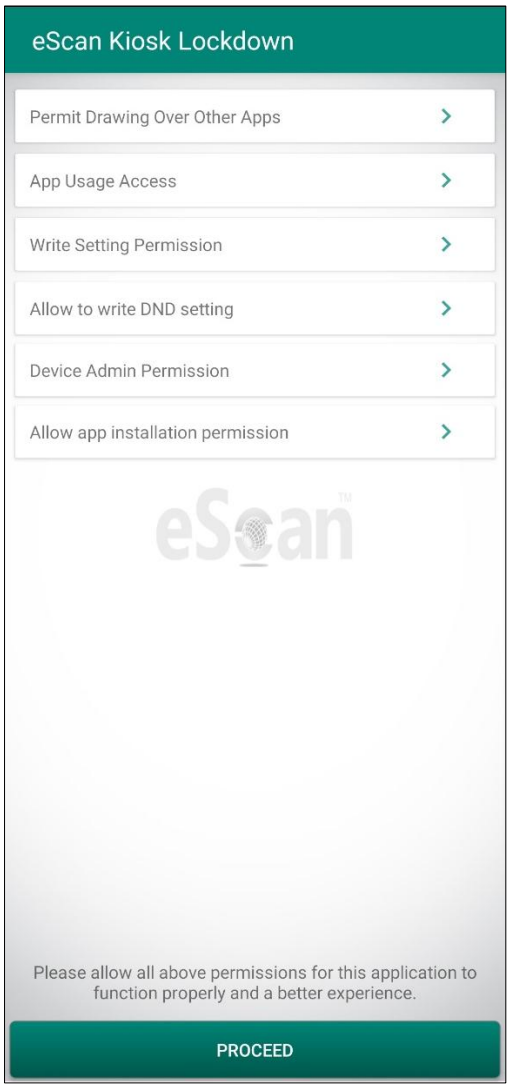
2. After an application gets installed, tap **OPEN**.

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.

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

4. Tap **Permit Drawing Over Other Apps.**



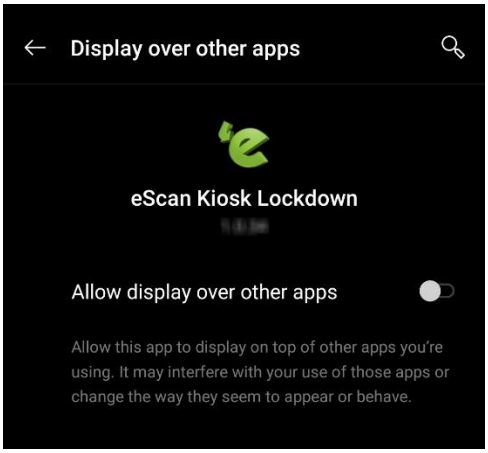
Tapping the displayed options will take you to the respective options in Settings, wherein you will have to tap the toggle button to grant all requested permissions.

 = Toggle disabled

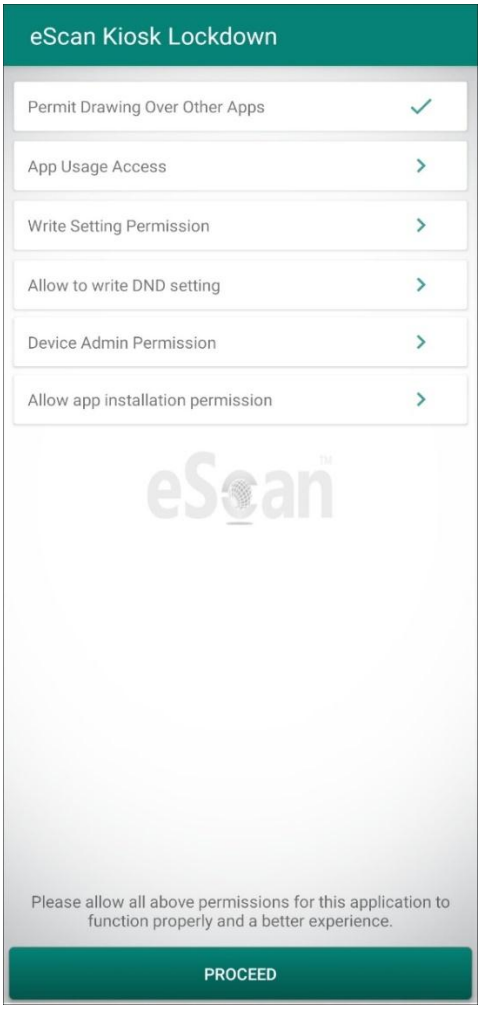
 = Toggle enabled

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

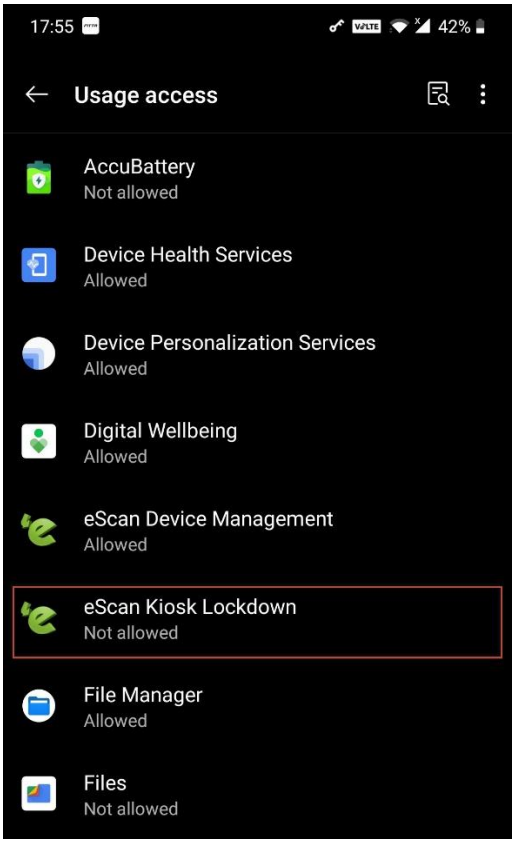
5. Tap **Allow display over other apps** toggle and then go back.



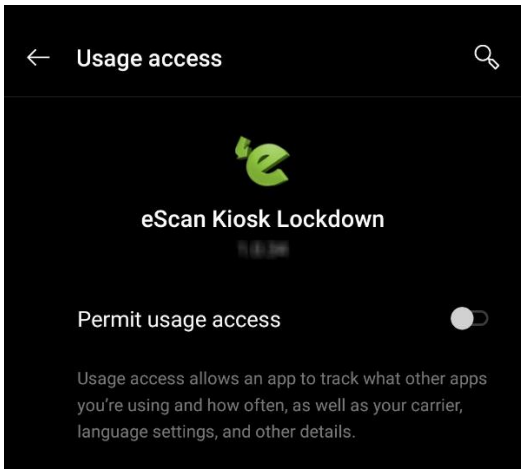
6. Tap **App Usage Access.**



7. Tap **eScan Kiosk Lockdown**.

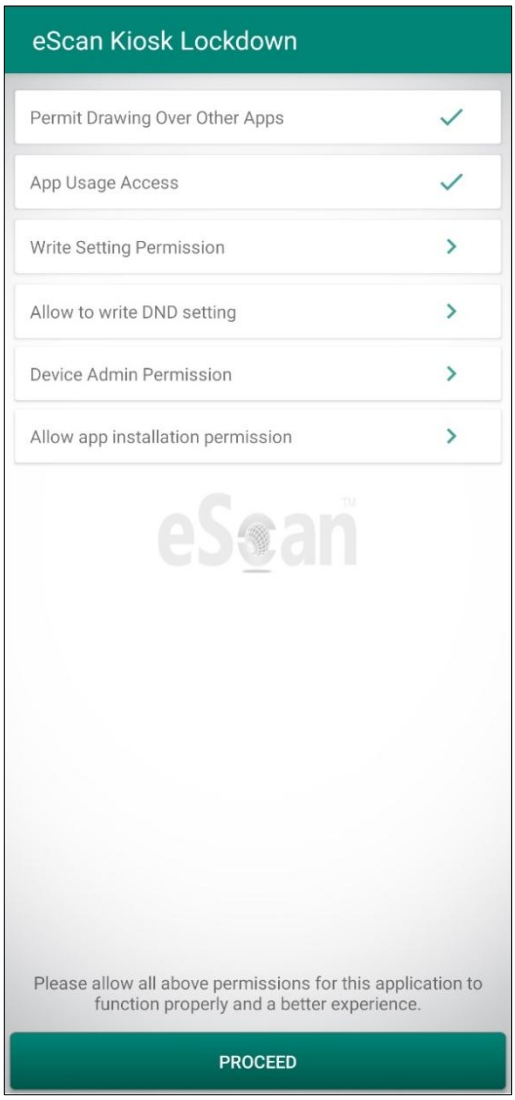


8. Tap **Permit usage access** toggle and then go back.

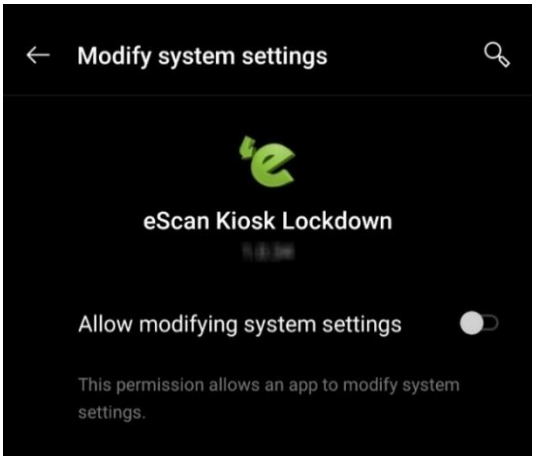


NOTE	The option **Permit usage access** maybe **Allow usage tracking** in your device. This option may vary depending upon the device manufacturer and android version.

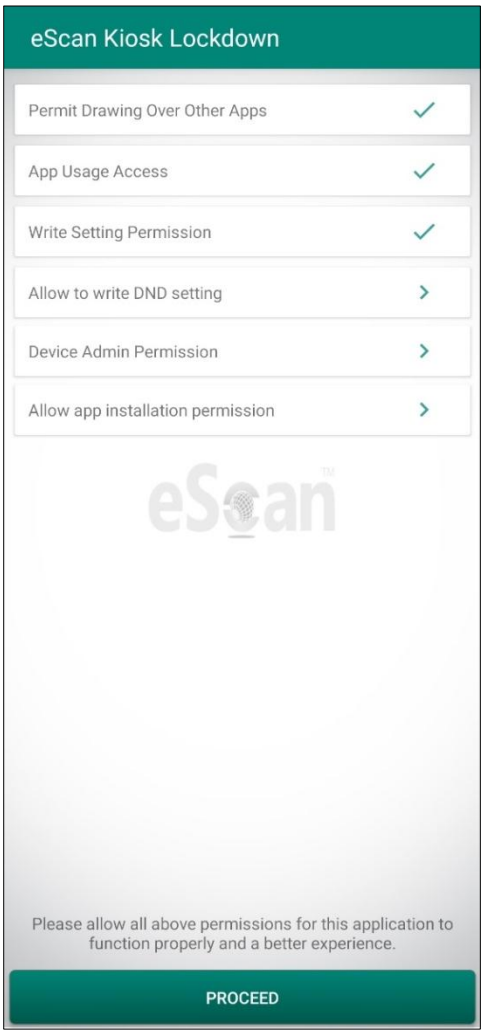
9. Tap **Write Setting Permission**.



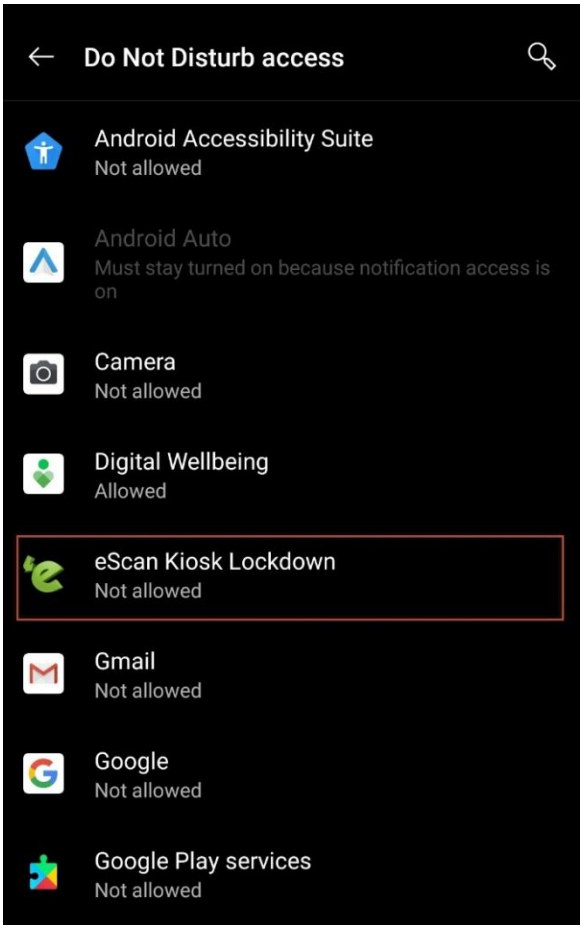
10. Tap **Allow modifying system settings** toggle and then go back.



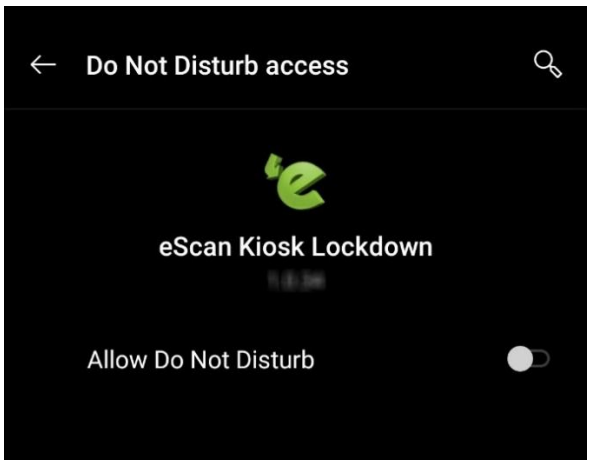
11. Tap **Allow to write DND setting**.



12. Tap **eScan Kiosk Lockdown**.

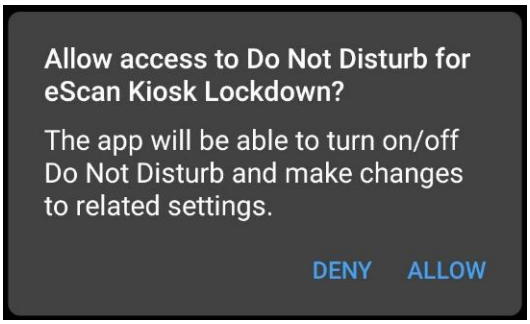


13. Tap **Allow Do Not Disturb** toggle.

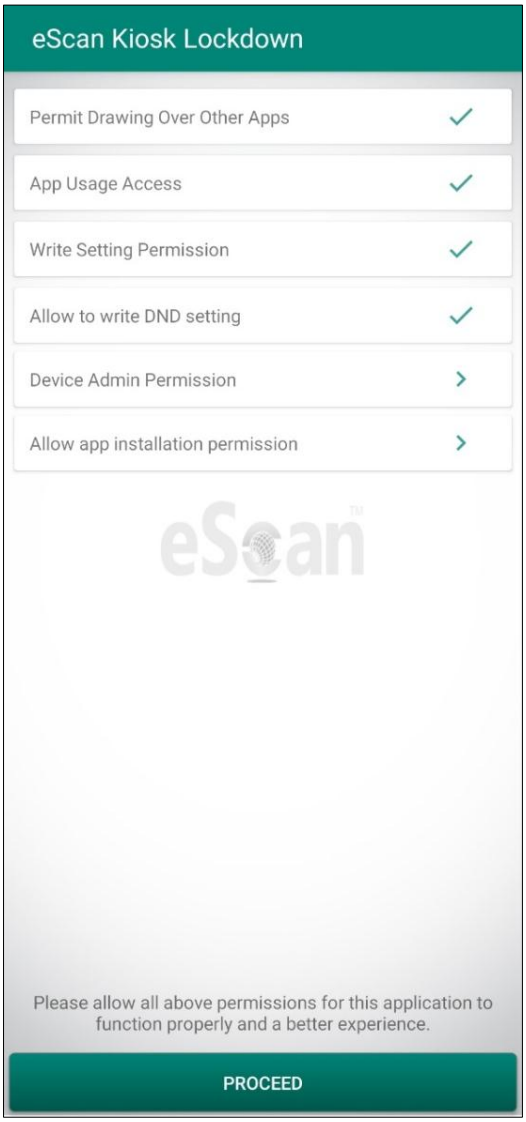


A prompt appears.

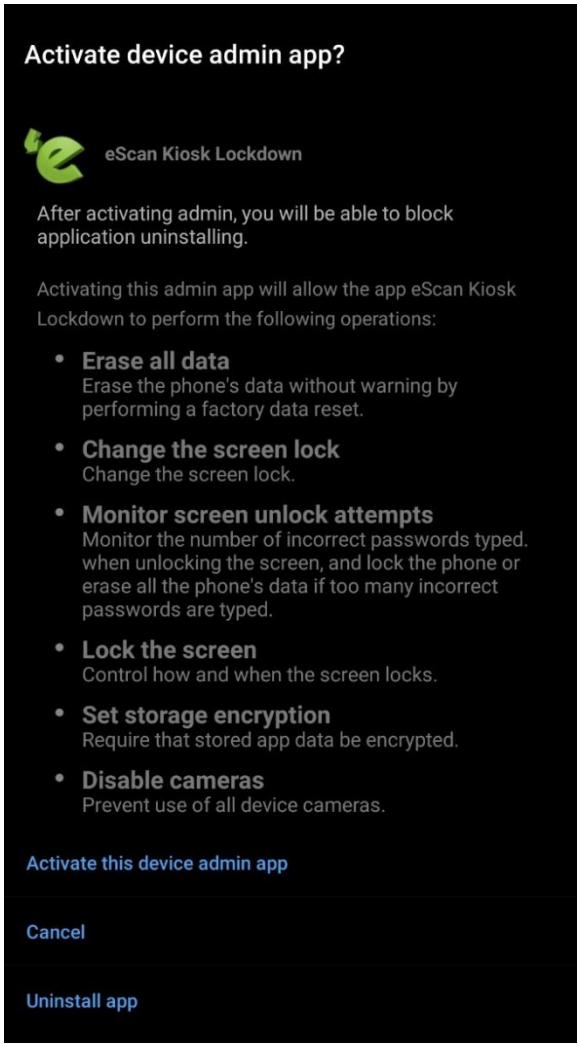
14. Tap **ALLOW** and then go back.



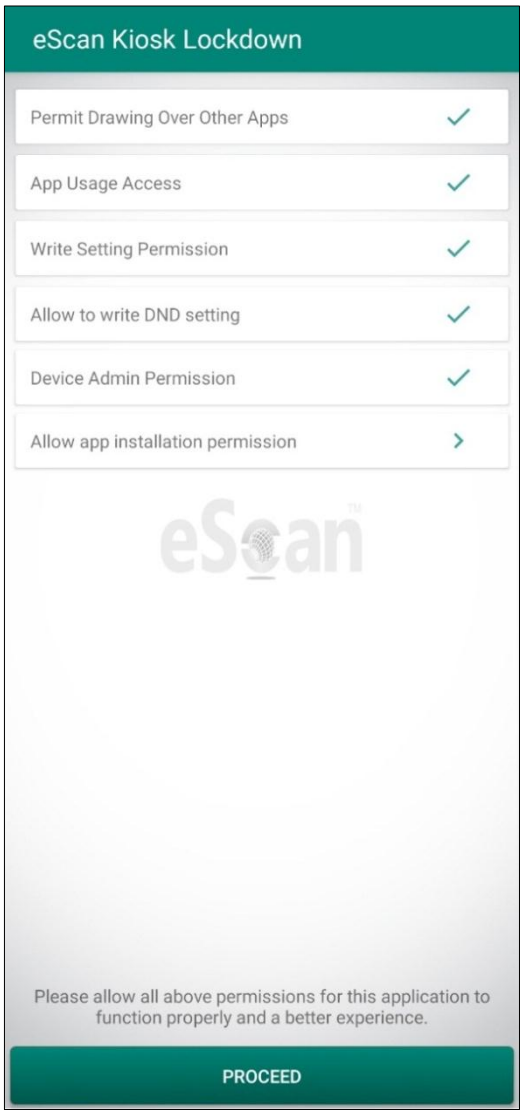
15. Tap **Device Admin Permission**.



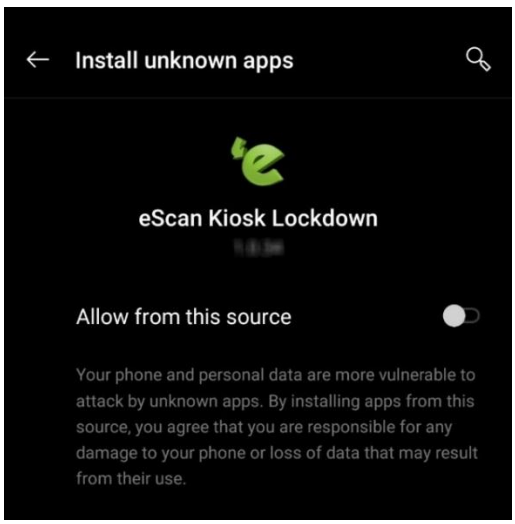
16. Tap **Activate this device admin app** option and then go back.



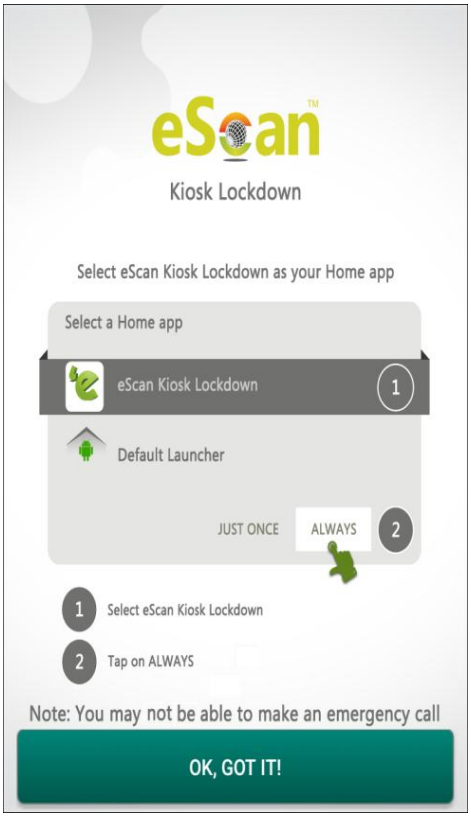
17. Tap **Allow app installation permission**.



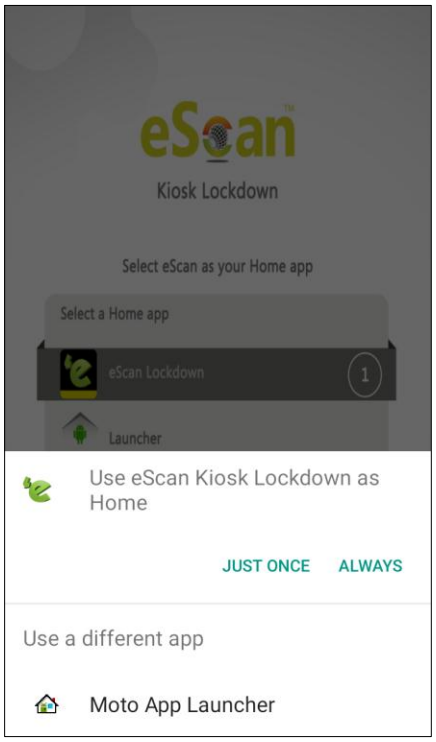
18. Tap **Allow from this source** toggle and then go back.



After all permissions are granted, an instructional image appears.



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

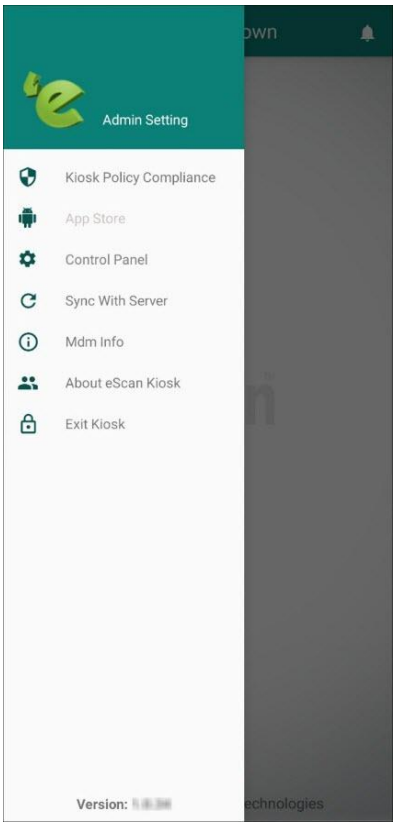


The device now runs in Kiosk mode and only the apps deployed via Kiosk Mode Policy are visible.

NOTE	The above image is for representational purposes only.

Tapping the bell icon 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 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

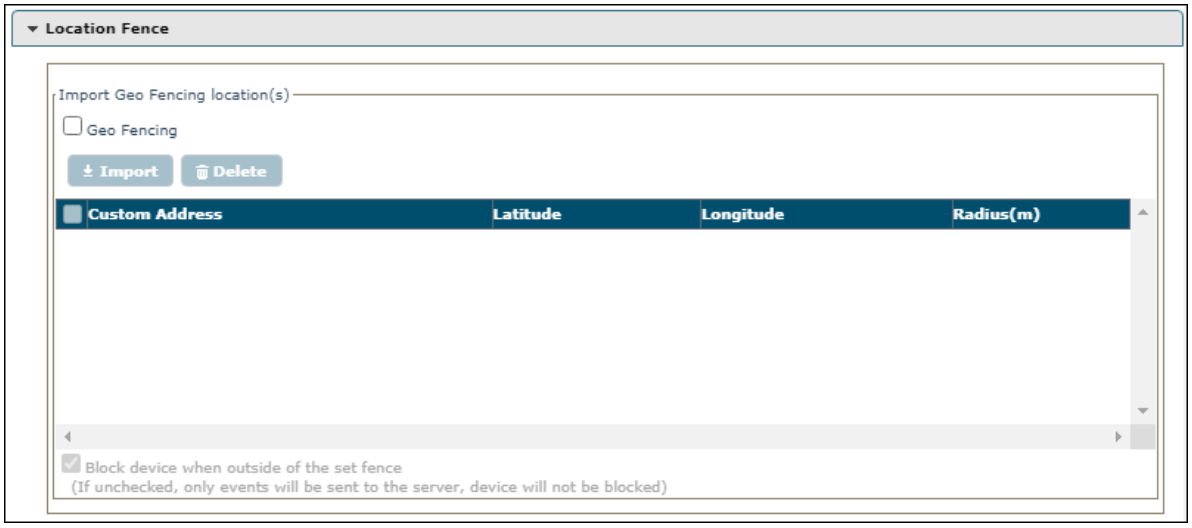
It displays general information about the Kiosk application, developer information and copyrights notice.

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, **click here**.



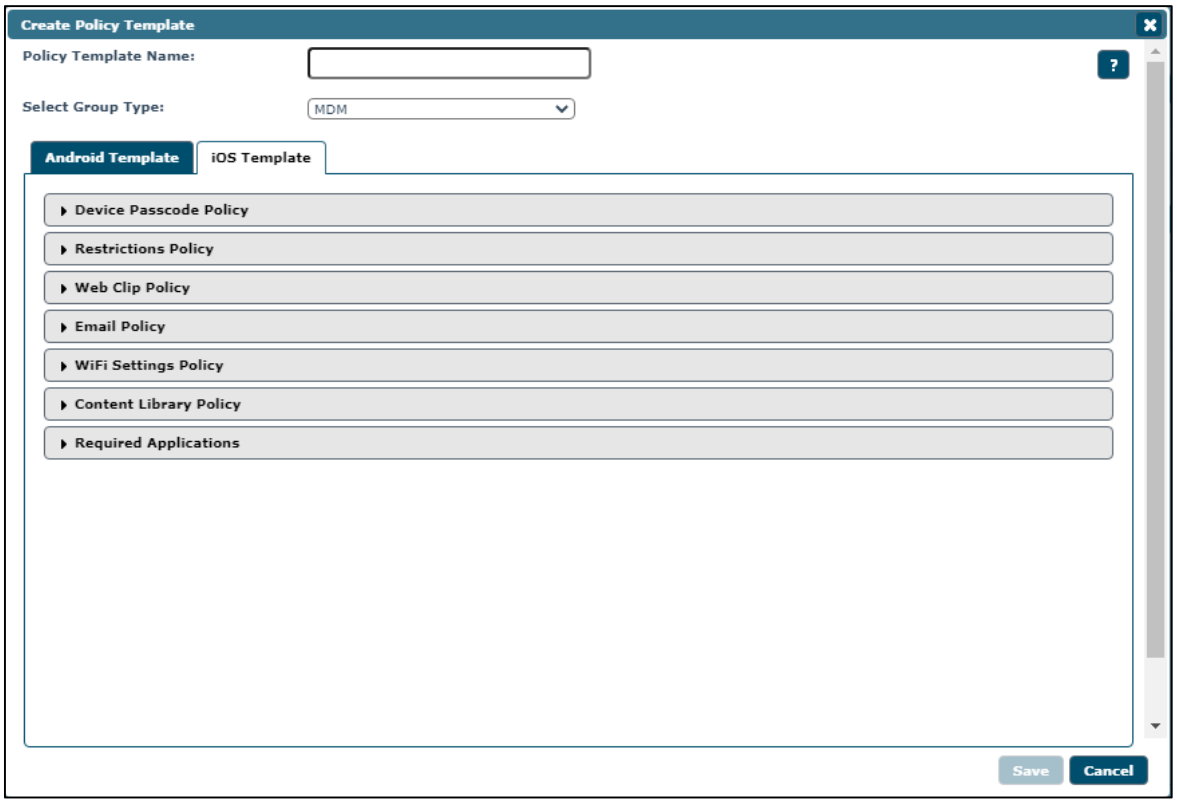
1. To configure Location Fencing policy, select Geo **Fencing** checkbox.
   After enabling this option, you can import and delete the fencing locations.
2. Click **Import** option to select the address and click **Save**.
3. To delete the added address, select the address and click **Delete**.

Block device when outside of the set fence

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

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

iOS Templates



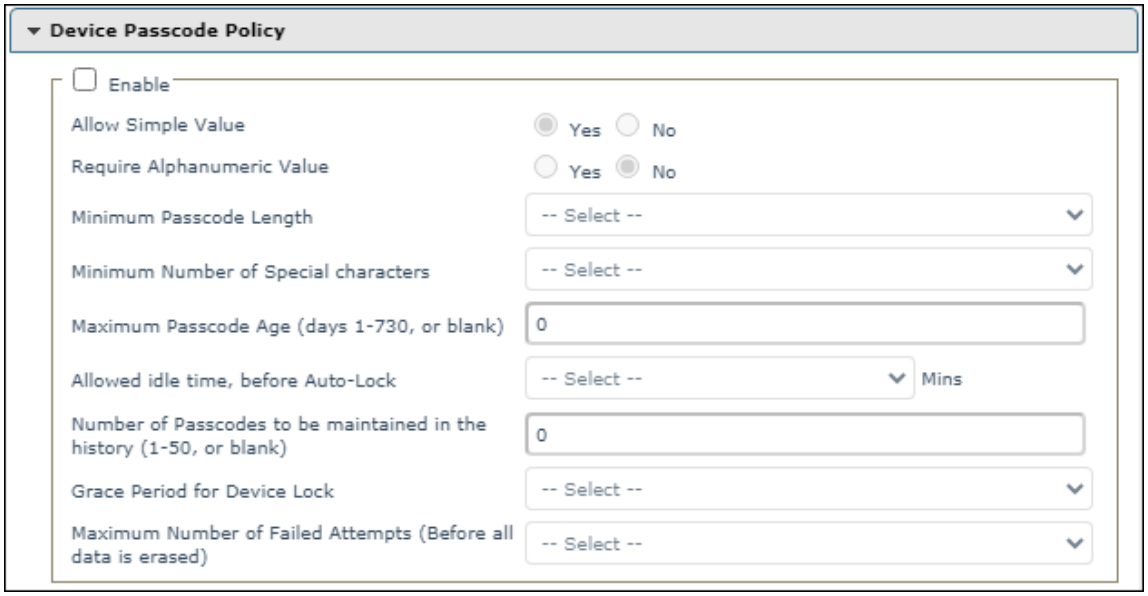
The iOS Template consists following policies:

- 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.



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.

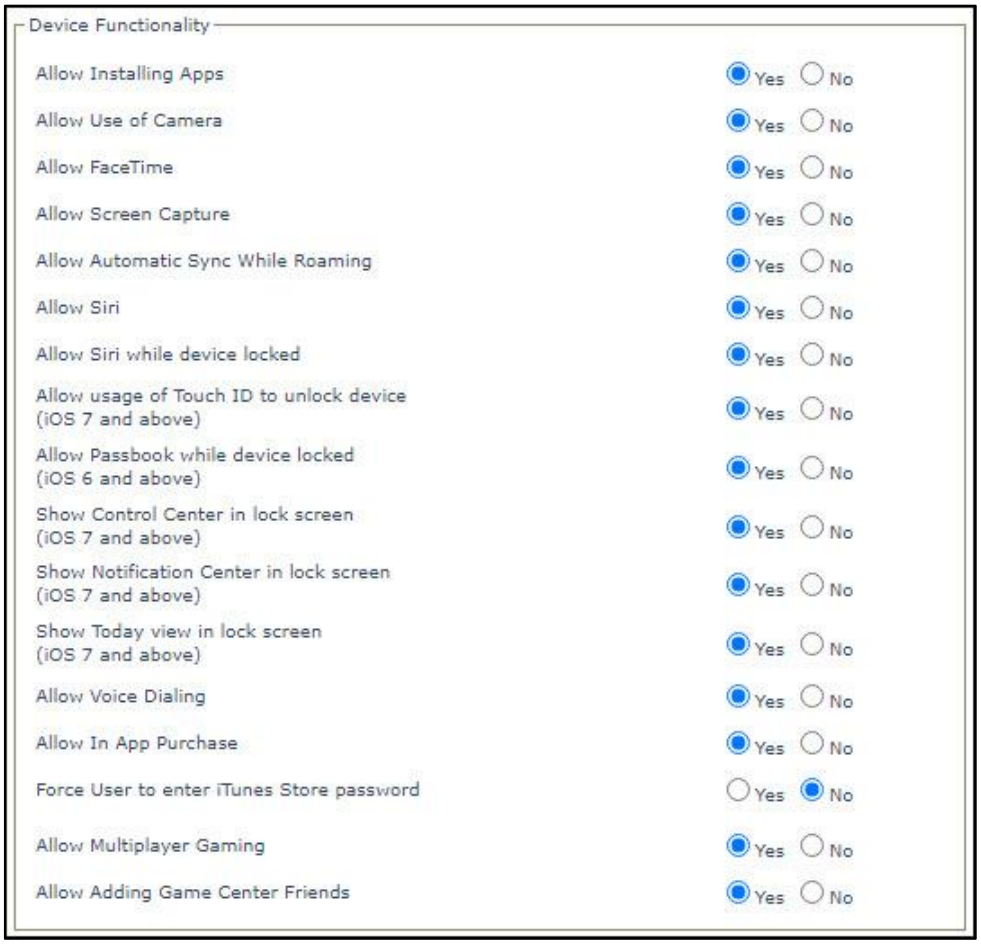
Maximum Number of Failed Attempts (Before all data is erased): This option lets you set the maximum number of failed attempts allowed for unlocking a device before all data on the device is erased.

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



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 **here**.

Show Control Center in lock screen (iOS 7 and above): Set this option to **Yes**, to allow users to access Control Center in the lock screen. Learn more about Control Center by clicking **here**.

Show Notification Center in lock screen (iOS 7 and above): Notification Center is a feature in iOS that provides an overview of application notifications. Set this option to **Yes** to allow users to view Notification Center in lock screen.

Show Today view in lock screen (iOS 7 and above): Set this option to **Yes**, to allow users to view Today View in lock screen.

Allow Voice Dialing: Set this option to **Yes**, to allow users to call their contacts via voice.

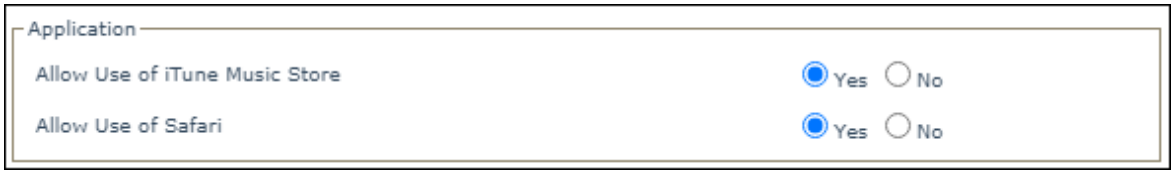
Allow In App Purchase: Set this option to **Yes**, to allow users to make in-app purchases.

Force User to enter iTunes Store password: Set this option to **Yes**, to force a user to enter their iTunes Store password.

Allow Multiplayer Gaming: Set this option to **Yes**, to allow a user to play a multiplayer game on their device.

Allow Adding Game Center Friends: Set this option to **Yes**, to allow a user to add Game Center friends.

Application



Allow Use of 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

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

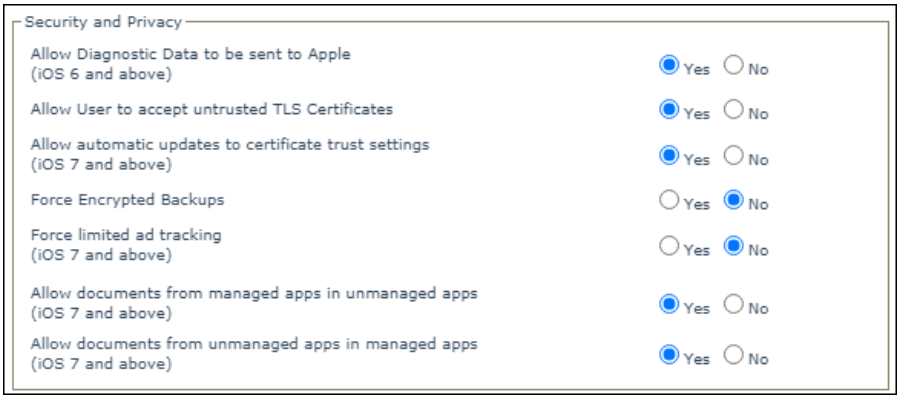
Allow Backup: Set this option to **Yes**, to allow backup of device data to iCloud.

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



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.

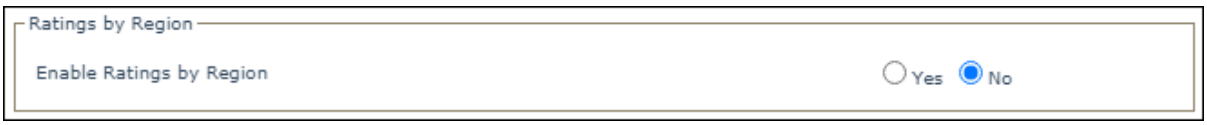
Allow documents from managed apps in unmanaged apps (iOS 7 and above): Set this option to **Yes**, to allow documents from managed applications to open in unmanaged applications.

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.

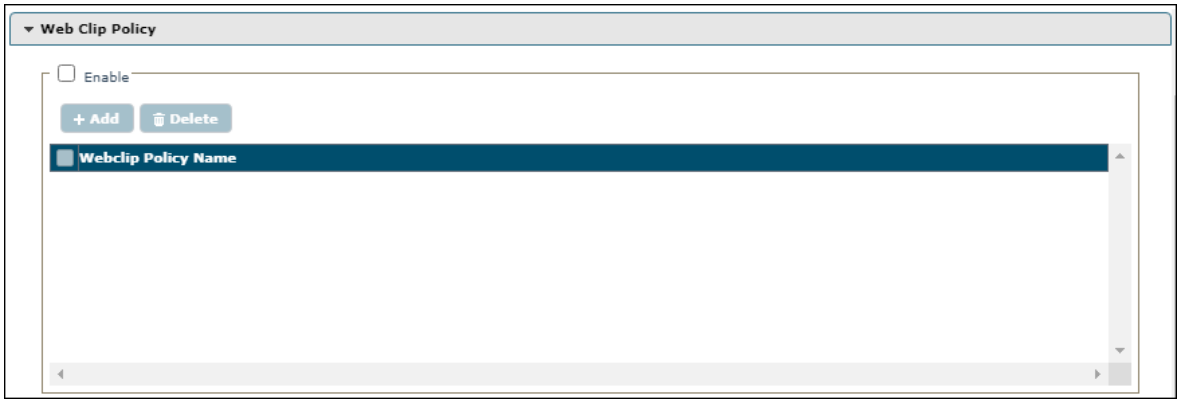
Ratings by Region



Enable Ratings by Region: Set this option to **Yes**, to enable content ratings by region.

Web Clip Policy

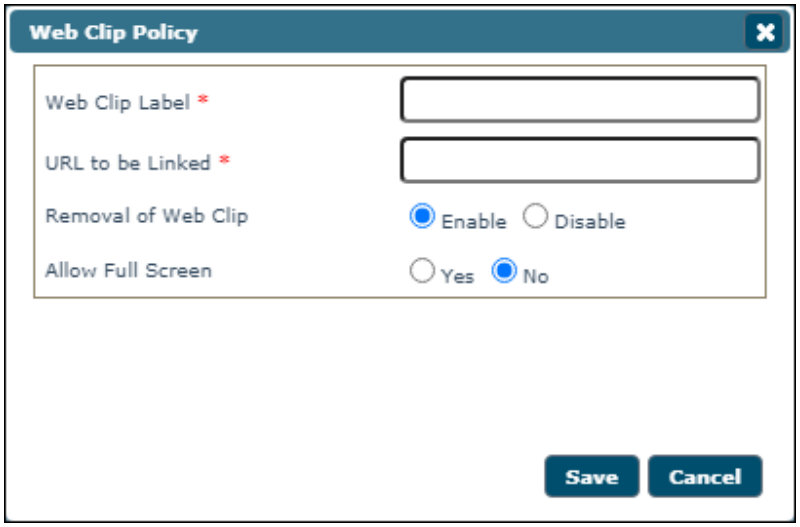
The Web Clip policy lets you get important websites on a device's home screen to let users access it quickly.
Select **Enable** checkbox to enable the configuration of Web Clip Policy.



Adding a Web Clip

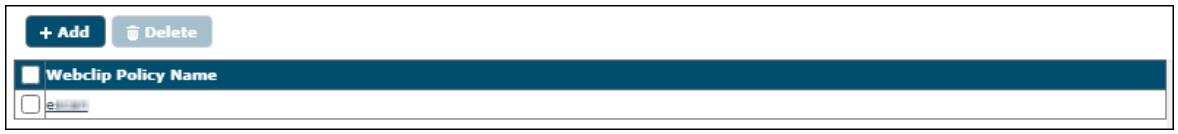
To add a web clip policy:

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



- **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.

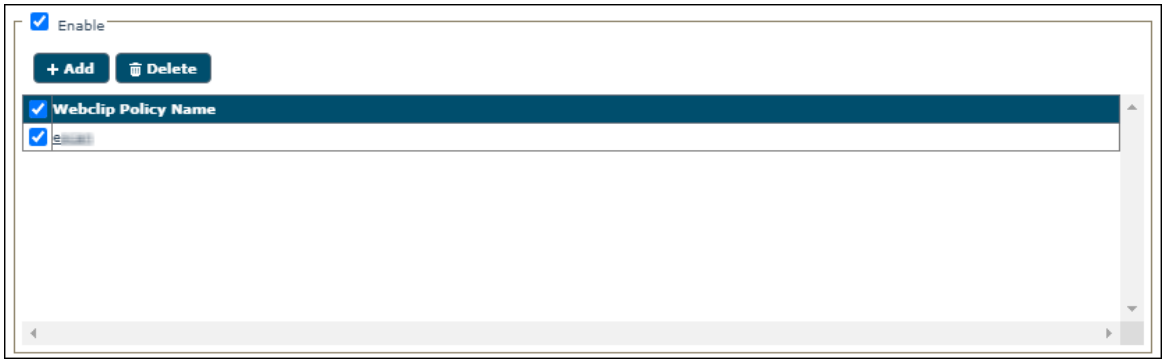
After entering all the details, click **Save**.
The new Web Clip policy will be added.



Deleting a Web Clip

To delete the existing web clip:

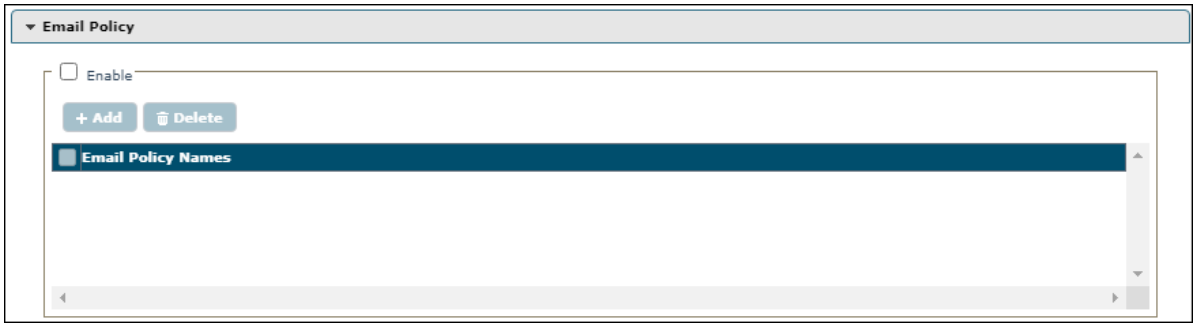
- Select a Web Clip and then click **Delete**.



The Web Clip policy will be deleted.

Email Policy

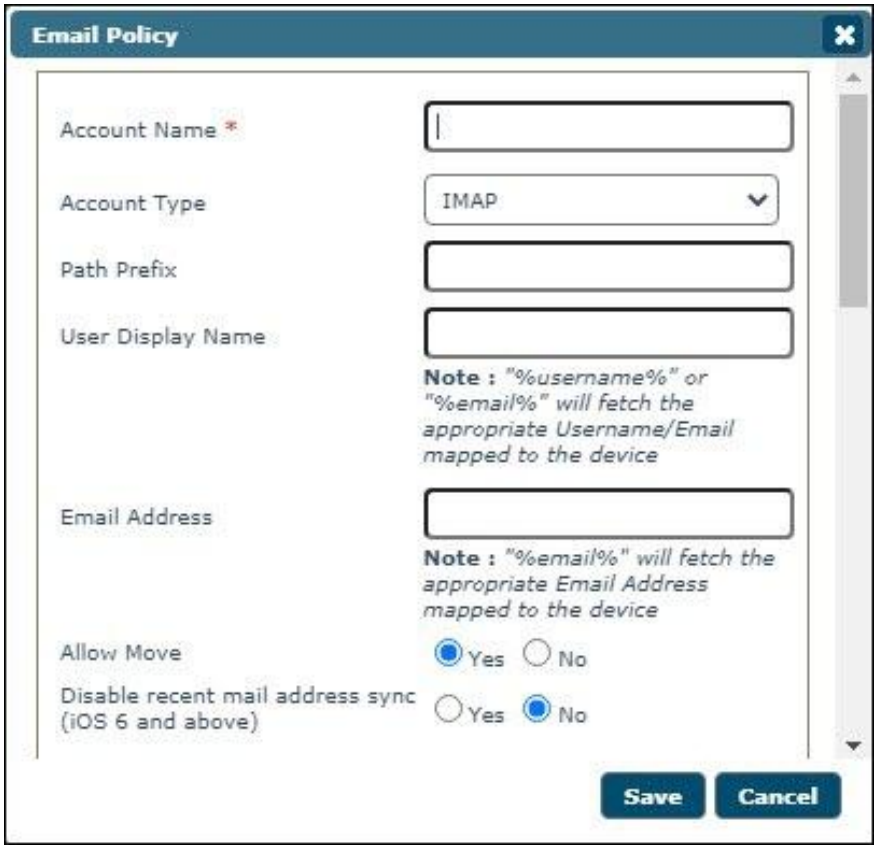
The Email Policy lets you set up an email account for the managed devices and define the settings for incoming and outgoing emails.
Check **Enable** to configure the Email Policy



Adding Email policy

To add Email Policy, follow below steps:

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



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.

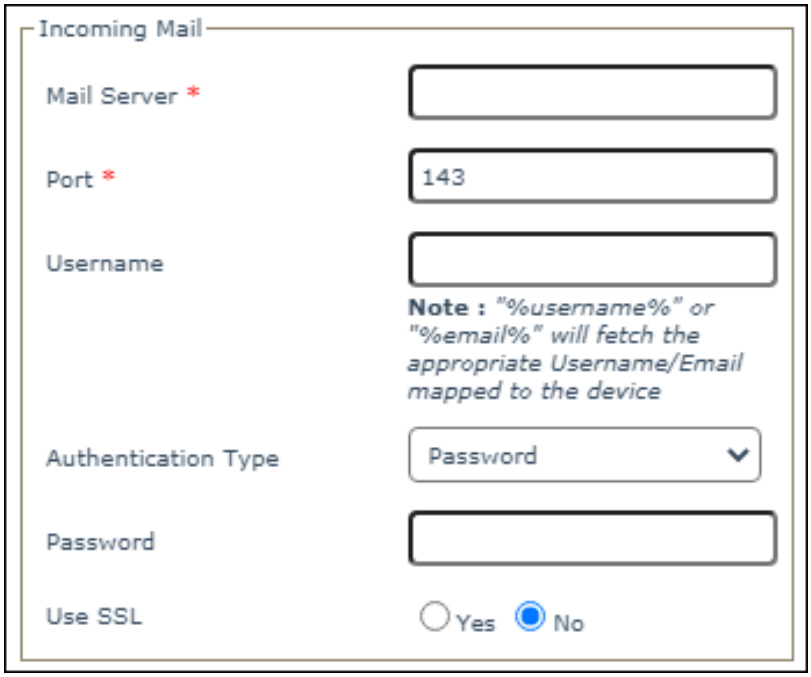
Email Address: Typing in the prefix "*%email%*" will fetch the appropriate email ID mapped to the device.

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, **click here**.
   - To learn more about Outgoing Mail, **click here**.
4. After filling the details, click **Save**.

Incoming Mail



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.

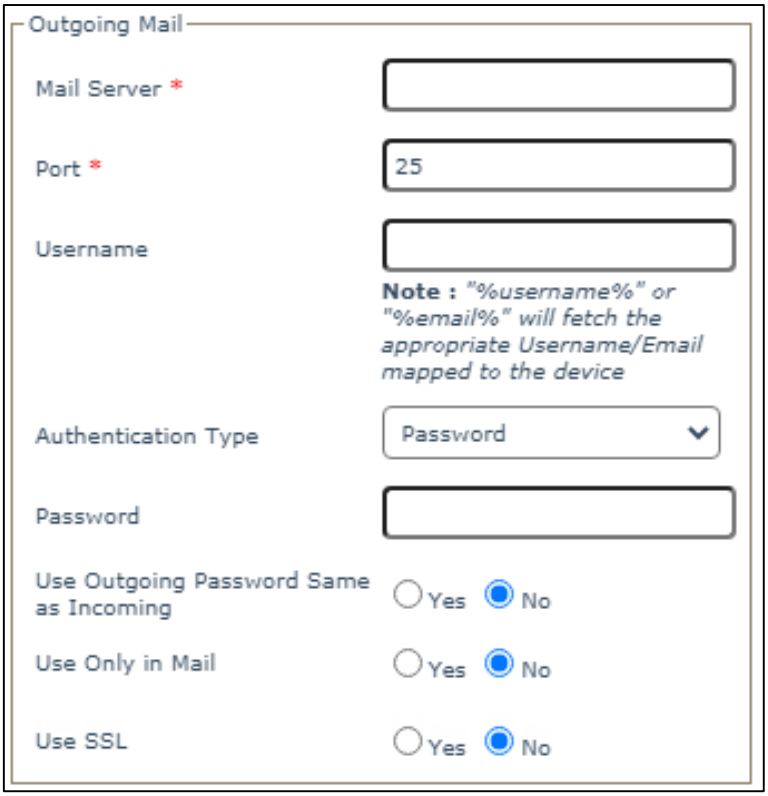
Authentication Type: Select an appropriate authentication type from the following options:

- 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



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.

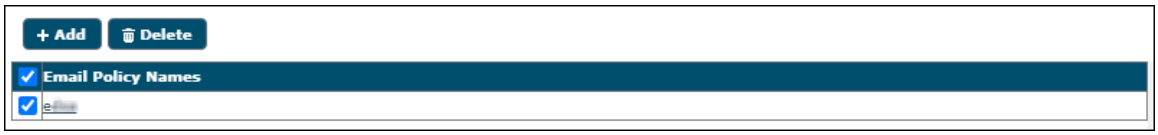
Use SSL: Determines whether or not the outgoing mail server uses SSL certificate.

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

Deleting an Email Policy

To delete an email policy, follow the steps below:

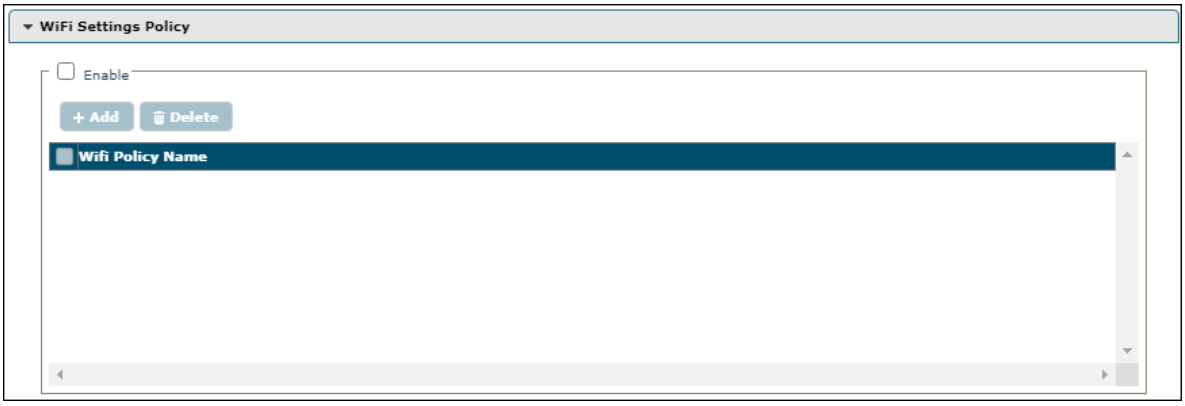
1. Select the particular Email Policy from the list.



2. Click **Delete**.
   The Email Policy will be deleted.

WiFi Settings Policy

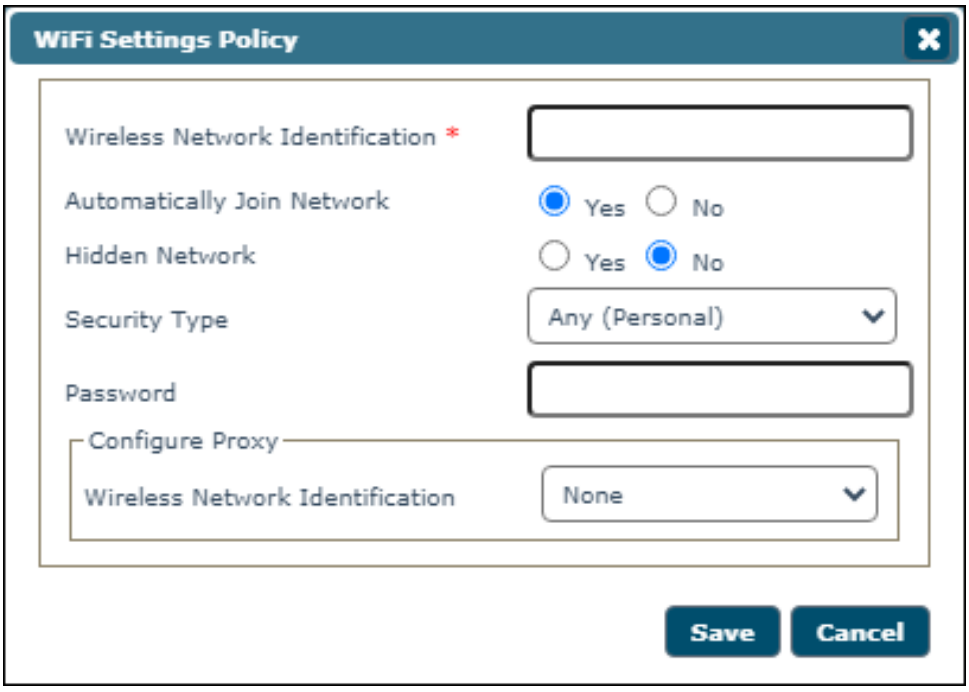
The WiFi Settings Policy lets you manage how a user connects their devices to a Wi-Fi network. Check **Enable** to configure the WiFi Setting Policy.



Adding a WiFi Settings Policy

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

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



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.

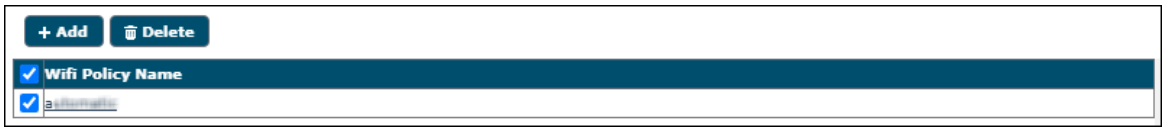
- None
- Manual
- Automatic

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.

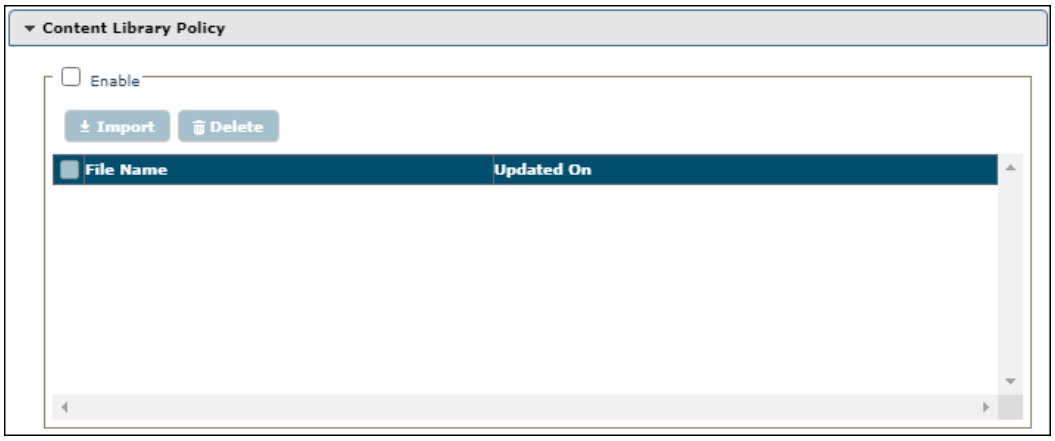


2. Click **Delete**.
   The WiFi Settings Policy will be deleted.

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, **click here**.

Select **Enable** checkbox to configure the Content Library Policy.



Importing a file

To import a file from Content Library:

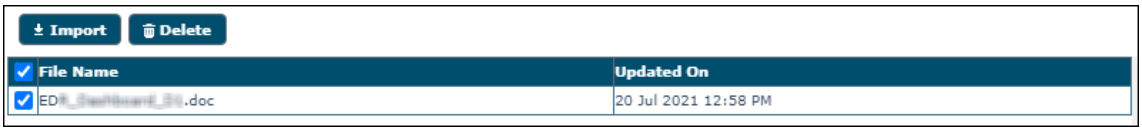
1. Select **Enable** checkbox and then click **Import**.
   Import Files window appears.

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**.



2. The selected file will be deleted.

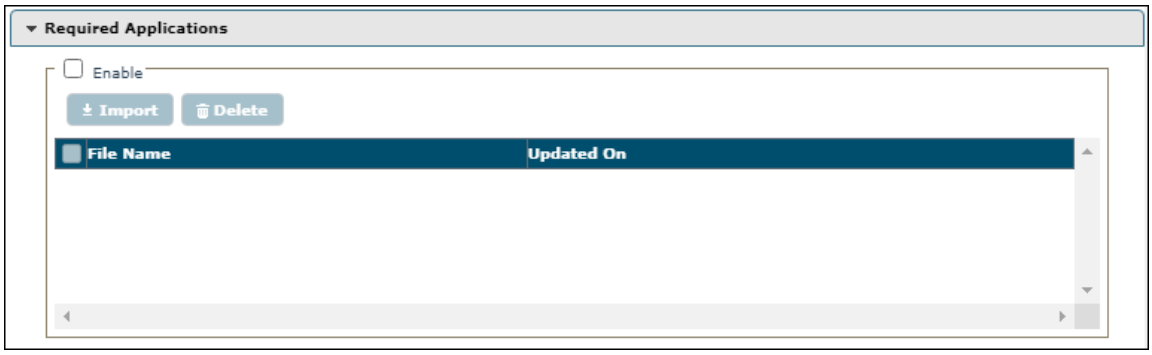
Required Applications Policy

The Required Applications Policy lets you import applications from the App Store module for installation on managed devices in the group through policy deployment.

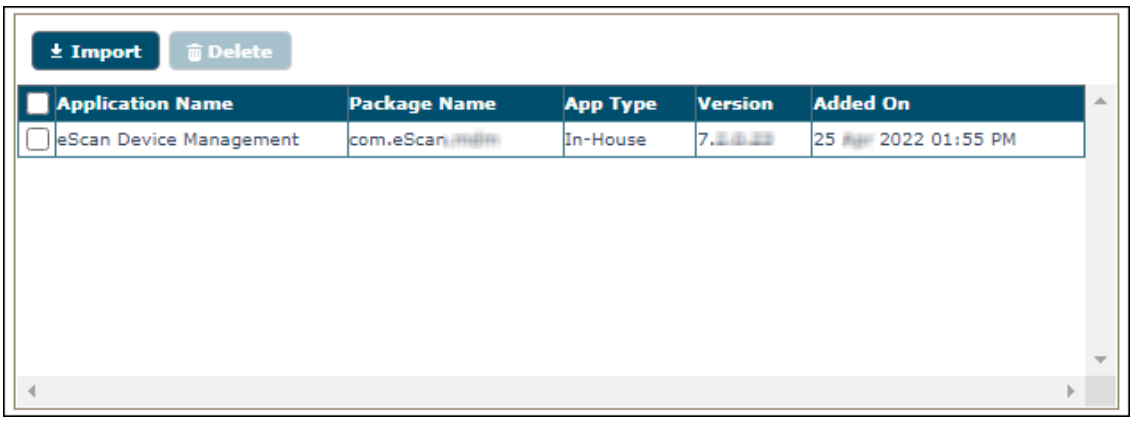
Importing an application

To import applications from the App Store, follow the steps given below:

1. Select **Enable** checkbox and then click **Import**.



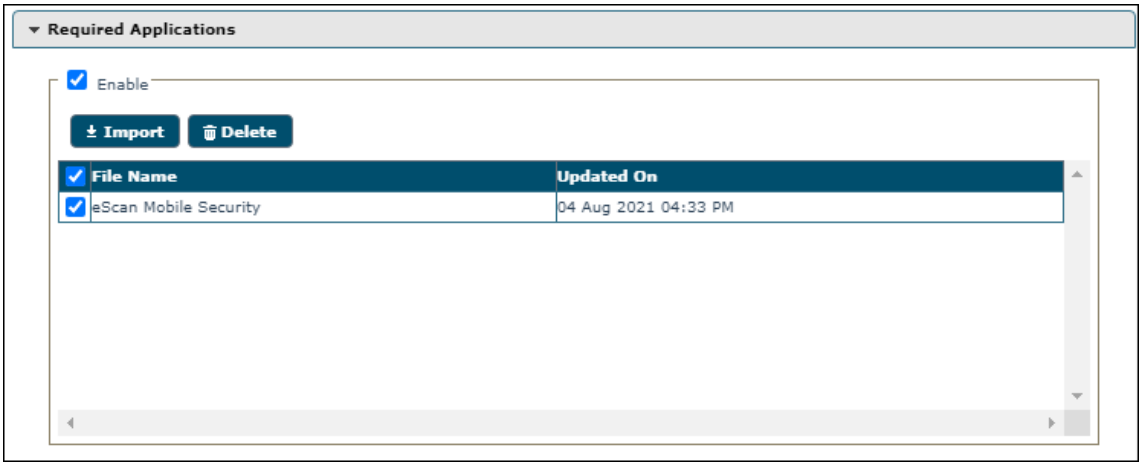
Import Application window appears.



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

Deleting an application

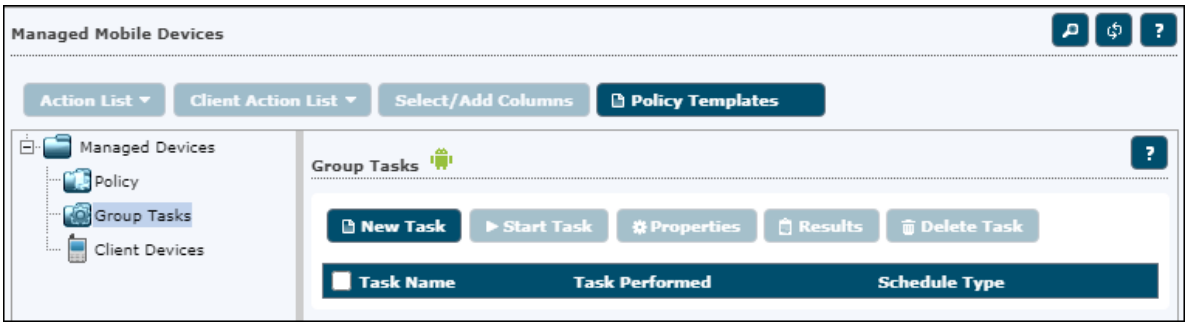
1. Select an application and then click **Delete**.



2. The selected application will be deleted.

Group Tasks

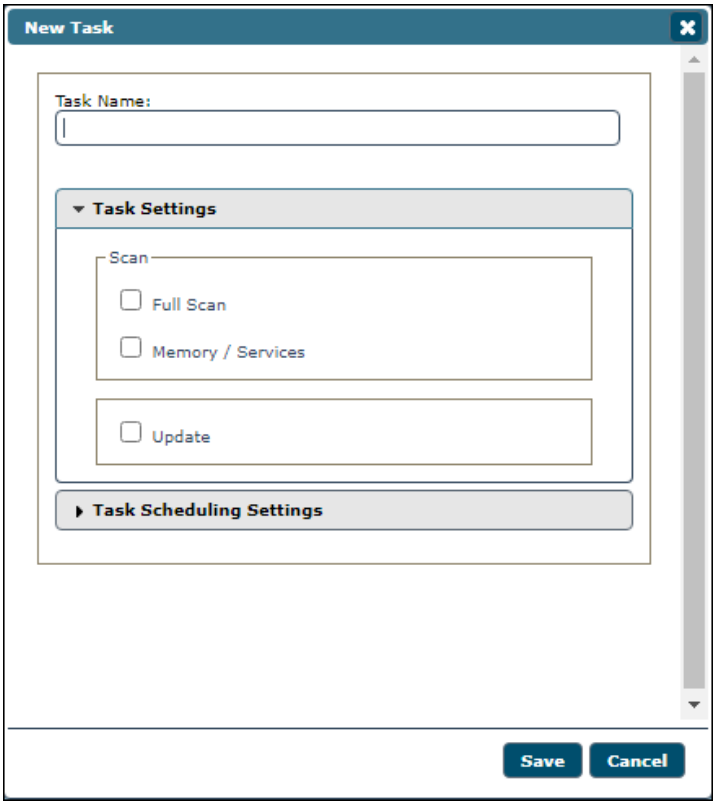
The Group Tasks option lets you create and schedule tasks for the devices in a group.



Creating a New Group Task

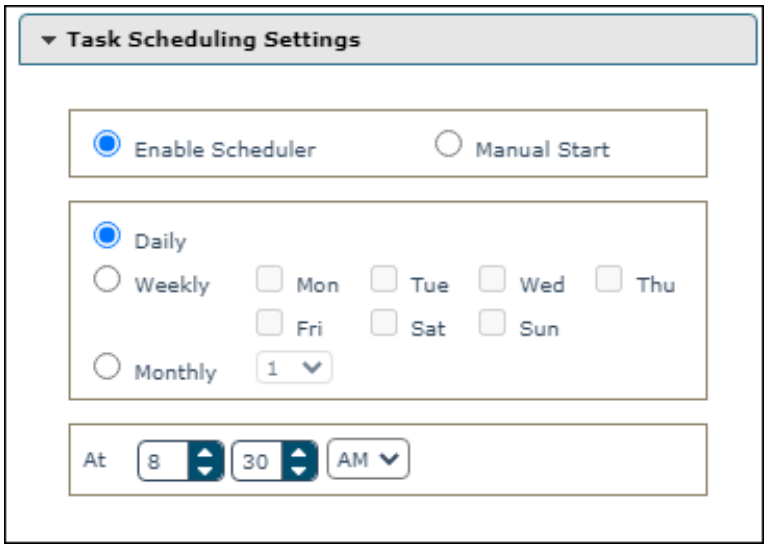
To create new group task, follow the below steps:

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



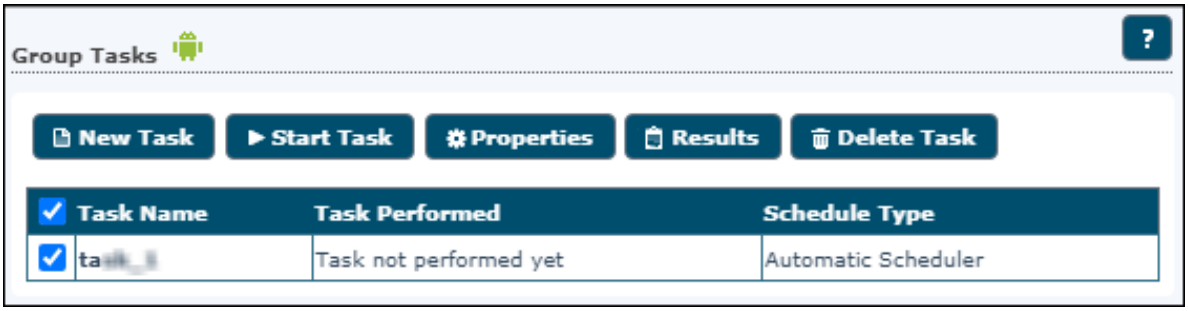
2. Enter a task name.
3. In **Task Settings** section, select the scan type to be run on a device.
4. By checking the Update, you can also let the application update its virus signature database.

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



6. Click **Save**.
   The task will be created instantly as per configuration.

Selecting a task enables following options:



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

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:

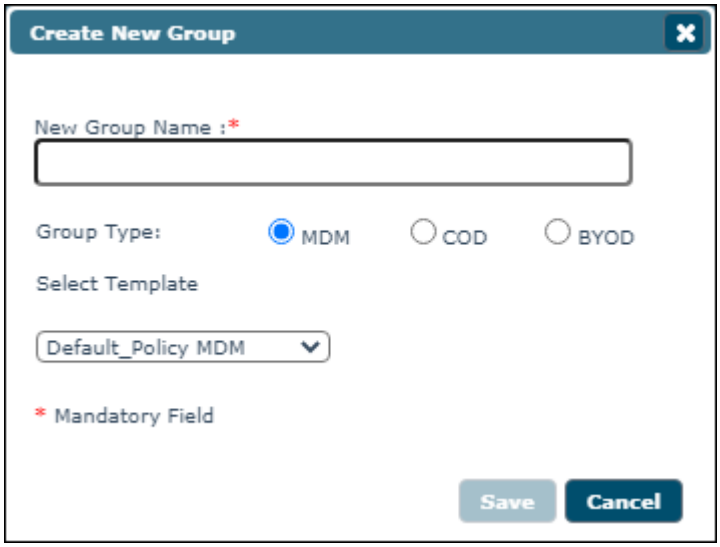
- Adding a device to the console
- Enrolling an added device

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**.

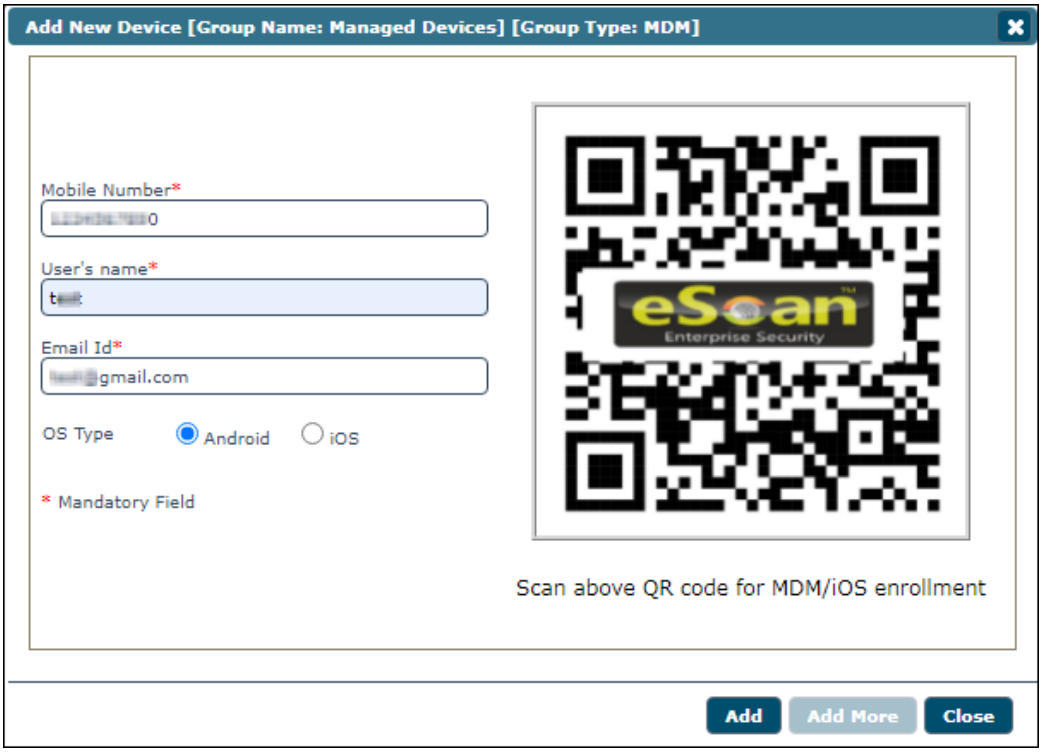


Group will be created.

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.



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.

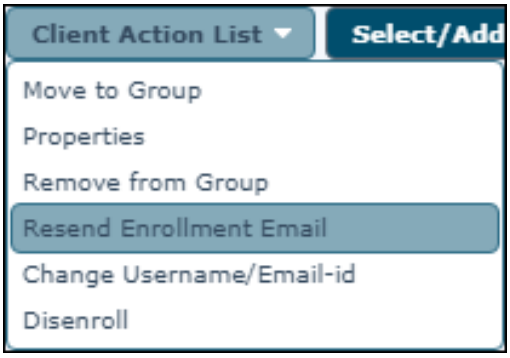
After adding a device to the group, you will see icon next to the checkbox. This icon indicates that the added device is not enrolled.

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.

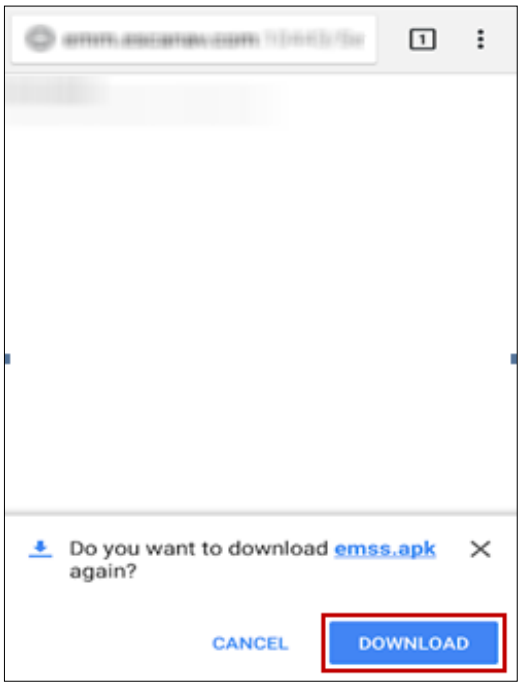
In case a user did not receive the enrollment email at the time of adding the device, you can resend it.

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



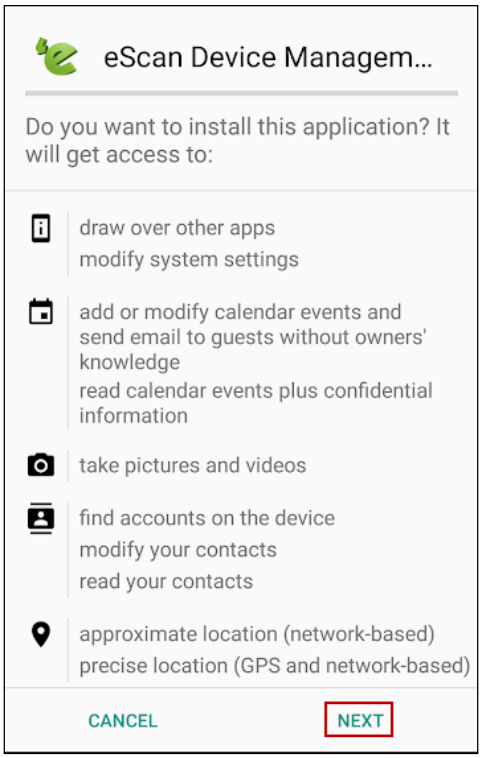
After receiving the enrollment email, the user should perform the following steps:

1. Tap the shared URL in the email.
   A prompt appears asking you to download the eScan MDM application.

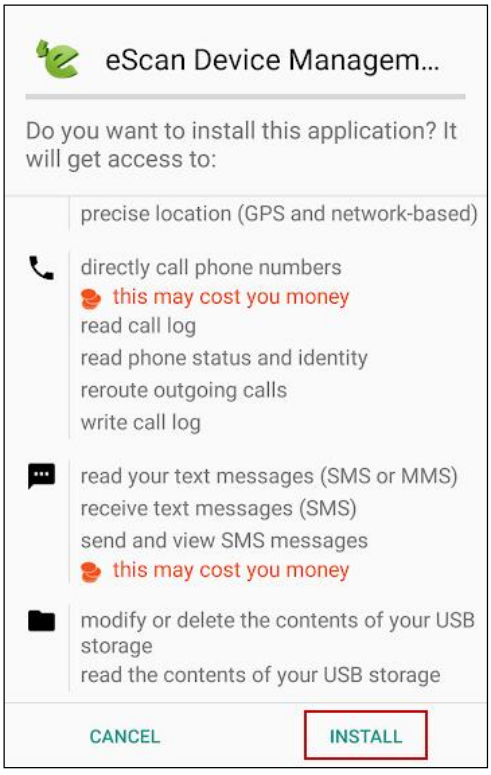


2. Tap **DOWNLOAD**.
   Tap the downloaded file and read thoroughly about the permissions asked by the application.

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



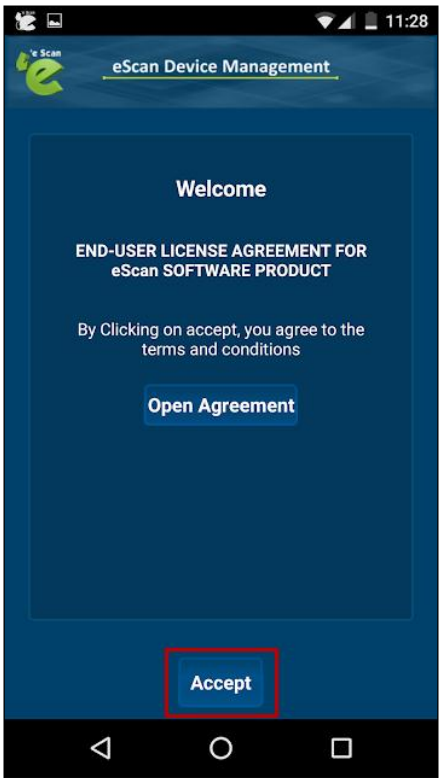
4. After reading the application's access permissions, tap **INSTALL**.



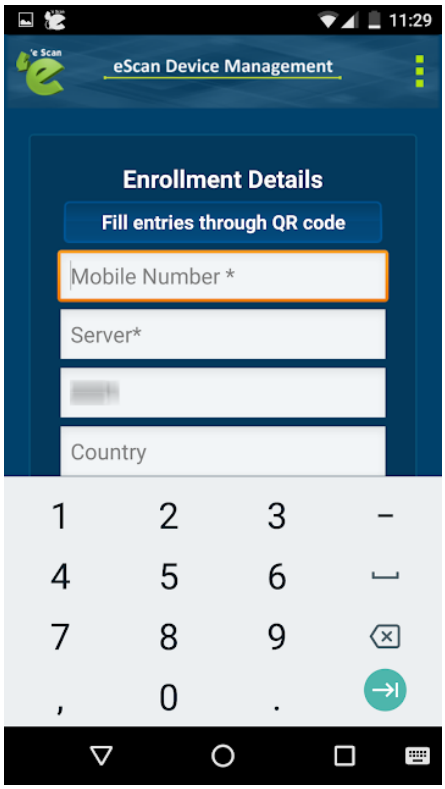
Open the "**eScan EMM**" app, after the installation is completed.

Welcome screen appears.

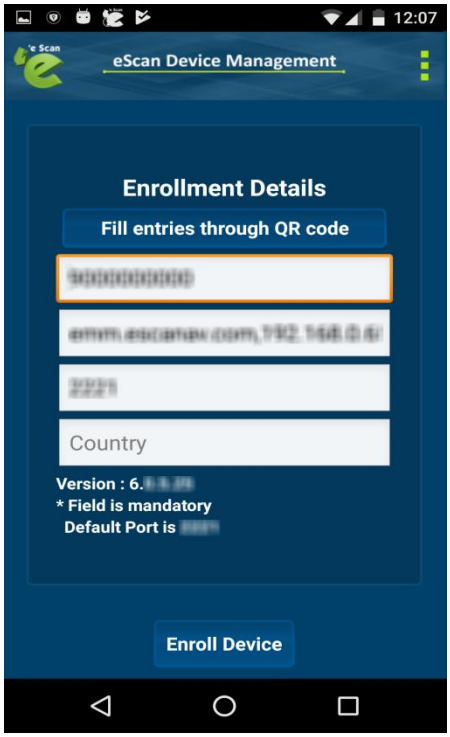
5. Tap **Open Agreement** and read the agreement completely.
6. After reading the agreement, tap **Accept**.



Enrollment Details form appears.

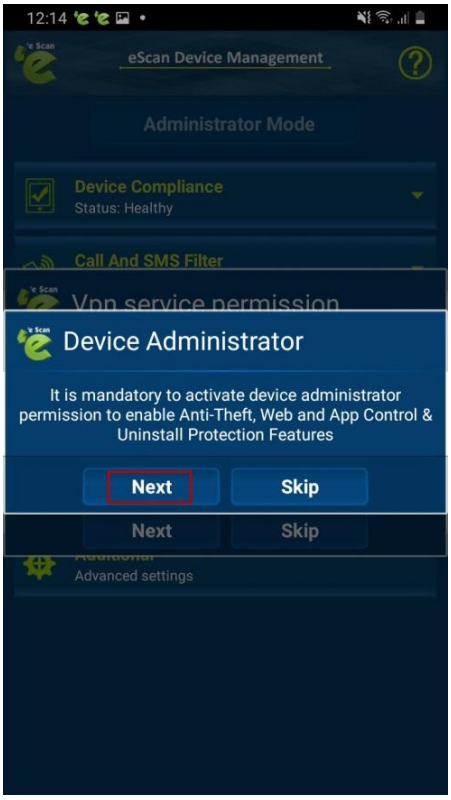


7. Enter the enrollment details mentioned in the email. To fetch the details automatically by scanning QR code, tap **Fill entries through QR Code**.
8. Doing so allows application to access device's camera. Match up the on-screen square with the QR code and hold device steady till the application scans it. After the device is scanned, the enrollment process starts automatically.

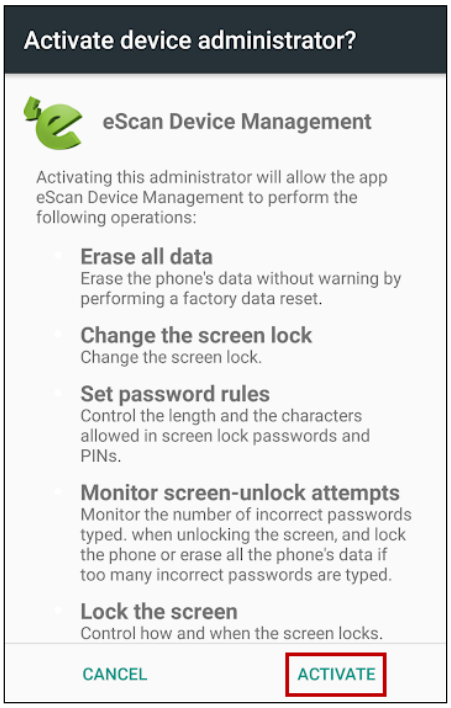


9. Device Enrollment begins. Wait till the device gets enrolled.

Device Administrator prompt appears.

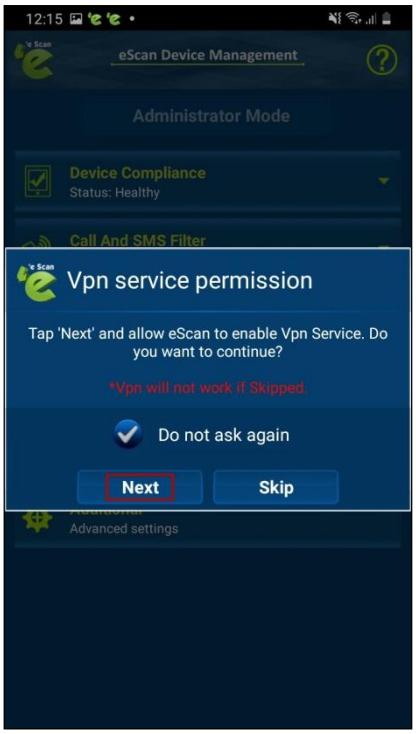


10. It is recommended that you tap **Next**.
    Activate device administrator prompt appears.

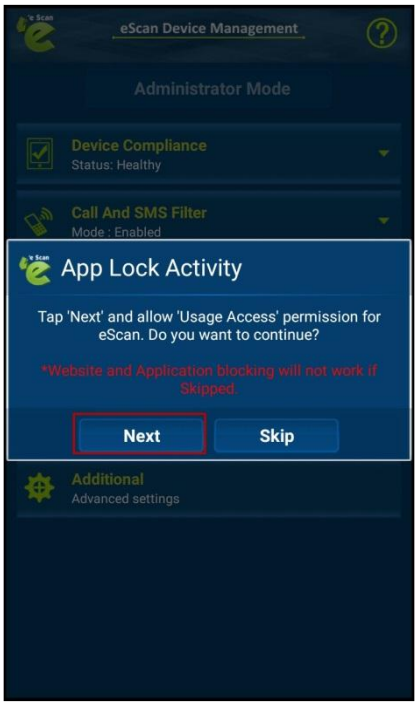


11. Read about the permissions completely and then tap **ACTIVATE**.

The Vpn service permission dialog box appears.

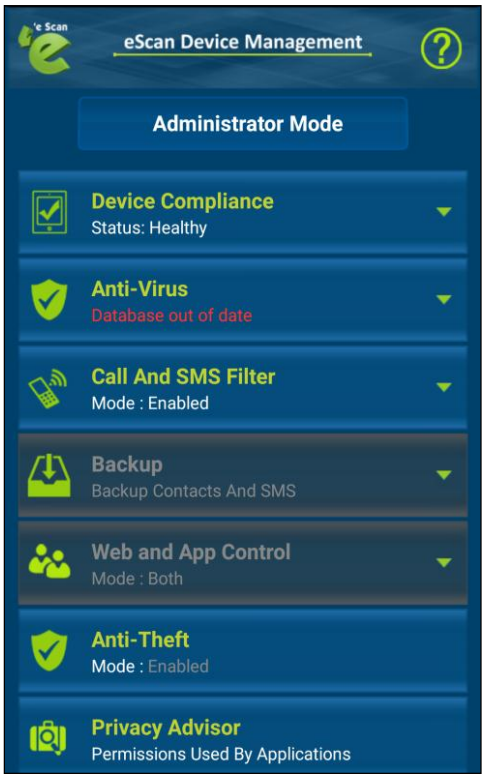


12. It is recommended that you tap **Next** as VPN won't work if you tap **Skip**.
    This permission is required for the proper functioning of the "App Specific Network Blocking" feature.
    App Lock Activity prompt appears.



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.

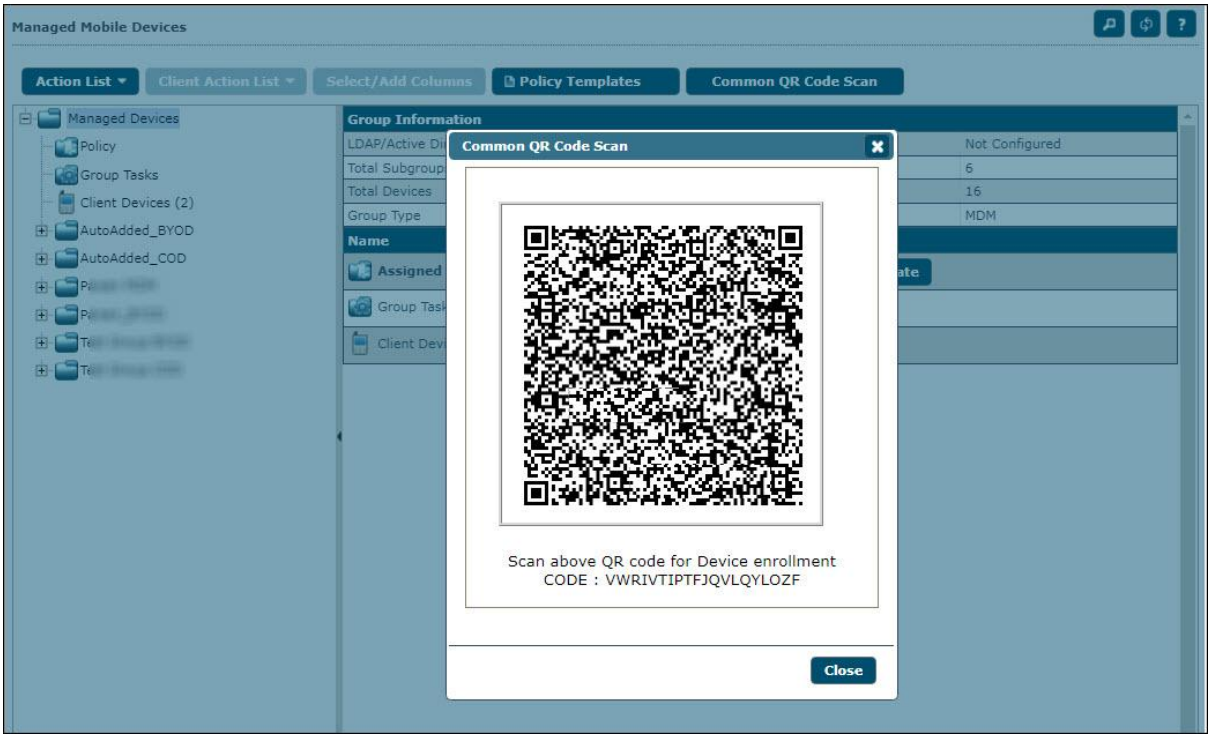
In case the device is provided by the enterprise, you can enroll the device as COD (Company Owned Device), where the security policies for the container will be applicable irrespective of the device location.

NOTE	The Container application can be accessed only after the eScan MDM application is installed and enrolled on the managed device.

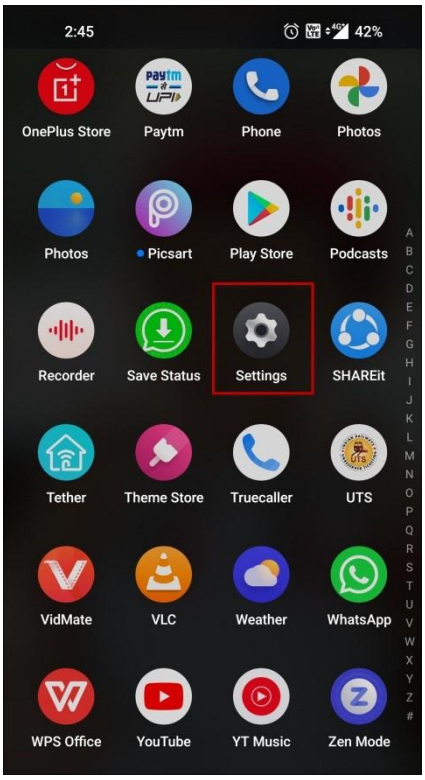
Installation and Enrollment of Android device to BYOD Group

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

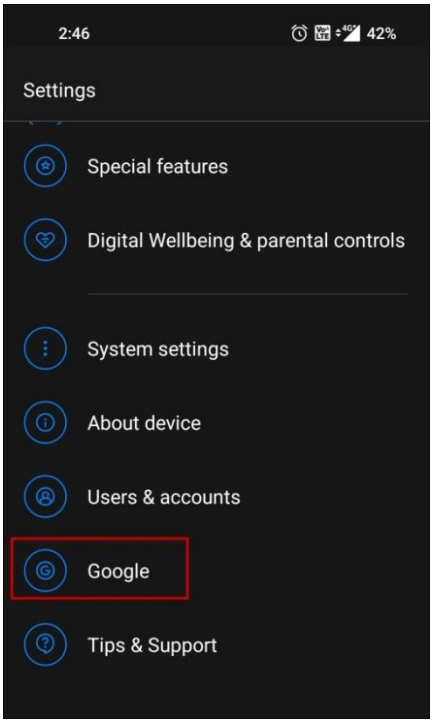
1. Click **Managed Mobile Devices** > **Common QR Code Scan**
   The Common QR code is displayed.



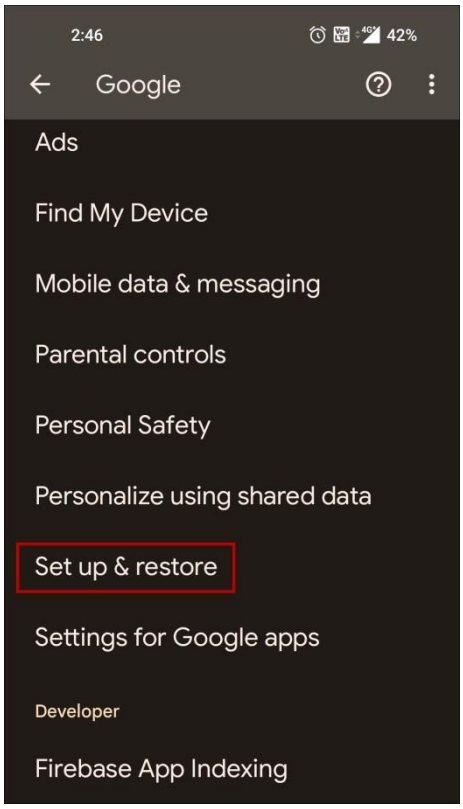
Connect the device to your WiFi network and perform the following steps:



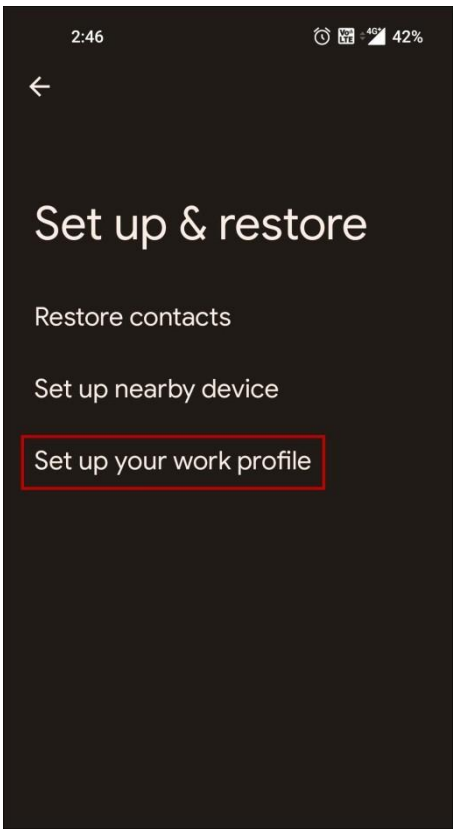
2. Open device settings.



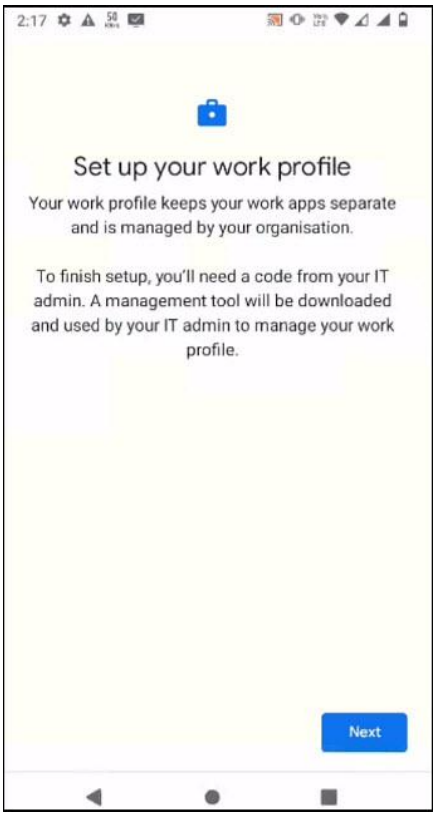
3. Tap on **Google**



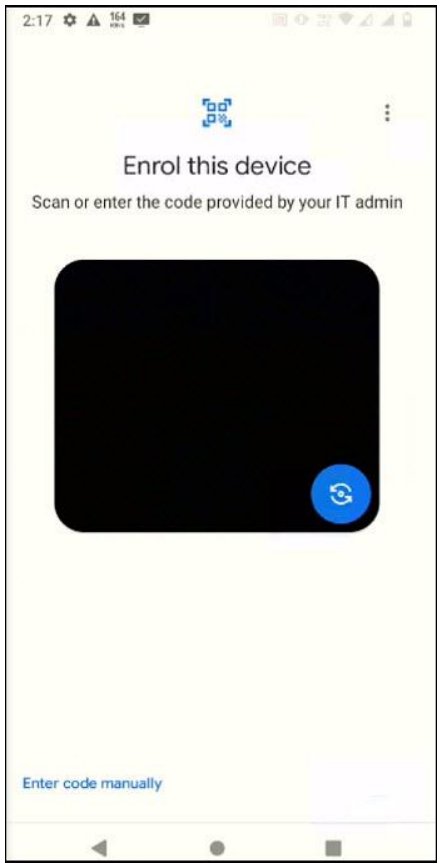
4. Tap on **Set up & restore**



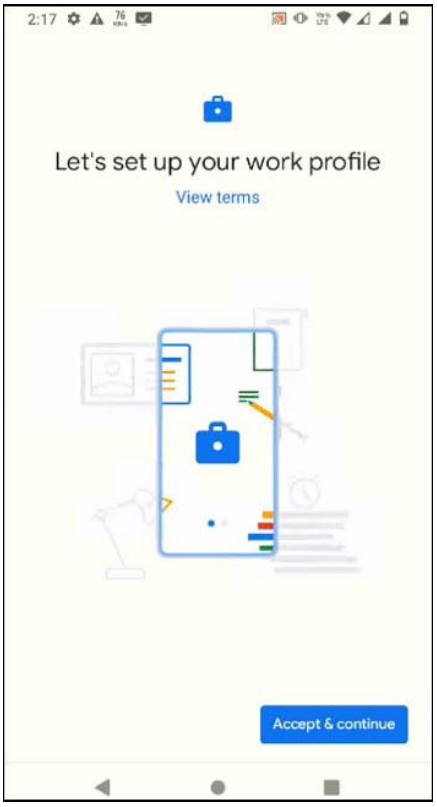
5. Tap on **Set up your work profile**


2:17
Set up your work profile
Your work profile keeps your work apps separate and is managed by your organisation.
To finish setup, you'll need a code from your IT admin. A management tool will be downloaded and used by your IT admin to manage your work profile.
Next

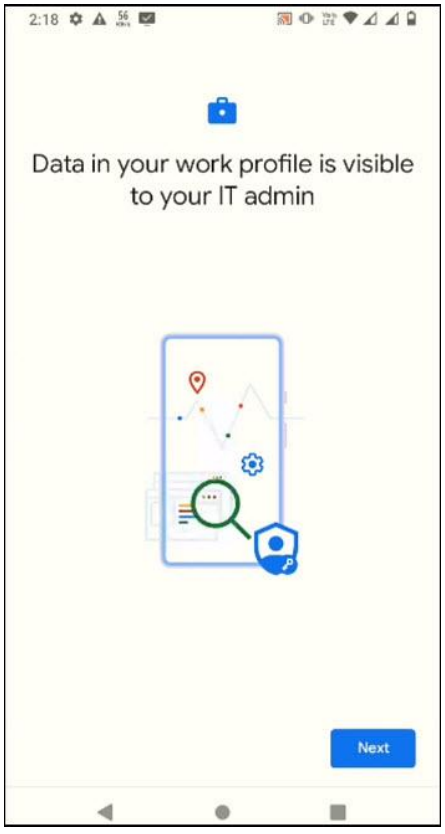
6. Tap on **Next**


2:17
Enrol this device
Scan or enter the code provided by your IT admin
Enter code manually

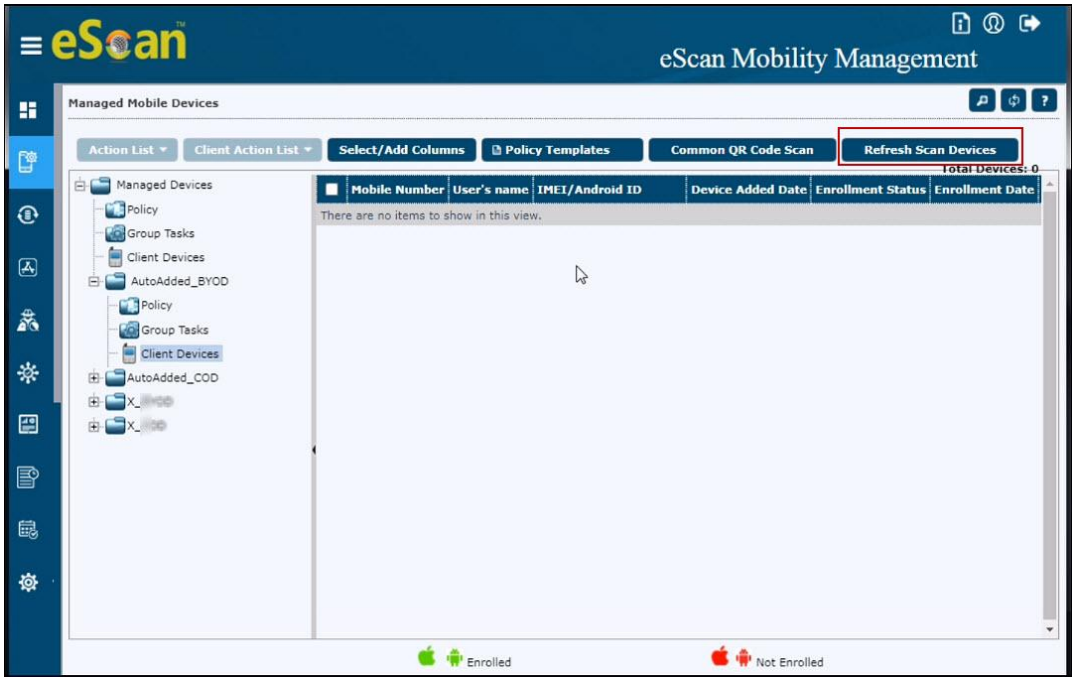
7. Scan the **Common QR Code** displayed on the web console.



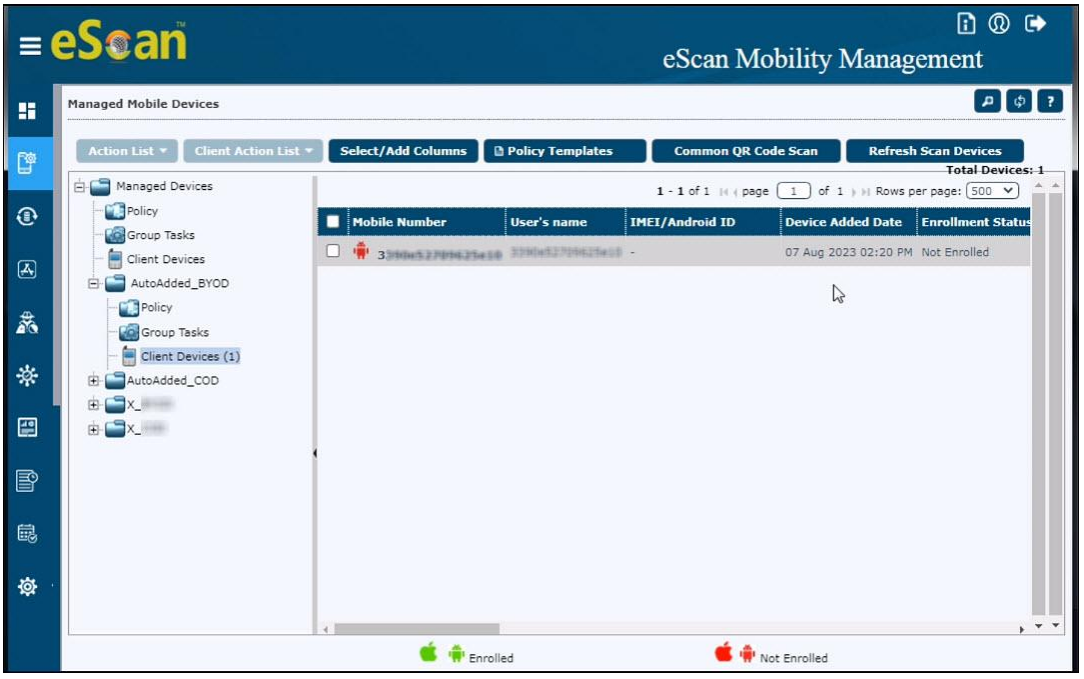
8. Tap on **Accept & continue**



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.

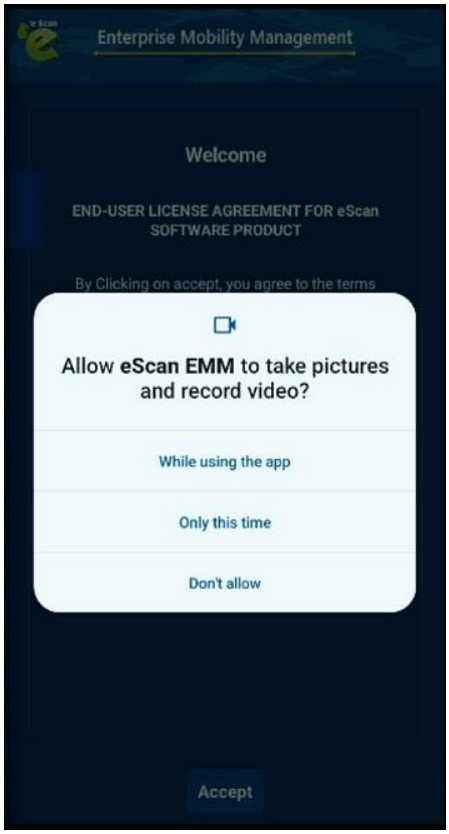


10. On a console, click on **Refresh Scan Devices** in the AutoAdded_BYOD group.
    As shown in the below image, the added device will appear with logo. This indicates that the device is added but not yet enrolled.

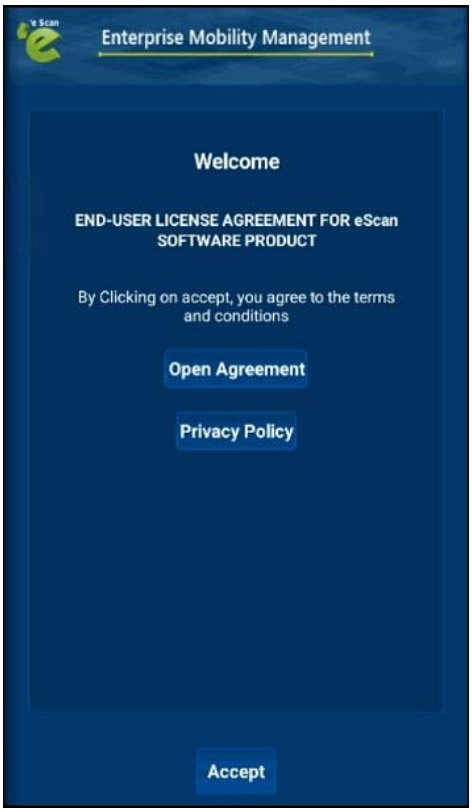


11. On a device, Go to Work profile and open **Play Store**

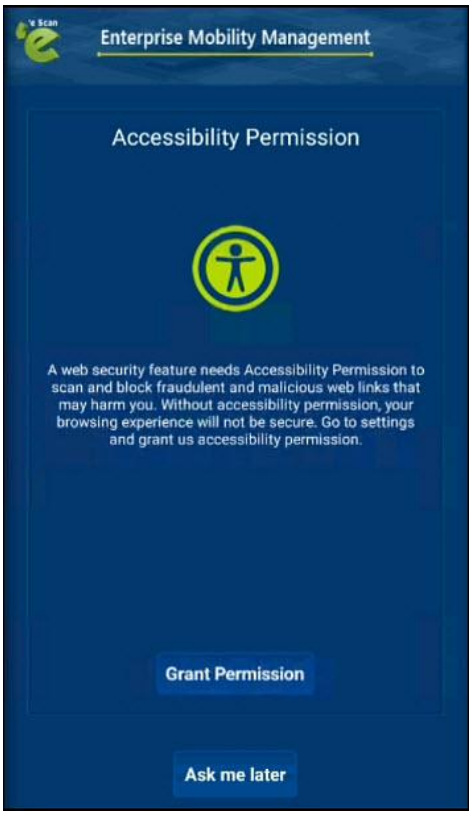
12. Open eScan EMM application



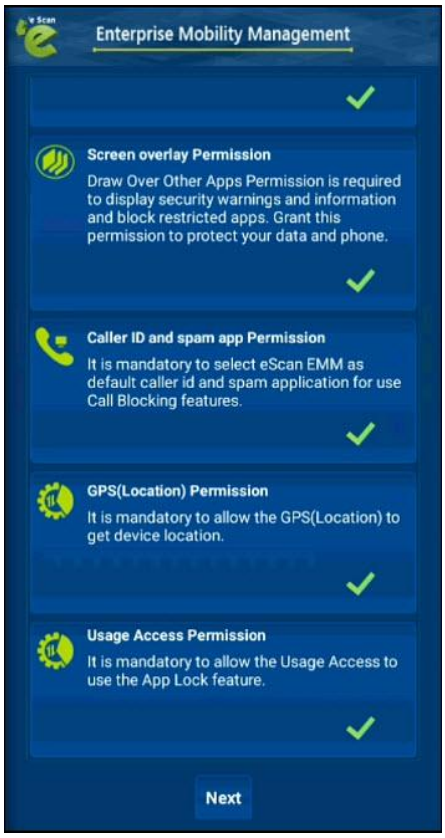
13. Allow Camera permission



14. Tap on **Accept** and allow Location permission

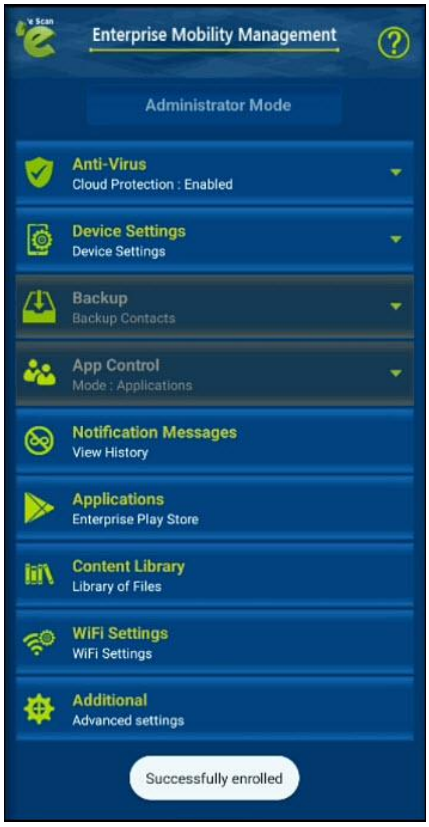


15. Grant necessary permissions



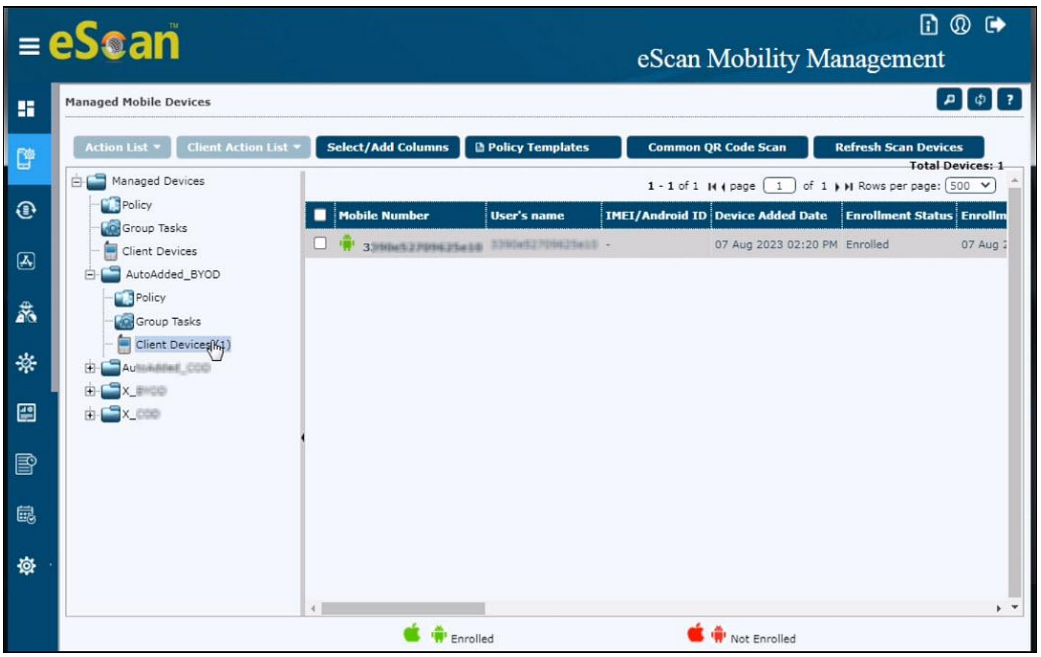
16. Tap on **Next**
    The Enrollment details will be displayed as shown in below image:

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.

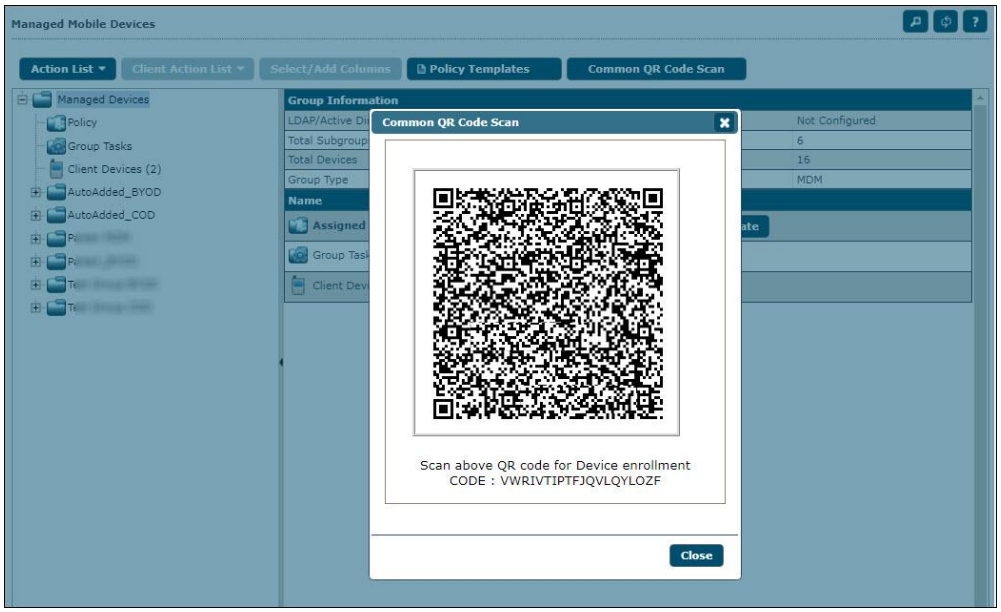
Installation and Enrollment of Android device to COD Group

Prerequisites

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

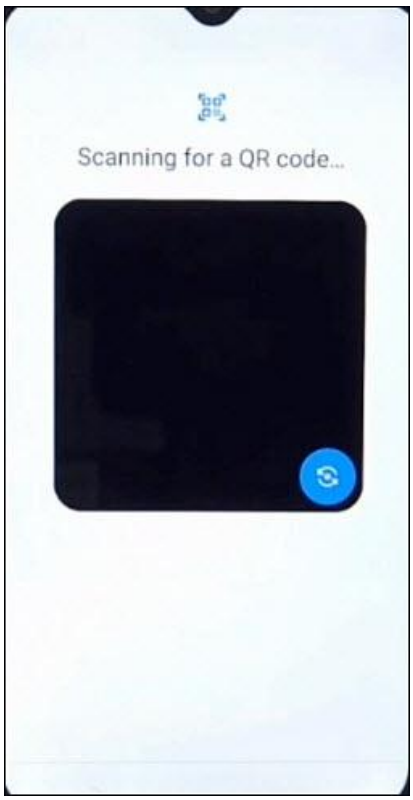
To add and enroll a device in the eScan Mobility Management (EMM), perform the following steps:

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



On a device, perform following steps:

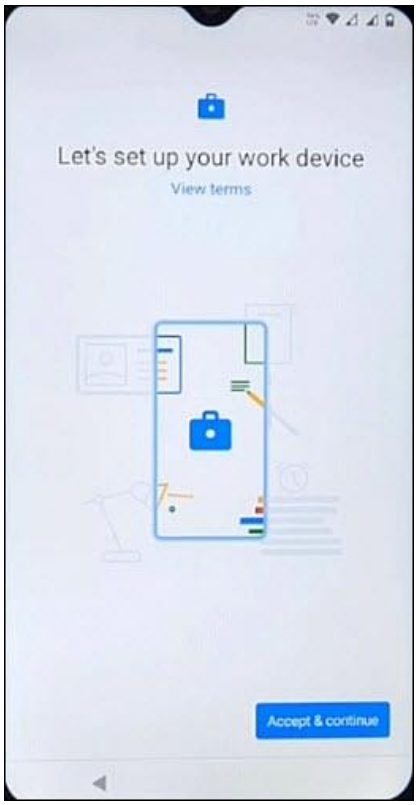
2. Tap **7** times on a screen to open QR Scanner



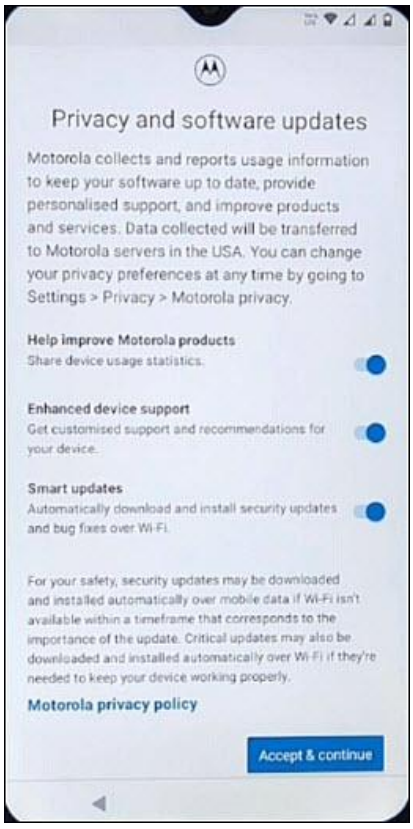
3. Scan the Common QR Code displayed on a console

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

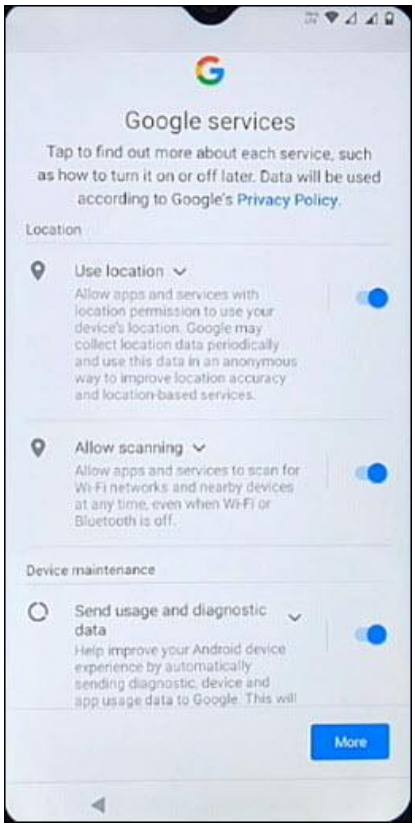
5. Tap on **Next**



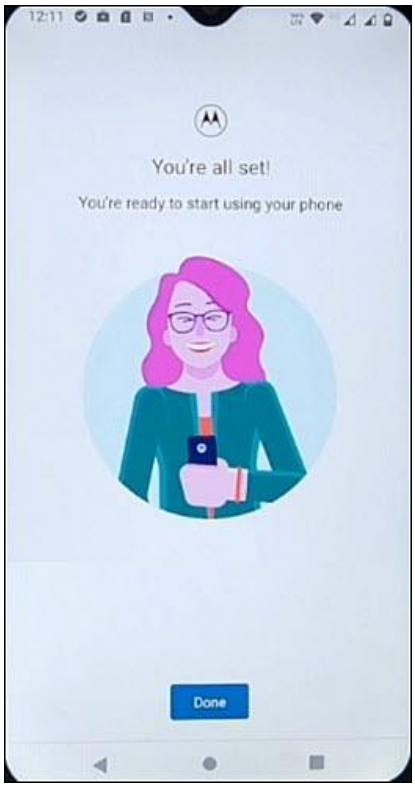
6. Tap on **Accept & continue**



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



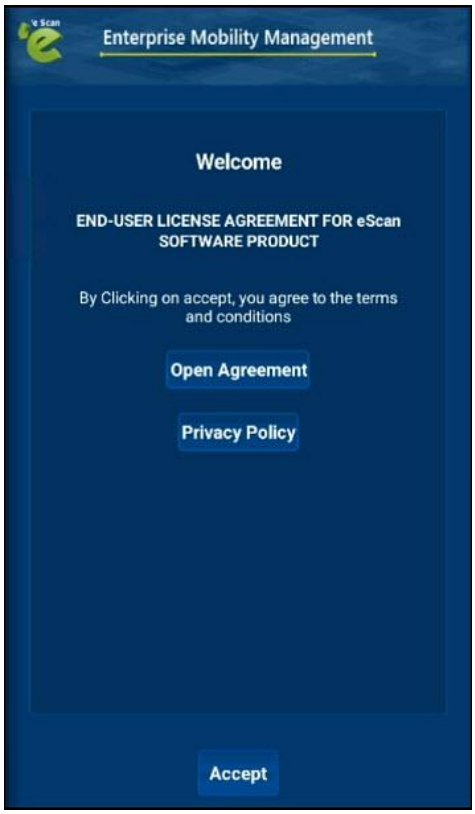
8. Tap on **More** and then tap on **Accept**



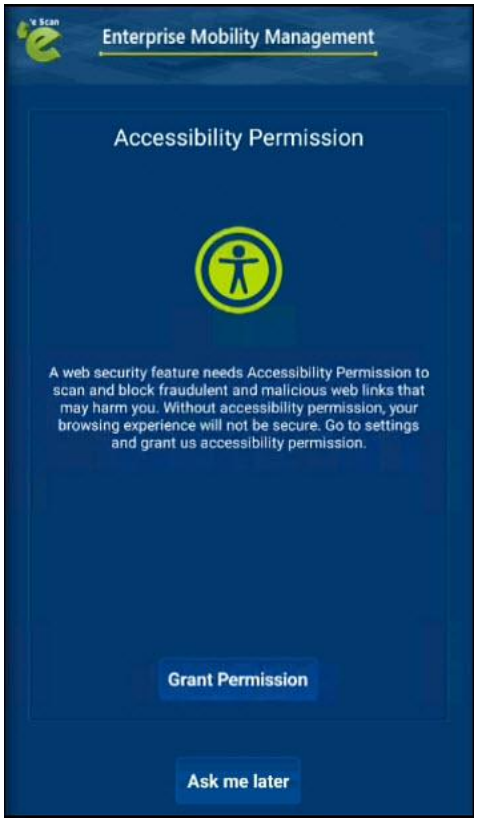
9. Tap on **Done**

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 logo. This indicates that the device is added but not yet enrolled.

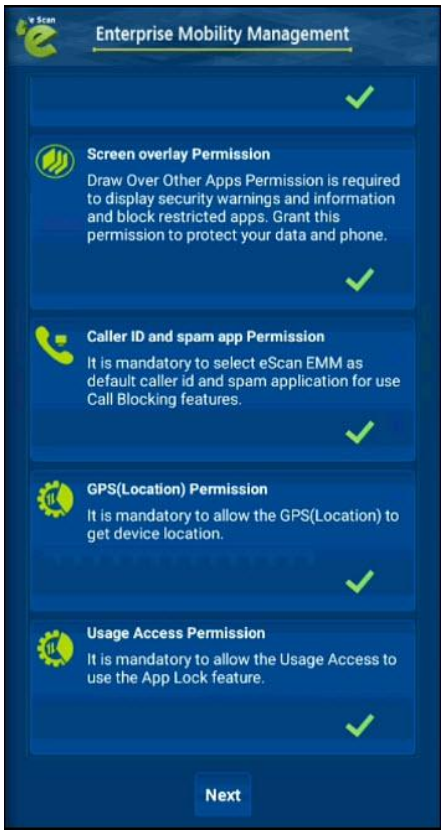
11. On a device, open **eScan EMM** application



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

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

Installation and Enrollment of iOS Device

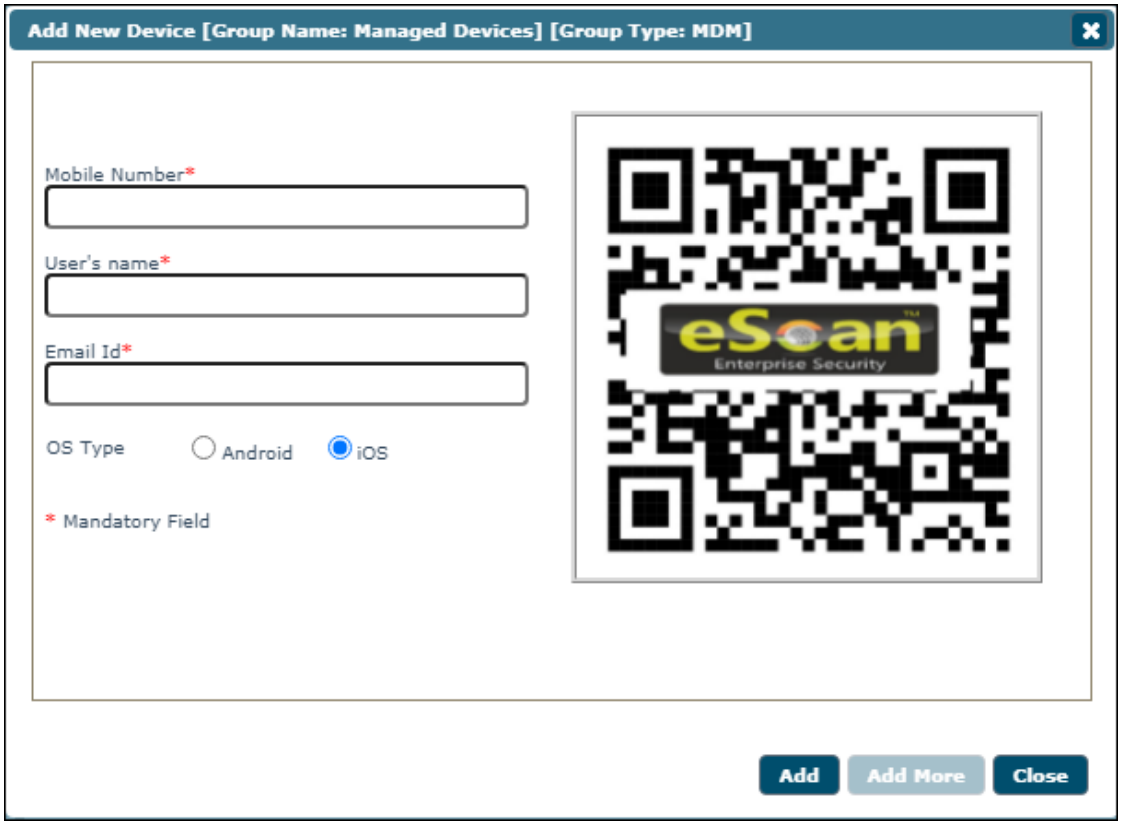
The enrollment procedure for an iOS device consists of two main steps:

1. Adding a device to the console
2. Enrolling the added device

Adding a device to the console

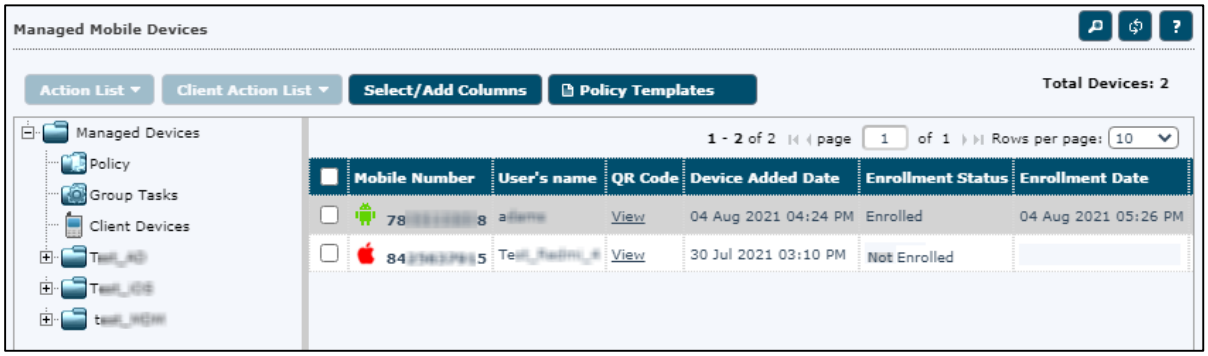
1. Click **Managed Mobile Devices** > **Action List** > **Add New Device**.

Add New Device window appears.



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.

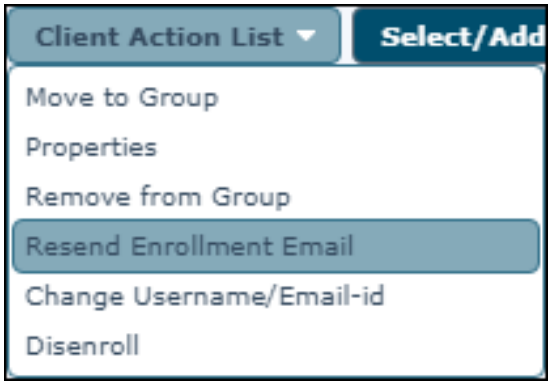


Notice the icon in the **Mobile Number** column; it denotes that the device is not enrolled.

Enrolling the added device

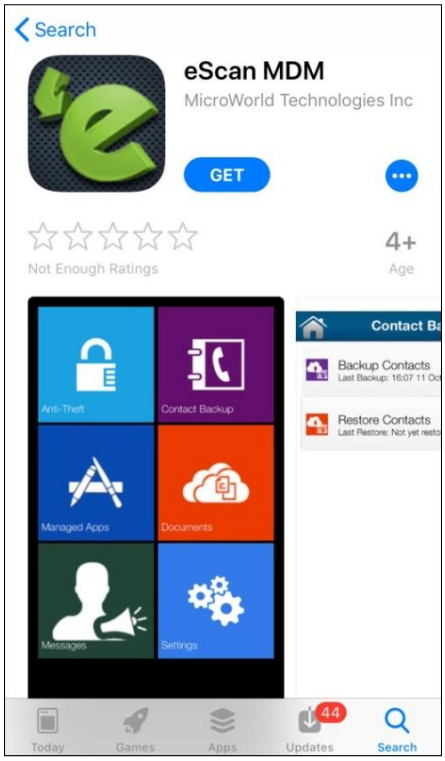
After a device is added to the console, an email containing the enrollment procedure will be sent to the specified email ID. This email will contain steps to download MDM application and details such as Mobile No, Server, and Port. In addition to this, it will also contain the QR code that will fetch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

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



After you have received the enrollment email, perform the following steps:

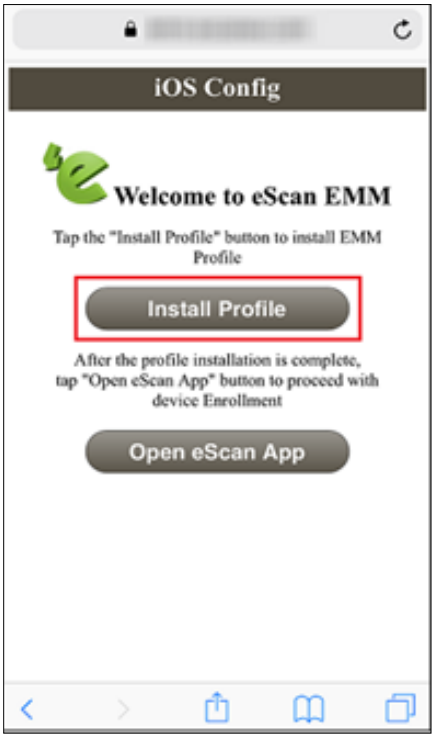
1. Download and install the **eScan MDM** application from the App Store.



2. Read the eScan Agreement completely and then tap **Accept**.

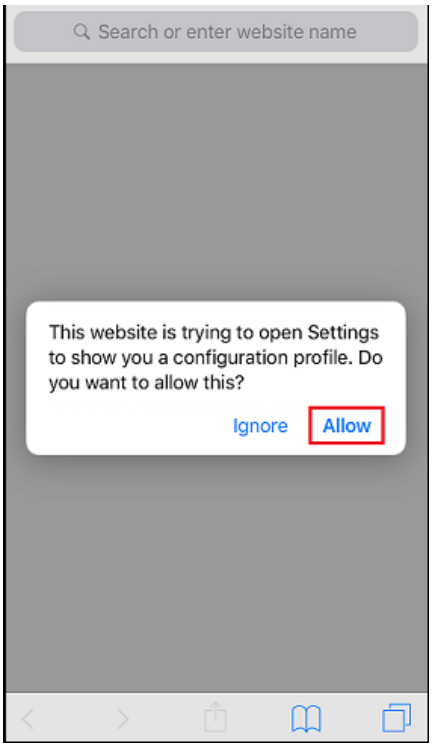
3. Launch the eScan MDM application and enter the details mentioned in the enrollment email, or fill in the details automatically via QR code by tapping **Read QR Code**. Doing so will turn on your device's camera. Match up the on-screen square with the QR code and hold your device steady till the application scans it. After the successful scan, the details will be automatically filled.

4. After the enrollment details are filled, tap **Enroll Device**.
The iOS Config screen appears.

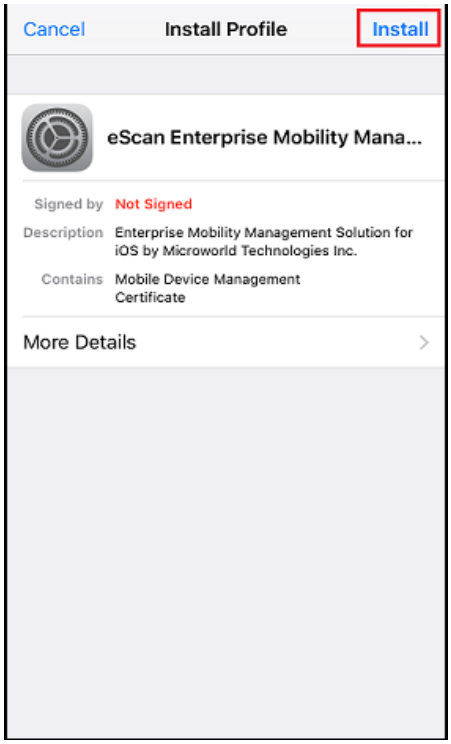


5. Tap **Install Profile**.

The application attempts to access your device's Settings. The following dialog box appears asking confirmation:

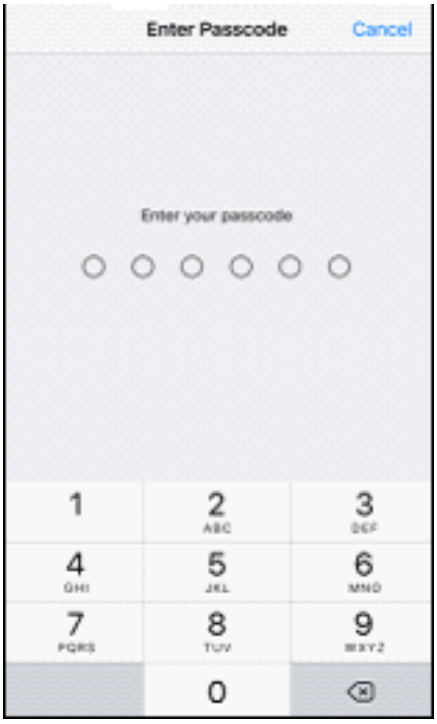


6. Tap **Allow**.
   Install Profile settings appear.

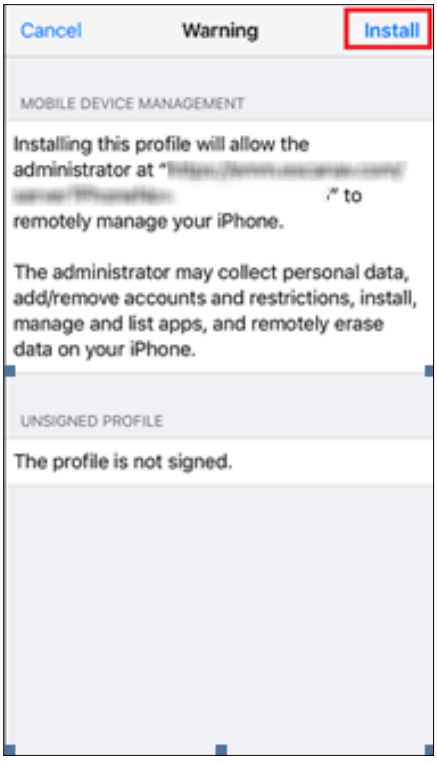


7. Tap **Install**.

Enter Passcode screen appears.

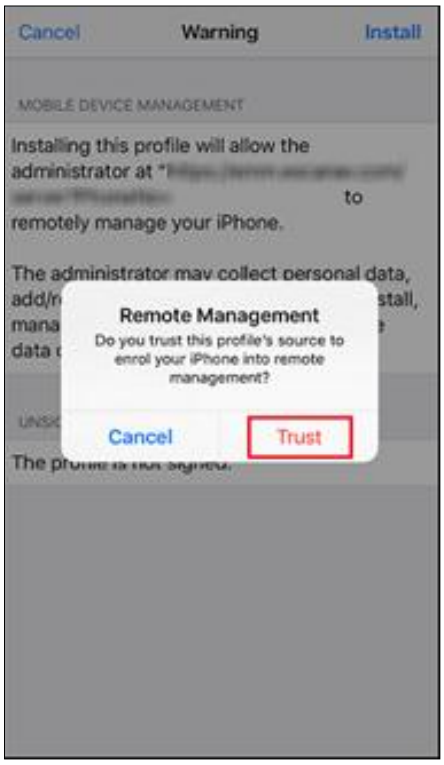


8. Enter the device's passcode to proceed with the installation.
   After entering the passcode, Warning message appears stating that an administrator will be able to remotely manage your device.

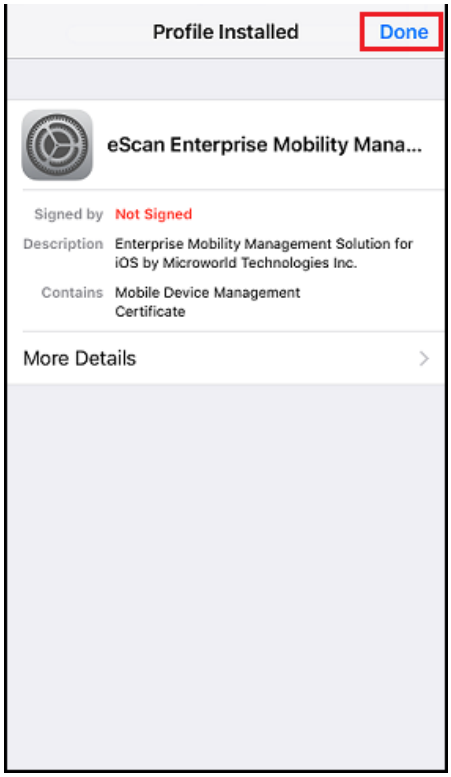


9. To proceed with the installation, tap **Install**.

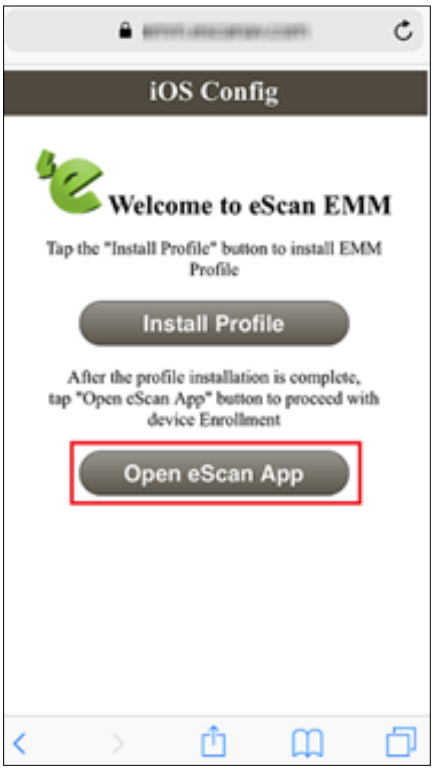
A pop-up message appears asking confirmation for remote management of your device.



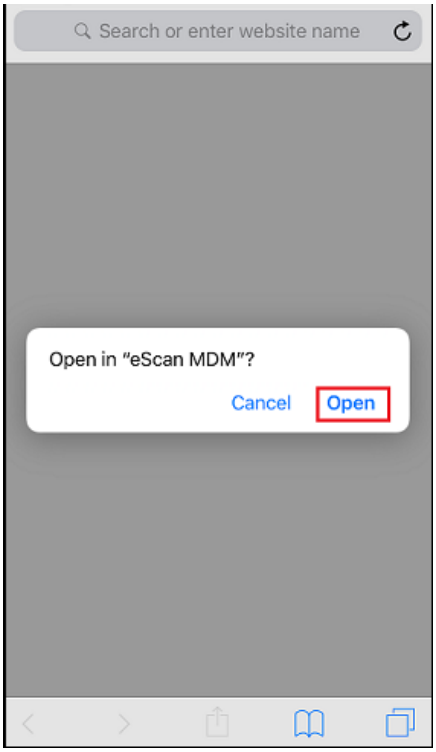
10. Tap **Trust**.
    The MDM profile will be installed on your device.
11. To exit the installation process, tap **Done**.



The iOS Config screen appears.



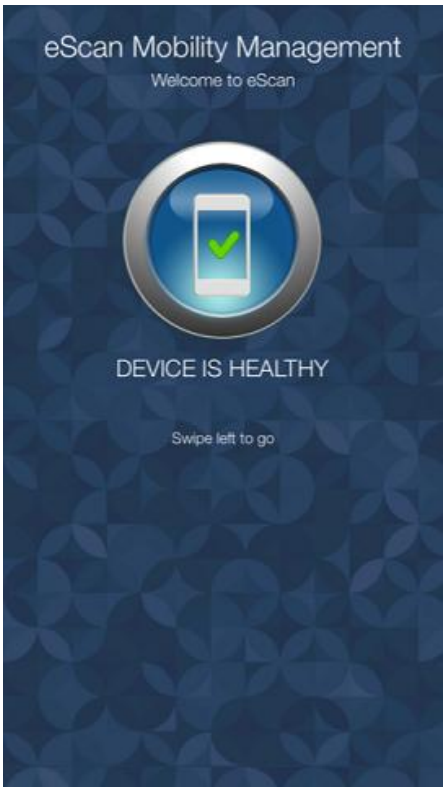
12. Tap **Open eScan App**.
    A pop-up appears.



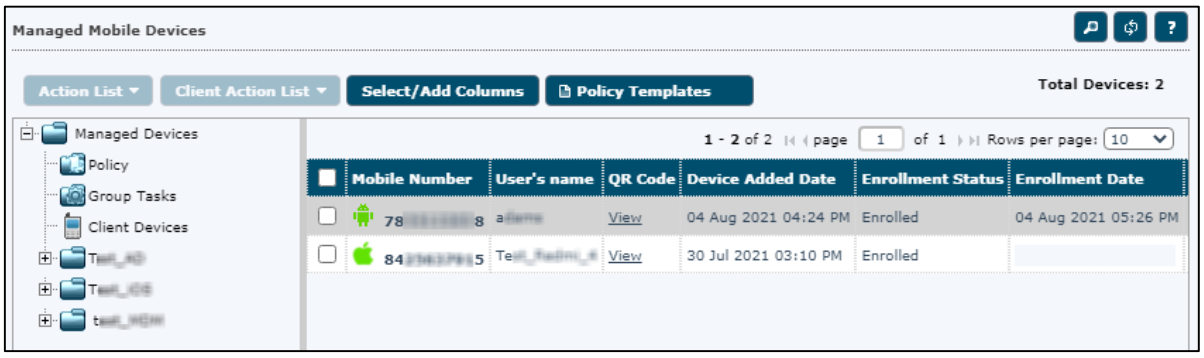
13. Tap **Open**.

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 and the enrollment status change to **Enrolled** from **Not Enrolled**.



Policy comparison of MDM, COD and BYOD Group Types

Policies for MDM	Policies for COD	Policies for BYOD
Anti-Virus Policy	Anti-Virus Policy	Anti-Virus Policy
Call & SMS Filter Policy	Application Control	Application Control
Web and Application Control	Additional Settings Policy	Anti-Theft Policy
App specific network blocking	Password Policy	Additional Settings Policy
Anti-Theft Policy	Required Applications Policy	Password Policy
Additional Settings Policy	Scheduled Backup (Contacts & SMS)	Required Applications Policy
Password Policy	Content Library Policy	Content Library Policy
Device Oriented Policy	Restriction Policy	Restriction Policy
Required Applications Policy	Wi-Fi Configuration	Location Fence
WiFi Settings Policy	System Updates	Wi-Fi Configuration
Scheduled Backup (Contacts & SMS)		
Content Library Policy		
Kiosk Mode Policy		
Location Fence		

NOTE	Policies sporting icon are applicable for container version of the application for BYOD and COD groups.

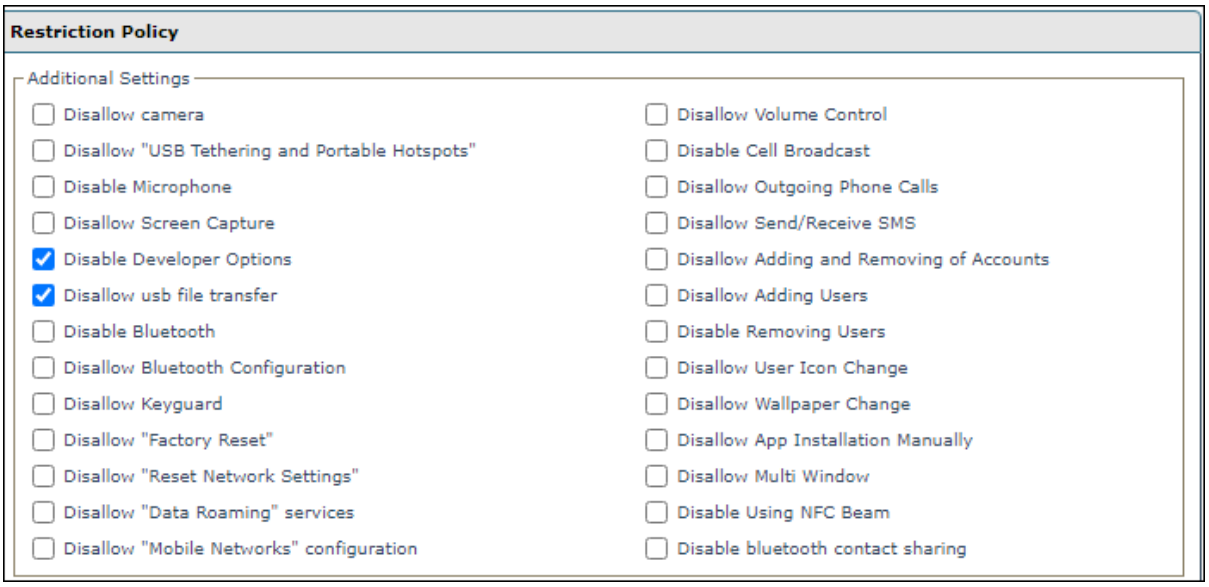
For detailed policy description for following policies, refer **Policies section under Managed Mobile Device**.

- 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.



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):

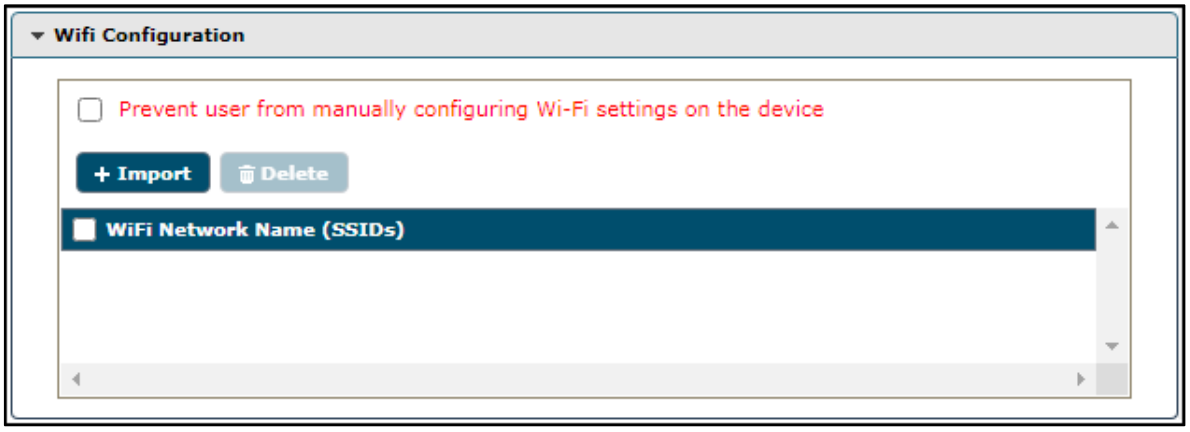
- **Disable WiFi Settings** - Select this checkbox to disable WiFi settings from being configured on a device.
- **Disable GPS Setting** - Select this checkbox to disable GPS settings.
- **Disallow Incoming Calls** - Select this checkbox to disallow incoming calls on a device.
- **Disable Bluetooth Setting**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

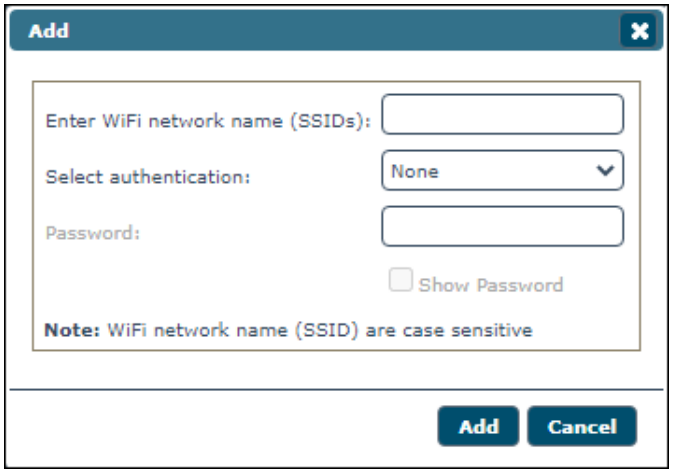


Prevent user from manually configuring Wi-Fi settings on the device: Select this checkbox to disallow users to configure Wi-Fi settings manually.

Importing a WiFi SSID

To import the Wi-Fi SSID:

1. Click **Import**.
   Add window appears.

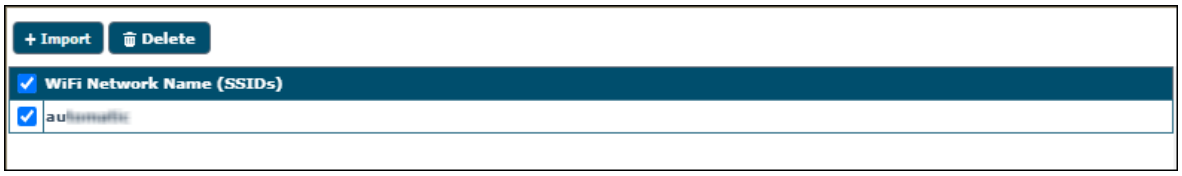


2. Enter the Wi-Fi network name (SSID) in the field.
3. Select authentication type.
4. Enter a password and then click **Add**.
   The Wi-Fi network will be added to the console.
   The devices will be allowed to connect only to the added Wi-Fi network SSID.

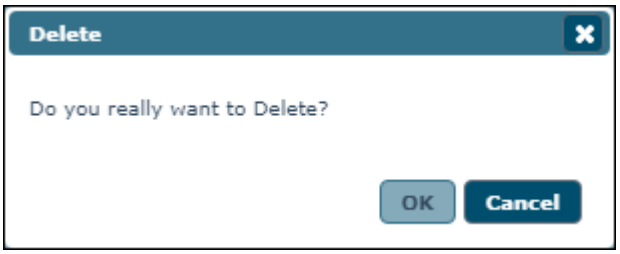
Deleting a Wi-Fi network SSID

To delete the Wi-Fi SSID:

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



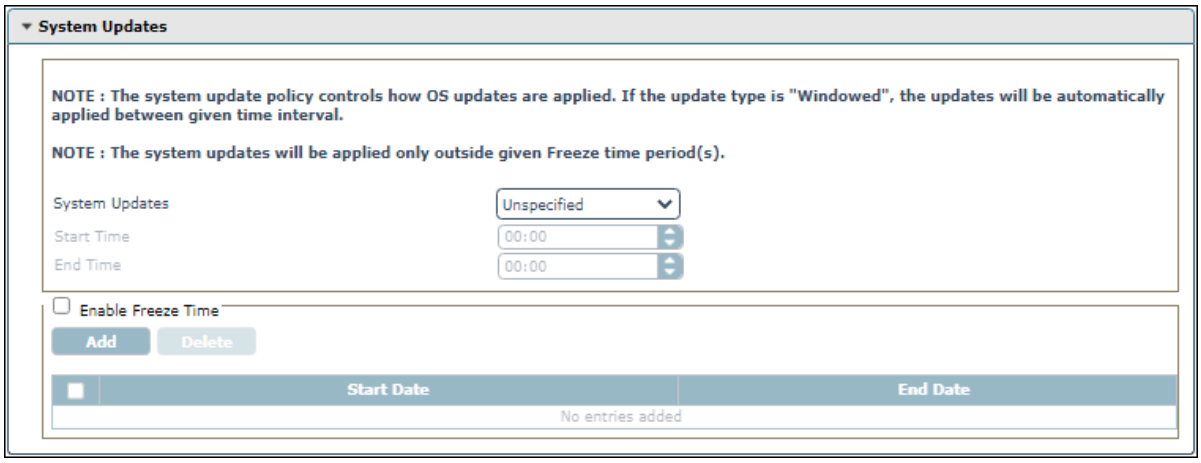
A confirmation prompt appears.



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.



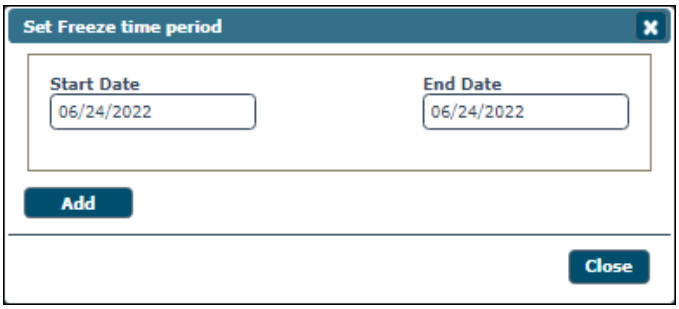
System Updates: Select the system update type from the drop-down list.

- **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.

NOTE	System will be get automatically updated between specified time interval, when you select update type as “Windowed”.

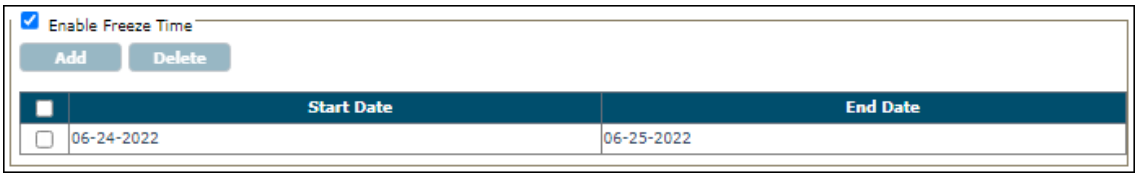
Enable Freeze Time: Select this checkbox to enable the freezing of system update for defined time period.
To add the freeze time:

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.

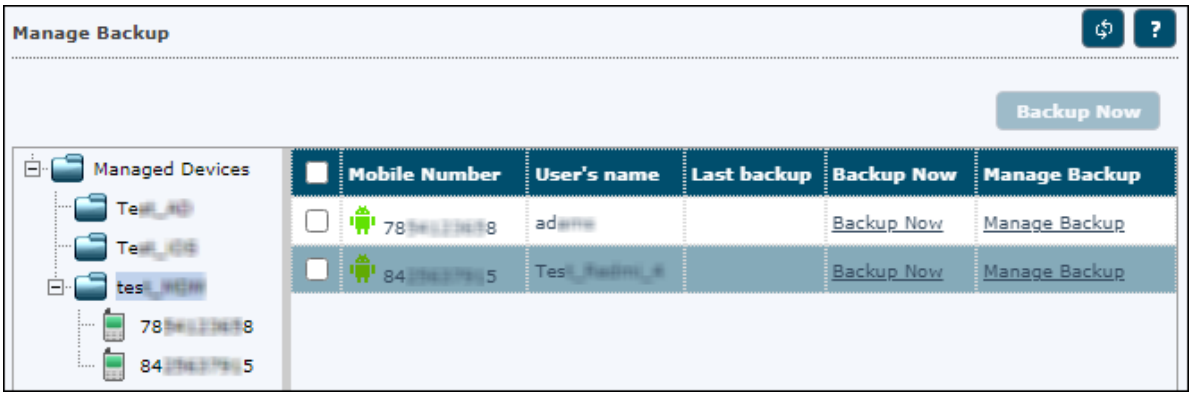


To delete the added freeze time, Select the freeze time you wish to delete, click **Delete** option.
The freeze time will be deleted.

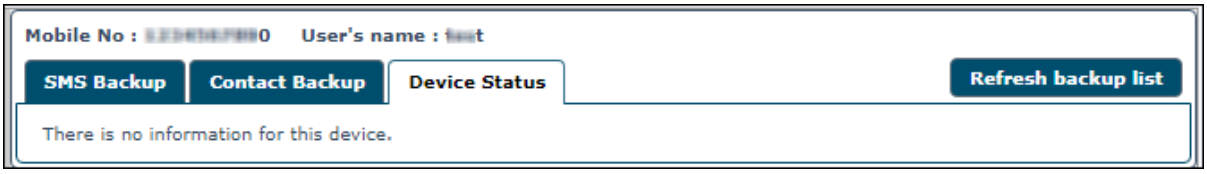
Manage Backup

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**.



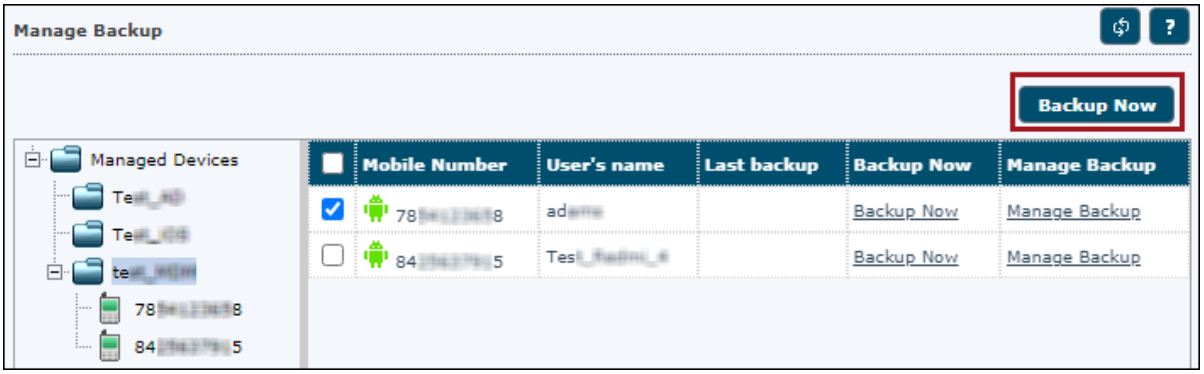
Clicking on a device shows information about its last **SMS Backup**, **Contact Backup,** and **Device Status**.



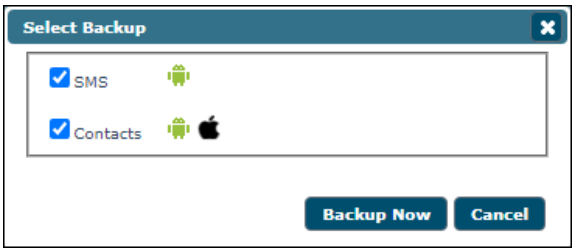
Taking a backup from devices to the server

To take a backup of device:

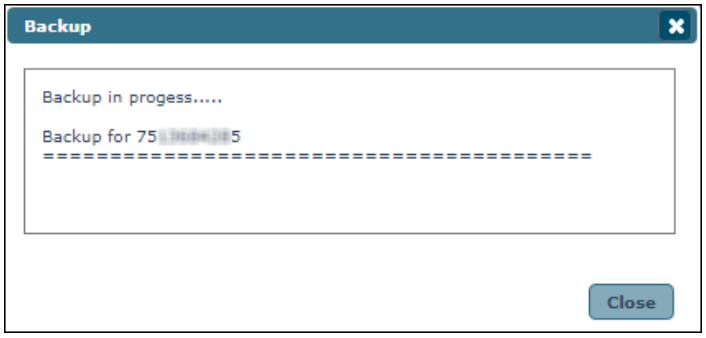
1. Click **Manage Backup** and select the specific group or devices of your wish to take a backup to the MDM server.
2. Selecting a device will enable **Backup Now** option.



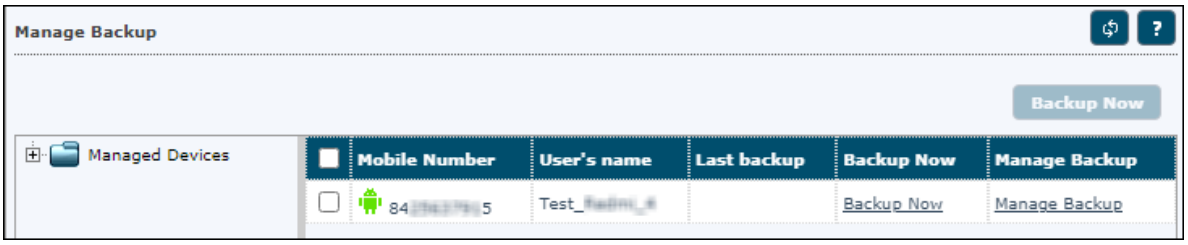
3. Select the desired backup option and then click **Backup Now**.



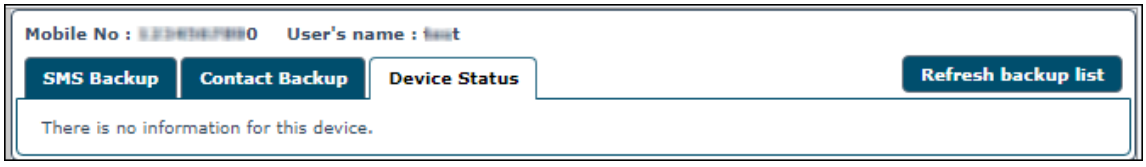
Backup window appears displaying the progress.



The report displays following fields:
Mobile Number, User's name, Last backup, Backup Now, Manage Backup.



Manage Backup: Clicking Manage Backup link displays following screen.

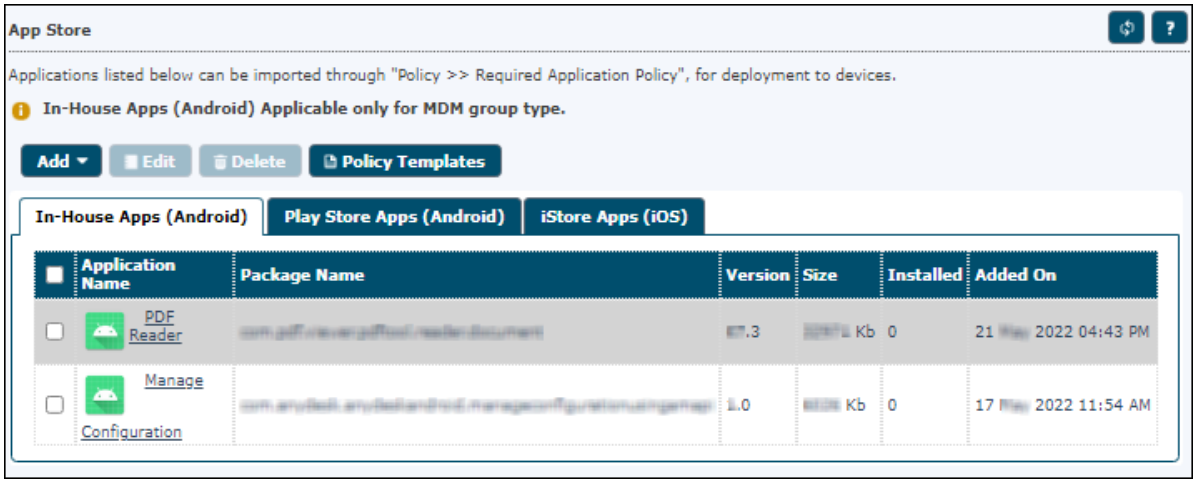


It displays the **SMS Backup**, **Contact Backup**, **Device Status** and **Refresh backup list**.

- **SMS Backup**: It displays the SMS backup status for the selected device.
- **Contact Backup**: It displays the contact backup status for the selected device.
- **Device Status**: It displays the following fields:
  Date-Time and Description
  - **Date-Time:** displays the date and time when the Contacts and SMS backup 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

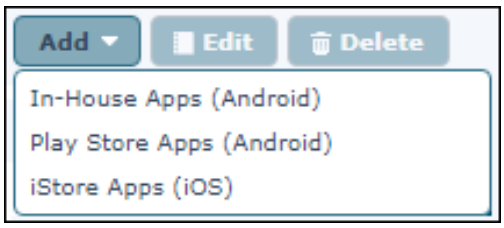
The App Store module lets you push applications on a device by policy deployment. The user will receive a notification to install an application. This module helps you push application(s) on multiple devices at the same time.



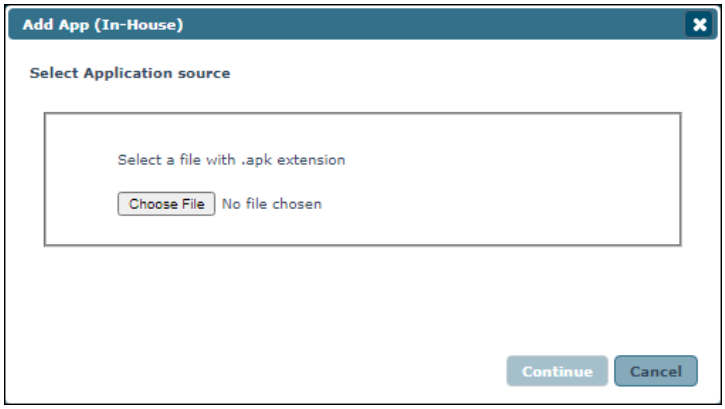
Adding an Android application with In-House Apps (Android) option

To add an application, follow the below steps:

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

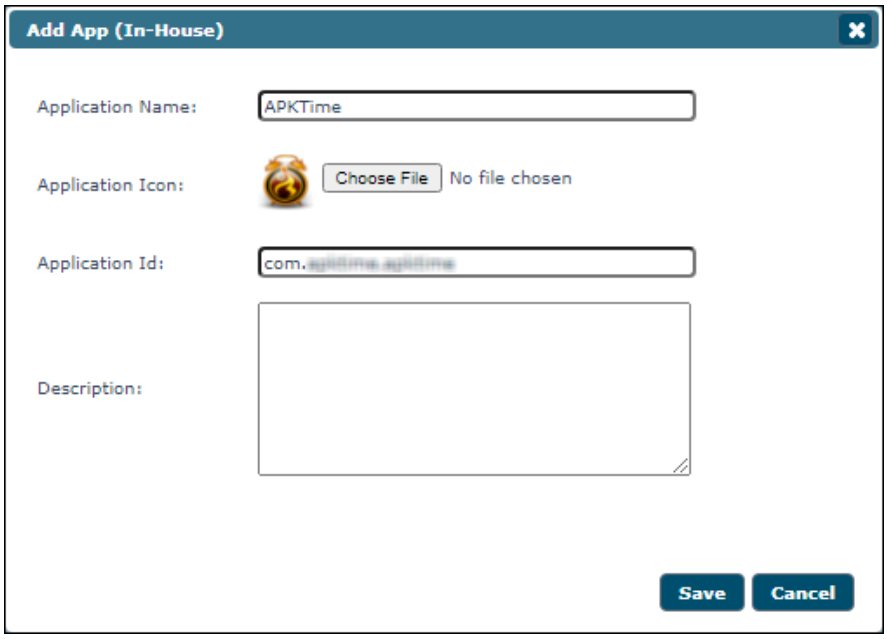


Add App (In-House) window appears.



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

3. After selecting the file, click **Continue**.
   Add Application window appears.



4. Write a brief description about an application and then click **Save**.
   The application will be added to the App Store.

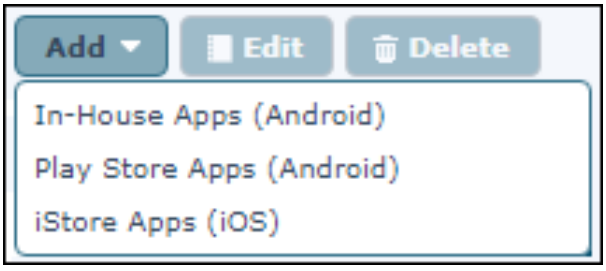
NOTE	In-House Apps (Android) is only applicable for MDM group type.

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.

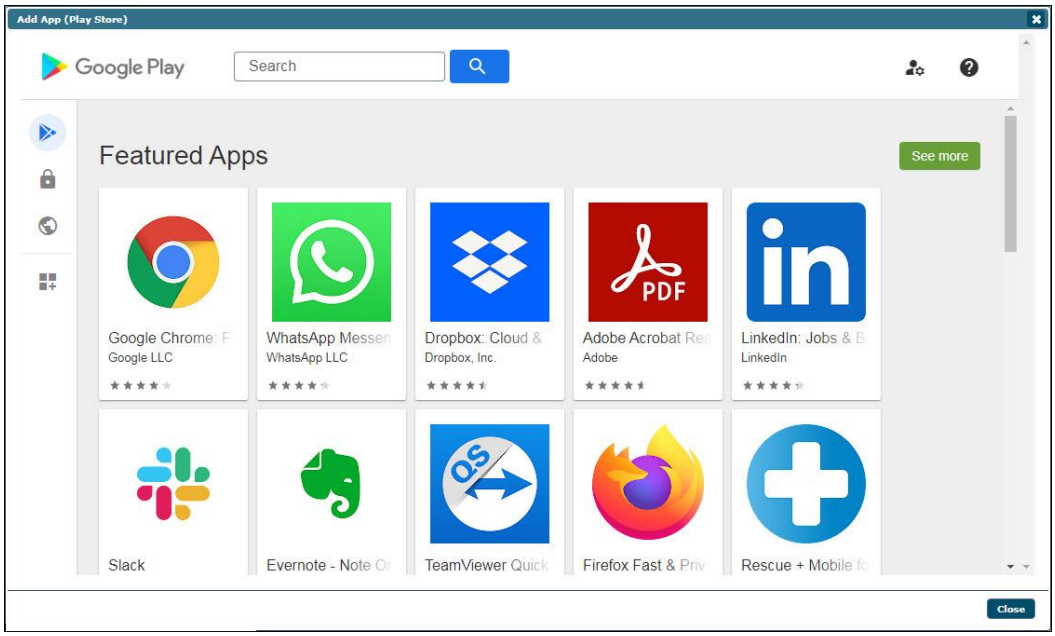
Adding an Android application with Play Store Apps (Android) option

To add an application, follow the below steps:

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



   Add App (Play Store) window appears.

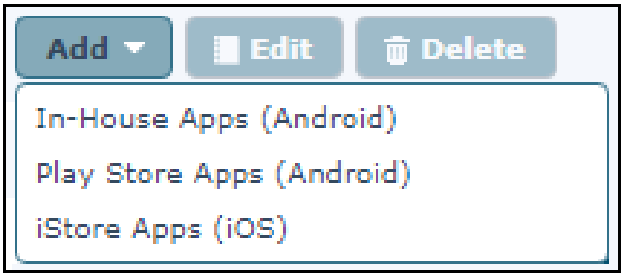


2. Search for required application.
3. Select appropriate application from list and approve it.
4. Click **Close**.
   The application will be added to the App Store.

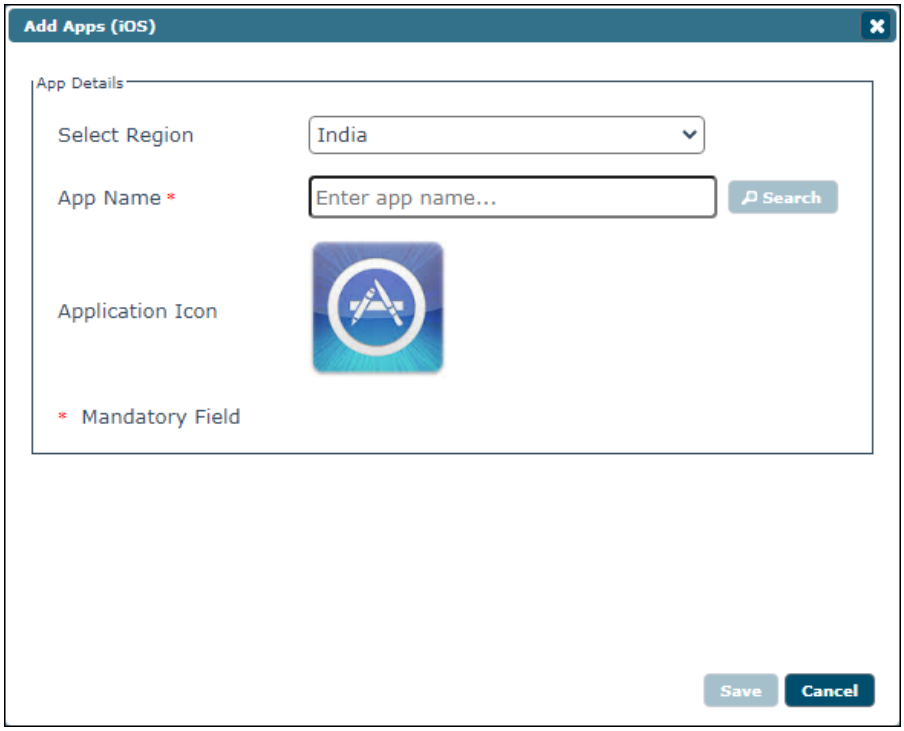
Adding an iOS application from iStore Apps

To add an application, follow the below steps:

1. Click **Add** > **iStore Apps (iOS)**.



Add Apps (iOS) window appears.



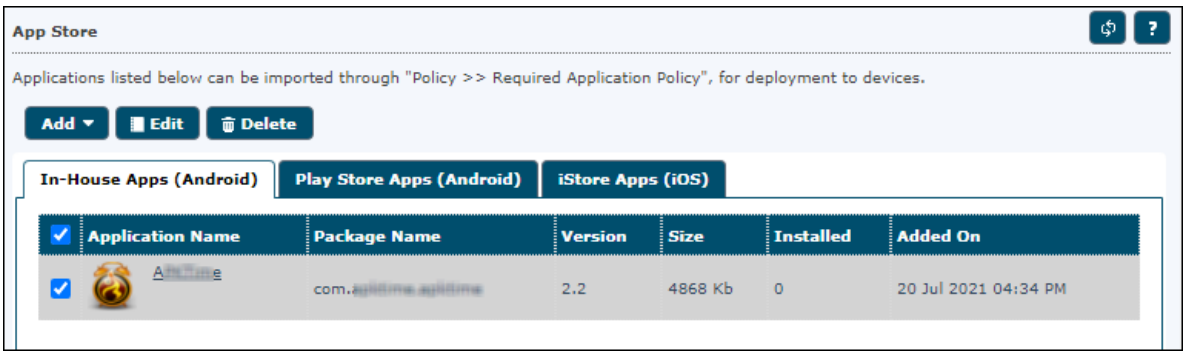
2. Select a region.
3. In the **App Name** field, enter an application name and select an appropriate application from the suggestions.
4. Click **Save**.
   The application will be added to the App Store.

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

Deleting an application from the App Store

To delete an application, follow the below steps:

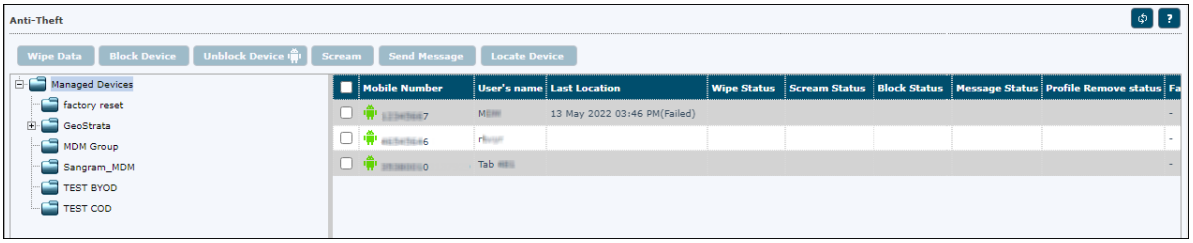
Select an application and then click **Delete**.



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.



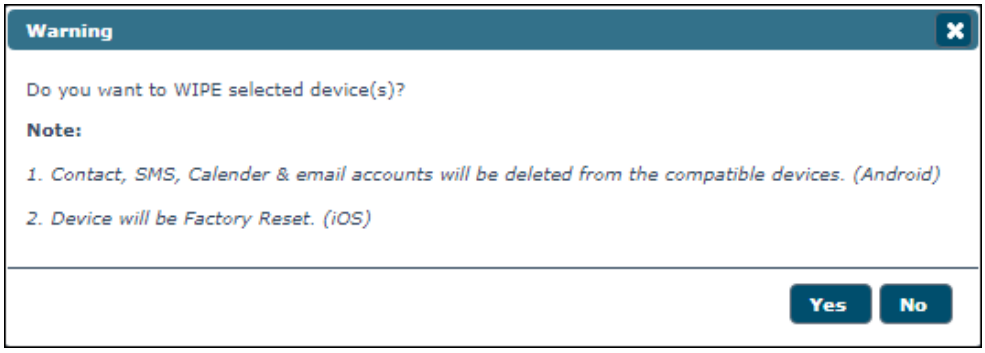
Selecting an added device enables following options:

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

Wipe Data

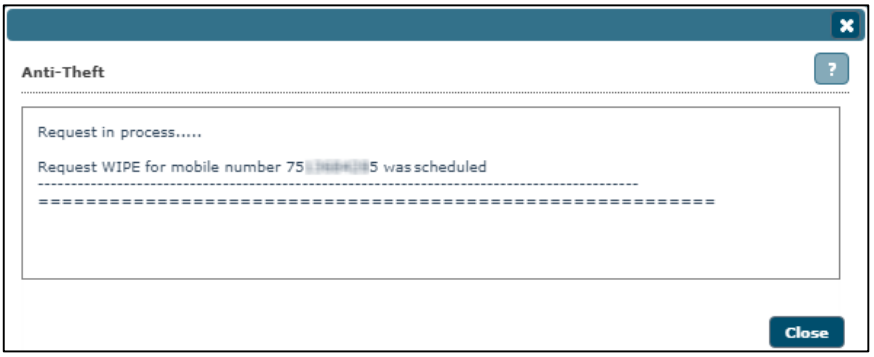
With this option you can delete entire data from the device if it gets lost or stolen.
To wipe the data:

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.

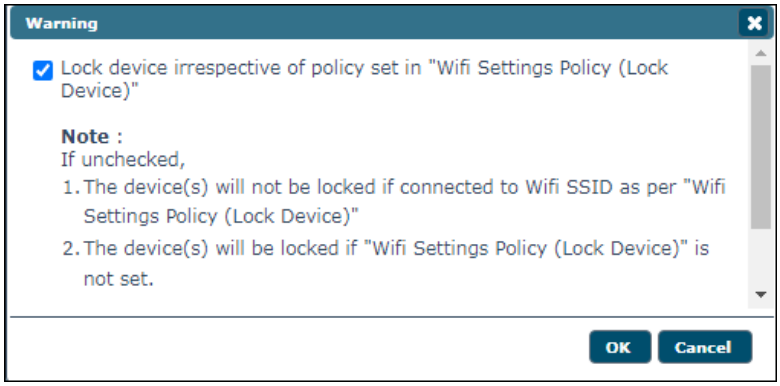


Wipe Data option will delete contacts, SMS, calendar data & email accounts from an Android device whereas, an iOS device it will be factory reset.

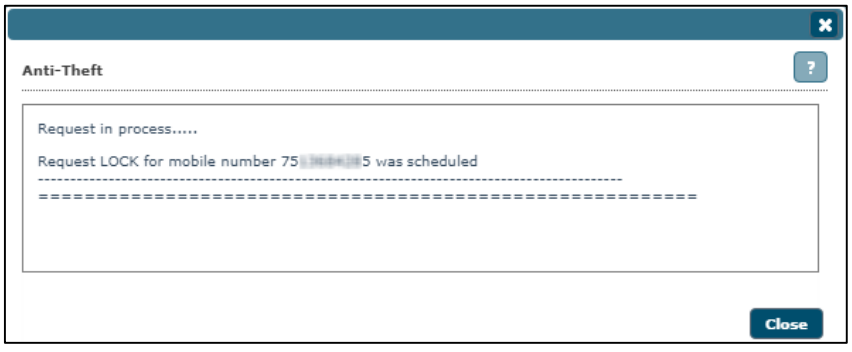
Block Device

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.

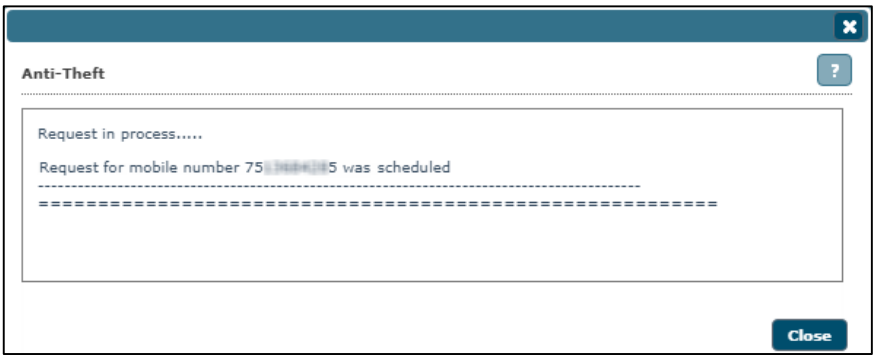


After the device is blocked, the device user will need Admin Access Password to unlock the device.

Unblock Device

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

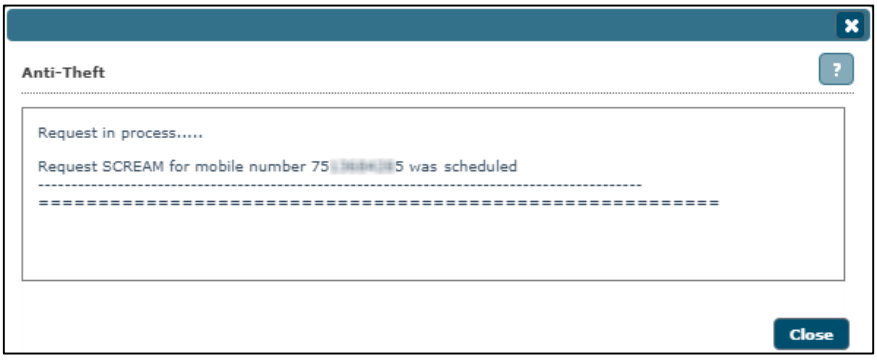
1. Select the device from the list of managed devices and then click **Unblock Device**.
   Following window appears showing request in process:



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:

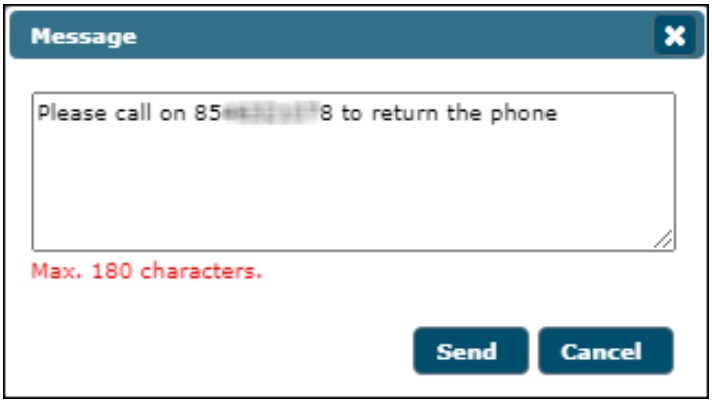


Send Message

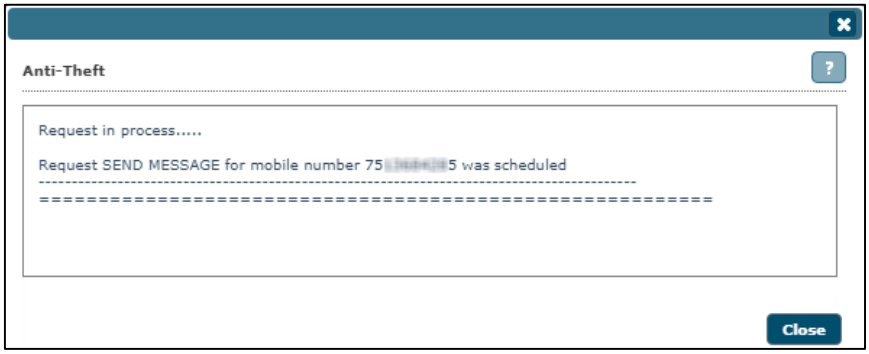
The Send Message lets you send a message to the device. This option can be used for both iOS and Android based devices. To send a message (notification message):

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

Message window appears.



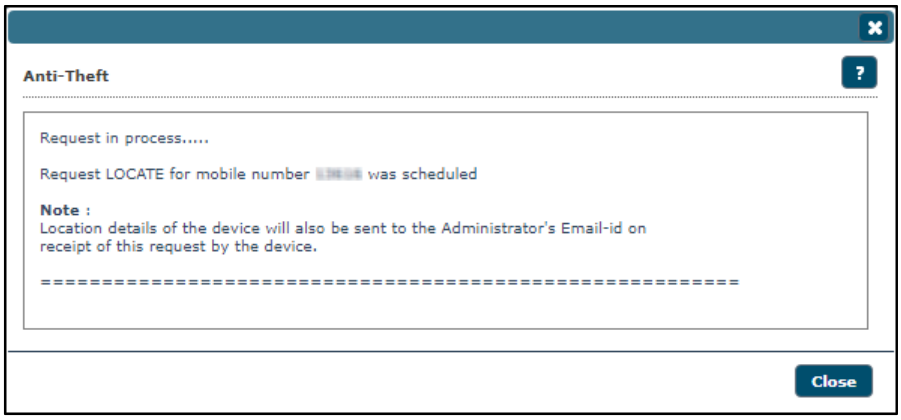
2. Type the message in the field and then click **Send**.



Locate Device

The Locate Device option lets you locate a device by using the wireless network or a device's GPS. eScan server displays the device location on Google Maps. This option can be used for both iOS and Android based devices. To locate a device:

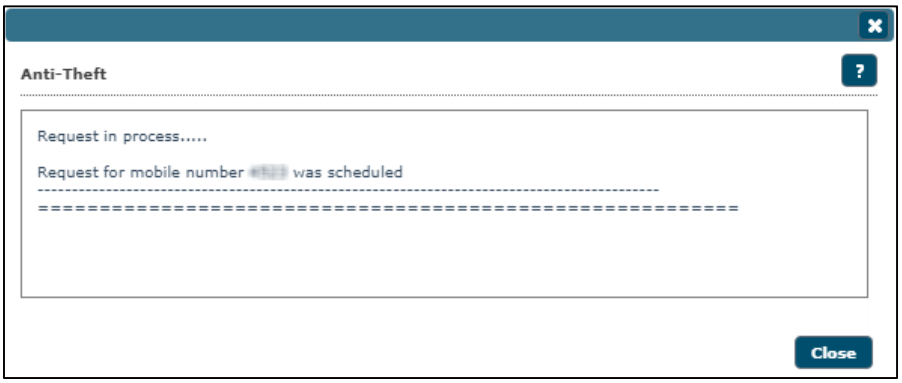
1. Select the specific device and click **Locate Device**.
   Anti-Theft window appears displaying process.



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:

1. Select the specific device and then click **Remove Work Profile**.
   Following window appears after removing the work profile from a device:



Factory Reset

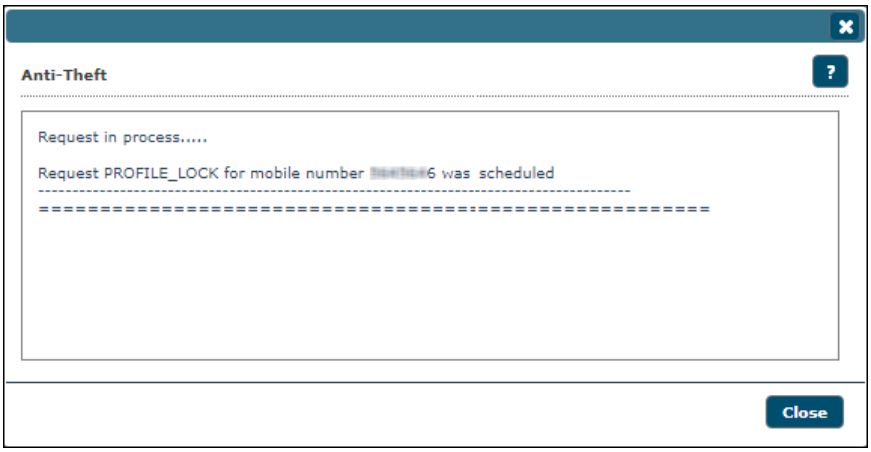
The Factory Reset option allows you Reset the device, in case of lost or stolen. This option can be used for both iOS and Android based devices. To Reset a device:

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:

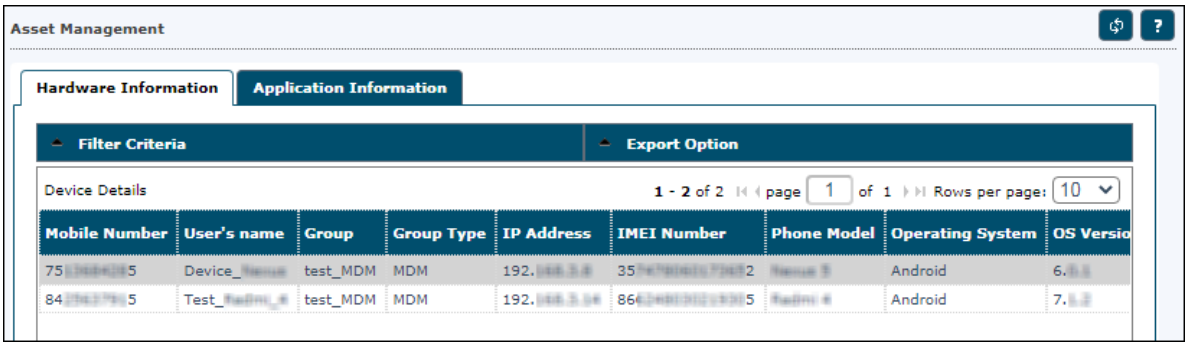
1. Select the specific device and click **Lock Device**.
   The command will be executed on the device.



Asset Management

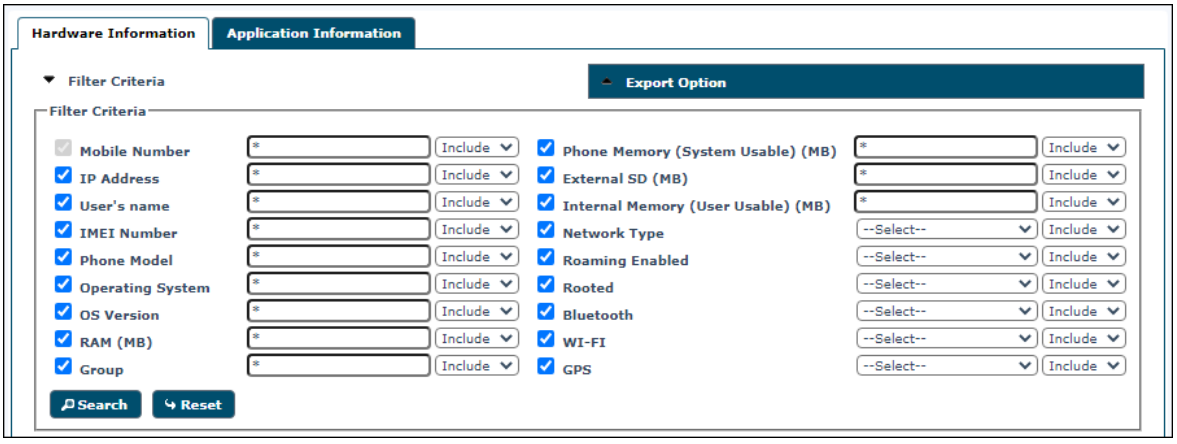
The Asset Management module displays detailed description of all the hardware configuration and applications installed on the managed devices.

Hardware Information



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.

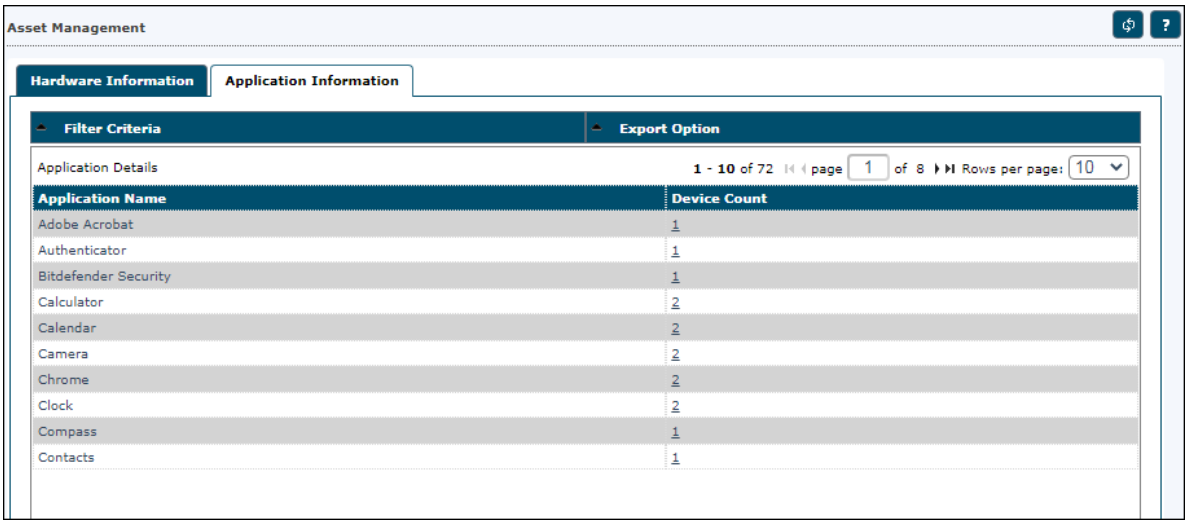


3. Select the checkbox next to each criterion and select **Include/Exclude** to include/exclude that particular criterion in the filtered report.
4. Select the desired criteria drop-down and then click **Search**.
   Details will be filtered in the table instantly.
5. Click **Reset** to set the default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

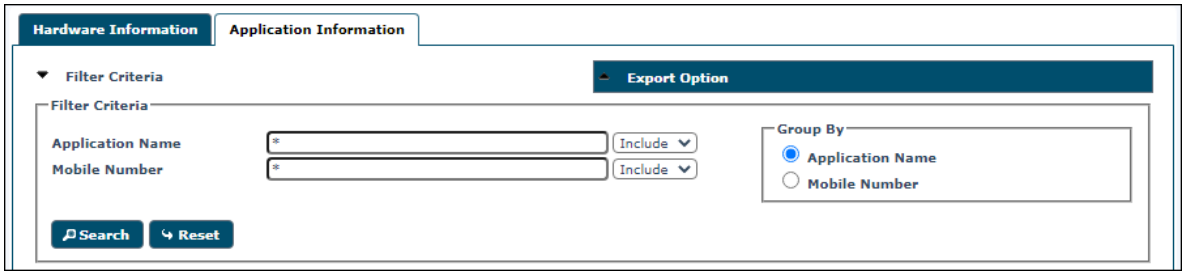
Following Hardware information is captured from Managed Devices.

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



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**.



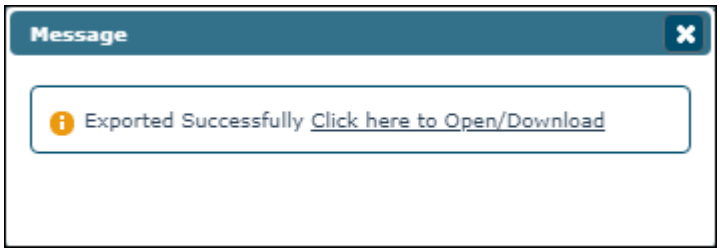
3. Select **Include/Exclude** to include otherwise exclude that particular criterion in the filtered report. All the information captured from the devices can be filtered on the basis of the application name or the mobile number associated with the device.
4. Select the desired criteria drop-down and then click **Search**.
   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

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

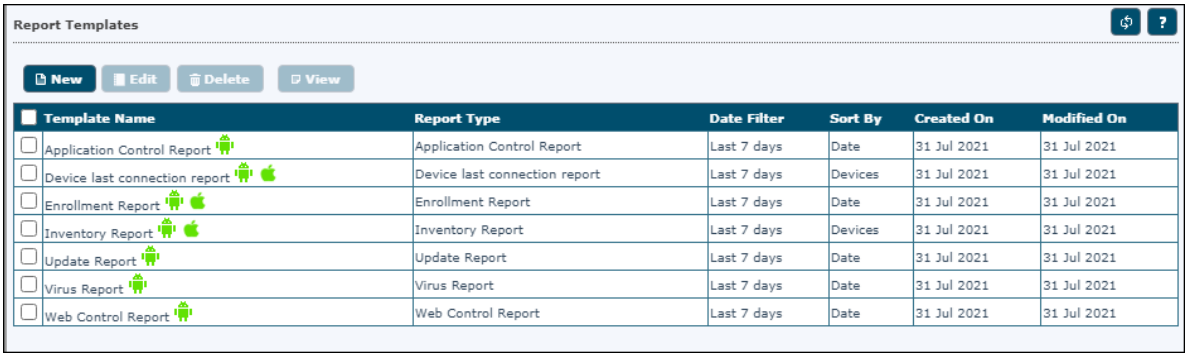
1. Select an export option of your preference and then click **Export**.
   A message appears informing about successful export.



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.

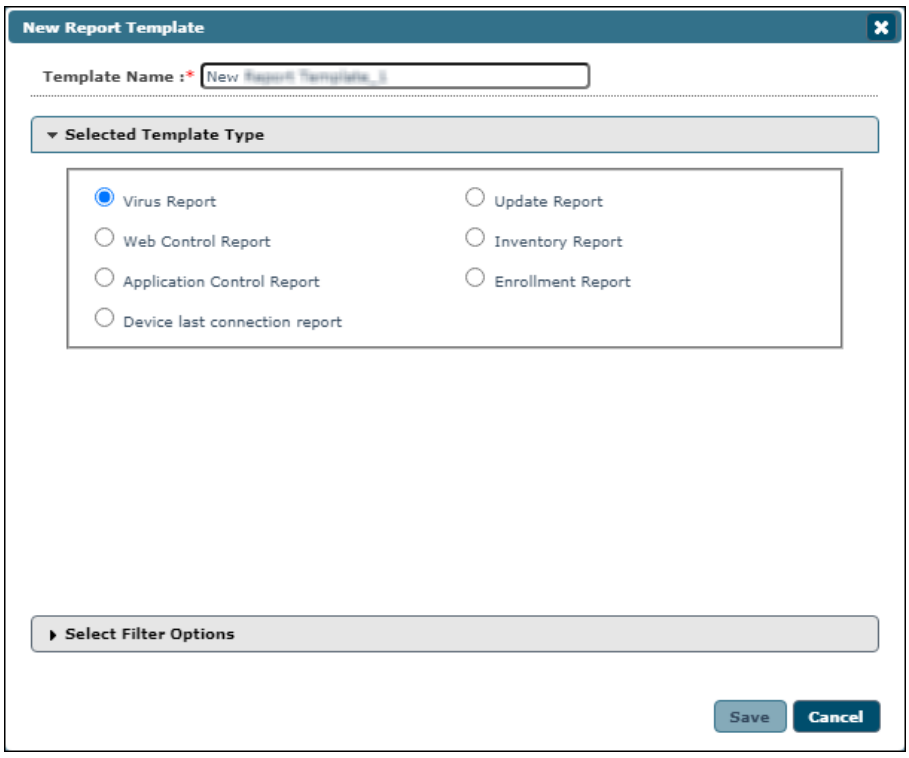


Template Name	Report Type	Date Filter	Sort By	Created On	Modified On
Application Control Report	Application Control Report	Last 7 days	Date	31 Jul 2021	31 Jul 2021
Device last connection report	Device last connection report	Last 7 days	Devices	31 Jul 2021	31 Jul 2021
Enrollment Report	Enrollment Report	Last 7 days	Date	31 Jul 2021	31 Jul 2021
Inventory Report	Inventory Report	Last 7 days	Devices	31 Jul 2021	31 Jul 2021
Update Report	Update Report	Last 7 days	Date	31 Jul 2021	31 Jul 2021
Virus Report	Virus Report	Last 7 days	Date	31 Jul 2021	31 Jul 2021
Web Control Report	Web Control Report	Last 7 days	Date	31 Jul 2021	31 Jul 2021

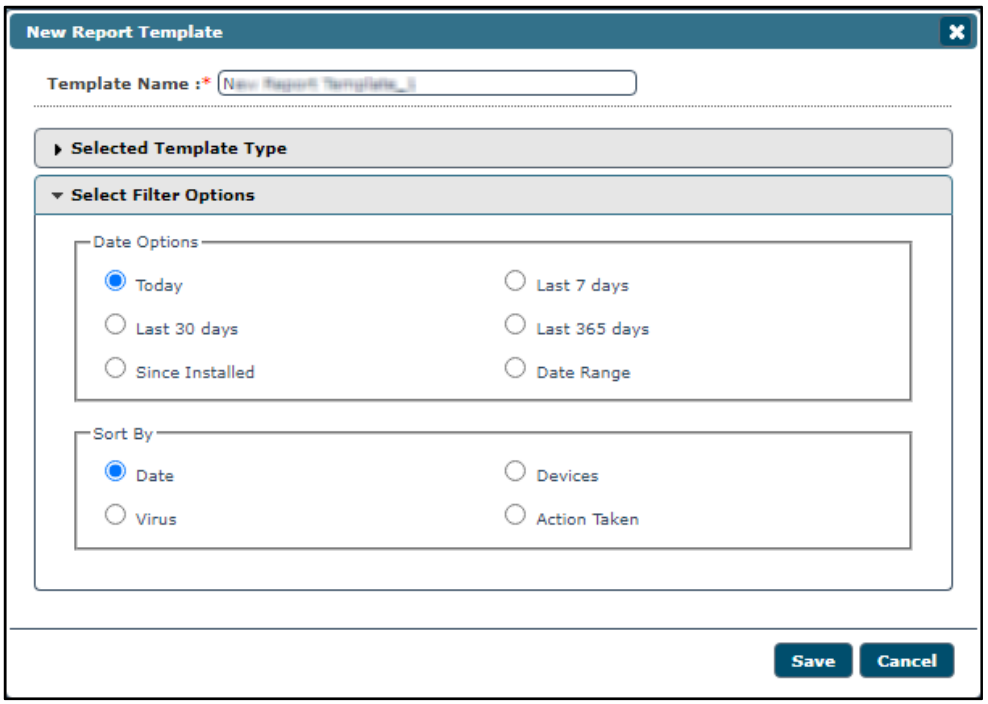
Creating a Report Template

To create a new Report Template:

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



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

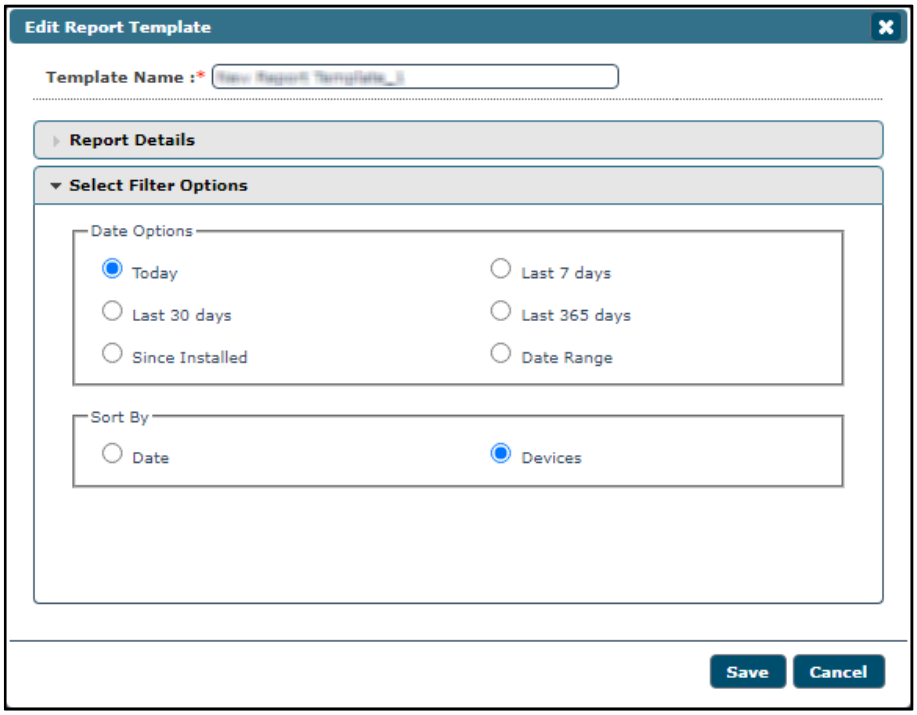


3. In **Select Filter Options** section, select an appropriate **Date Options** and **Sort By**, then click **Save**.
   A Report Template will be added.

Editing a Report Template

To edit an existing Report Template:

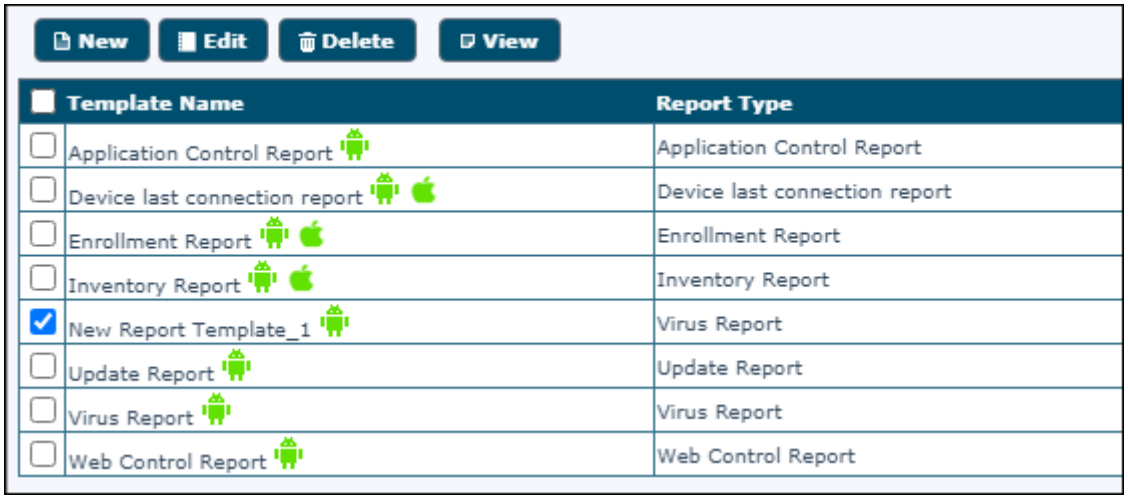
1. Select a Report Template and then click **Edit**.
   Edit Report Template window appears.



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**.

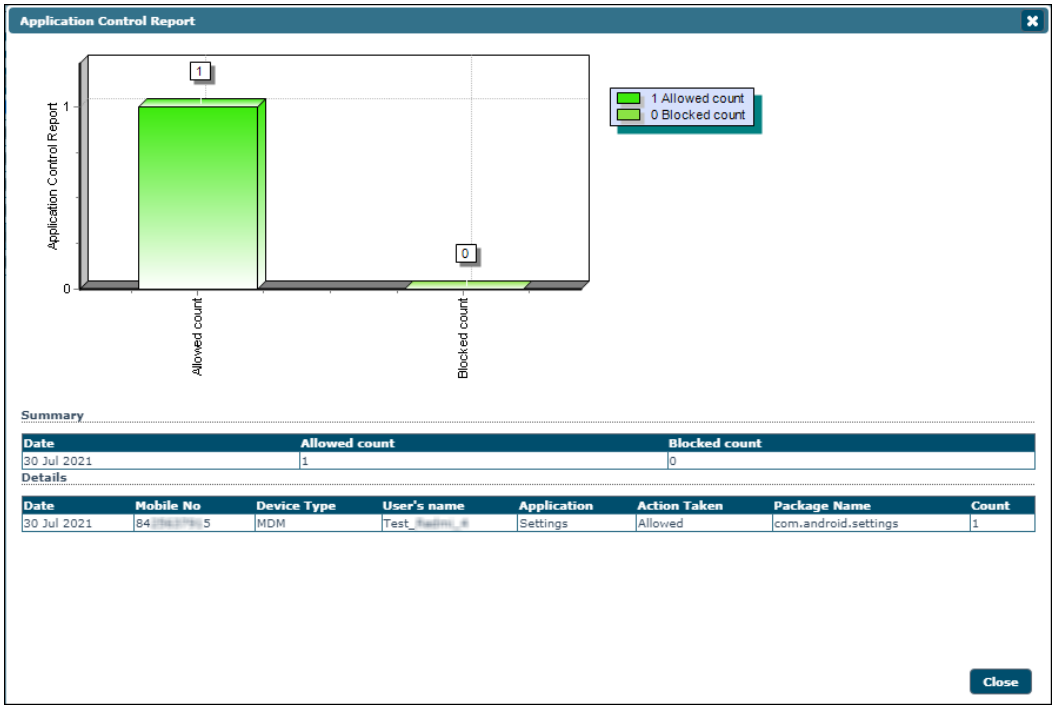


The Report Template will be deleted.

Viewing a Report

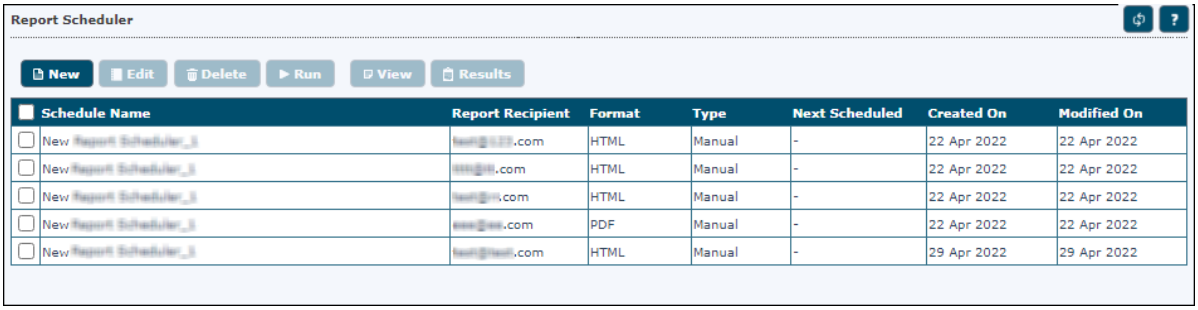
To view report details:

- Select the specific template and then click **View**.
  A window appears displaying specific details.

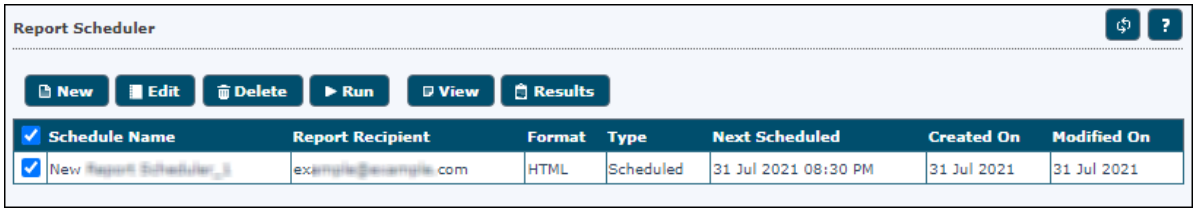


Report Scheduler

The Report Scheduler module lets you schedule a report based on the type of templates, specific group or device, file format and type of schedule.



Under Report Scheduler, following options are available. Except **New**, all other options are enabled only after selecting a template.
Select a Particular Schedule name to enable all the options.



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.

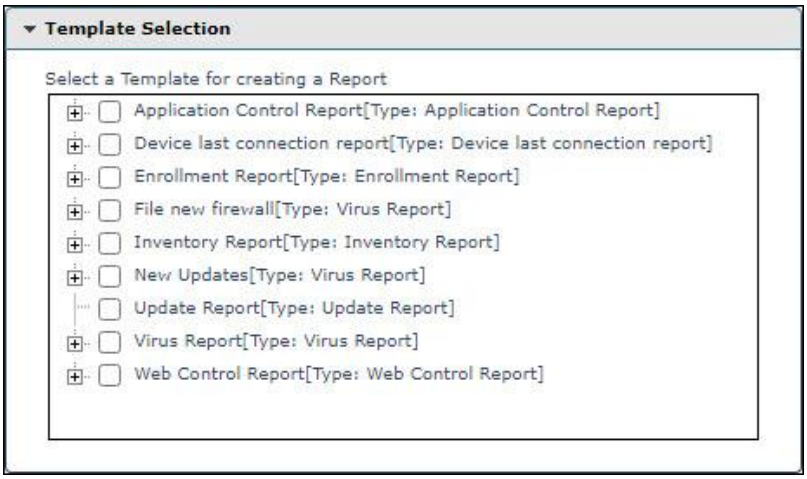
Adding a Scheduler

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.



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

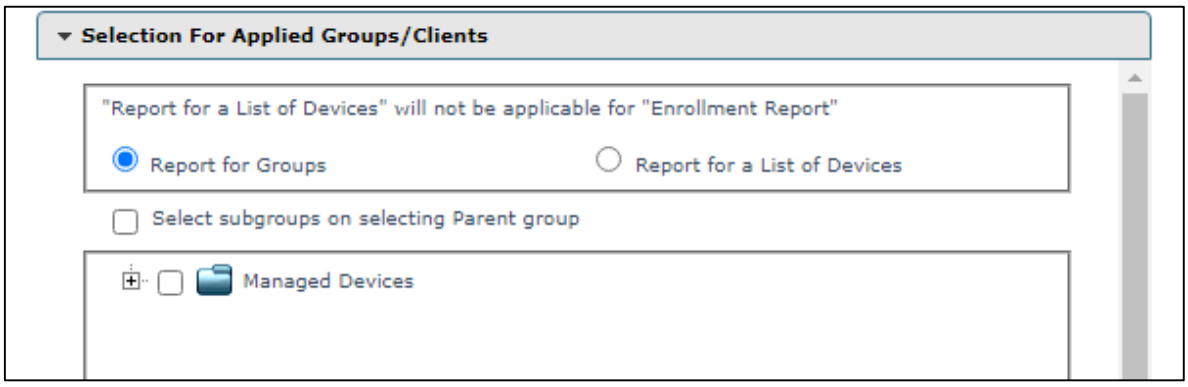
Select an appropriate template to create report.

Selection For Applied Groups/Clients

Select the groups for which you want to schedule the report:

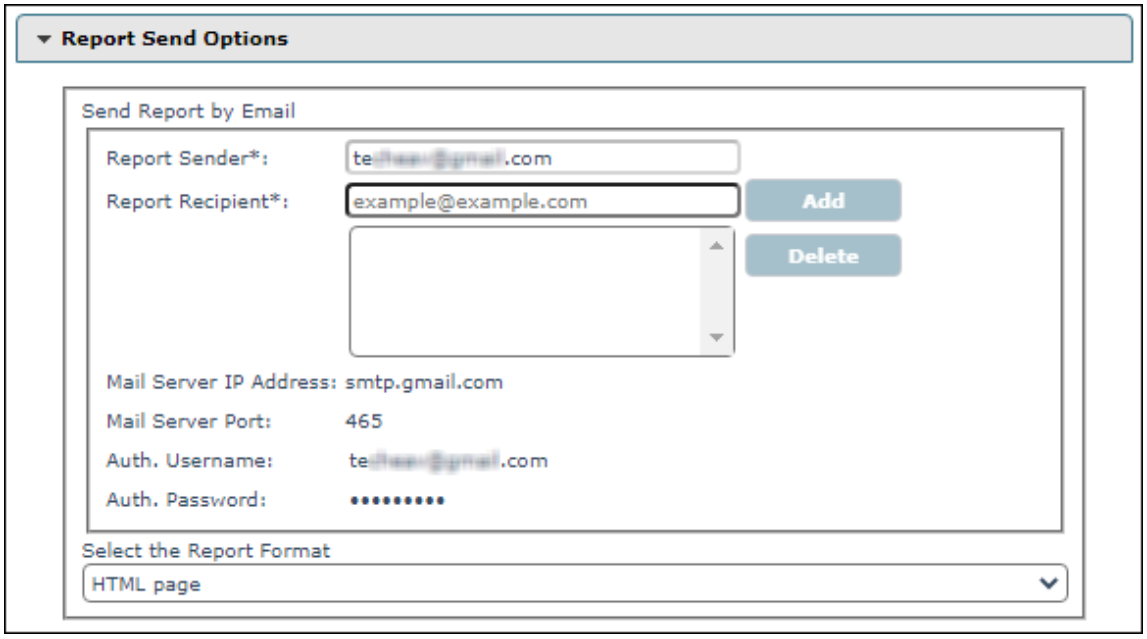
- Report for Groups
- Report for a List of Devices

Select **Report for Groups/Report for a List of Devices** tab to schedule a report for the specific groups.



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.



Add the following details under the **Report Send Options** section:

1. Send Report by Email

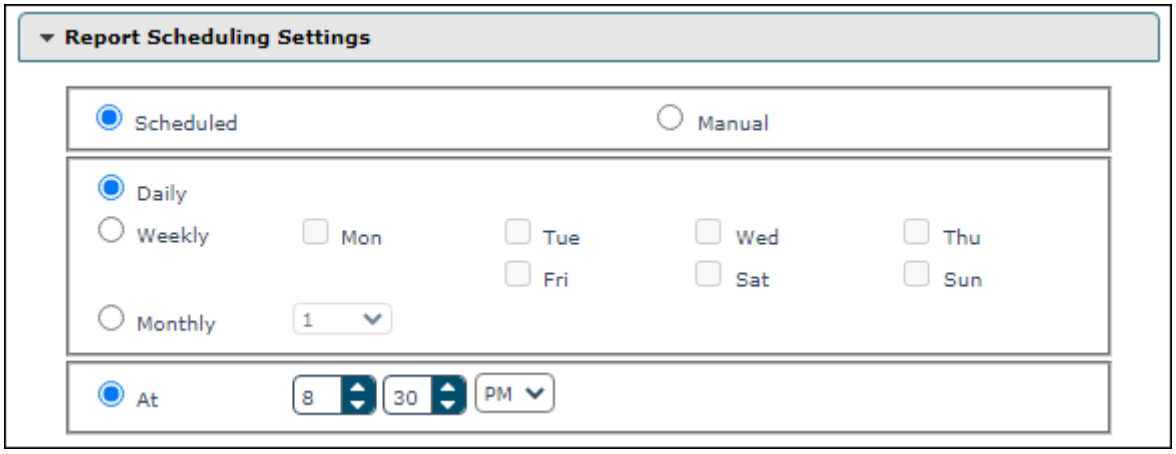
- **Report Sender** – The email address set for **Email Notification Settings** will be displayed here.
- **Report Recipient** – Enter an email address for the report recipient and then click **Add**. To delete the recipient email, select the specific email id and click **Delete**.

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



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

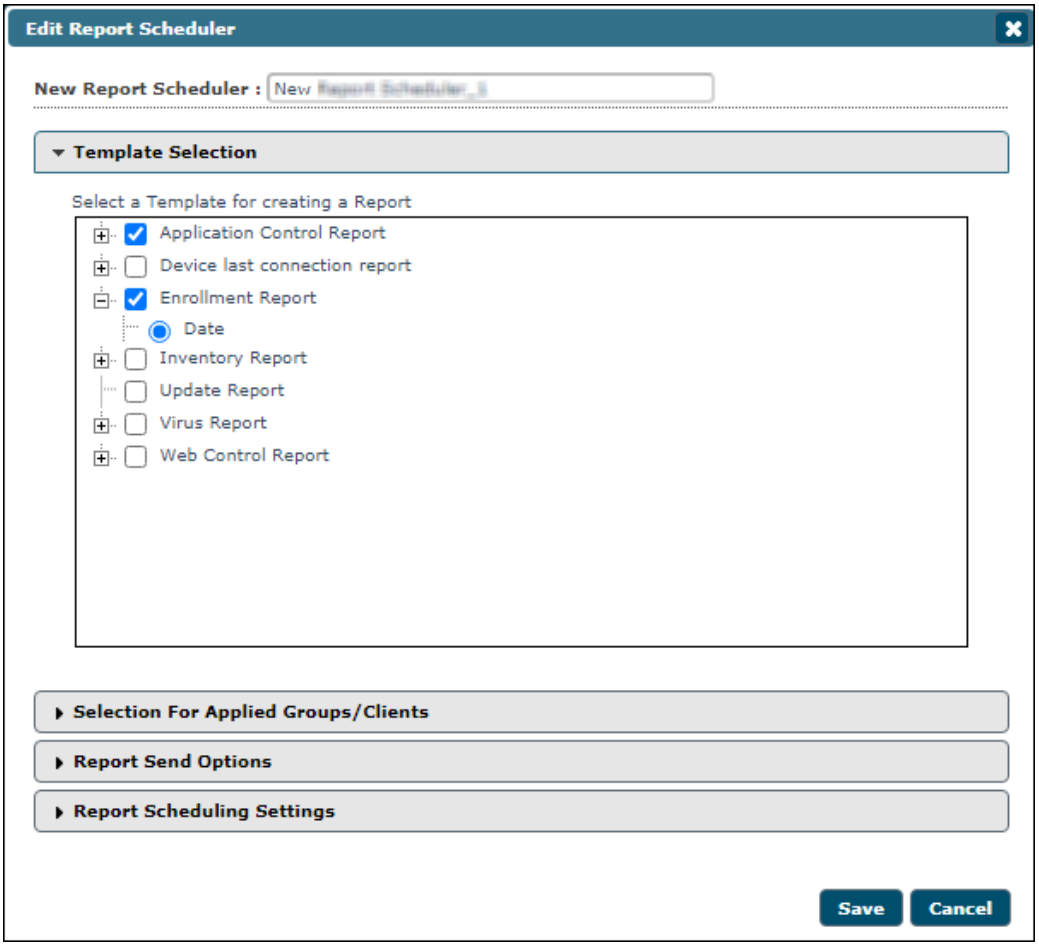
To run a schedule:

- 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.

Editing a Schedule

To edit a schedule:

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

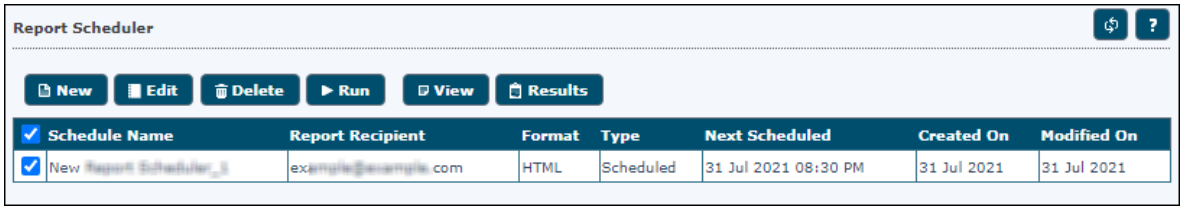


- Make the required changes and then click **Save**.
  The schedule will be updated.

Deleting a Schedule

To delete a schedule:

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

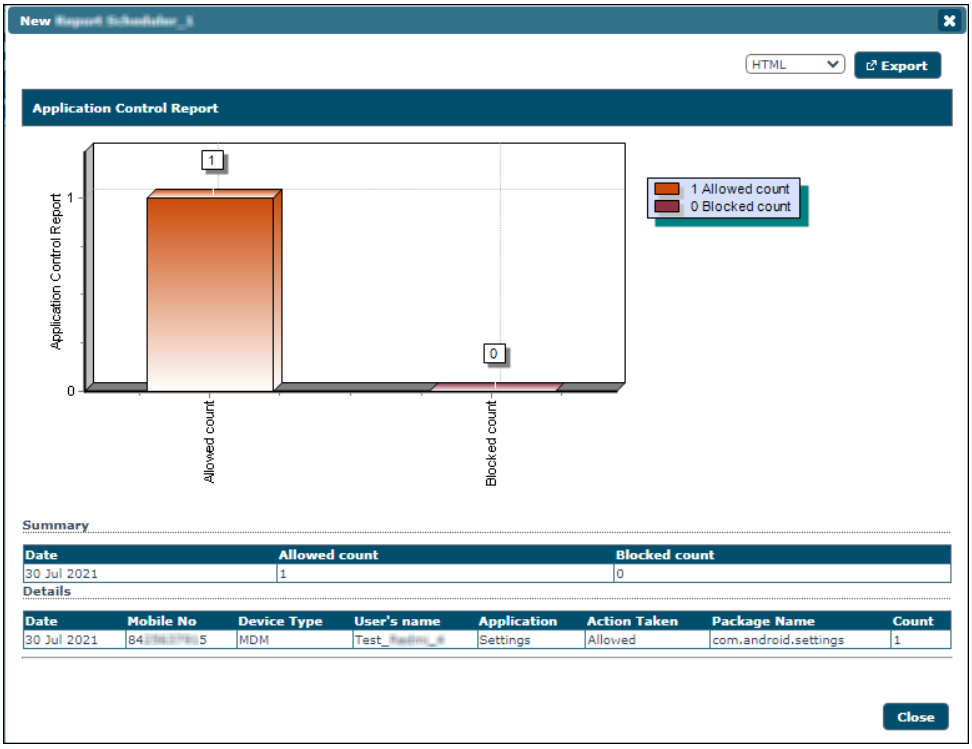


The selected schedule will be deleted.

Viewing the report

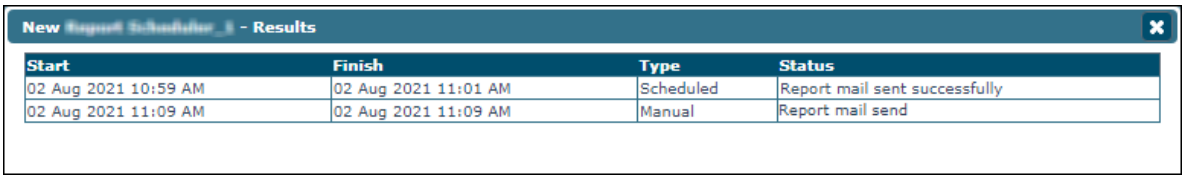
To view the report:

- 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.

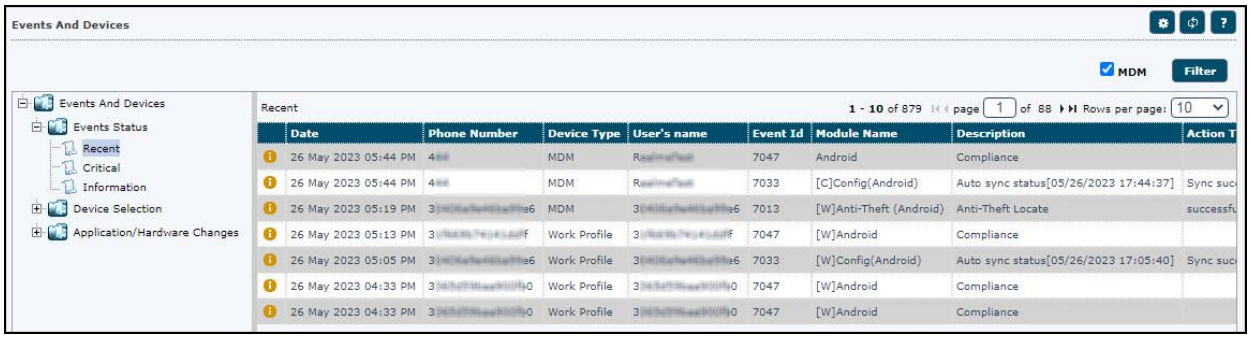


Events and Devices

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.



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.

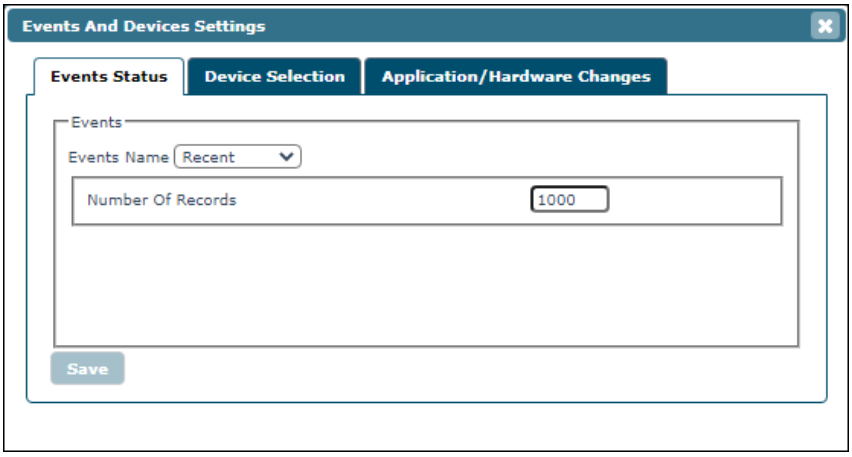
Events and Devices settings

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

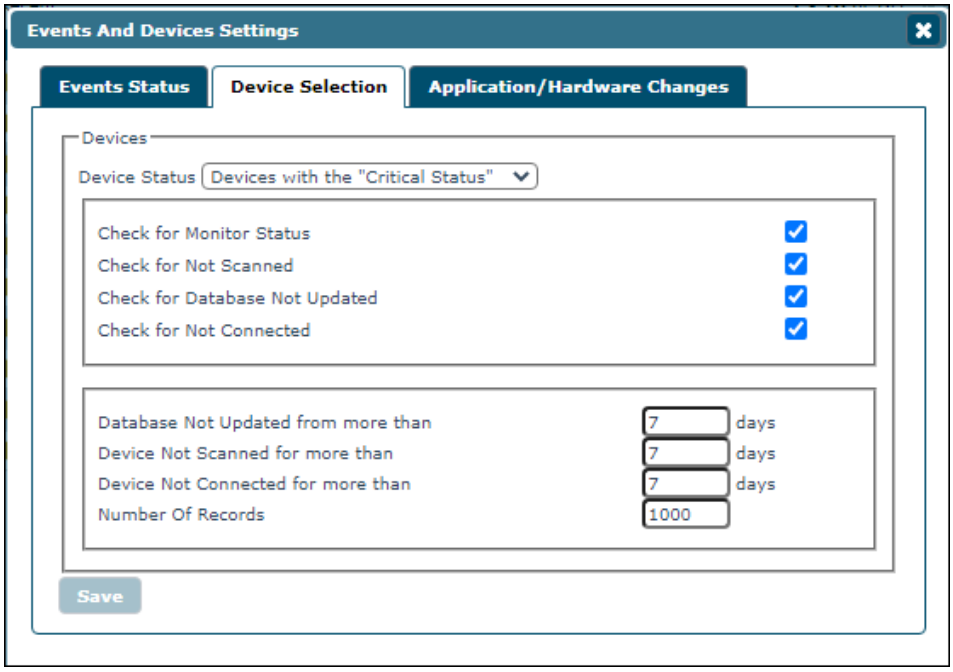
Event Status



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

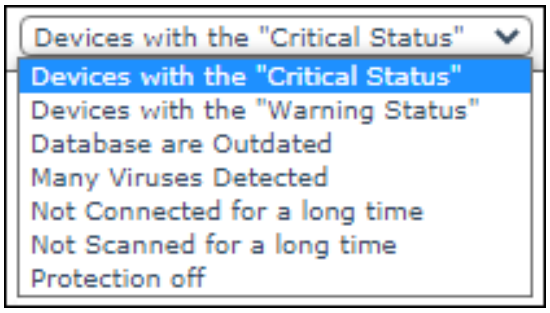
Device Selection

The following actions can be performed by selecting this tab.



Device Status

The Device Status drop-down consists following options:



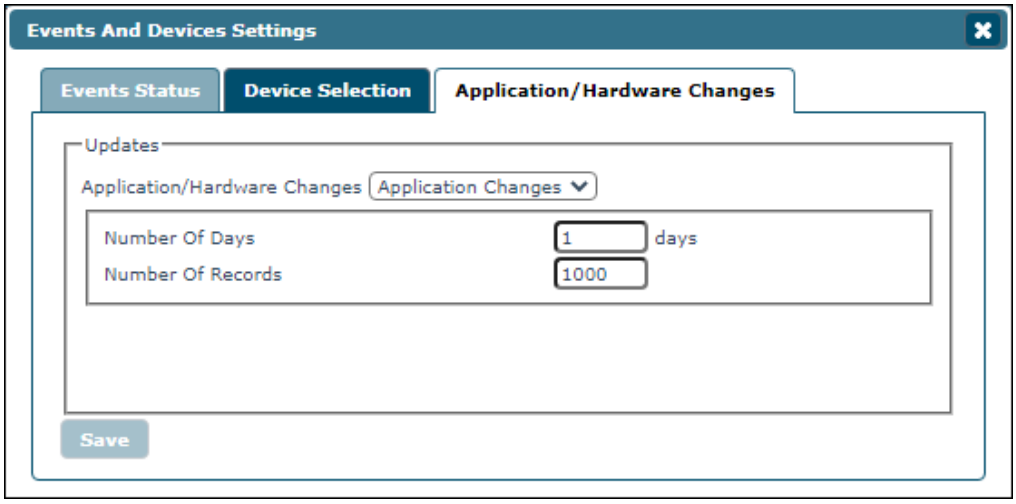
- Devices with the "Critical Status"
- Devices with the "Warning Status"
- Database are Outdated
- Many Viruses Detected
- Not Connected for a long time
- Not Scanned for a long time
- Protection off

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.



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

After doing necessary configuration, click **Save**.

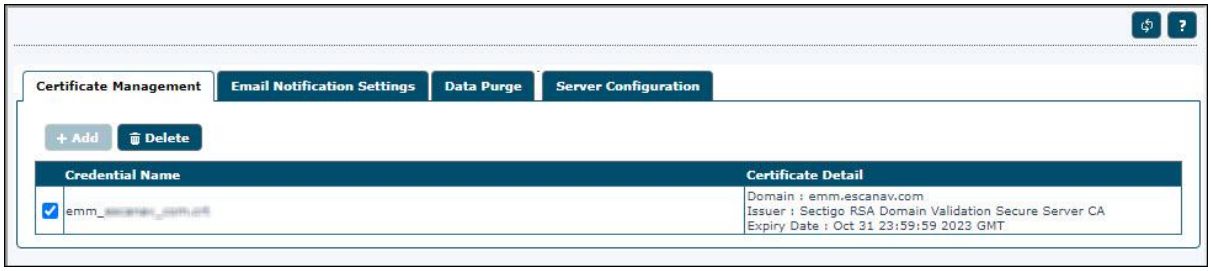
Settings

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.



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 **our website**, you are on a secured connection, as an SSL certificate installed on our domain **escanav.com**.
3. If you own the website as 'emm.mycompany.com', you need to get an SSL certificate for the domain emm.mycompany.com. You can buy it from a Certificate Authority or generate it for free.
4. The SSL certificate thus bought from a Certificate Authority has to be renewed every year. If you have generated the SSL certificate for free it has to be renewed every 3 months.
5. In order to have a secure communication between your server and Apple's server you will have to import the SSL certificate in the console.

Importing an SSL certificate

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.
3. 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.

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

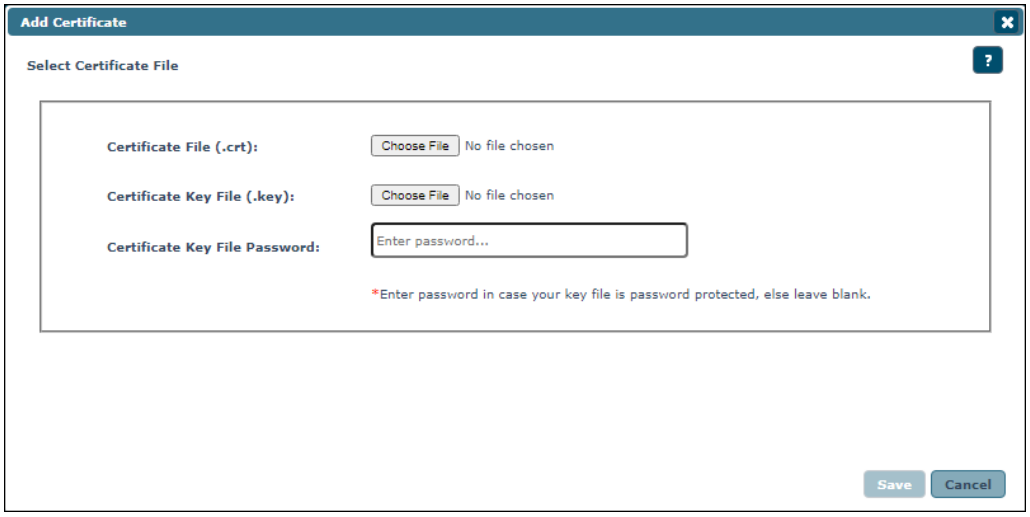
To add the CA certificate if

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

OR

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

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



4. Click **Choose File** and select the .crt and .key files.
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**".

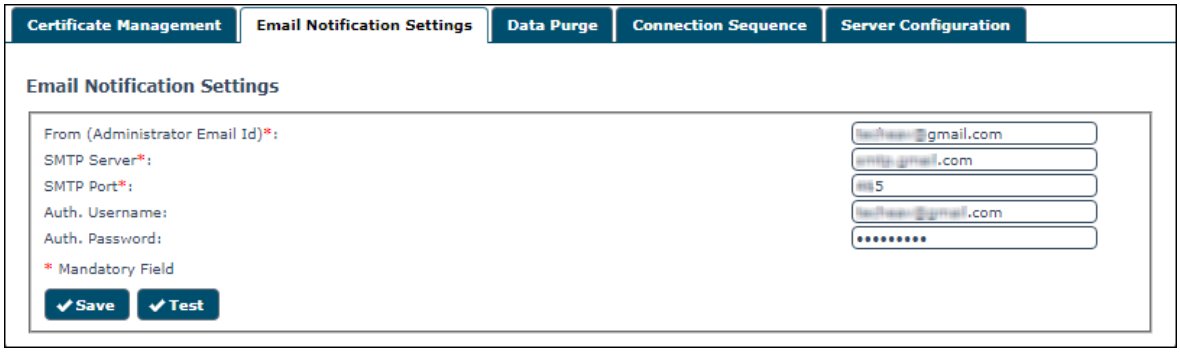
To delete the CA certificate

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.

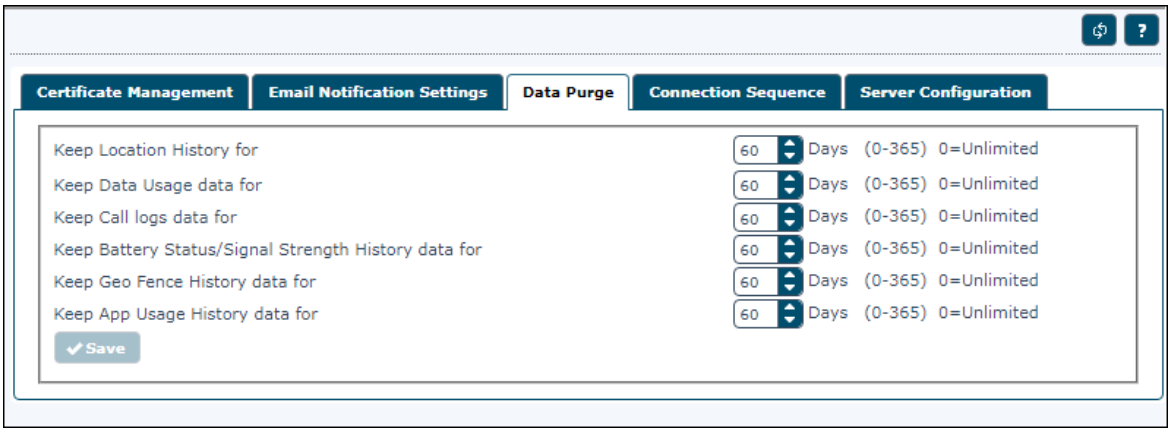


- **From (Administrator Email Id)**: Enter an Administrator email ID.
- **SMTP Server**: Enter the SMTP server IP address.
- **SMTP Port**: Enter the SMTP Port number.
- **Auth. Username**: Enter an authorized username.
- **Auth. Password**: Enter the password.

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.



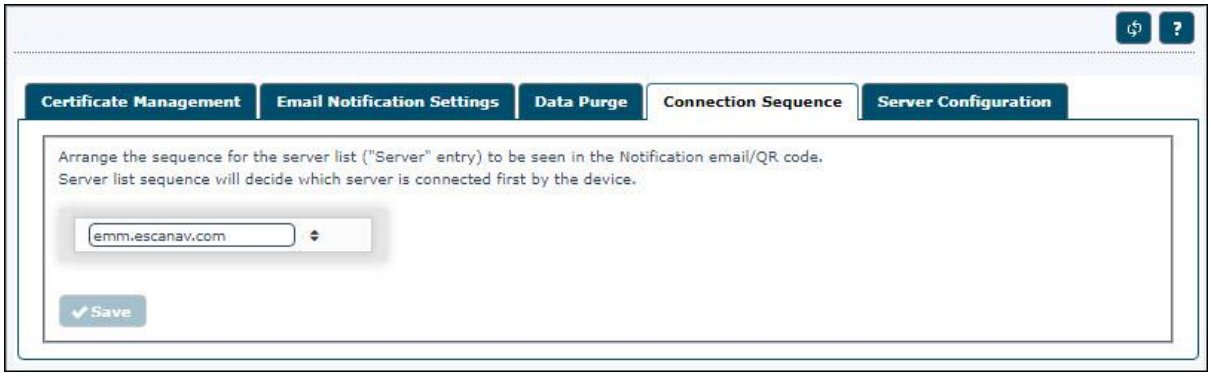
The data purge can be set for following data tables:

- 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.

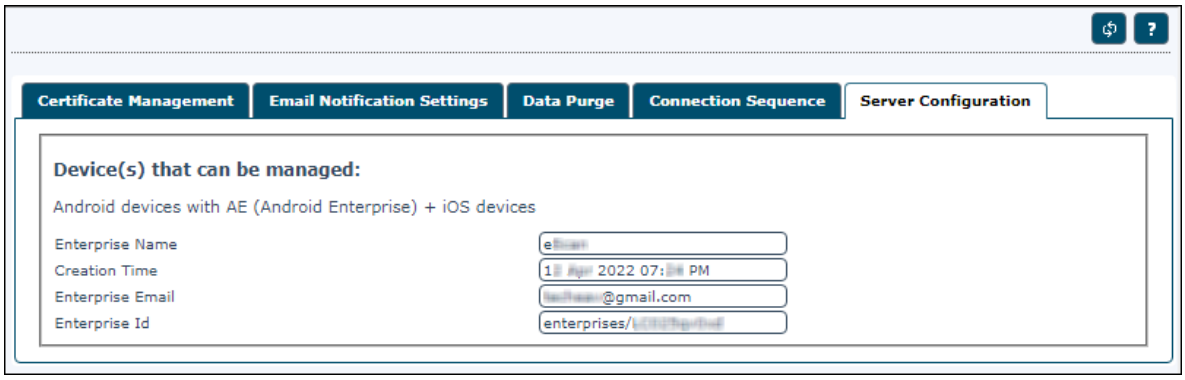
Connection Sequence

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.



Server Configuration

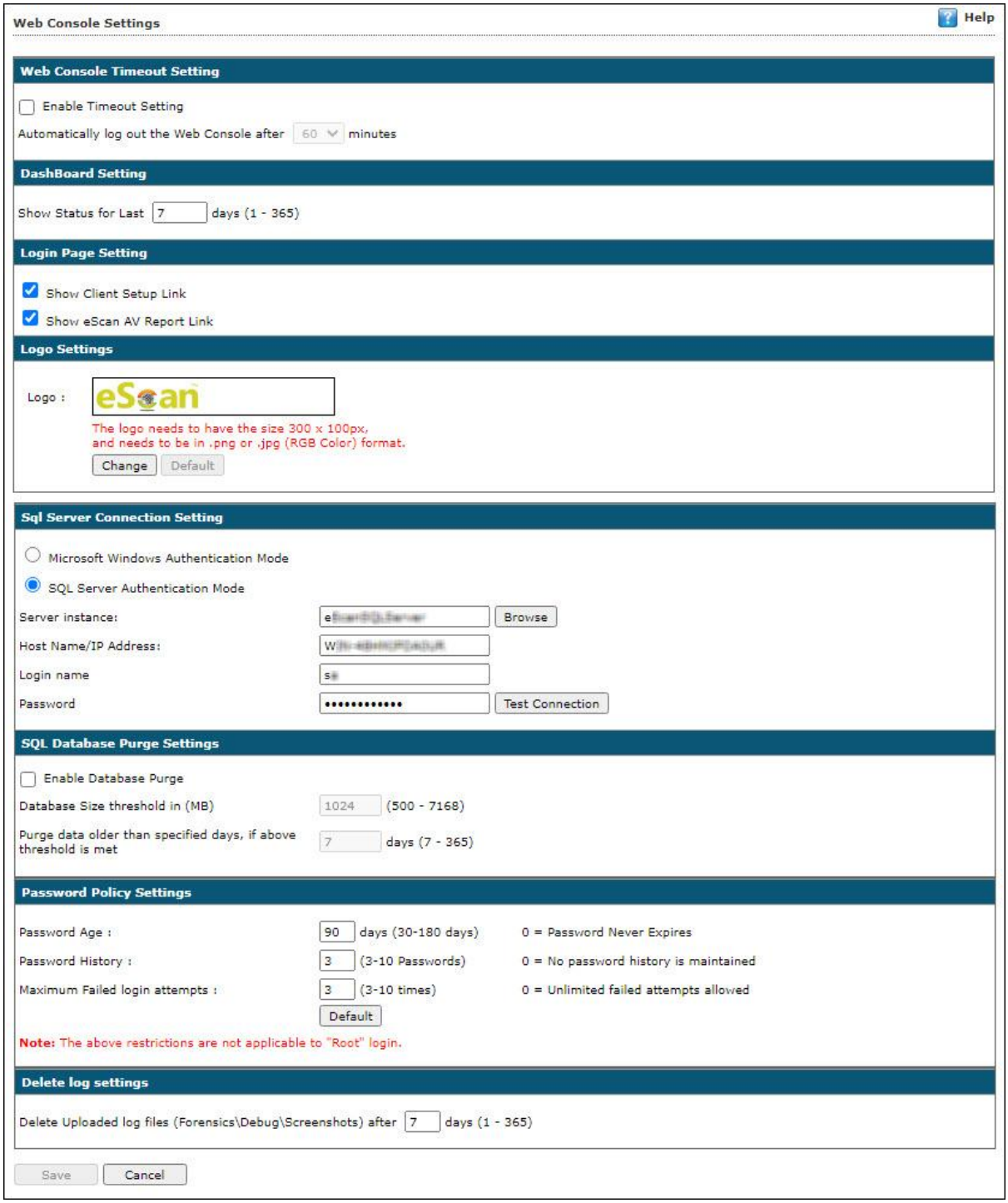
This setting displays the information of application server.



- **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 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.

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 Play Store or for iOS devices from App Store on your smart device. The Authenticator app needs camera access for scanning a QR code, so ensure you get an appropriate approval to use device camera in your organization. If a COD or BYOD policy restricts you from using device camera in your organization, enter the Account Key in the Authenticator app.

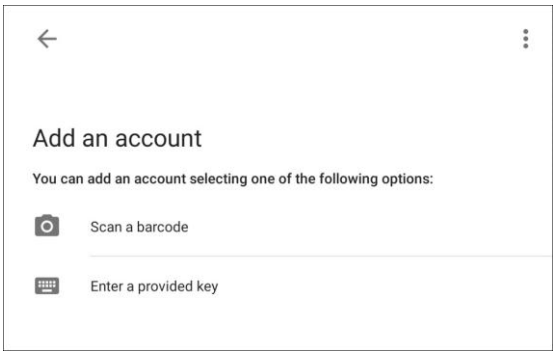
NOTE	Ensure that the smart device's date and time matches with the system's date and time or else TOTPs generated by app won't get validated.

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

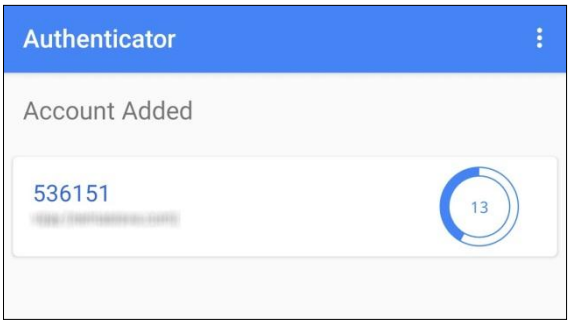
Enabling 2FA login

To enable 2FA login:

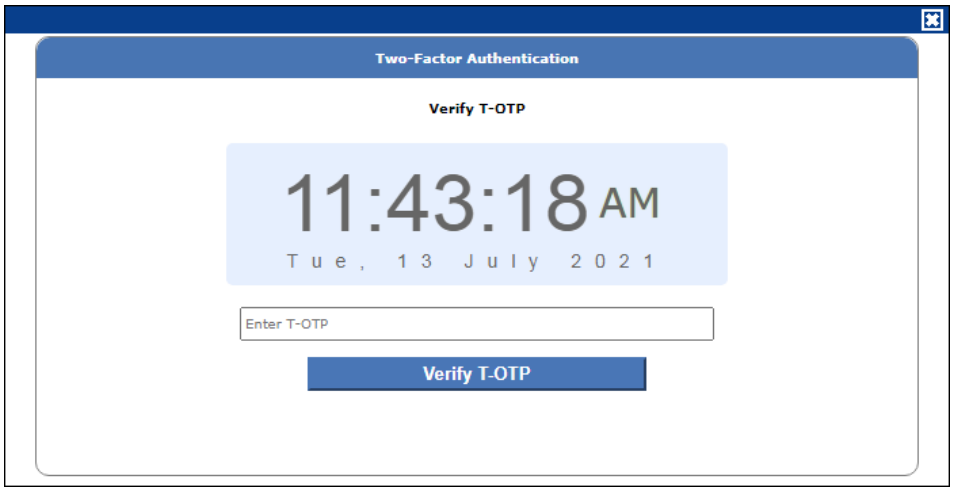
1. Go to **Settings** > **Two-Factor Authentication**.
2. Open the Authenticator app.
   After basic configuration following screen appears on smart device.



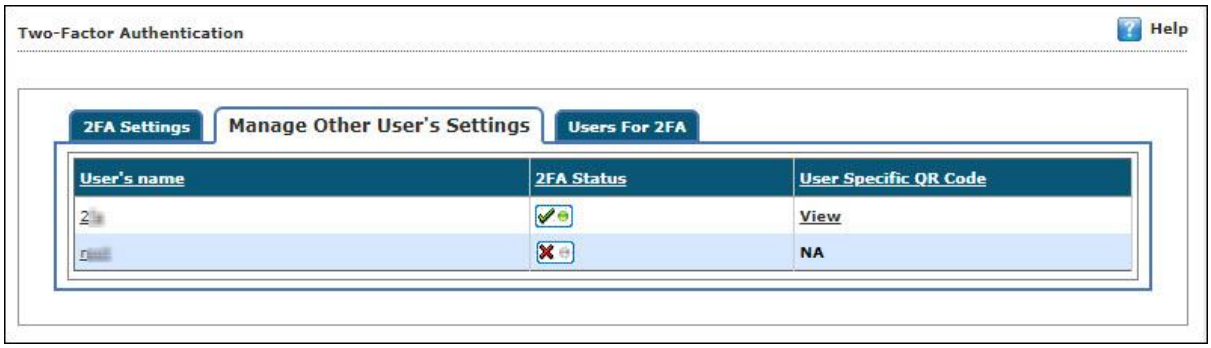
3. Select a preferred option. If you tapped **Scan a barcode**, scan the onscreen QR code via your smart device. If you tapped **Enter a provided key**, enter the Account Key and then tap **ADD**. After scanning the Account QR code or entering Account Key the eScan server account gets added to the Authenticator app. The app then starts displaying a Time-based One-Time Password (TOTP) that is valid for 30 seconds.



4. Click **Enable Two-Factor Authentication**.
   Verify TOTP window appears.



5. Enter the TOTP displayed on smart device and then click **Verify TOTP**.
   The 2FA login feature gets enabled.
6. To apply the login feature for specific users, click **Manage Other User Settings** tab. The tab displays list of added users and whether 2FA status is enabled or disabled.
   - 2FA Disabled
   - 2FA Enabled



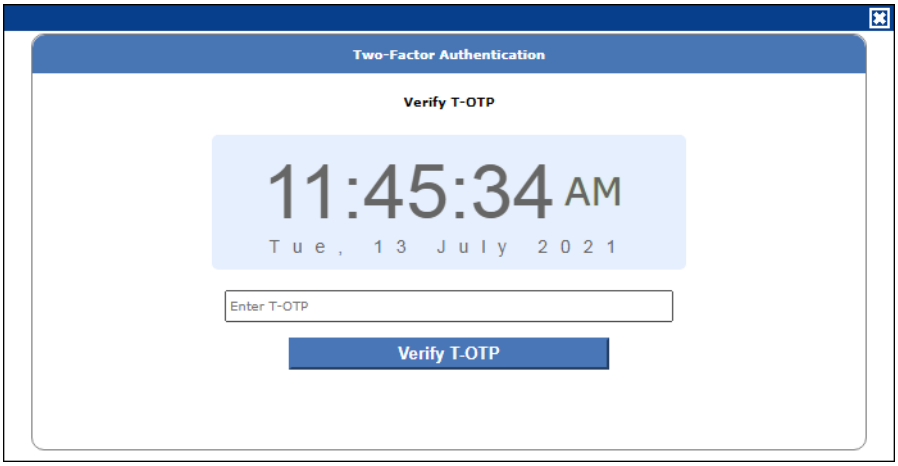
7. To enable 2FA login for an added user, click the button to check icon.
   The 2FA login for added users gets enabled. After enabling the 2FA login for users, whenever they log in to eScan web console Verify TOTP window appears.
8. To view QR code of added user, click on **View** option under the column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

Disabling 2FA login

To disable 2FA login:

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

Verify TOTP window appears.

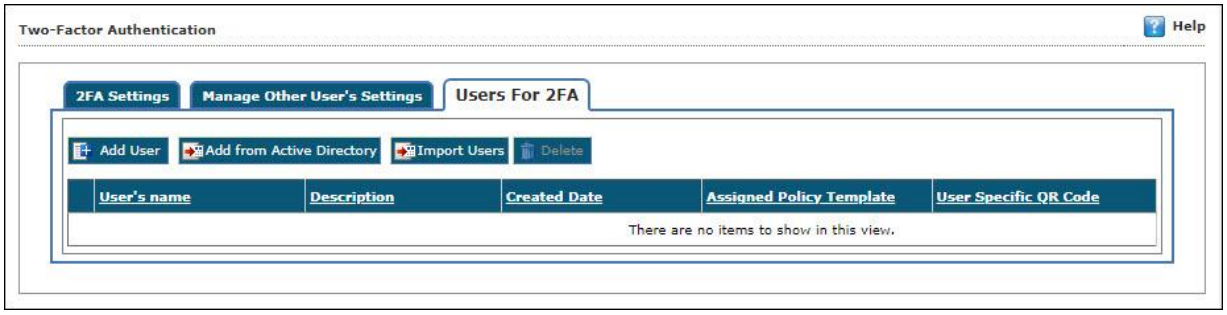


3. Enter the TOTP and then click **Verify TOTP**.
   The 2FA feature gets disabled.

NOTE	After disabling the 2FA feature and enabling it again, the 2FA login status will be reinstated for added users.

Adding Users for 2FA

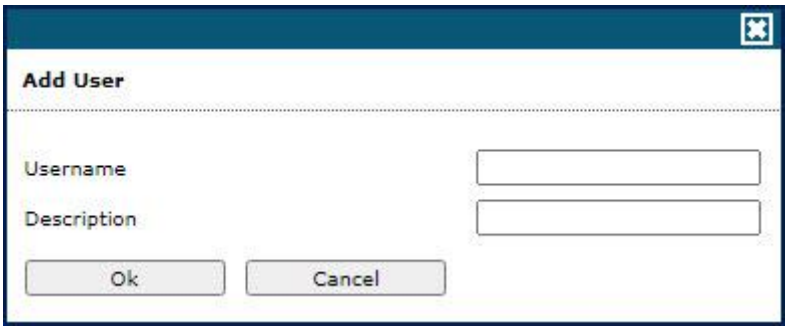
To Add users for Two-Factor Authentication, follow the steps mentioned below:



Method 1: Adding User

To add users for the same, follow the below steps:

1. Go to **Settings** > **Two-Factor Authentication** > **Users For 2FA**.
2. Click **Add User**.
   Add User window appears.

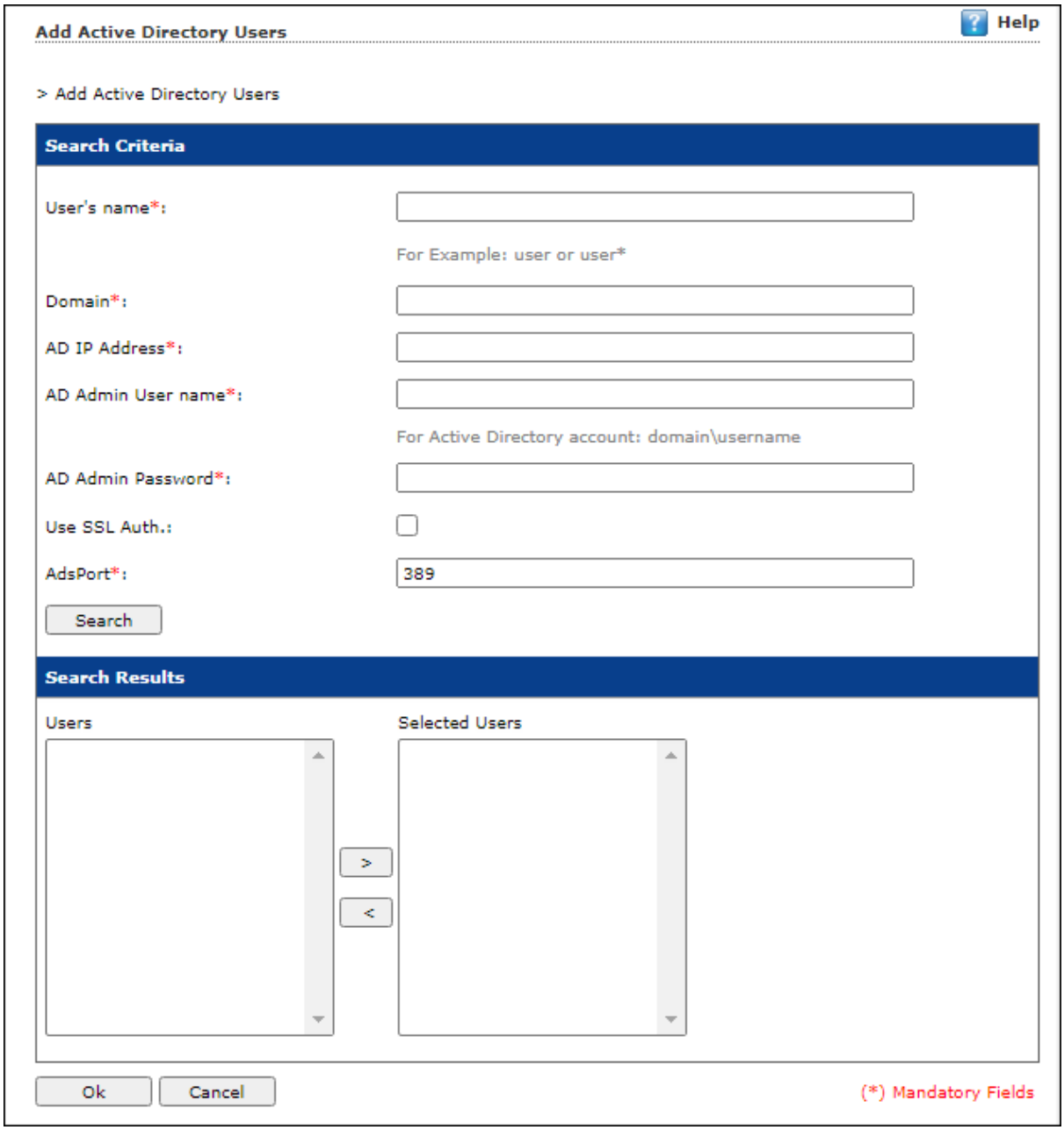


3. Enter the **Username** and **Description**.
4. Click **OK**.

Method 2: Adding User from Active Directory

To add users from Active Directory, follow the below steps:

1. Go to **Settings** > **Two-Factor Authentication** > **Users For 2FA**.
2. Click **Add from Active Directory**.
   Add Active Directory Users window appears.



3. Enter the required information.
4. Click **Ok**.
   The Active Directory Users will be added.

Method 3: Importing Users

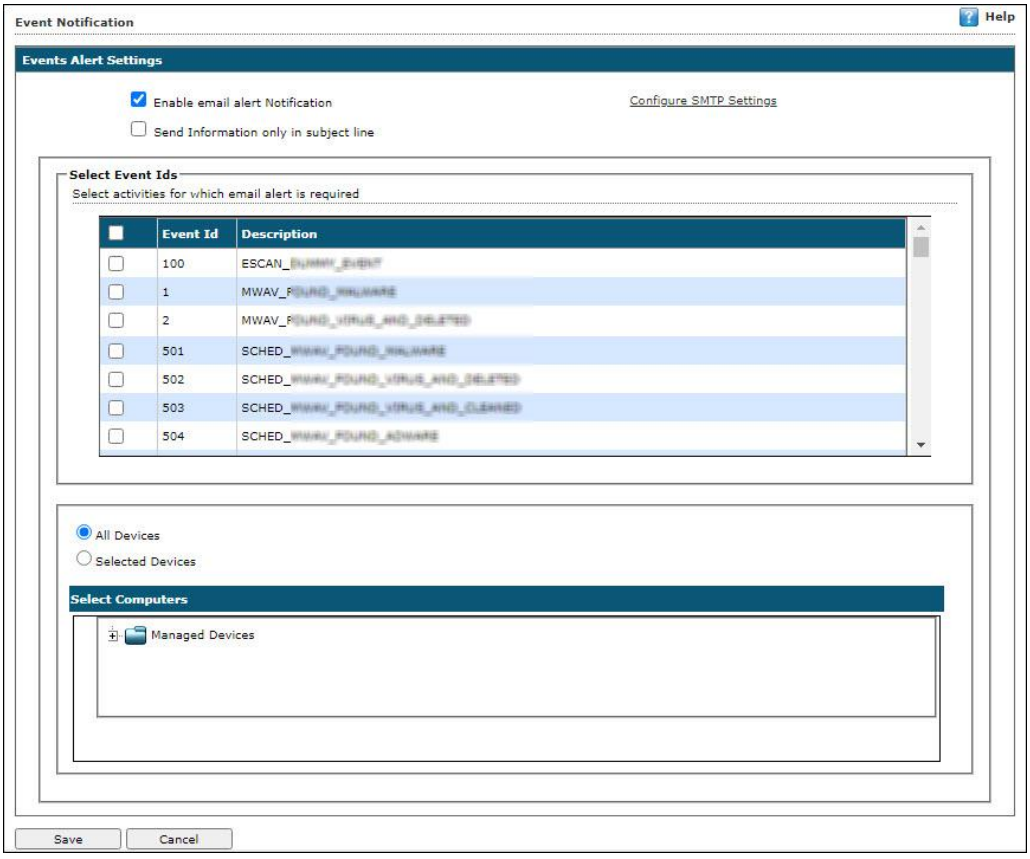
To import the users, follow the below steps:

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

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



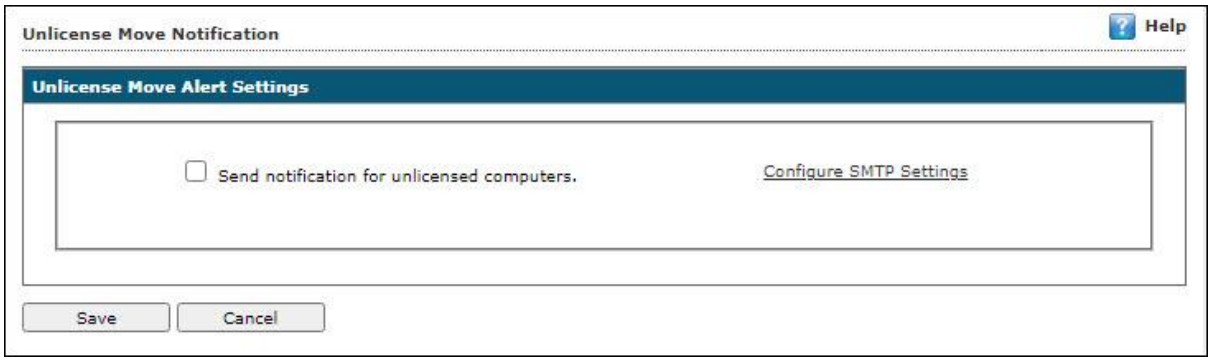
To configure Event alerts, follow the steps given below:

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.



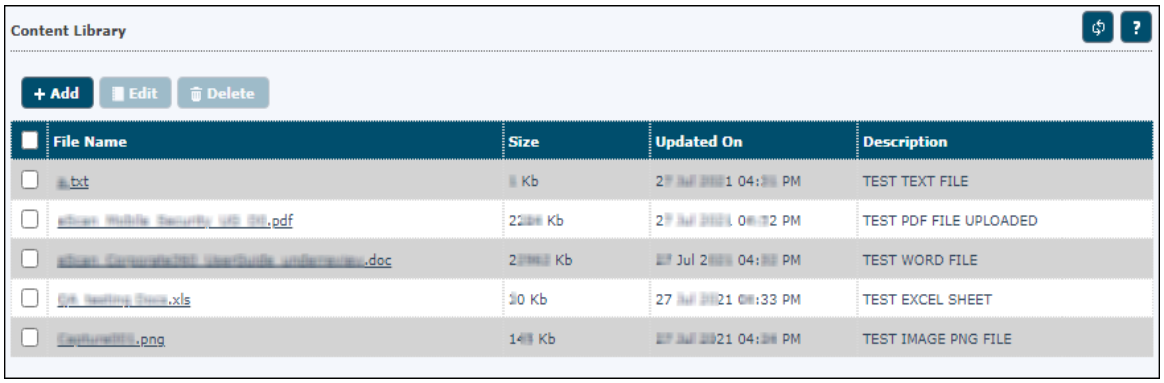
To configure Unlicense alerts, follow the steps given below:

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

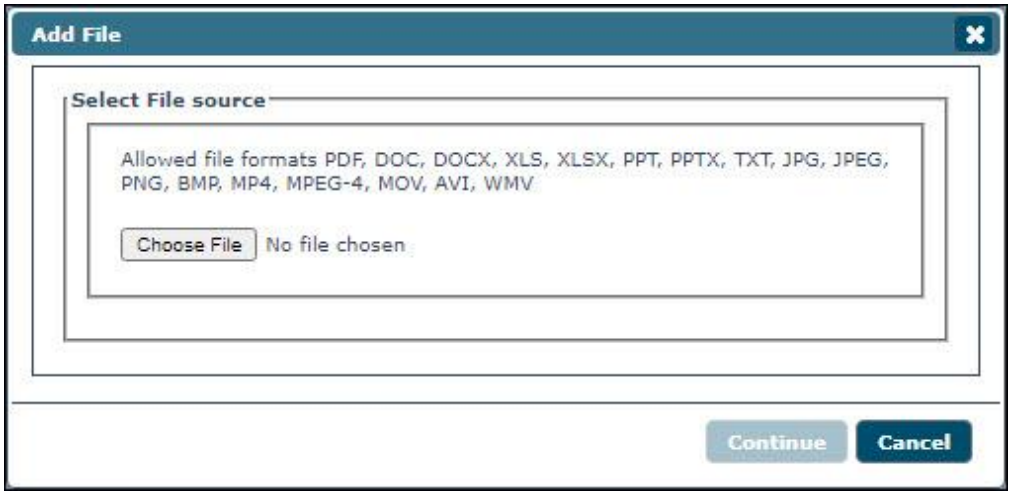
The Content Library module lets you deploy documents through the web console. The document types that can be deployed are .pdf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .jpg, .jpeg, .png, .bmp, .mp4, .mpeg-4, .mov, .avi, and .wmv. You can use this feature to share work related documents across multiple devices at the same time.



Adding a file

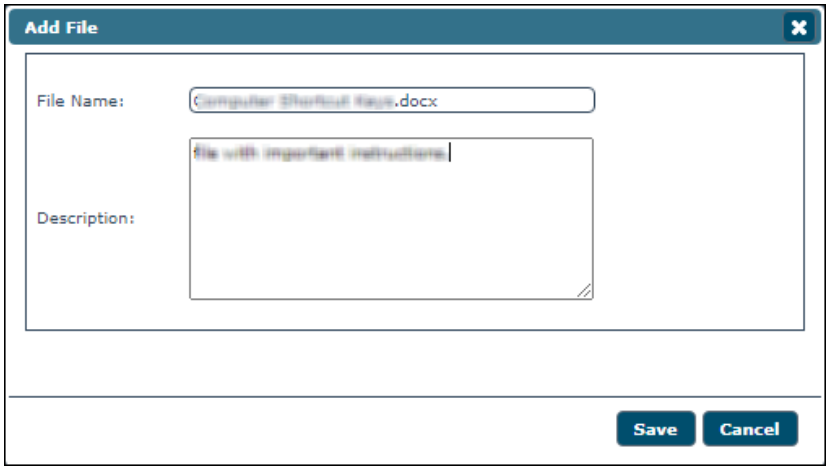
To add a file in Content Library:

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



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.



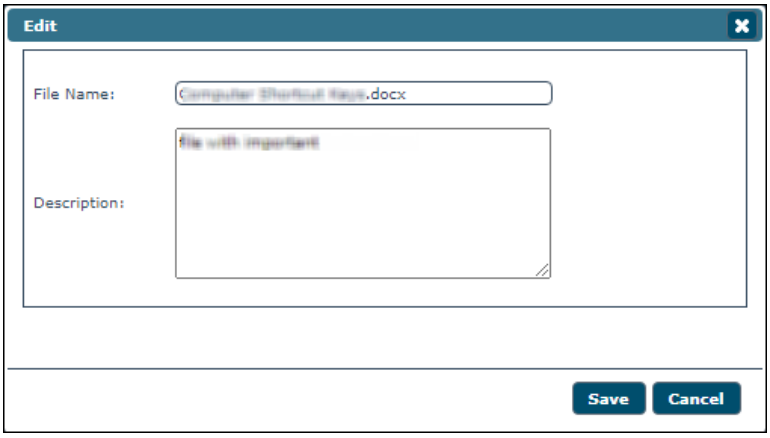
4. Write a description for the document and then click **Save**.
   The document will be added to the Content Library.

Editing a file description

To edit a file description:

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

Edit window appears.



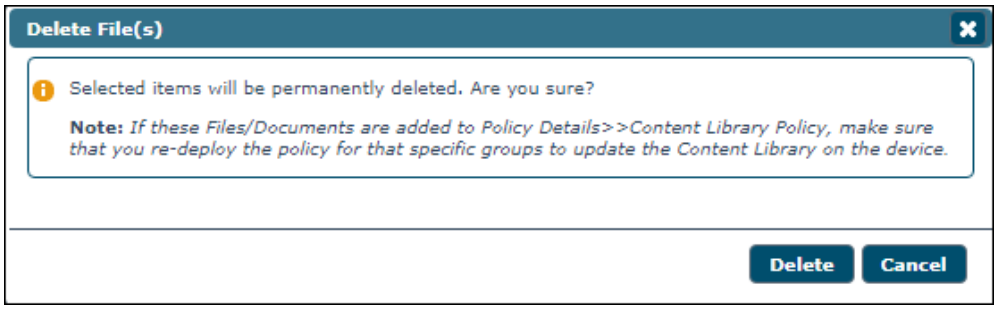
2. Edit the description and then click **Save**.
   The file description will be updated.

Deleting a file

To delete a file:

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

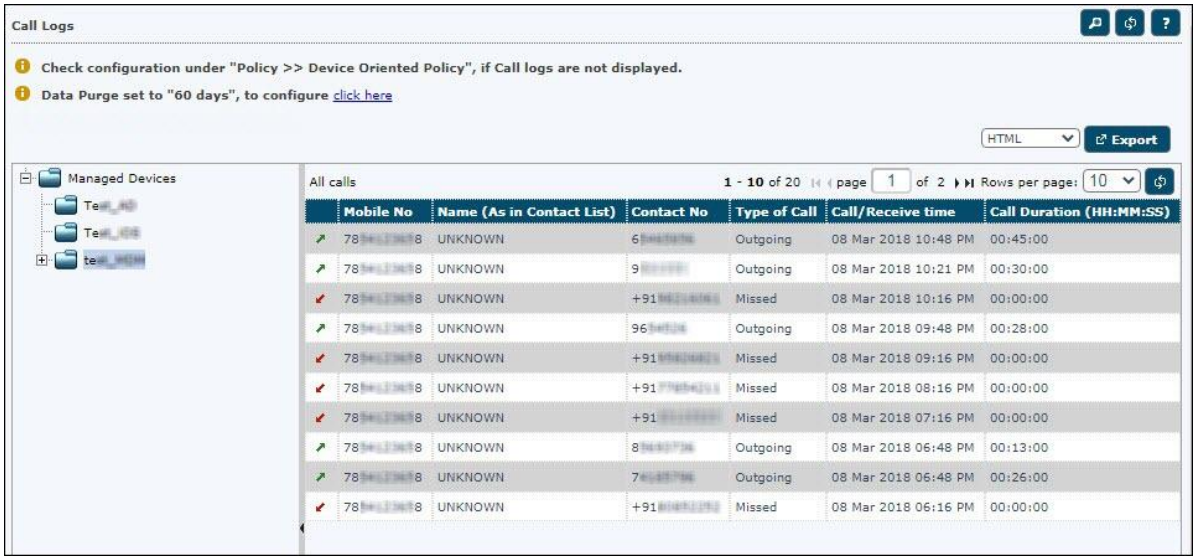
A confirmation prompt appears.



2. Click **Delete**.
   The file will be deleted.

Call Logs

The Call Logs module lets you maintain call logs of incoming and outgoing calls of all managed devices along with the call duration.



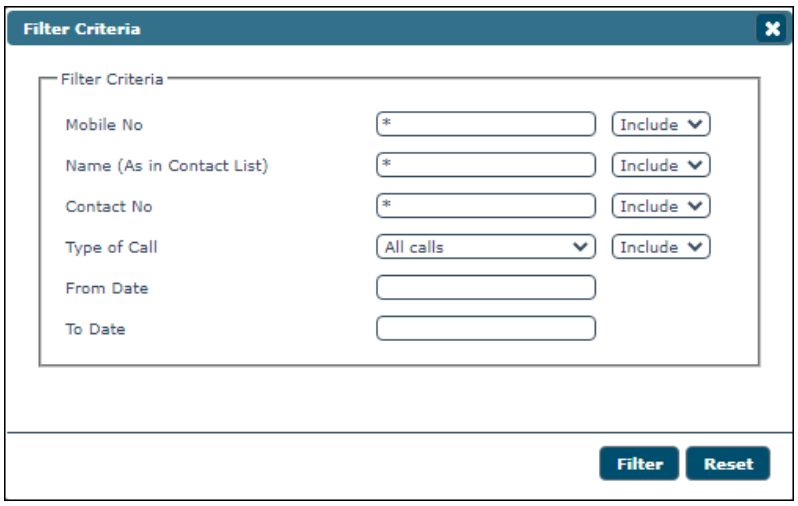
This module displays the list of all the incoming and outgoing calls. It will display the following details:

Column	Description
Mobile No	This column displays the mobile number.
Name (As in Contact List)	This column displays the contact name as saved in the contact list.
Contact No	This column displays the contact number with whom the user had a conversation.
Type of Call	This column displays whether the call was incoming or outgoing.
Call/Receive time	This column displays the specific time when the call was made or received.
Call Duration	This column displays the time duration of each call.

Filter Call Logs

To filter the Call Log information:

1. Click **Filter Criteria** icon.

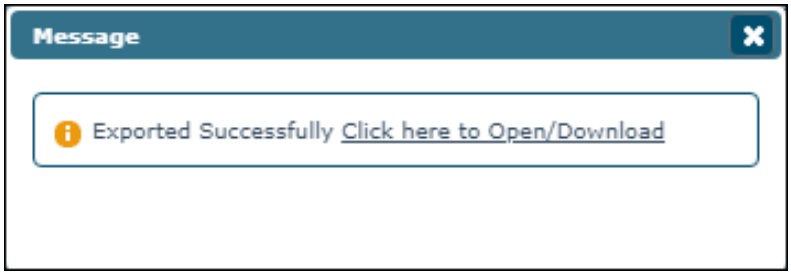


2. Select the checkbox next to each criterion and select **Include/Exclude** to include/exclude that particular criterion in the filtered report and date.
3. Click **Filter**.
4. Click **Reset**, to set default values.

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

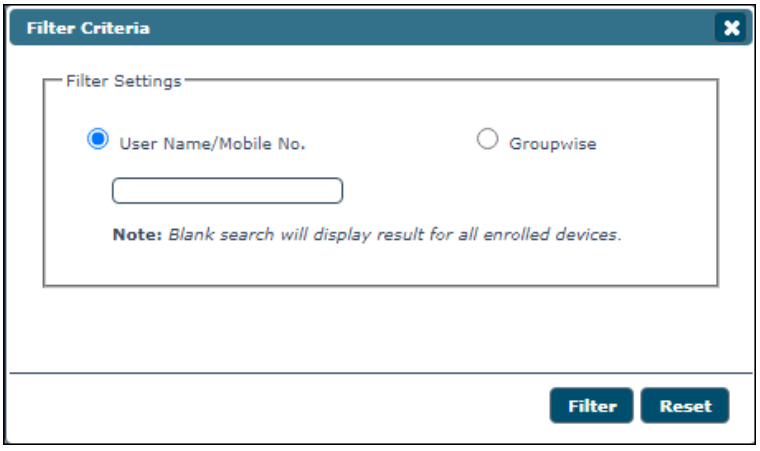
The Data Usage module lets you keep a track of cellular data usage of a device.

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.



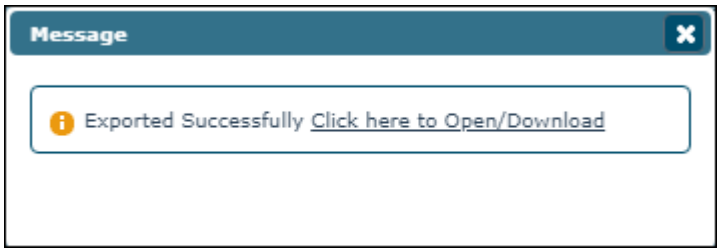
2. Select the checkbox next to each criterion and select **Include/Exclude** to include/exclude that particular criterion in the filtered report and date.

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.

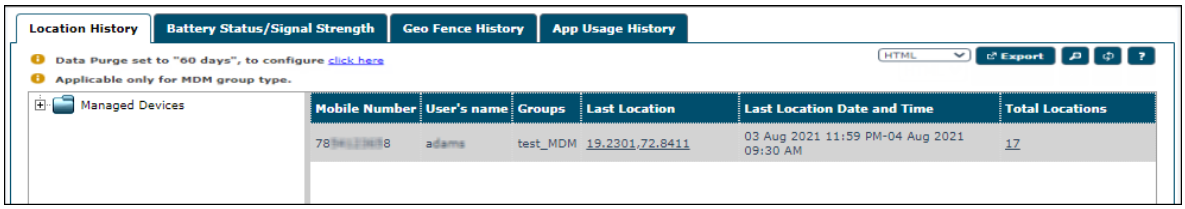
History

The History module consists following tabs:

- Location History
- Battery Status/Signal Strength
- Geo Fence History
- App Usage History

Location History

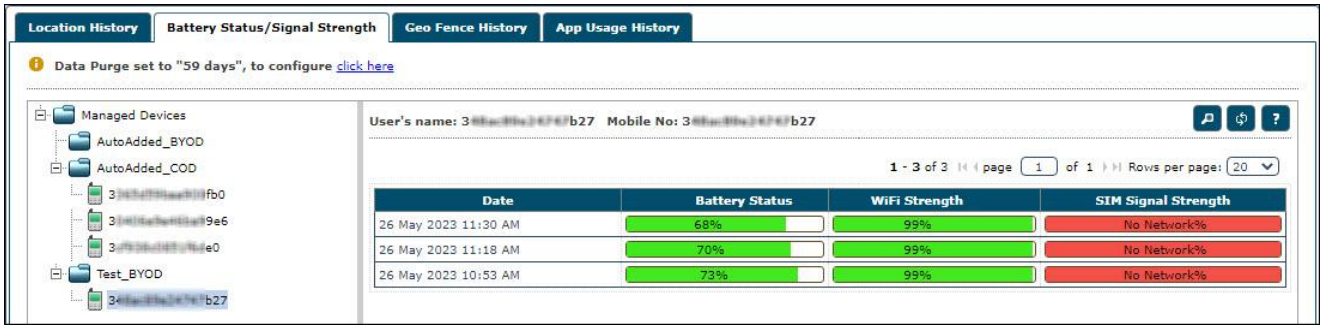
This tab displays the location details of all enrolled devices. It also displays the location where the device was last active and helps you track total number of locations where the device was active.



Column	Description
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

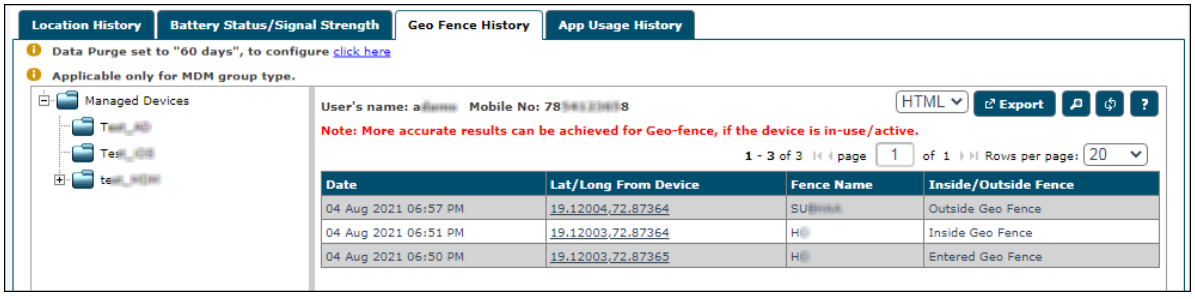
This tab displays the status of battery, Wi-Fi, and SIM signal strength of a device.



Column	Description
Date	This column displays the date.
Battery Status	This column displays the available battery on a device.
Wi-Fi Strength	This column displays the available Wi-Fi strength of a device.
SIM Signal Strength	This column displays the available SIM signal strength of a device.

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).

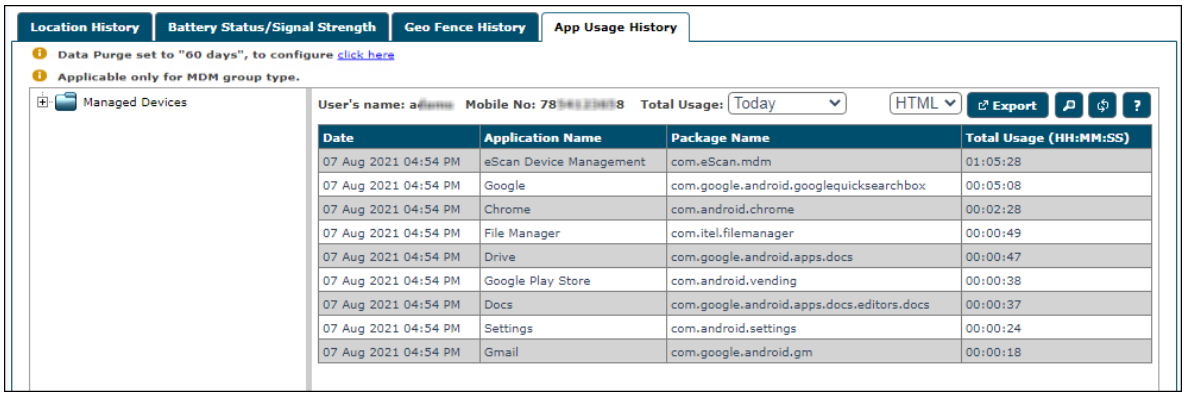


Column	Description
Date	This column displays the date.
Mobile Number	This column displays the mobile number of the device.
User's name	This column displays the user name of the device.
Last Visited Fence	This column displays the name of the last visited fence.
Status	This column displays the fencing 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.



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 been used.

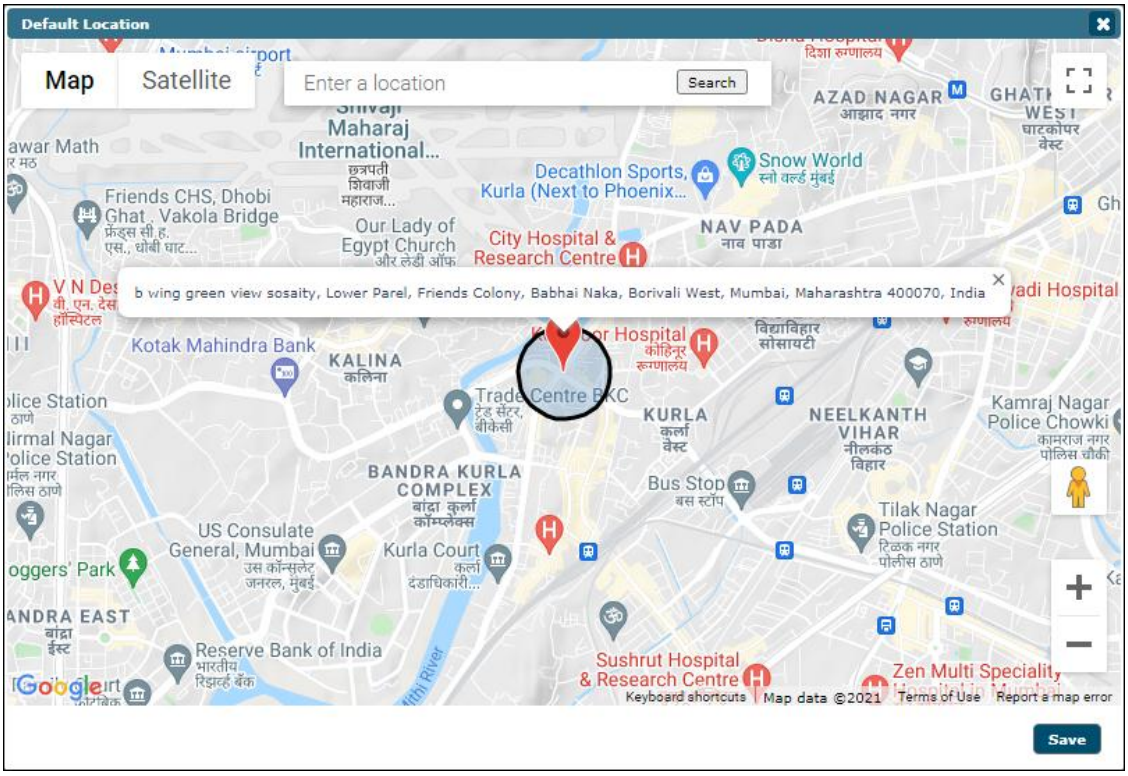
Fencing Location(s)

Geo-Fencing refers to drawing a virtual barrier around a location using a device's Global Positioning System (GPS) or Internet Protocol (IP) address. Technically, geo-fencing can be any size radius from a particular location, anywhere from 25m to 5000m in stretch. You can define an address on the map and set the radius around that address. If the device is in that region, the policy set by the administrator will be active on the device.

Creating a Fencing Location

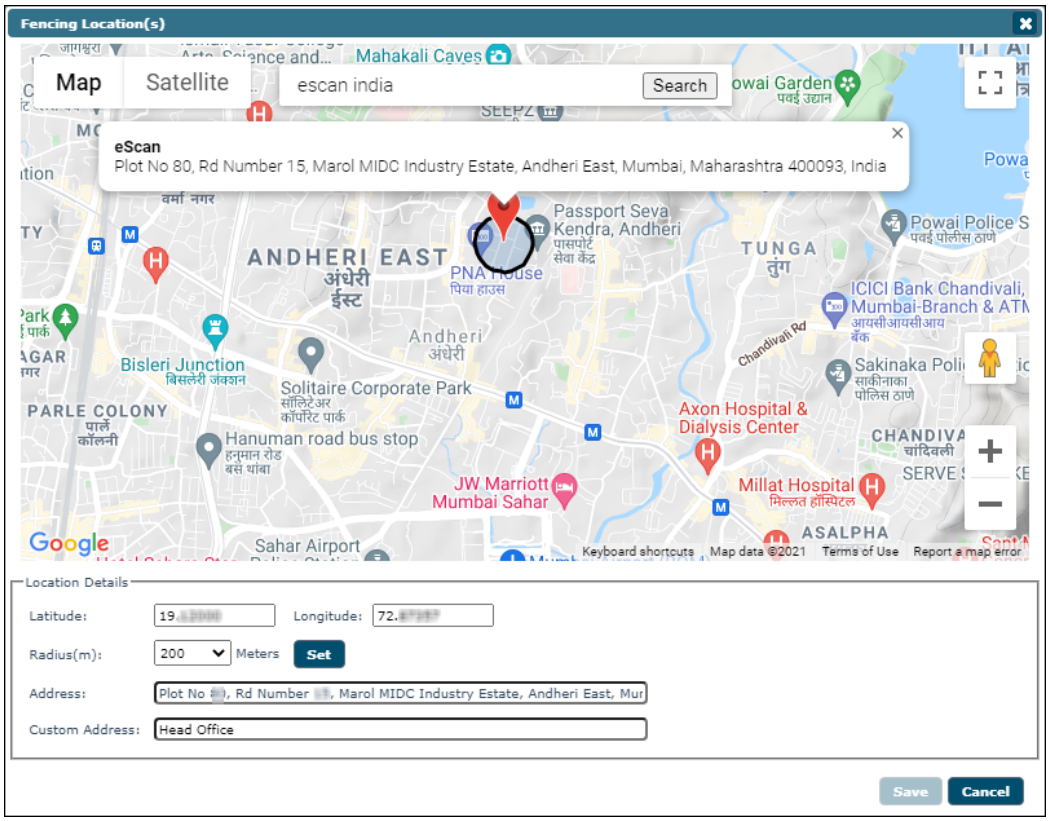
To create a Fencing Location, it is necessary that a default location must be set first.

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.

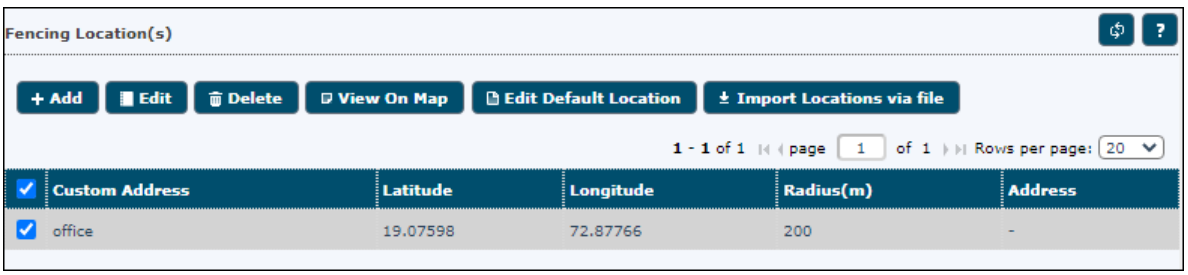


4. Enter the location and select the appropriate one from suggestions.
5. Click the **Radius** drop-down to select an appropriate radius and then click **Set**.
6. In the **Custom Address** field, enter a name for your fencing location.
7. After entering all the details, click **Save**.
   The default location will be saved.

Editing a Fencing Location

To edit a fencing location:

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

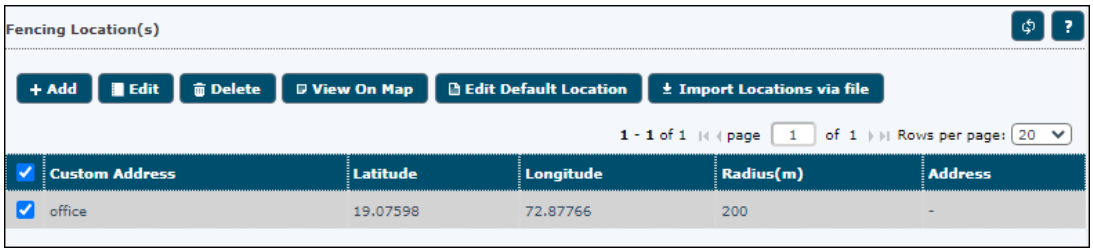


2. After making the necessary changes, click **Save**.
   The fencing location will be modified.

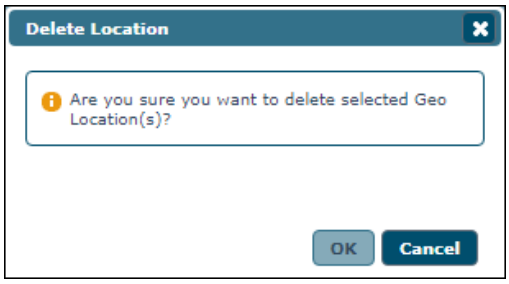
Deleting a Fencing Location

To delete a fencing location:

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



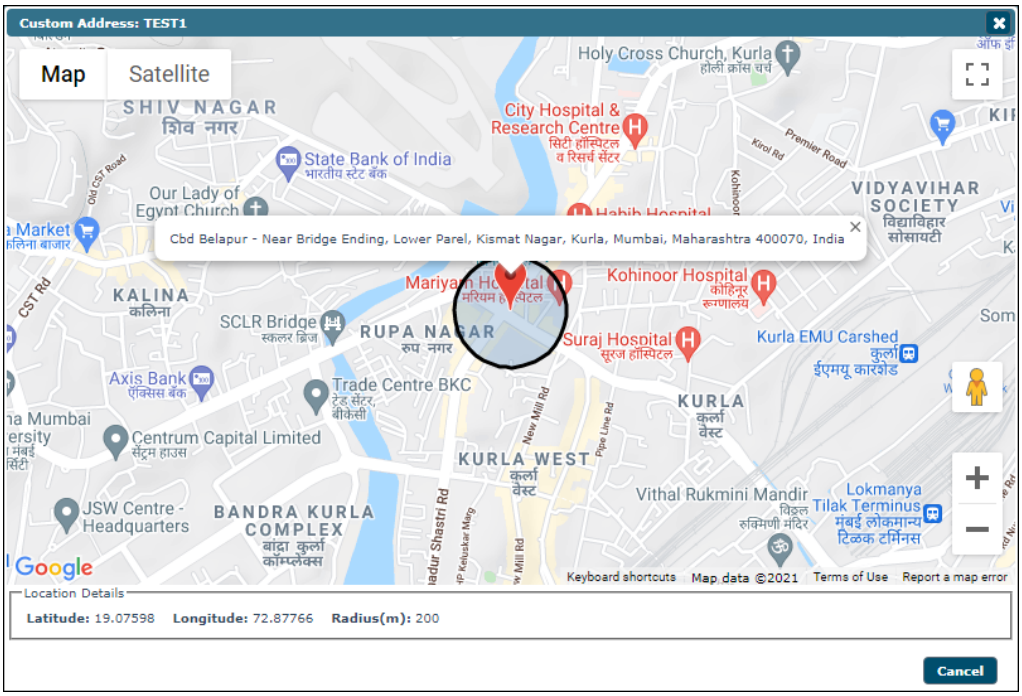
A confirmation prompt appears.



2. Click **OK**.
   The fencing location will be deleted.

View On Map

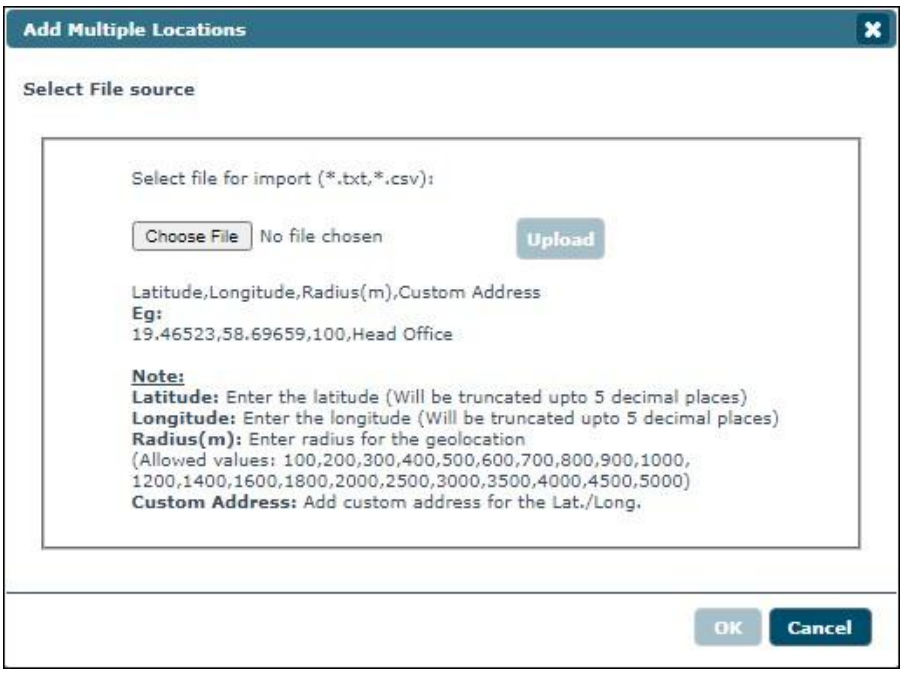
Clicking **View On Map** lets you view the selected location on the Google Maps.



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.



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

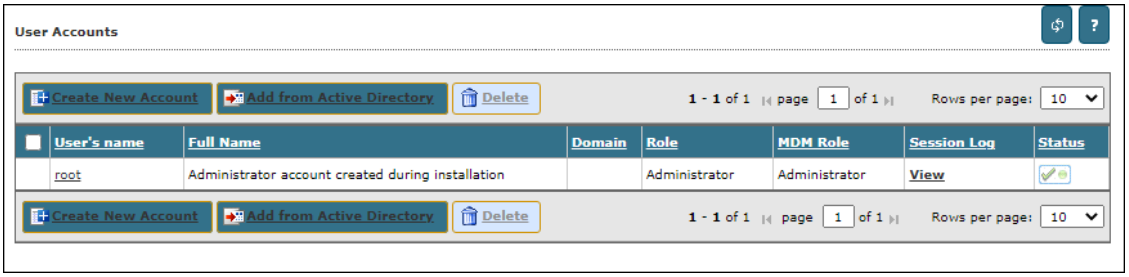
Administration

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

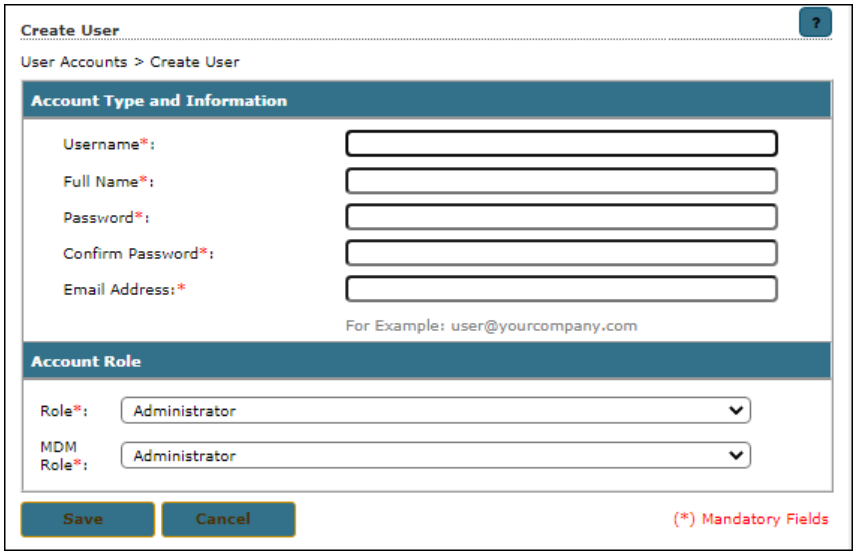
With User Accounts sub module, you can assign Administrator role to added users and reduce the workload. This sub module displays a list of users and their details such as Domain, Role, Session Log and Status and many more. You can create new user accounts and also add them from Active Directory.



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.

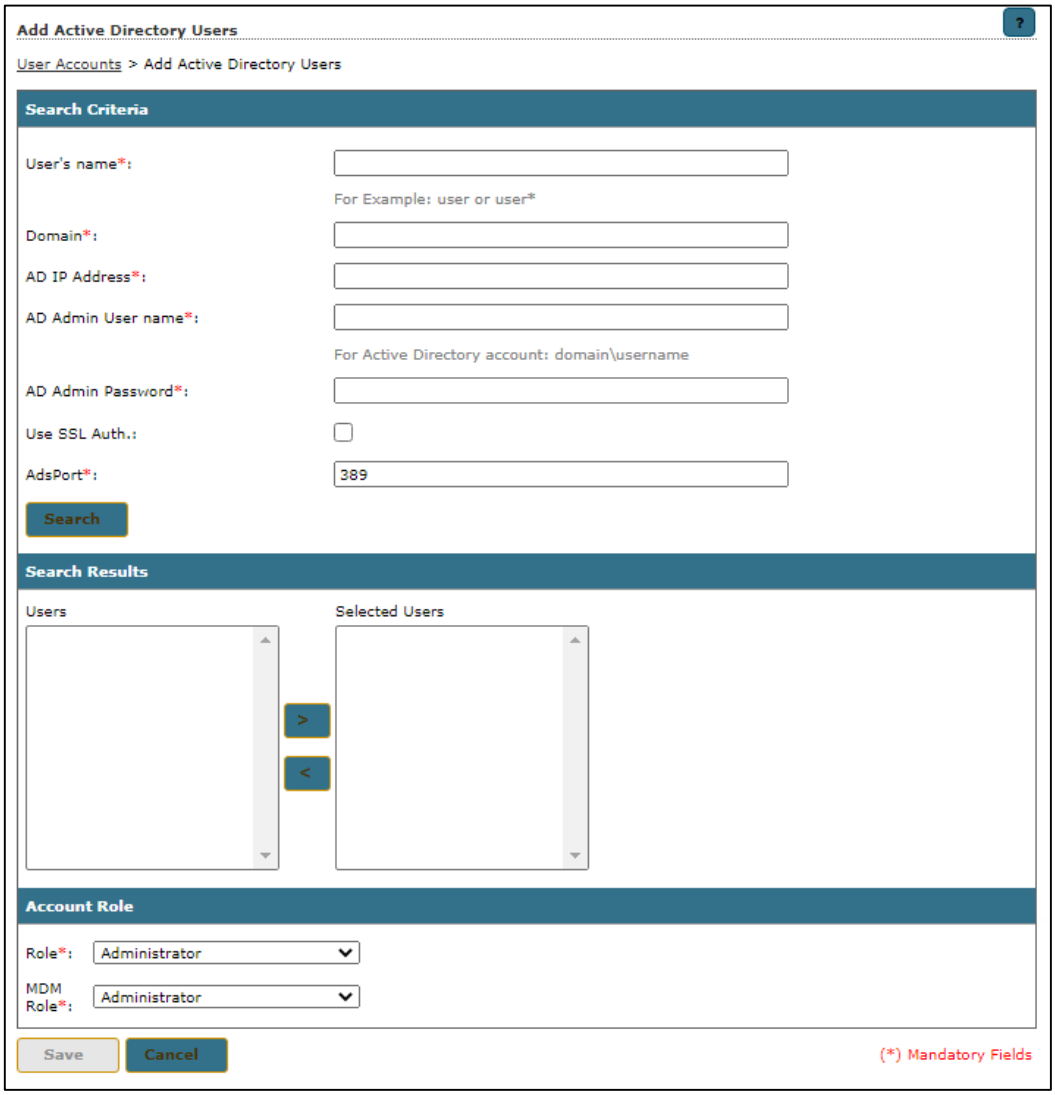


2. After filling all the details, click **Save**.
   The user will be added to the User Accounts list.

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.

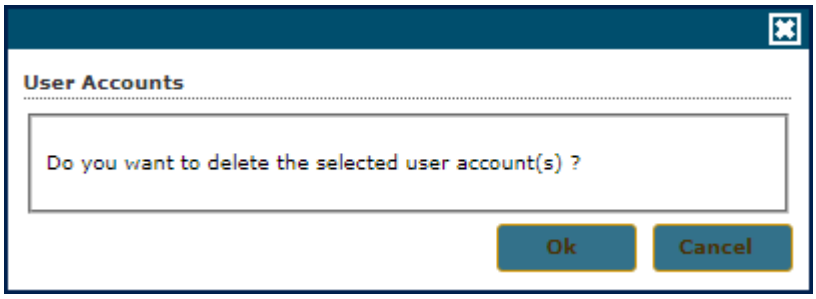


2. After filling **Search Criteria** section details, click **Search**.
3. A list of users will be displayed in the **Users** section.
4. Select a user and then click > button to add the user to **Selected Users** section.
5. Vice versa the added user can be moved from **Selected Users to Users** by clicking <.
6. Click **Save**.
   The user will be added to the User Accounts list.

Deleting a User Account

To delete a user account, follow the steps given below:

1. In the User Accounts screen, select a user and then click **Delete**.
   A confirmation prompt appears.

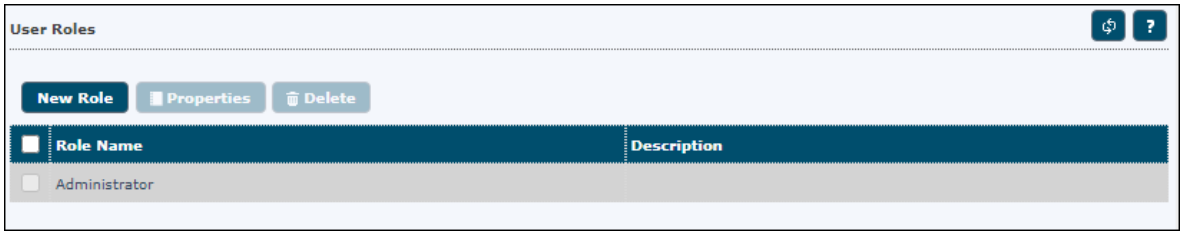


2. Click **OK**.
   The User Account will be deleted.

User Roles

The User Roles submodule lets you create a role and assign it to the User Accounts with variable permissions and rights as defined in the role being assigned to them. It can be an Administrator role with set of permissions and rights Group Admin Role or a Read only Role.

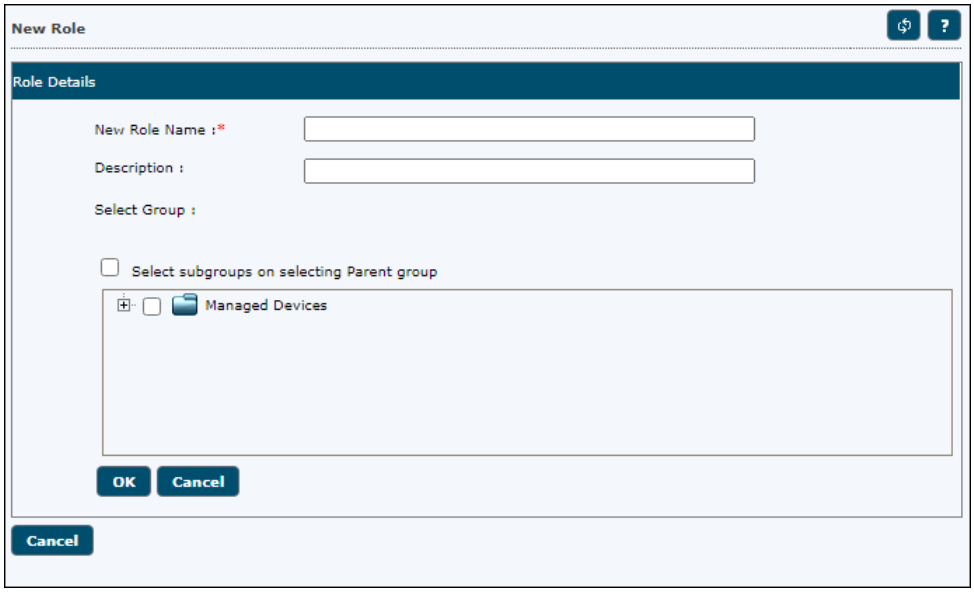
You can re-define the properties of the created role for configuring access to various section of eScan Mobility Management Console and the networked devices. It also lets you delete any existing role after the task is completed by them. It allows the administrator to give permission to subadministrators to access defined modules of eScan and perform installation/uninstallation of eScan on network devices or define policies and tasks for the devices.



Adding a User Role

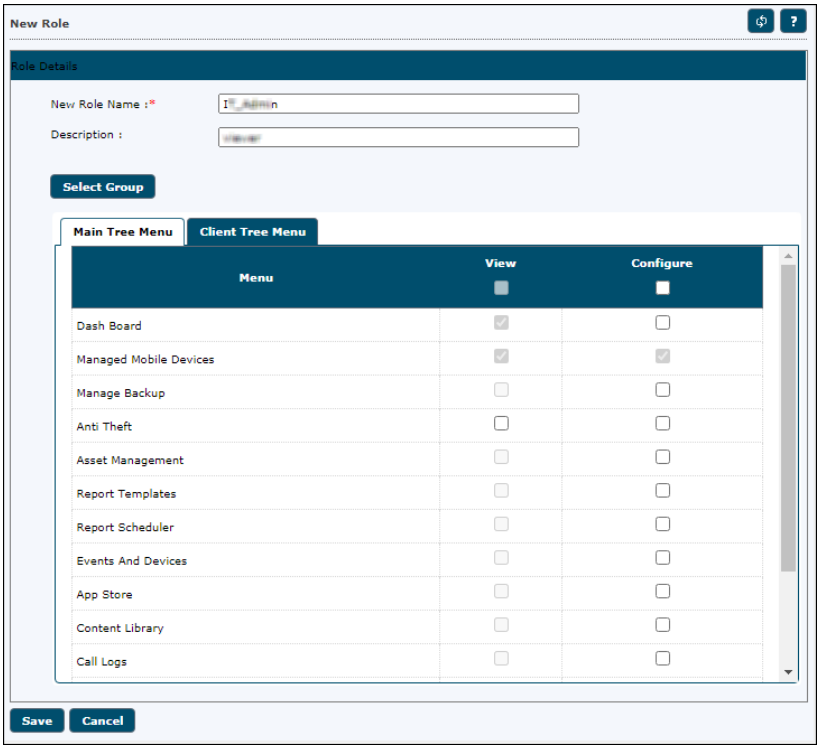
To add a new user role, follow the steps given below:

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

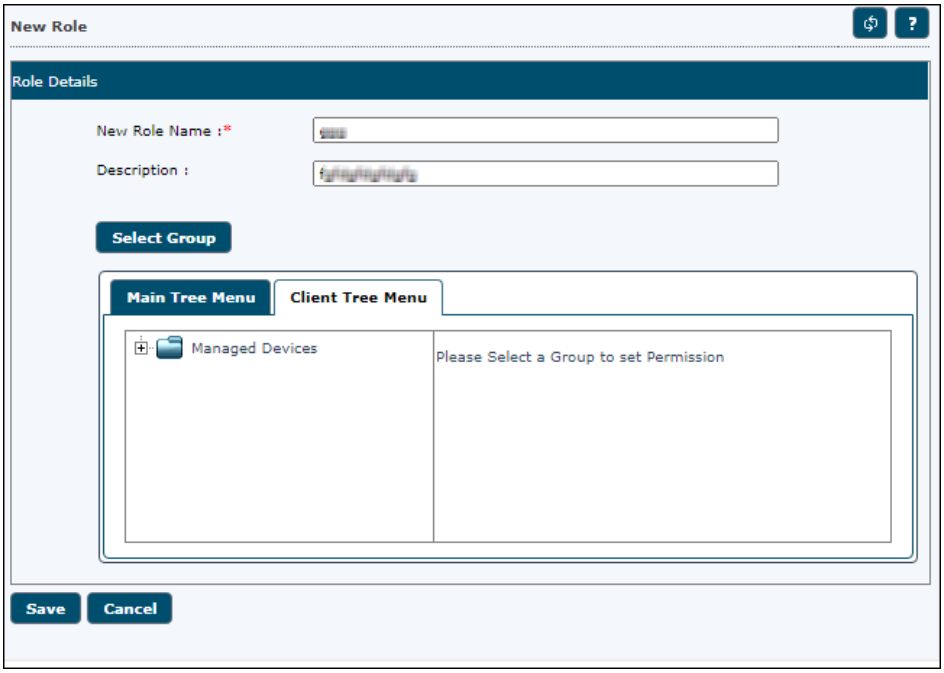


2. Enter name and description for the role.
3. Click **Managed Devices** and select the specific group to assign the role.
4. The added role will be able to manage and monitor only the selected group's activities.
5. Select the checkbox **Select subgroups on selecting parent group**, if you want to select 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.

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.

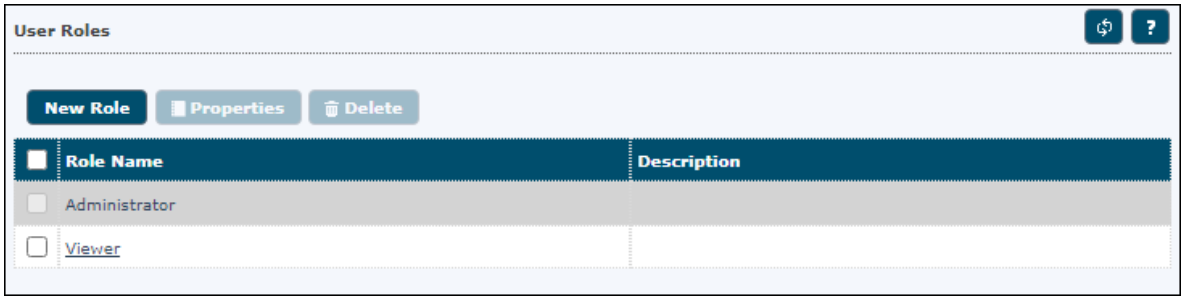


7. Select the checkboxes that will allow the role to view/configure the settings.
8. After selecting the necessary checkboxes, click **Save**.
   The role will be added to the User Roles list.

Role Properties

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

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



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.

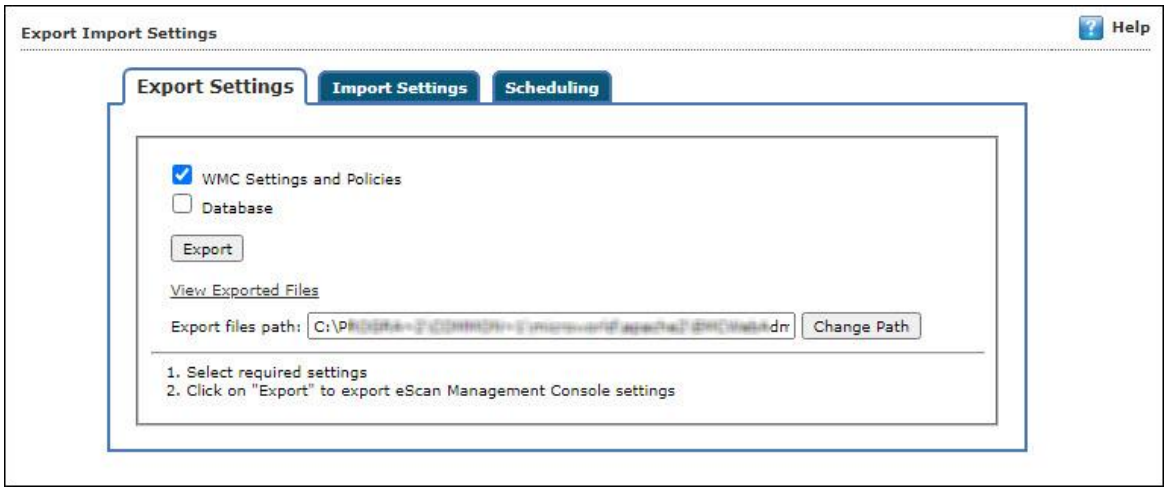
Export & Import

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.

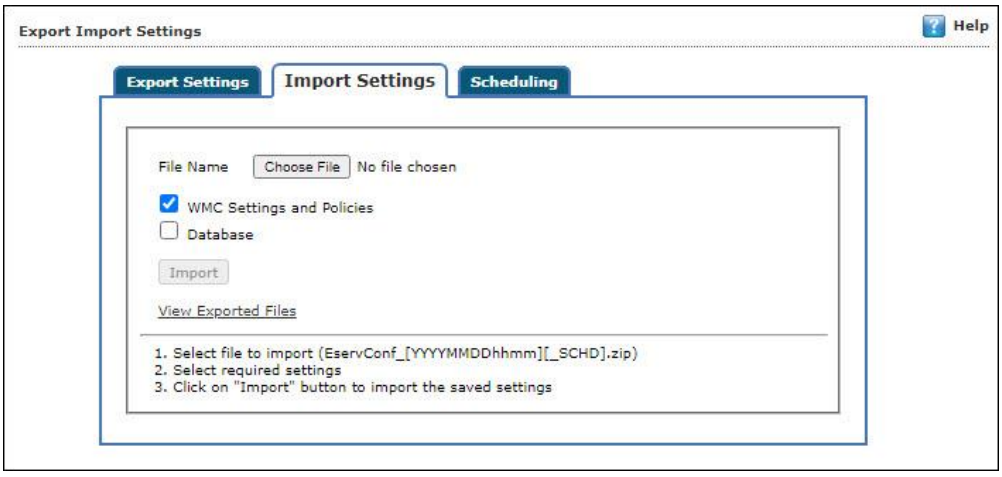


2. To backup **WMC Settings and Policies** and **Database**, select both the checkboxes.
   The backup file will be exported to the path shown in **Export files path** field. To change the file path, click **Change Path**. In the Add Folder window, enter the file path and click **Add**.
3. Click **Export**.
   The backup file will be exported to the destination path. A success message appears at the top displaying date, time, and a download link for the exported file.

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.

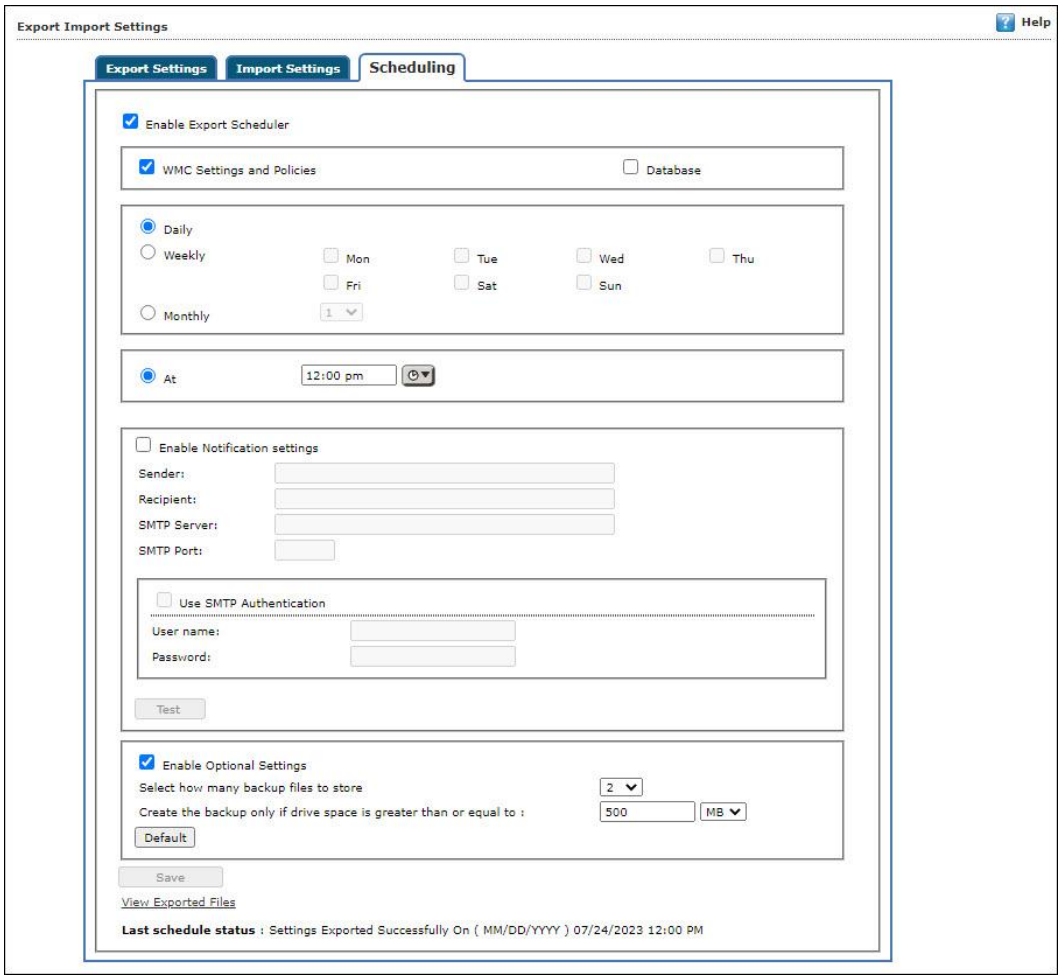


2. Click **Choose File**.
3. To import **WMC Settings and Policies** and **Database**, select both the checkboxes.
4. Click **Import**.
5. The backup file will be imported. A success message is displayed after complete import.

NOTE	• After successfully taking a backup, eScan asks you to restart the server. • The Import Settings tab lets you import only Settings and Policies or Database.

Scheduling

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

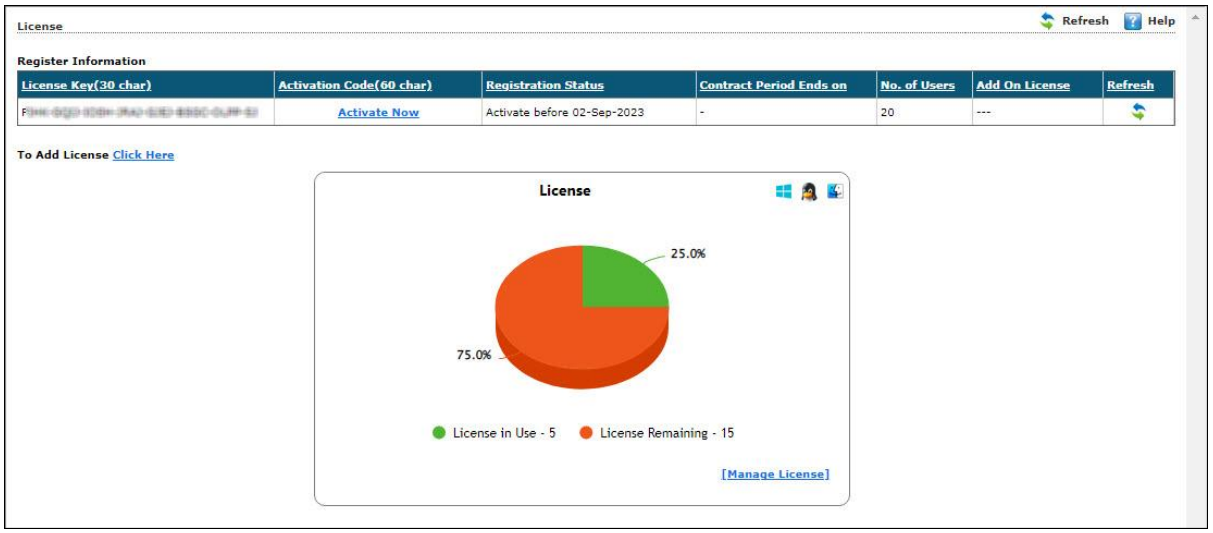


To create a Schedule for export, follow the steps given below:

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

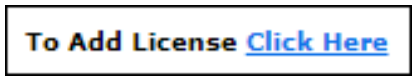
The License module lets you manage user licenses. You can add, activate, and view the total number of licenses available for deployment, previously deployed licenses and remaining licenses with their corresponding values. The module also lets you move the licensed devices to non-licensed devices and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



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.

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:

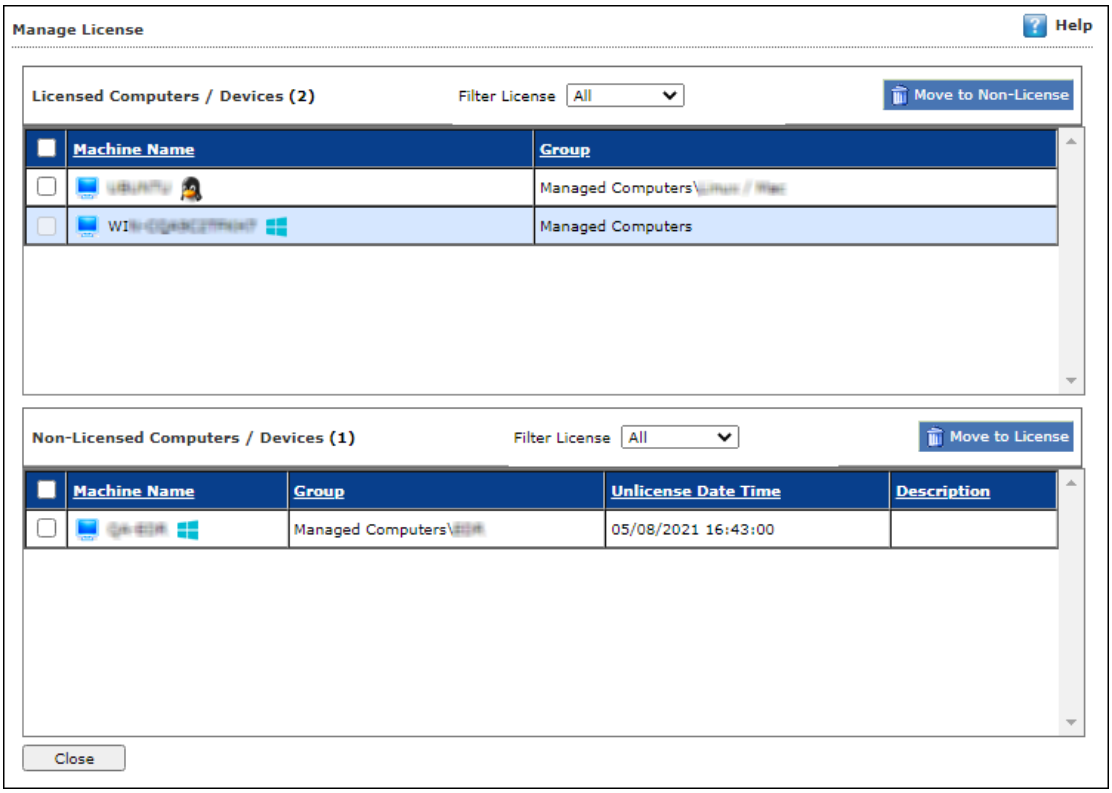
1. In the License statistics box, click **Manage License**.
   Manage License window appears.

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.



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**