Quick Heal®

Security Simplified

Seqrite Mobile Device Management

Administrator's Guide

Version 1.6

Copyright & License Information

Trademarks

Seqrite is a registered trademark of Quick Heal Technologies Ltd.

License Terms

Installation and usage of Seqrite Mobile Device Management is subject to user's unconditional acceptance of the Quick Heal end-user license terms and conditions.

To read the license terms, visit www.quickheal.com/eula and check the End-User License Agreement for your product.

About This Document

This manual covers all the information required to install and use Seqrite Mobile Device Management. The following table lists the conventions that we followed to prepare this manual.

Convention	Meaning
Bold Font	Anything highlighted in bold indicates that it is a menu title, window title, check box, drop-down menu, dialog, button names, hyperlinks, and so on.
	This is a symbol used for a note. Note supplements important points or highlights information related to the topic being discussed.
	This is a symbol used for a tip. Tip helps users to apply the techniques and procedures to achieve a task in an easy way.
	This is a symbol used for warning or caution. This is an advice either to avoid loss of data or damage to hardware.
<Step 1> <Step 2>	The instruction mentioned in the numbered list indicates actions that you need to perform.
You	Admin
User	Mobile, Tablet, or Phablet users
Entities	Users, departments, devices, groups, policy, configuration, and app configuration.
Company	The organization who have registered with Seqrite MDM.
Enable	To turn on the button or to access the feature and its sub-sections.

Document History

Release No	Change Date	Change Summary
1.6	September 2018	• Migrated to FCM from GCM for better communication with Android devices.

What's New in this Version?

Features	Description	Section
Firebase Cloud Messaging	Migrated to FCM from GCM for better communication with Android devices.	---

Contents

MDM Features for Android

Feature list for Android devices:

	Feature	Android
Features	**Enrollment**	
	Enrollment	✓
	Antivirus	
	Real-Time Protection, Scheduled Scan, Remote Scan, MDM App auto upgrade	✓
	Action on device	
	Sync, Locate, Scan, Block, Unblock, Exit Launcher, Fetch Logs, Locate & Trace, Reset Password, Broadcast Message, Push Fence Configuration, Disconnect, Uninstall, Call/SMS Monitoring	✓
	Ring	✓
	Wipe	✓
	Uninstall Protection	✓
Configuration	**Anti-Theft Configuration**	
	Notification on SIM change, Lock device on SIM Change, Lock device on Airplane Mode, Block device on SIM Change	✓
	Web Security configuration #	
	Browsing Protection, Phishing Protection, Web Protection, Blacklist/Whitelist URLs, Category Based blocking	✓
	Wi-Fi Configuration	
	Support different security options	✓
	Schedule Scan Configuration	
	Scheduling new Scan	✓
	Network Usage Configuration	
	Data usage monitoring for Wi-Fi, mobile data, and roaming	✓
Policy	**Policy**	
	Requires Password, Password Age, Device Autolock	✓
	Block USB Connection	✓
	Block Safe Mode	✓
	Block Camera	✓
	Restrict Factory Reset	✓
	Block Bluetooth	✓
	Restrict Bluetooth Configuration	✓
	Block Wi-Fi	✓
	Block Open Wi-Fi	✓
	Block Mobile Hotspot, Block NFC	✓
	Block Mobile Data while roaming, Block Auto-Sync while Roaming, Block Outgoing Call in Roaming, Location Service GPS, Sync Frequency	✓
	Block Certificate	✓
	Block Screen Capture	✓
	Block Text Copy and Paste	✓
	Block Pop-ups for Safari, Block Fraud Warnings for Safari, Accept Cookies for Safari	✓
	Block iTunes App	✓

	Feature	Android
	Block App Store	✓
	Set Google Account	✓
	Block Primary Microphone	✓
	Block Siri	
	Device Time-out	✓
	Set Auto Time Zone	✓
	Block the user to Switch Profile	✓
	Device Accessibility Service & App Usage	✓
	Block the user to Modify accounts	✓
	Block USB Debug Mode	✓
	Block App Control	✓
	Block the user to Add User Profile, Block the user to Delete User Profile	✓
	Block the user to Configure Network Setting	✓
	Block Outgoing Calls	✓
	Block Mount Physical Media	✓
	Wi-Fi On Sleep Mode	✓
	Block App Installation from Unknown Sources	✓
	Block Notification Area	✓
	Block Cellular Data	✓
	Block Mock Location	✓
	Block Outgoing MMS and SMS	✓
	Block Airplane Mode	✓
App Management	**App Management**	
	Restrict access to newly installed apps	✓
	Whitelist App	✓
	Recommend app to install, Apps to Uninstall	✓
	Fully Block the blacklisted apps	✓
	App Repository	✓
	Individual Device Level App control	✓
	App blocking based on Category	✓
Other	**Fencing**	
	Geo, Time, Wi-Fi Fence	✓
	App Launcher	
	Advance Launcher, Exit Launcher, App Request	✓
	Broadcast Message	
	Broadcast message	✓

* MDM manages these devices using native OS level support. You may not need to install agent or client software on these devices. MDM supports Android 4.4 and later versions.

Chapter 1

Introducing Seqrite Mobile Device Management

In the present era, organizations are providing smartphones, tablets, and handheld devices to their employees for better communication and enhanced productivity. In such a scenario, to secure and monitor such mobile devices, we have a one-stop-solution called Seqrite Mobile Device Management (MDM). Using the Seqrite MDM console, the administrator of an organization can remotely monitor, secure, manage, and track all types of mobile devices thereby reducing the risk of losing corporate data. It also helps in ensuring that all the employees follow the information security policies of using mobile devices.

This chapter includes:

Seqrite MDM allows the administrator to configure settings remotely on one or many devices at the same time.

In case the mobile devices are lost or stolen, the organizations are always at the risk of business data misuse or loss. Seqrite MDM helps the organizations to block the stolen or lost devices, prevent data pilferage by wiping the data from the device, and trace the device location to help recover the devices.

Benefits of Seqrite MDM

- Secure and manage all the Android devices.
- Secure data and resources, enhance user productivity, reduce costs, and maintain communications.
- Perform portal administration functions.
- Monitor the device usage via policy and configurations.
- Make devices compliant with policies.
- Monitor network data usage and Call/SMS.

- Manage device app via App Configuration.
- Prevent misuse of the device by launching Seqrite Launcher.
- Monitor the device by applying fencing parameters such as time, location, and Wi-Fi.
- Generate the customized report as per your requirement.
- Ability to take remote access of enrolled mobile device

How does Seqrite MDM work?

Seqrite Mobile Device Management (Seqrite MDM) works on the Client-Server architecture where the console (Hosted on Cloud) manages all the mobile devices. The client agents can be installed on almost all the flavors of mobile platforms (Android, iOS). For a detailed description of console and client agent system requirements and compatibilities, see System requirements. Seqrite MDM Admin gets full control of the device in order to manage, monitor, or track the device.

Seqrite MDM helps the Admin to deploy and enroll Seqrite MDM client on the mobile device over the air. Seqrite MDM apply certain policies and configurations (App Configuration, Web Security Configuration, Anti-theft, Network Data usage, fence Configuration, etc.) on the device. Seqrite MDM client act on the device silently and apply most of the restrictions without user intervention. Seqrite MDM client is having built-in antivirus, which keeps the devices safe from any virus attack.

Chapter 2

Getting started

To install Seqrite Mobile Device Management, ensure that you comply with the following requirements:

Prerequisites

Before installing Seqrite Mobile Device Management on your computer, follow these guidelines:

- Device must be connected to the Internet via any network (Mobile data/Wi-Fi).

System requirements

To use Seqrite Mobile Device Management, you must ensure the following requirements.

Mobile device specifications	Android version 4.4 and later.
Browser requirements	Administrator Web panel, IE 9+, Firefox 10+, Opera 10+, Google Chrome (latest versions,) and Safari (latest versions)
Terminology	**User**: An employee who enrolled the device with MDM.
	Administrator: A user with access to the MDM portal to manage the devices.

To check for the latest system requirements, visit our website at www.quickheal.com.

Chapter 3

Registration

You must register your product soon after installing it.

This chapter includes the following sections.

Registration

The registered MDM user can avail of all the features of Seqrite MDM. You must register your company with the Seqrite MDM portal.

Registering with Seqrite MDM

To register with the Seqrite MDM portal, follow these steps:

1. Access the following URL: https://cloud.mdm.seqrite.com/
2. On the Sign In page, click **Register Company**.

   The Register Company page appears.

   Note:

   If you have already registered, then enter the Username and Password. If you have forgotten your password, click **Forgot Password**. Enter your email address and security code and click **Submit**. An email with a reset password link is sent to the registered email address to reset the password.

3. On the Registration page, enter the **Contact Information**, **Company Information**, and **Verification Code** in the corresponding text boxes.
4. Select the **I have read and accept the Terms and Agreement** check box and click **Submit**.

   After verification of your request by our corporate sales executive, you will receive a confirmation email from Seqrite MDM, which includes the product key and **Sign Up** link.
5. In the confirmation email, click the **Sign Up** link.

   Sign Up page is displayed.

6. On the Sign Up page, enter your personal information, **Security Code**, and **Product Key**.

   For product key, check your registered email.

7. Click **Create a new account**.

   A success message is displayed if the Sign Up process is successful.

   You will receive a confirmation link on your registered email to set the password.

8. Click the link given in the confirmation email to navigate to the Set Password page.

9. On the Set Password page, enter the **Password**, **Confirm Password**, and **Security Code**.

   A password should have at least one number, one special character, one upper case character, and one lower case character.

10. Click **Submit**.

    Password is set successfully.

    - If you wish to reset the password, click **Reset Password**.

      An email with instructions to reset the password is sent to your registered email address.

    - To log on to the Seqrite MDM portal using your registered email address and the password, click **Go back to Login page**.

Chapter 4

Dashboard

Dashboard is the default screen that is displayed after you log on to the Seqrite Mobile Device Management (MDM) portal. Dashboard is unique and helps to navigate easily to all the components of the Seqrite MDM portal.

This chapter includes the following sections.

The Seqrite MDM dashboard is divided into various sections as follows:

- **Notifications**: The upper-right section of the Seqrite MDM portal shows various types of notifications.
- **PROFILE**: The PROFILE section shows information about the logged-in user. This section allows the user to reset the password of Seqrite MDM, edit the information of logged-in user, and also provides log out option.
- **Global search**: Provides a common option to search all the Seqrite MDM entities (user, department, device, group, policy, configuration, app configuration, and IMEI number of the device) from any page of the MDM portal. You can search by entering any keywords related to the entities. Global search option is available on all the pages of the Seqrite MDM portal.
- **Menus**: The left vertical section of Seqrite MDM portal includes menus, which helps the user to navigate to the different sections of Seqrite MDM. The menus include Manage, Profiles, Apps, Fencing, Reports, and Admin.
- **Dashboard center**: The middle section of dashboard displays different statuses, which are showed in the form of tiles, graphs, and count.

- **Informative section**: The lower section of Seqrite MDM portal provides many important and useful links such as Support, Privacy Policy, License Agreement, Share Feedback, and release notes for the current Seqrite MDM version.

Notifications

In Notifications section, all the notifications can be viewed, marked as read, and they can be cleared. Seqrite MDM provides different types of notifications as follows:

Notification type	Description
Enrollment notification	These are device enrollment notifications.
App request notification	These are the requests to install an app on the device via App Launcher.
Device notifications	These notifications include device infection notifications and non-compliance notifications.
Import notification	These notifications are received when an import of any item is initiated or completed.

PROFILE

The Profile section on the upper-right corner of dashboard shows the user name and the lock sign. This section gives information about the logged-in user and allows to edit the user profile. The Profile section shows the following information:

Profile sections	Description
Name and email ID	Shows the name and email ID of logged-in user.
Edit	Helps to edit the user details such as user name, contact details, department, and privileges. Also, allows to edit the enrolled devices of the user.
Change Password	With this option, the Amin gets the privilege to reset the password to access the Seqrite MDM portal.
Sign Out	Helps to log out of Seqrite MDM portal.

Menus

Menus direct you to the different features of Seqrite MDM portal. Menus include:

Menus	Description
Manage	Manage menu provide options to manage different users, departments, devices, groups, and user roles.

Profiles	Profiles allows you to apply policies and configurations to groups and devices.
Apps	With Apps, you can create an app repository and app configurations for the devices.
Fencing	This menu restricts the devices and app usage with the help of digital fence. The Admin can configure and apply the fence on different groups.
Reports	Provides reports of all the activities carried out on Seqrite MDM. Standard reports for infection status, network data usage, and app-compliance report can be generated. The Admin can also create a customized report as per requirement.
Admin	This section allows the Admin to edit the setup services, configure MDM and Launcher upgrade settings, search activity and action logs, edit company settings and Launcher wallpaper, and view license details.

Dashboard Center

The middle section of dashboard includes the following sections:

Section	Description
License status	Displays the license status of Seqrite MDM. It informs about trial version expiry date, license expiry, and remaining license expiry days.
Devices	Shows the number of devices added to the Seqrite MDM portal.
Rooted	Displays the number of enrolled devices that are rooted.
Uninstallation Unsecure	Displays the number of devices whose Device Administrator check for MDM App has been removed. These devices are vulnerable to MDM app uninstallation (that is - any user can uninstall the MDM Client App from these devices).
Blocked	Displays the count of the devices that are blocked by Seqrite MDM.
Enrollment Status	The chart displays the statuses of the devices, which are added to the Seqrite MDM portal. Mouse hover over the chart shows the device enrollment statuses, which includes; Inactive, Pending, Approval Pending, Approved, Disapproved, and Uninstalled. • To view the devices with particular status, click that status on the chart. You will navigate to the Devices page, where you can view the devices and enrollment details. • To view all the details of the devices, click **View details**.

Section	Description
Device Connected Since	Displays the total number of devices that are connected to the Seqrite MDM server in a particular period. Mouse hover over the chart will show the defined time by the Seqrite MDM portal. The defined time options are Today, Last 7 days, Last 15 days, Last 30 days, not connected, and Before 30 days. • Click a particular time period on the chart to navigate to the Devices page, where a list of the devices enrolled in that particular period is displayed. • To view all the details of the devices, click **View Details**.
Violation Status	Displays the status and number of the devices that have violated the restrictions applied. Mouse hover over the chart will show the violation statuses. This violation report includes the devices which were listed under Policy Non Compliant, Configuration Non Compliant, App Control Non Compliant, Launcher Non Compliant, and Device Communication Non Compliant. If the devices have violated any of the above-listed restrictions, then the devices will be listed on the chart. • Click the particular violation on the chart to navigate to the Manage Devices page, where a list of the devices which violated the restriction is displayed. • To view all the details of the devices, click **View Details**.
Infection Status	Displays the graph statistics of virus infections detected on the devices, which are enrolled with the Seqrite MDM portal. Mouse hover over the graph shows the names of the viruses detected, the number of devices infected on a particular date and a link to view the details. This shows the status of infection for the devices that were added to the MDM network in the last 30 days. • You can view the entire infection details on the Infection Status Details page. To view the infection details, hover over the graph tips and click the **View Details** link**.** • **Infection Status Details page**: Lets you view the details of the infection status and affected devices on a particular day. The Infection Status details include: Id, Device Name, Threat Names, Date, and Device Status. You can also view the number of viruses detected, the number of virus types, and the number of infected devices on a particular date.
Top Threats	Displays the list of threats, which have affected the large number of devices and the count of the affected devices.

Section	Description
Network Usage Status	The graph displays the status of the network usage for all the devices enrolled with the Seqrite MDM portal. The network usage is displayed with respect to Wi-Fi, mobile data, and roaming. The bar graph displays a date-wise Internet data usage of all the devices. To view the network usage date-wise, you can use the following options: Today, Last 7 days, Last 30 days, Last 15 days, and current month.  Tip: If **Today** is selected, the data consumed in each hour for the last 24 hours is displayed. This bar graph shows the data used for a selected time.
Top Network Usage Devices	Displays the list of the devices that consume more network data. You can view the name of the device and the data used by the device. • To view the Reports page, click **View Details.** The report shows Internet usage of the devices with respect to Wi-Fi, mobile data, and in roaming status.
Top Network Usage Apps	Displays the list of the apps that are network-intensive and consume more network bandwidth. You can view the name of the app and the data used by that app. • To view the Reports page, click **View Details**. The report shows the network usage of apps with respect to Wi-Fi, mobile data, and in roaming status.
Top Installed Apps	Displays the list of the applications that are downloaded and installed by most of the users. You can view the name, category of the app, and the count of the devices on which the app is installed. • To exclude the recommended standard apps, select the **Exclude recommended apps** check box on the right side of Top Installed Apps section. • To view the App Repository page and view all the installed apps within the MDM network, click **View Details.**

In addition, there are few buttons available on the upper section of dashboard to navigate directly to the dashboard sections:

Buttons	Description
Overview	Helps to navigate directly to the upper section of dashboard.
Infection Status	Helps to navigate to the Infection Status section of dashboard.
Network Usage	Helps to navigate to the Network Usage section of dashboard.

Informative Section

In the lower section of the portal on the task bar, different informative section links are provided as follows:

Section	Description
Support	Shows options to contact Seqrite and get all the available support.
Privacy Policy	Displays privacy policy of Seqrite MDM.
License Agreement	Shows the end-user license agreement.
Share Feedback	The Seqrite MDM Admin can provide their valuable feedback about Seqrite MDM.
Release Notes	Shows the release notes of the current Seqrite MDM version.

Common UI Terminologies

On all the pages of Seqrite MDM portal, few common field and buttons are available. The table below gives information on common UI terminologies:

UI terminology	Description
Global search	Helps to search the entities from any part of MDM portal.
Search	Helps to search an entity by entering particular keywords as per your requirement. When you search anything from Users and Devices list page, make sure the respective column is available on the list page. Tip: To search the users or devices according to the mobile number, make sure that the mobile number column is visible on the respective list pages. If the column is not present, then the search for mobile number will not reveal the correct result. To get the relevant result, you should select the mobile number column from Filter columns list.
View	This list helps to select and view the number of records per page. Click inside the list and select the number of records to be viewed in single instance.
Add	The Add button is available on all the pages of the modules. With the help of the Add button, you can add the required entity to the Seqrite MDM portal. This button is also available on the Details page of all the components of the Seqrite MDM portal.

UI terminology	Description
Import	Use the Import option to import the entities to the Seqrite MDM portal. This option is helpful if you have a long list of entities or if you have exported the entities from the Seqrite MDM portal earlier. This button is available on all the list pages of the components of the Seqrite MDM portal. • You can import entities from Manage section, Policies, and Geo Fence. • Select the .csv file from the location. To view the sample .csv file format, click **Download CSV sample Format**. Only .csv file format is supported. In case of importing the policy, only .xls file format is supported. Ensure to check dependencies before creating the new policies.
Export	With the Export option, you can export the entities from the Seqrite MDM portal. This option is helpful if you have to export the long list of entities registered with the Seqrite MDM portal and want to retain them. You can import the other entities back to Seqrite MDM easily whenever you require. This button is available on all the list pages of the components of the Seqrite MDM portal.
Filter columns	The Filter columns tab is available on all the list pages of Seqrite MDM portal. Seqrite MDM provides an option to filter the table columns and to choose the desired columns on the list page. • The Users and Devices list page tables have a limitation to choose the columns. On Users list page, you can select up to 4 columns and on Devices list page, you can select up to 8 columns only. • The Standard reports and activity logs section do not show the Filter columns option. To filter the columns, follow these steps: 1. To filter any columns from the list page, click **Filter column**. The list of available columns with check boxes is displayed. 2. Select the desired column name check box which is to be displayed in the table. Or clear the check box of the column which is not to be displayed on the list page table.
Previous	This button is available on the Overview pages of few modules. This button helps to go back to the previous entity and view the details of the previous entity.

UI terminology	Description
Next	This button is available on many Overview pages of the modules. This button helps to proceed to the next entity and view the details of the next entity. For example, if you are on the Overview page of User 1 and click the Next button, you are directed to the Overview page of User 2.
Pagination	Helps to navigate easily through the huge number of records.
Sort icon 	Every table column on Seqrite MDM portal has the following sorting icon. With this icon, you can organize the column data in ascending or descending order.
With selected	On selecting single or multiple entities on any list pages, the With selected option is displayed. The With selected list provides multiple options according to the entities.

Chapter 5

Notifications

Seqrite MDM portal offers different types of notifications, which are received and displayed on the upper-right section of the title bar. Notifications inform you about all the actions that have taken place on the MDM account and device status. The number on the Notification icon shows the count of newly received notifications.

This chapter includes the following sections.

Notifications Dialog

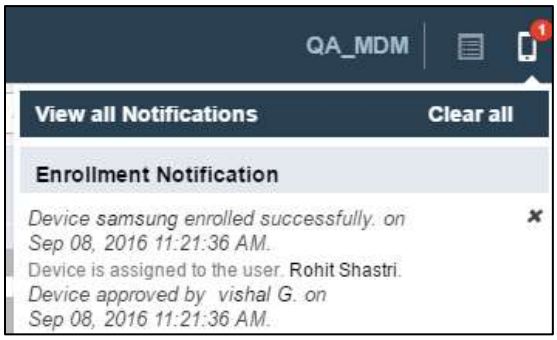

Figure 1

As you click any notification icon, a notification dialog appears, see Figure 1. The notification dialog shows few of the newly received notifications with the description and date and time when the notification was received.

The notifications dialog shows the following options:

Options	Description
View all Notifications	This option when clicked, navigates you to that specific notifications list page where all the notifications are displayed.
Clear all	With this option all the notifications from the notification dialog are cleared. If notifications are not available or are cleared, the notification dialog will show “You have no notifications.”
Mark as read (multiplication sign)	When the multiplication sign is clicked, that notification is marked as read and is removed from the notification dialog. All the notifications Marked as read are added to the notifications list page.

Notifications List Page

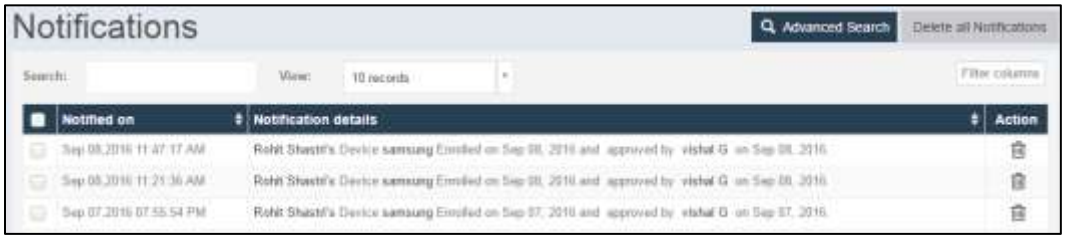

Figure 2

When you click the View all Notifications link on notifications dialog, you are directed to the notifications list page, see Figure 2. Seqrite MDM have different types of notifications and the list page format for all the types of notification is similar. The Notifications list page shows all the available notifications for the specific type of notification. The notifications table shows the following information about the specific notification type:

Columns	Description
Notified on	Shows when the notification was received.
Notification details	Shows the details of the notification.
Action	Delete is the available action for all the individual notifications.

Advanced Search for Notifications

Advanced Search option is available on all the notifications page, which allows you to search the notifications.

Searching notifications

To search the notifications, follow these steps:

1. Log on to the Seqrite MDM portal and click any of the notifications icon.
2. In the notifications dialog, click **View all Notifications**.
3. On the Notifications page, click **Advanced Search**.

   Notifications can be searched using the following parameters:

   - **Select limit from**: Select the limit to view the notifications for a particular period. The available options are Today, Since Yesterday, Last 7 days, Last 30 days, Last 3 months, Last 6 months, and Last 1 year.
   - **Select Notification Type**: Search by selecting the type of notifications such as Enrollment Notification, Device Notification, Info Notification, and App Request Notification.
   - **Select Report Type**: Search by selecting the type of the report.

     Note:

     The Report Type option is available only on the Device Notifications page.

4. Click **Search** to view the results related to the selected search criteria.

   The search result is displayed.

With selected Options for Notifications

All the types of Notifications list pages show the With selected option. This option is visible when you select single or multiple notifications. The available option in the With selected list is:

- **Delete**: Helps to delete single or multiple selected notifications.

Using With selected option for notifications

To use the With selected option for notifications, follow these steps:

1. Log on to the Seqrite MDM portal and click any of the notifications icon.
2. In the notification dialog, click **View all Notifications**.

   Notifications list page is displayed.

3. Select a single or multiple notifications check boxes which are to be deleted.

   The With selected option is displayed.

4. From the With selected list, select **Delete** and then click **Submit**.

   The selected action is carried out on single or multiple selected notifications.

App Request Notifications

The Note icon on the upper-right side of the task bar indicates app request notifications. The notification dialog shows all the notification requests that the device user has sent from App Launcher. The Admin receives a notification whenever the device user requests to install an app on the device via App Launcher. You can accept or reject the app request sent by the device user. To know more about the Launcher, see Seqrite Launcher.

Viewing app request notifications

To view the app request notifications, follow these steps:

1. Log on to the Seqrite MDM portal and click **App Request Notification** (Note icon).
2. In the App Request Notification dialog, click **View All App Requests**.

   The Notifications page is displayed with a list of App Request Notifications.
3. To view the details of the selected app request notification, click **View Details** on the App request notification.

   The Device App Request notification is displayed.

Device app request report

This report provides the details of all the app requests received and the number of pending app requests. You can select the app request from the list and approve or reject the request. When rejecting the app request, you must mention the reason for rejection.

Rejecting the app request

To reject the app request, select the request and click **Reject**. Enter the rejection reason and then click **Reject**.

Device Accessibility Notification

The mobile icon on the upper-right side of the task bar indicates device accessibility notifications. This notifications informs about the disconnected/disabled of accessibility service of Seqrite MDM/Launcher. If this notification is viewed, then the accessibility services on the device would not be working as expected, that is, the web security and app control functionality would not be functioning.

- To rectify this problem, you should contact the device user to enable the accessibility service, if already ON, then ask the device user to turn OFF the device and again turn it ON. If this problem still persists, then ask the device user to restart the device.
- Even after restarting the device, if the problem sustains, then re-enroll the device.
- If the issue is resolved, then you need to close this notification.

Enrollment Notifications

The mobile icon on the upper-right side of the task bar indicates enrollment notifications. The enrollment notifications dialog shows few newly received device enrollment notifications. It lists all the notifications related to the device enrollment. These notifications include the status of the device enrollment such as; Approval, Approval Pending and time and date of the device enrollment. You can approve or disapprove the device enrollment directly via enrollment notifications.

When the device enrollment request is approved by clicking the **Approved** option on the notification dialog, the approval command is sent to the device.

Viewing enrollment notifications

To view the enrollment notifications, follow these steps:

1. Log on to the Seqrite MDM portal and click **Enrollment Notification** (mobile icon).
2. On the enrollment notification dialog, click the **View all Notifications** link.

   The enrollment notifications list page is displayed.

Disapproving device enrollment request

When the device enrollment request is disapproved, the MDM client app will be uninstalled from the device. You can directly disapprove the device enrollment request from the notifications section or send an SMS to disapprove the device enrollment.

To disapprove the device enrollment request, follow these steps:

1. Log on to the Seqrite MDM portal and click **Enrollment Notification** (mobile icon).
2. On the enrollment notification dialog, the requested enrollment notification will show Approve and Disapprove options.
3. Click the **Disapprove** option.

   The Confirmation to disapprove the device dialog is displayed.
4. In the confirmation dialog, click **Disapprove**.

   A check box **Disapprove device by sending SMS** is available on the confirmation screen. If mobile number of the device is not available, then this check box will be dimmed. When the mobile number of the device is available, then you can send the device disapproval via SMS also.

Device Notifications

The bell icon on the upper-right side of the task bar indicates the device notifications. The device notifications dialog shows few newly received notifications related to the device reports. The device notifications include infection notifications and non-compliance notifications. Each

device notification will show a View Report link. When the View Report link is clicked, a complete summary of the device infection or non-compliance is displayed.

Viewing device notifications

To view the device notifications, follow these steps:

1. Log on to the Seqrite MDM portal and click **Device Notifications** (bell icon).

   Device notifications dialog displays few newly received notifications.

2. On the device notifications dialog, click the **View all Device Notifications** link.

   The device notifications list page is displayed. You can view all the notifications related to the device status.

Infection Notification

This report gives the summary of the infection on the devices. It includes all the details of the scan such as Report type, Threat detected, and Files Scanned. If no virus is detected, only the information about the scan is displayed in the report.

Viewing the device scan summary

The device scan summary gives information about the threat detected, threat information, and if any action has been taken.

To view the device scan summary via notifications, follow these steps:

1. Log on to the Seqrite MDM portal and click **Device Notifications** (bell icon).

   Device notifications dialog displays few newly received notifications.

2. Go to that device notification, of which you need to view the scan summary and click the **View Report** link available in front of it.
3. The Device Scan Report shows the following information:
   - Report Type: Shows the type of the report; Real-time protection.
   - Threats detected: Shows total number of threats detected.
   - Table shows the threat information:
     - Icon: Shows the icon of the diagnosed threat.
     - Name: Shows the name of the threat.
     - Threat: Shows the type of the threat. For example; adware, Potentially Unwanted Programs.
     - Type: Shows the type of threat. For example; application and file.
     - Location: Shows the location of the threat.
     - Installed on: Shows the date when the threat was installed on the device.
     - Action: Shows if any action has been taken on the threat.

- Action Taken Date: Shows the date when the action was taken on the threat.

Non-compliance Report

The non-compliance report is generated when the device does not comply with the policies or configurations applied. If report is not displayed, then you can send the sync command to the device to fetch the latest report.

Viewing the device non-compliance report

To view the device non-compliance report, follow these steps:

1. Log on to the Seqrite MDM portal and click **Device Notifications** (bell icon).

   Device notifications dialog displays few newly received notifications.

2. Go to that device notification, of which you want to view the non-compliance report and click the **View Report** link available in front of it.
3. The Device Non-Compliance Report shows the non-compliant policies and configuration information as follows:
   - The policies table shows the name of the device and the recommended policy, and the following information:
     - Policy: Shows the name and type of the policy.
     - Reason: Shows the reason for device non-compliance with respect to the policy.
     - Reported Date: Shows the date when the device was non-compliant with the policy.
     - Resolved Date: Shows the date when the policy non-compliance was resolved.
     - Status: Shows the status of the policy.
   - The configuration table shows the following information:
     - Configuration Type: Shows the type of the configuration.
     - Name: Shows the name of the configuration.
     - Reason: Shows the reason of device non-compliance with respect to configurations.
     - Reported Date: Shows the date when the configuration non-compliance occurred.
     - Resolved Date: Shows the date when the configuration non-compliance was resolved.
     - Status: Shows the status of the configuration.
4. Click **Close**.

Import Notifications

The info icon on the upper-right side of the task bar indicates the import notifications. These notifications are displayed when an import action is initiated or completed. The import notifications dialog shows few newly received notifications related to the import and fence activities.

Import Notification

The import notifications include the status of the import action such as initiated, progress, completed, etc. The notification includes the name of the item imported, import status, date, time, and Admin name who has initiated the import action.

To download and view the status of the import action, you can click the **Download Output File** link.

Fence Notification

The fence notifications show information about the device and device owner, the date and time when the device entered the defined fence, and the successful application of fence restriction. On each fence notification, the user name, device name, and fence config has a hyperlink, which directs you to the respective entities.

Viewing import notifications

To view the import notifications, follow these steps:

1. Log on to the Seqrite MDM portal and click **Import Notification** (info icon).

   Import notifications dialog displays few newly received notifications.

2. On the import notifications dialog, click the **View all Notifications** link.

   The import notifications list page is displayed. You can view all the notifications related to the import and fence activities.

Battery Notification

Whenever the battery level goes below 15%, the Admin receives the notification that the device has reached the low battery level.

Delete All Notifications

The Delete all Notifications option helps to delete all the notifications of the specific type of notification. This option is available on all the Notification pages. To navigate to Notification page, click the View all Notifications link on any notifications dialog.

Deleting all notifications

To delete all the notifications of a particular notification type, follow these steps:

1. Log on to the Seqrite MDM portal and click any of the notifications icon.

   Notifications dialog appears.

2. Click the link to view all the notifications.

   Notifications list page is displayed.

3. To delete the notifications from the Notifications list page, you can use either of the options:

   - In the upper-right corner, click the **Delete all Notifications** button. On the confirmation screen click **OK**.

     All the notifications of a specific notification type are deleted.

     OR

   - On notifications list page, select the notifications check boxes which are to be deleted. The With selected option is displayed. From With selected list, select **Delete** > click **Submit** > click **OK**.

Chapter 6

Manage

The Manage menu helps the Admin to manage the MDM account. The submenus available in the Manage menu helps you to add and control the users, departments, devices, groups, and user roles. This section provides a platform to enroll the devices and perform various actions.

The Manage menu includes the following submenus.

Users

The Users option allows you to add and manage user of Seqrite MDM portal. After you add a new user to the Seqrite MDM portal, you can edit the details and assign the admin privileges to the user.

Advanced Search for Users

The Advanced Search option on the upper-right side of the Users page allows you to perform an advanced search of the users.

To find users with the Advanced Search option, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Users** > **Advanced Search**.

   Advanced search parameters are displayed.

   Note:

   By default, only three search categories are displayed. To customize the categories, click **Modify** and select the desired category check box.

2. Select the required search parameters.

   The search parameters are as follows:

   - **Select Department**: Select the department to search the users from the specific department.
   - **Select Device Ownership**: Select either Personal or Corporate to search the users by the device ownership.
   - **Select User Role**: Select the role option from the list to search the users according to their user role.
   - **Select Created By**: Select this option to search the users according to their creator name.

3. Click **Search**.

   - To reset the selected criteria, click **Reset**.

Users List Page

The Users list page displays all the users available in the Seqrite MDM portal. On Users list page, you have a privilege to choose the table columns of your choice. You can select maximum of four columns only. The system do not allow you to select more than four columns.

When searching users with respect to any criteria, make sure the criteria-related column is available in the table. The table shows the information about all the available users.

Note:

- At a time, only four columns can be selected from the Filter column list on the Users list page.
- If symbol **A** is shown next to the User Name, then it indicates that the selected user is an Admin.

With Selected Options for Users

The With selected option appears on the Users list page when you select single or multiple users. The available With selected options for users are:

- **Send Enrollment Request**: Sends an enrollment request to single or multiple selected users' devices. You can enroll a device with Seqrite MDM via Email/SMS, QR Code, and Enrollment with ADO Enablement.

  To know more about the enrollment, see Enrolling a new device.
- **Delete**: Deletes single or multiple selected users.
- **Export CSV**: Exports a list of single or multiple selected user details in the .csv format.
- **Export PDF**: Exports a list of single or multiple selected user details in the .pdf format.

- To use the With selected options for the users, log on to the Seqrite MDM portal and click **Manage** > **Users** > select a single or multiple users > select the required With selected option and click **Submit**.

Adding a user

The user with the admin privilege can add the users to the Seqrite MDM portal.

To add a new user, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Users** > **Add**.

   The Add User page is displayed.

2. Enter the First Name, Last Name, Email, Phone No., Mobile No, and select a Department. You can also upload a photo of the user.

3. Click **Save**.

   The user is added successfully.

 Tip:

- You can also add a user from the User Details page by clicking the **Add** button.
- The **Previous** or **Next** buttons available on the upper-right side of the User Details page help to easily navigate to the other users.

Overview and edit user details

After the user is added to the Seqrite MDM portal, the User Details page is displayed. You can view and edit the entire personal information or assign the admin privileges to the selected user.

For example, if you want to assign the privileges to another user to manage the MDM portal, you must select the user and assign the respective user role type with the help of Edit tab. You can also view the number of devices enrolled or enroll a new device to the selected user.

Overviewing user details

To navigate directly to the User Details page, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Users**.

2. In the Users table, select the user name and then click the **Edit** icon.

   The User Details page is displayed with the following options:

   - **Overview**: Shows the personal information of the user enrolled with the Seqrite MDM portal. The personal information includes First Name, Last Name, Email, Department, Photo, Phone No., Mobile No., Last Login, Enrolled Devices, and User Role(Type). You can also view the date and time when the user was created. In addition, you can enroll a

device through the available options; Enrollment via email/SMS, QR code, and Enrollment with ADO Enablement.

- **Edit**: Allows to edit the personal information of the user. The Edit tab includes the Edit details and Privileges sections.
- **Enrolled Devices**: Shows the number of devices assigned to the selected user. You can also enroll a new device to the selected user.

Editing user details

Seqrite MDM has the option to edit the MDM user details.

To edit the user details, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Users**.
2. In the users table, select the user to be edited and click **Edit** icon > **Edit** tab > **Edit details**.
3. Edit the information as per your requirement and click **Save**.

   The user information is successfully edited.
4. Click **Privileges**.
5. To assign admin privileges to the selected user, select the **Allow admin access** check box and enable the privileges section.

   If the Allow admin access check box is not selected, then other sections on the page are not active.
6. Change the user role and click **Save**.

   To know more about user roles, see User Roles.

   After you select the user role, the privileges of the selected admin type are assigned to the user.

   Note:

   After you assign the admin privileges to the user, the user gets an email to set the password to access the MDM portal. To know more about privileges, see Privileges.
7. Click the **Enrolled Devices** tab.

   If the devices are enrolled with the user, you will see a list of enrolled devices. From the devices list, you can either edit or delete a single device.
8. To enroll new devices to the selected user, click the **Enroll new device** button.

   The Add Device dialog appears.
9. Enter Device Name, select Ownership and Group. You can send an enrollment request to the device by selecting the **Send Enrollment Request** check box. Then the enrollment

request is sent to the device. To know more about the enrollment, see Enrolling a new device.

Tip:

To send the enrollment request for multiple devices from the users list, select the users. The **With selected** option is displayed. From the With Selected list, select the **Send Enrollment Request**. Select the enrollment option and click **Submit**.

10. Click **Create**.

    The new device is successfully enrolled.

    You can also view the number of devices enrolled to the user. After enrolling the new device, the device is added to the enrolled devices list and to the devices list page.

Importing users

Seqrite MDM users can be imported easily in CSV file format. In one instance, maximum of 1000 users can be imported.

To import users, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Users** > **Import**.
2. In Import Users page, click **Select File** and browse the file that is to be uploaded.

   To get more information about the file format, click **Download CSV file format**.
3. Click **Import**.

   The users get imported successfully.

Exporting users

Seqrite MDM users can be exported in CSV or PDF format.

To export the users, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Users** > **Export**.

   CSV and PDF options are displayed.
2. Select the desired format.

   Users are exported in the selected file format.

   Similarly, multiple selected users can be exported using the **With selected** option.

Deleting users

In Seqrite MDM, you can delete single or multiple selected users.

To delete the users, follow these steps:

Users can be deleted using any of the either options:

- On Users list page, select a single user and click the **Delete** icon in Actions column.
- On Users list page, select single or multiple users. The **With selected** option is displayed. From the list, select **Delete** and then click **Submit**.

Departments

The Departments option lets you add a new department to the Seqrite MDM portal. After you create a department, you can add the users to the department, edit the department details, and create groups of the selected departments. You can also assign departments up to N-level hierarchy.

Advanced Search for Departments

The Advanced Search option on the upper-right side of the Departments page allows you to perform an advanced search for departments.

To find a department with the Advanced Search options, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Departments** > **Advanced Search**.

   Advanced search parameters are displayed.
   - **Select Parent Department**: Search departments by selecting parent department.
   - **Select Created By**: Select this option to search department by the creator name.
2. Click **Search**.
   - To reset the selected criteria, click **Reset**.
   - To customize the categories of the Advanced Search, click **Modify**.

Departments List Page

The Departments list page displays all the departments which, are part of the Seqrite MDM portal. The table displays the information about all the departments.

With selected options for Departments

The With selected list appears on the Departments page when you select a single or multiple department. The available options in the With selected list are:

- **Delete**: Helps you to delete the multiple selected departments.
- **Export CSV**: With this option, you can export a list of single or multiple selected departments' information in the .csv format.
- **Export PDF**: You can export a list of single or multiple selected departments' information in the .pdf format.
- **Create Group**: This option helps you to create group of single or multiple selected departments at the same time.
  - Select the required With selected option and click **Submit**.

Overviewing Department Details

After the department is created with the Seqrite MDM portal, the Department Details page is displayed. You can view the entire information of a selected department and add users to the selected department.

To navigate directly to the Department Details page, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Departments**.
2. On Departments page, select the department and click the **Edit** icon.

   The Department Details page is displayed. The following options are available:

   - **Overview**: Shows the details of the selected department. The details include Department Name, Parent Department, Total Users, and Description. The information also includes recently added users, if any. To view the users added to the selected department, click **Show all**.
   - **Edit**: Helps you to edit the department information. The Edit tab includes the Edit details and Users section.

Adding a department

To add a new department, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Departments** > **Add**.
2. On Add Department page enter the **Department Name**, **Parent Department**, and **Description**.

   Department hierarchy: In Seqrite MDM, there is an N-level hierarchy. One level will be a parent department and the remaining levels will be the child departments.
3. To create a new group of the department, you can select the **Create Group** check box.

   New group is created with the same department name.
4. Click **Save**.

   New department is created as well as the group.

   You are directed to the Overview page of the newly created department where you can view the department details.

Editing department details

The Edit details option allows you to edit the information of the added department.

To edit the department details, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Departments.**
2. On Departments page, select the department and click the **Edit** icon > **Edit** tab > **Edit details.**

   Edit the information such as Department Name, Parent Department, and Description.
3. Click **Save**.

   You have successfully edited the department information.

   If required, you can click the Users section and add the users to the department.

Adding users to the department

The Users section allows you to view the number of users added to the selected department. You can also add the users to the selected department.

To add users to a department, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Departments**.
2. On Departments page, select the department and click the **Edit** icon > **Edit** tab > **Users** > **Add user to department**.

   The Add user to department dialog is displayed.
3. Select the users that you want to add to the selected department.
4. Click **Add Users**.

   Users are added successfully to the selected department.
   - To delete a user of the department, again go to Users section and select the user and click **Remove**.

Deleting department

The departments can be deleted using any of the either options:

- On the Departments list page, select a single department and click the **Delete** icon from the Actions column.
- On Departments list page, select single or multiple departments. The With selected option is displayed. From the list, select **Delete** and then click **Submit**.

Devices

The Devices option is the most significant module of the Seqrite MDM portal. You can perform the following actions on the devices:

- Add a new mobile device, assign ownership, assign an owner to the device, and assign a group.
- View and edit the device information.
- Send an enrollment request and perform the required actions on the device.
- Apply or edit configurations and apply other security settings on the device.
- Trace the location of the device and view a list of the applications that were installed on the device.
- View and manage the apps.
- View the activity report of the device.
- Monitor the network data usage and view the calls and SMSs report.

Device status

In Seqrite MDM, devices play a vital role. Each device in Seqrite MDM database shows a device status. All the statuses are represented by symbols. The mouse hover over the symbol shows the device status tooltip.

Different device status includes:

- **Approval Pending**: Device has requested the server for approval.
- **Inactive**: Device is inactive for specific time period.
- **Disapproved**: Server has not granted permission for the device enrollment.
- **Approved**: Device is approved by the server.
- **Uninstalled devices**: Seqrite MDM has been removed from the device.
- **Disconnected**: Admin has disconnected the device.

Advanced Search for devices

The Advanced Search option allows you to perform an advance search of the devices. Many search categories have been provided by Seqrite MDM to search the devices. The search categories can be customized to get the required result.

To search devices with advanced search option, follow these steps:

1. Log on to Seqrite MDM portal and click **Manage** > **Devices** > **Advanced Search**.

   Advanced Search parameters are displayed.

2. Select the parameters. The search parameters include the following options:
   - **Select Policy**: Helps you to search the devices with the help of a policy.
   - **Select Device Status**: Helps you to search the devices by selecting the device status.

- **Select Compliant Status**: Helps you to search the devices with device compliant status.
- **Select Created By**: Helps you to search the devices by the creator name who added the device.
- **Select Device Ownership**: Helps you to search the devices with device ownership.
- **Select Device Type**: Helps you to search the devices using device types such as tablet, mobile, or phablet.
- **Select Group**: Helps you to search the devices from a particular group.
- **Select Device Block Status**: Helps you to view a list of the devices having a blocked status. To search, you can select Yes or No.
- **Select Device Root Status**: Helps you to search the rooted devices on Seqrite MDM portal. To search the rooted devices, you can use Yes option.

 Note:

Out of all the advanced search categories, only three options are displayed by default. To change the search categories, you can click **Modify**.

3. To view the result, click **Search**.

   To change the search categories, click **Reset**.

ADO Enroll

ADO Enroll (Android device owner) is a type of device enrollment process where you can make Seqrite MDM the Device Owner and further follow the enrollment process.

1. On Devices list page, click the **ADO Enroll** button.
   - A document is displayed, which explains how to assign the device ownership to Seqrite MDM.

     To know more, see Enrollment using ADO.

Devices List Page

The Devices list page lists all the available devices on Seqrite MDM portal. On the Devices list page, you can select maximum of eight columns only. The system doesn't allow you to select more than eight columns.

To search any device with respect to any criteria, make sure the criteria-related column is available in the table.

The table below displays the information of the devices as follows:

Note:

You can select only eight (8) columns at a time from the Filter column list.

Columns	Description
Id	Displays the Id of the device.
OS	Shows the operating system of the device.
Status	Shows device status.
Device Name	Displays the name of the device.
Owner	Shows the name of the device owner.
Group	Shows the group name assigned to the device.
Policy	Shows the policy name assigned to the device.
Fence Config	Displays the name of the fence configuration applied to the device.
Mobile No.	Shows the mobile number of the device.
Enrollment Date	Shows the device enrollment date and time.
Ownership	Shows whether the device is a corporate or personal device.
Device type	Shows the type of the device such as mobile, tablet, or phablet.
Last Updated	Shows the last updated date and time of device details.
Uninstallation Unsecure	• If the status is Yes, then the user can uninstall/remove the MDM App from the device. • If the status is No, then the user cannot uninstall/remove the MDM App from the device.
Launcher Status	Shows the current Launcher status on MDM client app. The Launcher status can be activated or deactivated.
Manufacturer	Shows the name of the device manufacturer.
Model	Shows the name of the device model.
Launcher Version	Shows the version of launcher that is available on client app.
IMEI Numbers(s)	Shows the IMEI number of the devices and is beneficial to search the device with IMEI number.

Columns	Description
Action	The action items include: **Edit**: Helps you to edit the device information. **Delete**: Helps you to delete a single selected device.

With selected Options on Devices List Page

The With selected list appears on the Devices list page when you select single or multiple devices. The available options in the With selected list are:

- **Send Enrollment Request**: Allows you to send enrollment request via email or an SMS.
- **Delete**: Allows you to delete multiple selected devices from the MDM server.
- **Move to group**: Allows you to move the selected devices to the selected groups.
- **Export**: Allows you to export the details of multiple selected devices in the CSV or PDF format.
- **Apply Configuration**: Allows you to apply configurations on multiple selected devices. The configurations include Anti-Theft, Web Security, Wi-Fi, Schedule Scan, App Configuration, and Network Usage.
- **Device actions**: Allows you to perform device actions on multiple selected devices. The device actions include Approve, Sync, Locate, Trace On, Trace Off, Scan, Broadcast Message, Call/SMS Monitoring ON, Call/SMS Monitoring OFF, Exit Launcher, and Uninstall. To know more about device actions, see the Device Actions table below.
    - Select the required With selected option and its sub-options (if any) and click **Submit**.

After you execute the device actions on the device, the status of the action can be viewed on the Action Details page. To know more about the device actions page, see Action Details.

Enrolling a new Android device

Device Enrollment is the process of enrolling the mobile device with the Seqrite MDM portal. After enrollment, the mobile device users become members of the Seqrite MDM portal. After completing the enrollment, you can manage the device functionality, configurations, and perform the actions remotely. The device can be enrolled via Email/SMS, QR Code, or Enrollment with ADO Enablement.

Enrollment via Email/SMS

In this process, the enrollment command is sent via email or SMS. You can select this option when the device is with the user.

To enroll a new device via SMS/Email, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On Devices list page, select single or multiple selected devices.

The With selected option is displayed.

3. From the With selected list, select **Send Enrollment Request** > **Enrollment via Email/SMS** > and click **Submit**.

   The enrollment details dialog is displayed.

   Note:

   You can also send an enrollment request to the device from the Overview tab of the Device Details page.

   The enrollment via SMS is applicable only to the users settled in India.

   After sending the enrollment request, the device user will receive the enrollment details (Company Code and OTP) via Email and SMS. The user has to tap the enrollment link on the device, which navigates the user to the enrollment page. The user has to follow the instructions given on the enrollment page. Now, the user must download and install the MDM client app and enter the Company Code and OTP in the given text box on the enrollment wizard.

4. After the user taps the **Enroll** button, the Activate Device Administrator screen is displayed.
5. To activate the Device Administrator, tap **Activate**. The company code and OTP details will be validated. The device gets enrolled with the help email/SMS.
6. After the device enrollment process is completed, you will receive the enrollment approval request. After the user completes the enrollment, the device status changes to **Approval pending**.
7. You need to approve the enrollment request by sending the **Approve** command to complete the enrollment process.
8. After the device is approved, you can perform the device actions from the Device Overview tab of Devices list page. To know more about device actions, see Device Actions.

Enrollment via QR Code

Select this method of enrollment when you have the mobile devices with you and will be doing the enrollment on your own. After the enrollment process is completed, distribute the mobile devices to the users. Additionally, this QR code can also be sent to the user via email and the user can scan that QR Code to enroll the device.

Note:

The QR code enrollment is applicable only to the Android devices.

To enroll a device using QR Code, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On Devices list page, select devices.

The With selected option is displayed.

3. From the With selected list, select **Send Enrollment Request** > **Enrollment via QR Code** > click **Submit**.

   The enrollment details dialog is displayed.

   Note:

   You can also send an enrollment request to the device from the Overview tab of the Device Details page.

   The company code, OTP, Enrollment URL, Owner Email, Device id, and the Auto Approval check box is displayed.

4. The **Auto Approval** check box will be selected by default to approve the device automatically. Now, bring the device in front of the computer screen to scan the QR code.
5. On the **Enrollment Details** screen of the device, tap the arrow available on the header of the enrollment wizard. The Scan QR Code option is displayed.
6. Tap the arrow next to the Scan QR Code option to scan the QR code on the device. The camera app opens.
7. Bring the device before the QR code available on the desktop and scan it.
8. After the QR code is detected, the Activate Device Administrator screen is displayed.
9. To activate the Device Administrator, tap **Activate**. The QR code details will be validated.

   The device gets enrolled with the help of QR code.

Note:

- In both the enrollment process (Email/SMS or QR Code), for KNOX devices, the user will be prompted to agree the KNOX agreement. After the user accepts the agreement, the Device Administrator for MDM app will be disabled and the user will not be able to activate it again.
- All the Samsung devices may not indicate that they support KNOX. Thus, even for such devices, when enrolling MDM, the KNOX/Samsung privacy agreement is prompted. On accepting the privacy agreement, all the KNOX-specific policies are applied on the device.

Enrollment using ADO

ADO stands for Android device owner. Seqrite MDM requires Android Debug Bridge (ADB) to enable Device Owner Mode on the device. Thus, ADB helps to set a bridge between the computer and the connected device, and also perform multiple device actions, which in turn helps to set Seqrite MDM as Android device owner (ADO). When enrolling with ADO:

- you must configure ADB on your computer.
- your supported Android devices must be of 5.0 or later versions.

After the ADB is installed on your computer, connect your device having Seqrite MDM installed on it and run the following command:

adb shell dpm set-device-owner com.seqrite.client/.components.receivers.MainDeviceAdminReceiver

Note:

Make sure there are no accounts configured on your device.

When you receive a success message, the device is considered as a Device Owner. Further, you can continue with the device enrollment process.

Using ADB make Seqrite MDM the Device Owner

To view how to enroll the device using ADB and making Seqrite MDM as Device Owner, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On Devices list page, click **ADO Enroll** button.

   A document is displayed with prerequisites and the complete process of making Seqrite MDM the Device Owner.

Enrolling device with ADO enablement

To assign Seqrite MDM Client your device ownership, you must follow these three steps:

1. Use a new device or factory reset your device. With factory reset, you will permanently delete your personal data. Make sure you take backup of your data. To factory reset your device, follow these steps:
   i. On device, tap **Settings** > **System** > **Reset**. Please note that the terminology in your device may differ.
   ii. Tap **Reset Phone**.
2. Provision (assign Seqrite MDM Client your device ownership) your device using QR code.
   i. After factory reset of the device, a Welcome screen is displayed.
   ii. On the Welcome screen, tap 6 times below the word Welcome.
   iii. The setup wizard prompts you to connect to the Internet and download a QR code reader. In QR code setup screen, tap **Next**.
   iv. Choose the appropriate option to connect to the Internet.
   v. After connecting to the Internet, the Google Play services downloads a module that contains a QR code recognition engine.
   vi. Click **Accept & Continue** to accept the Google terms and conditions and let the QR reader installation begin.
   vii. Open the email received from your Administrator and scan the QR code available in the email with your device. In the next screen, tap **OK** and then tap **Next**.

The ADO enrollment process using QR code is completed.

3. Enroll Seqrite MDM Client.
    i. After assigning Seqrite MDM Client the device ownership, you must follow the Seqrite MDM enrollment process by tapping the Seqrite MDM icon on the device. Further follow the instructions on the screen.

Adding devices

To add a new device, follow these steps:

1. Log on to the Seqrite MDM portal and navigate to **Manage** > **Devices** > **Add**.

   The Add Device page is displayed.

2. Enter Device Name, Ownership, Owner, and Group.

   The default policy is assigned by default when a new device is added to the Seqrite MDM portal.

3. After you select the owner, the Send Enrollment Request option is displayed. For newly added devices, select the **Send Enrollment Request** check box to send the enrollment request.

   You can send the MDM enrollment request to the user device in two ways; Enrollment via Email/SMS and Enrollment via QR Code. Select the option as required.

4. Select the group.

   The policy is applied by default.

5. Click **Save**.

   The enrollment details to enroll via Email/SMS and Enrollment via QR Code is displayed.

6. Enroll the device using the details.

   The device is added successfully.

   To know more about enrollment, see Enrolling a new device.

Overviewing device details

After the device is enrolled with the Seqrite MDM portal, the Device Details page is displayed.

To navigate directly to the Device Details page, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On Devices page, select a device that is to be viewed and click the **Edit** icon.

   On the Device Details page, following tabs are displayed.

   - Overview: Helps you to view device details.
   - Edit: Helps you to edit device details.
   - Location: Helps you to trace or locate the device.

- App Inventory: Helps you to view the app inventory of the device.
- Network Usage: Helps you to view network usage of the device.
- Remote Control: Helps you to take the control of user's device remotely.
- Call/SMS Logs: Helps you to view call and SMS logs.
- Activity: Helps you to view the device activities.

On the Device Details page, Overview section shows the following information about the device.

Options	Description
Device Stats	
Enrollment Date	Shows the device enrollment date and time.
Battery Level	Shows the battery level of the device.
CPU Usage	Shows the CPU usage of the device.
Signal Strength	Shows signal strength in decibel.
Network Details	Shows the network used by the device.
SIM Carrier(s)	Shows the service provider name.
Device Storage	Shows available storage on the device.
Device Details	
Owner	Shows the device owner name.
Ownership	Shows the ownership of the device whether personal or corporate.
Group	Shows the group assigned to the device.
Policy	Shows the policy assigned to the device.
Fence Config	Shows the fence configuration applied on the device. The applied fence configuration can be turned on/off.
MDM App Version	Shows the version of MDM mobile app.
Device Status	Shows device status. See secret code.
Launcher Status	Shows the status of the Launcher.
Enrollment Status	Shows the device enrollment status.
Uninstallation Unsecure	If Yes, then the MDM App is not secure from uninstallation. The User can uninstall/remove the MDM App from the device. If No, then MDM App is secured from uninstallation. User cannot uninstall/remove the MDM App from the device.
Hardware and Storage	

Options	Description
Mobile Number	Shows mobile number.
Device Type	Shows device type; mobile, tablet, or phablet.
Model	Shows model of the device.
OS Type	Shows operating system of the device.
Manufacturer	Shows the manufacturer of the device.
IMEI Number	Shows the IMEI number of the device.
SIM ID (s)	Shows the SIM ID of the device.
MAC Address	Shows the MAC ID of the device.
Bluetooth MAC Address	Shows the Bluetooth MAC ID.

Turn on/off the fence configuration

If fence configuration is applied on the device, then the applied fence configuration name is displayed on the Overview page. It also shows an option to turn on/off the fence configuration for the device. If you turn off the fence configuration, then all the fence restrictions are removed from the device until you turn on the fence configuration again. When the fence configuration is turned off, the default restrictions (policy, web security configuration, and app configuration) are applied on the device.

Unblock the blocked device using secret code

In case the device status is blocked, you can send the secret code to the user device mentioned against the Device Status option to unblock the device. To view the secret code, click **Secret Code**.

Exit Launcher using passcode

On the Device Details section in case the Launcher status is activated and if the user wants to exit the launcher, then the user must enter a passcode to exit the launcher for a limited time. Then the user will contact you for the passcode. You can share the launcher passcode with the user by clicking **Launcher Passcode**. At least five passcodes will be created for a device. A user can exit the Seqrite launcher for at least five times until all the passcodes are used. These passcodes are generated for the first time when the launcher app configuration is applied to the device. You can also update to new launcher passcodes by clicking the **Update** option.

Note:

If the MDM app on the user device is not updated to the latest version, a prompt appears to upgrade the MDM app. Clicking **Upgrade MDM app** will send a message to the device to upgrade the MDM app.

Selecting actions for the device on Overview page

The Select an Action list is displayed on the left side of the Overview page. You can perform various actions using these commands on the device. The actions can be displayed as per the device status.

- If the device is in uninstalled or pending state, then the Select an Action list shows two options; Enrollment via Email/SMS and Enrollment via QR Code.
- If the device status is in Approval Pending state, then the Select an Action list shows three options; Approve, Disapprove, and Disconnect.
- If the device status is in Approved state, then the Select an Action list shows the following options;

Device actions	Description
Sync	Helps you to sync the selected device with the MDM server. After sending this command the device will send the latest app details, scan, and compliance report to the server.
Locate	This command fetches the current location of the Android device and shows it on the server.
Scan	This command initiates virus scanning on the Android device and forwards the scan report to the server.
Ring	This command plays the ringtone on the selected Android device.
Block	This command blocks the Android device completely and the user cannot access the device. This command should be used in critical situations only.
Unblock	This command unblocks the blocked Android device.
Exit Launcher	This command allows the user to exit the launcher temporarily or permanently.
Fetch Logs	This command is to fetch the activity logs, which are performed on the device. Click **Download Device Logs** on the upper-right side of the Device Details page to download the logs. You can download the logs in formats such as .txt, .log, crash files, etc.

Device actions	Description
Wipe	This command will wipe off the device data. The Wipe option includes different types of wipes such as Full Wipe, SD Card, Factory Reset, and Custom Wipe.
Reset Password	This command is to reset the password of the selected device through MDM.
Broadcast Message	This command is to broadcast a message to the Android device. To know more about Broadcast Message, see Broadcasting Message.
Reapply Anti-Theft	This command is to reapply the latest version of mapped Anti-theft configuration on the selected device. It is recommended to use this command when previously applied Anti-Theft configuration fails to execute on the device.
Reapply Web Security	This command is to reapply the latest version of the Web Security configuration on the selected device. You can use this command when previously applied Web Security configuration fails to execute on the device.
Reapply Policy	This command is to reapply the latest version of mapped policy on the selected device. You can use this command only when the previously applied policy fails to execute on the device.
Reapply App Configuration	This command reapplies the latest mapped App Configuration on the selected device. You can use this command only when the previously applied app configuration fails to execute on the device.
Reapply Wi-Fi	This command is to reapply latest mapped Wi-Fi configuration on the selected devices. You can use this command only when the previously applied Wi-Fi configuration fails to execute on the device.
Reapply Schedule Scan	This command is to reapply the latest version of Schedule Scan on the selected device. You can use this command only when the previously applied Schedule Scan fails to execute on the device.
Reapply Network Usage Configuration	This command is to reapply the latest version of the Network Usage configuration on the selected device. You can use this command only when the previously applied Network Usage configuration fails to execute on the device.
Push Fence Configuration	This command is to apply a fence configuration on the selected device.

Device actions	Description
Disconnect	This command will disconnect the device from the MDM server. After the command is executed on the device, the device cannot be managed by the Seqrite MDM portal.
Uninstall	This command is to uninstall the MDM client app from the selected device.
Disapprove	This option helps you to disapprove the selected devices. This command is to disapprove the enrollment request of the device. This action can be applied only to the devices whose status is Approval Pending.

Exiting launcher temporarily or permanently

You can exit launcher temporarily or permanently as follows:

Exit launcher permanently

When exiting the launcher permanently, the launcher exits for the infinite time duration. To reactivate the launcher, the admin will send the activate command using the Activate Launcher link on the device overview page. When the Enable launcher command reaches on the device, the launcher gets activated.

Exit launcher temporarily

When exiting the launcher temporarily, the admin can specify the duration to exit the launcher in minutes, hours, and days. To send the exit launcher command, the admin uses the Exit Launcher option from the device actions list on the device overview page. After completing the exit time, the launcher activates automatically. The admin has the privilege to exit the launcher or activate the launcher at any time. In any case, the device user wants to exit the launcher, the device user requires a passcode and the passcode is provided only by the admin. To know more about the passcode, see Exiting launcher using passcode.

Note:

- In both the instances (temporary and permanent launcher exit), the Launcher Status on the device overview page remains as deactivated.
- When the launcher is in exit state (permanent or temporary), the Activate Launcher button is displayed next to the launcher status on device overview page. On clicking the Activate Launcher button, the launcher gets active on the device immediately.

Exiting the launcher

The user can exit the launcher using the follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices** > select the device > click **Edit** icon.

The Device Details page is displayed.

2. From Select an Action list, select **Exit Launcher** and then click **Submit**.

   On the device, a confirmation screen is displayed to exit the launcher.

3. Options to exit the launcher are displayed. Select the required option.

   - **Exit launcher permanently**: Select this option, to exit the launcher for infinite time duration.
   - **Exit launcher temporarily**: Select this option, to exit the launcher for a specific time duration. Enter the time in the **Launcher Exit Duration** text box and then select the time in minutes, hours, or in days as required.

4. Enter the **Security Code** as displayed and then click **Exit Launcher**.

   The command is sent to the device and its activity log is generated.

Sending exit launcher command to multiple devices of a group

You can exit the launcher on multiple devices by selecting and sending Exit Launcher command from Devices list page. With Advance Search, you can filter the devices and send the Exit Launcher command to those devices.

To send exit launcher command to multiple devices of a group, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. Select the devices to which Exit Launcher command is to be sent.

   The With selected option is visible.

3. In With selected list, select **Device actions** > **Exit Launcher** > **Submit**.

   The exit launcher command is sent to all the selected devices of a group.

Activating the launcher

The admin can activate the launcher using the following steps:

1. Log on to the Seqrite MDM portal, and click **Manage** > **Devices** > select the device > click **Edit** icon.

   The Device Details page is displayed. On this page, the launcher status is displayed as Deactivated and Activate Launcher link is provided.

2. To exit the launcher deactivation mode, click the **Activate Launcher** link.

   The command to activate the launcher is sent to the device. After the Enable launcher command reaches on the device, the launcher gets activated.

Wiping the device data

To wipe the device data, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices** > select the device > click **Edit** icon.

The Device Details page is displayed.

2. From Select an Action list, select **Wipe** and then click **Submit**.

   The confirmation dialog to Wipe the device date -up is displayed.

3. Select the type of wipe that you want to perform.
   - **Full wipe**: Select this option to wipe all the data from the device.
   - **SD Card**: Select this option to wipe all the data of the SD card.
   - **Factory Reset**: Select this option to reset the device to factory settings and all the data will be wiped off including Seqrite MDM app.
   - **Custom Wipe**: If you select this option, the Custom Folder and File Type options are enabled. Select the folder that you want to wipe. You can also select the type of the file that you want to wipe off from the selected device. The file types are images, videos, audio, and files.
4. Enter the **Security Code** as displayed and then click **Wipe**.

Note:

- On Android devices, the Wipe command clears SD card data, SMS, Call Logs, calendar, etc.
- If the Wipe command fails to wipe the data from the device, then the wipe command status will be shown in the Device Activity tab as Failed with a reason for failure.

Broadcasting message

The Broadcast Message command helps to send the broadcast message. The message may be an information or it may require an action to be taken.

Note:

The Broadcast command is applicable only to the Android devices.

Informative message

This option helps to send any message from the Seqrite MDM portal to the users. Select the High Priority check box if the informative message is a priority message. For a higher priority message, the user gets a pop-up on the device.

Action Required message

This message type is selected when you want the user to take some action. The Action Required message is a high priority prompt message by default. The recipient user needs to take the action required by tapping **Change Settings** on the prompt.

To send a broadcast message, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices** > select the device > click **Edit** icon.

   The Device Details page is displayed.

2. From Select an Action list, select **Broadcast Message** and then click **Submit**.

   The Broadcast Message dialog is displayed.

3. Enter the message that is to be broadcasted. Select the message type. If required, select the High Priority check box. Click **Broadcast.**

   The message is broadcasted successfully.

Edit

The Edit tab allows you to edit the device details and its configurations. You can change configurations such as Web security, Wi-Fi, Anti-Theft, Schedule Scan, Network Data Usage, and App Configurations. The changed configurations on the console are automatically applied to the mobile device. The Edit tab includes the Edit details and Configurations sections.

Edit details

This section lets you edit the information of the added device.

Editing device details

To edit the information of the device, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On Devices page, select the device and click the **Edit** icon > **Edit** tab > **Edit details**.
3. Edit the required information such as Device Name, Ownership, Device Type, Owner, and Group.
4. Click **Save**.

   The device information is edited successfully.

Configuration

In this section you can view the configuration applied to the device. You can also assign or change the configurations for the selected device.

Note:

If the device is associated with any device group, to which the app configuration is applied, then the app configuration cannot be edited. To enable and edit such app configuration, you need to move the device to a group that does not have App Configuration applied to it.

Editing device configuration

To apply a configuration on the device, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On Devices page, select the device and click the **Edit** icon > **Edit** tab > **Configurations**.
3. You can edit or update Wi-Fi, Web Security, Anti-Theft, Schedule Scan, Network Data Usage, and App Configurations as required.

   To know more about various configurations, see security profile Configurations.
4. Click **Save & Apply**.

   You have successfully configured the device.

Location

Helps to locate and trace the device. The Location tab shows Locate and Trace On options.

Options	Description
Locate	This command is to fetch and locate the current location of the selected device. Note: Location will be fetched only if the Location Services is enabled on the device.
Trace On	This command is to carry out the continuous trace for the selected device. You can define the time to trace the device location whenever the user changes the location (moves more than 100 meters). To trace the devices, you can select the frequency such as 10 minutes, 20 minutes, 30 minutes, 45 minutes, and 60 minutes.
Location view list	This list helps you to view the traced location. You can view the traced locations for Today, Since Yesterday, Last 7 days, Last 15 days, Last 30 days, Last 3 months, and From beginning (as per their time of location).
Clear	With the Clear option, you can delete the tracked locations. • To delete all the traced locations, click **Clear**. • To delete the particular location, select the check box of the traced location and click **Clear.**
Export	With Export, you can get the detailed information about the traced locations. You can export the details in CSV or PDF file format. • To get information about all the traced locations, just select the export option. • To get information about a specific traced location > select the location > click **Export** > select the export option.

Tracing device location

The device can be traced with the Trace On option. The Locations tab shows the details of the traced devices such as:

- A list of traced locations.
- You can select the traced locations and view the locations on the map.
- You can select and delete the tracked locations from the list.
- When the trace is on, the activity log is in progress and when the task is completed, its status changes to complete.

To trace the device location, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On the Devices page, select a device that is to be traced and click the **Edit** icon > **Location** tab.
3. Turn on the **Trace** option.
4. On the Configure Trace Frequency dialog, select the **Trace Frequency** in minutes and click **Configure**.
   - The Trace On command is submitted successfully.

   Note:

   To trace any device, the GPS option on the device should be enabled (turned on).

   If the Trace Frequency value is set to low frequency, then the battery consumption of the device will be high.

   In the activity logs, the Trace On command will be in-progress till the admin sends the Trace Off command to the device.

Locating device location

The device location can be located with Locate option. You need to send an SMS and get the confirmation to location the device.

To locate the device location, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On the Devices page, select a device that is to be located and click the **Edit** icon > **Location** tab and on the map, click **Locate**.
3. In the confirmation dialog, click **Locate**.
   - To send an SMS and get the confirmation to locate the device, select the **Locate device by sending SMS** check box. Then click **Locate**.

   The Device Locate command is sent to the device.

App Inventory

App Inventory is the list of apps installed on the mobile device. If any command is pending with respect to app inventory; a small exclamatory icon is displayed on the App Inventory tab and also on the app in the app list. When hovered over the icon, the pending command is displayed. With the App Inventory option, you can perform the following actions:

- Install or add new apps to the device via Google Play, Custom App URL, Upload Custom APK, and App Repository. You can also add a specific version of the app as per your requirement.
- Whitelist or block or uninstall an app if required.
- Uninstall/Install button is provided to uninstall or install the App Launcher on the selected device. If the Launcher is active on the mobile device, the button will show as Uninstall Launcher, and if the Launcher is not active on the mobile device, the button will show as Install Launcher. To know more about App Launcher, see Activating Launcher.

  Note:

  The administrator can install or uninstall the app Launcher only when the app configuration is added to the selected device and the launcher is mapped with the device.

- You can install an app on an Android device via Google Play and App Repository.

App Status

The apps listed on App Inventory page shows different status as follows:

- **Installed**: This status is showed when the app is already installed on the device.
- **Published**: The app that is recommended by the Admin to install on the device will have the status as Published.
- **Recommended**: If the user installs the app which has Published status, then the app will have the status as Recommended.
- **Whitelisted**: If any installed app is whitelisted by you then that app will have the status as Whitelisted.
- **Blocked**: The app shows blocked status if the app is fully blocked or when the app is uninstalled using the Uninstall command in App Inventory. When the app is added to the uninstall list from App Configuration, then the app will have the status as Blocked.

Advanced Search for Apps

If any app cannot be searched with simple search option, then Advanced Search option helps to search the apps with the help of app type, status or category.

To search apps with Advanced Search option, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On Devices page, select the device and click **Edit** icon > **App Inventory** > **Advanced Search**.

3. Select the app type, app status, and app category.

   All the options can be selected or only one.

4. Click **Search**.

   The Search result is displayed.

   To edit the search criteria, click **Reset**.

With selected options on App Inventory page

The With selected list allows you to perform actions on a single or multiple selected apps. The available options in the With selected list are:

- **Whitelist**: Helps to white list a single or multiple selected apps. The whitelisted apps are accessible on the Android device.
- **Block**: Helps to block a single or multiple selected apps. The blocked apps are accessible on the Android device.
- **Uninstall**: Helps to uninstall the single or multiple selected apps. The uninstalled app is blocked on the Android devices.
    - Select the required option and click **Submit**.

Note:

- If the Launcher is activated, then only the list of active apps is displayed on the App Inventory page.
- You cannot uninstall any of the listed active apps.

Viewing app inventory

To view app inventory, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On the Devices page, select the device and click **Edit** icon > **App Inventory** tab.

   The App Inventory list is displayed.

Adding apps to the device

To add an app to the device through app inventory, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On the Devices page, select the device and click the **Edit** icon > **App Inventory** > **Add App**.

   The options to add apps are displayed.

3. Select the appropriate option and add the apps to the device.

   To know more about how to add an app through the various options, see Adding Apps via App Repository.

Network Usage

The Network Usage option lets you monitor Internet data usage of the selected device if the network usage configuration is applied on the device. After the Network Usage configuration is applied to the device, the Seqrite MDM app starts monitoring the Internet data with respect to Wi-Fi, mobile data, and in roaming status. You can view the percentage of utilized mobile data for the mobile data plan that you have set on the device for the billing cycle. The enhanced graphical representation of network usage has been provided for easy monitoring of the network usage.

Searching network data usage

As a user, the network data usage statistics can be drawn for number of days or by selecting a date range. The available options to search network data usage are Today, Last 7 days, Last 15 days, Last 30 days, Current Month, and Select a Range.

To search a network data usage for specific number of days or a date range, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On the Devices page, select the device and click **Edit** icon > **Network Usage**.
3. Select the number of days or the date range from the list.

    Tip:

   If you select Today from the Select a Range option, you can see the hourly usage of mobile data for the last 24 hours.

4. Click **Search**.

   To change the search criteria, click **Reset**.

Data Plan Details

This option helps you to view the detailed information of the mobile data and Wi-Fi usage in a selected range of period. This data usage information is provided in MB's.

- To change the current data plan, select the Billing Cycle Start Date, Number of Days, Mobile Data Plan Limit, and Wi-Fi Daily Usage Limit, and click **Save**. You can change this data plan whenever required with the help of **Settings** button.

 Note:

If you select Today from the Select a Range option, you can see the hourly usage of mobile data for the last 24 hours.

Parameters	Description
Network Usage Configuration	Shows the name of the network configuration of the device. Clicking the network configuration name will navigate you to the Network Usage Configuration Details page. To know more about network configurations, see Network Usage Configurations.
Billing Cycle Start Date	Shows the date on which the billing cycle begins.
Number of Days	Shows the number of days in one billing cycle.
Mobile Data Plan Limit	Shows the limit of the mobile data plan.
Wi-Fi-Daily Usage Limit	Shows the daily limit of the Wi-Fi usage.
Mobile Data Usage %	Shows the percentage of the mobile data usage in a specified mobile data billing cycle.
Setting icon	The Setting icon, which is available next to Data Plan Details, helps you to change the Billing Cycle Start Date, Number of Days, Mobile Data Plan Limit, and Wi-Fi Daily Usage Limit of the device, if required. Note: If the data plan modified using this Setting icon, then the modified network usage configuration will have more preference and the changes will not be applies on the device.

Network Usage

This section shows the graphical representation of network usage in a selected date range. The chart shows the usage of network data through Wi-Fi, Mobile Data, and Roaming. The data usage information is provided in MB's. Mouse hover over the chart to see the details of network usage by Wi-Fi, Mobile Data, and in Roaming status.

Top 10 App Usage

This section displays the top 10 apps that consumed the maximum Internet data in the selected date range. The mouse hover over the pie chart shows the details of Internet data usage by the apps. This option also shows the apps, which consumed maximum Internet data in the selected date range. It gives the details of the Internet data usage by the user and help you to configure the app configuration.

Network Usage Graph

Displays the daily bar graph representation of data usage in the selected date range. The data usage shown in the bar graph is combined usage of Mobile Data, Wi-Fi, and in the Roaming

status of the device. The values shown in the graph are based out of Data Usage in MB and days on that specified date range. The mouse hover over the graph shows the entire details of the usage. You can see the total network usage via Wi-Fi, mobile data, and in roaming. This graphical representation and network usage data ease the monitoring and tracking of data usage.

Usage Information

This option gives a detailed quantifiable information on the Internet data usage on a daily basis. The table below informs about the usage parameters and their description.

Parameters	Description
Mobile Data (in MB)	Shows the mobile data usage on a specified date.
Wi-Fi Data (in MB)	Shows the Wi-Fi data usage on a specified date.
Roaming Data (in MB)	Shows the usage of data on the device when the device is in Roaming status on a specified date.
View Details	Displays the details of the Internet usage of the apps on the device for specified date. To navigate to the App Network Usage Details page, click **View Details**. To know more, see View Details.

Note:

You can view the usage information by sorting the table based on date, mobile data, Wi-Fi data, and roaming data.

Viewing network usage details

The View Details option shows the usage of the Internet by apps on the device. You can also view the individual contribution of the app in utilizing the Internet data for a specified date or in the selected date range. It also shows the entire network usage of all the apps present on the device and the network usage of an app via Mobile Data Plan, Wi-Fi Data, and in Roaming status. To navigate to the App Network Usage Details page from Usage Information section, click the **View Details** option.

- **App Network Usage Details**: Displays the Internet data usage by apps on user's device for a selected date or date range. This app displays the data usage with respect to Wi-Fi, Mobile, and Roaming by all the apps on a device for the selected date range.
- **Select Date Range**: Shows the selected date range.

Columns	Description
Icon	Shows the icon of the app.
App Name	Shows the name of the app.
Mobile Data (in MB)	Shows the usage of Mobile Data by the app.

Wi-Fi Data (in MB)	Shows the usage of Wi-Fi Data usage by the app.
Roaming Data (in MB)	Shows the usage of data for apps in roaming status.

Call/SMS Logs

The Call/SMS logs help you to view the calls, video calls, SMS, and MMS from the device. This option track call logs, video calls, SMS and MMS sent and received from the devices. This tab gives a report of dialed, received, rejected, and missed calls. The duration of calls get logged. The detailed logs help you to monitor the calls and SMS usage on all the devices.

Note:

The Call/SMS Logs option is supported only when the calling feature is enabled on your device.

Advanced search for call and SMS logs

The Advanced Search option allows you to perform an advanced search for the call/SMS logs. This option includes the following parameters:

- **Select Log Type**: With this option, you can search the logs for incoming, outgoing, missed, or rejected calls or SMSs.
- **Select Call/SMS Type**: With this option, you can select the type of call or SMS, such as call, video call, SMS or MMS.
- **Select Date Range**: With this option, you can select the particular date range to view the logs.

To search call and SMS logs with advance search, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On the Devices page, click **Edit** icon > **Call/SMS Logs** > **Advanced Search**.
3. Select either or all the search categories such as log type, call/SMS type, and date range.
4. Click **Search**. The search result is displayed.

Viewing call and SMS logs

The call and SMS logs are visible only if the Call/SMS Monitoring option is enabled on the console and the device logs are synced with the console.

To view Call/SMS logs, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On the Devices page, select the device and click the **Edit** icon > **Call/SMS Logs**.

   The following options are available:

Options	Description
Log Type	Shows different call type such as Dialed, Received, and Missed.
Phone Number	Shows the phone number of a particular mobile.
Name	Shows name of the contact. Note: If the call is from an unknown number, then the field will be empty.
Time	Shows the date and time of the call.
Duration	Shows duration of the call in seconds HH: MM: SS.

Enable call and SMS monitoring

On allowing to monitor call and SMS of a particular device, the user can view the calls and SMS details of the device on the portal. The calls and SMSs can be monitored after enabling the Call/SMS Monitoring option and synchronizing the device call and SMS logs with the server.

Note:

You can enable this option only when the device is approved.

To enable call/SMS monitoring, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. Perform one of the following steps:
   - On the Devices page, select the device and click **Edit** icon > **Call/SMS Logs.**
   - When you select the device, the With selected option is displayed. From the With selected list select **Device actions** and then from next list select **Call/SMS Monitoring ON** and then click **Submit**.
3. Turn the Call/SMS Monitoring slider to **ON**.

   The Sync Logs option is displayed.
4. Click **Sync Logs**.

   The device syncs with the server and the latest calls and SMS logs are displayed.

Exporting call and SMS logs

The call and SMS log can be exported in CSV and PDF format.

To export the call and SMS logs, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On the Devices page, select the device and click **Edit** icon > **Call/SMS Logs** > **Export**.

3. Select either CSV or PDF format.

   Log is exported.

Clearing call and SMS logs

The Clear all logs option helps to clear all the call, SMS, video, and MMS logs.

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On the Devices page, select the device and click **Edit** icon > **Call/SMS Logs** > **Clear all logs**.
3. On the confirmation screen, click **OK**.

Note:

Receiver name and number will not be available for outgoing MMS and if the user deletes any MMS before synchronizing, then the deleted MMS will not be shown in the server.

Remote Control

The Remote Control (RDC) feature helps the Seqrite MDM Administrator to get remote access of the user's device. It is extremely beneficial in case of emergency when the user is travelling or out of office. In such scenario, the MDM administrator can take remote access of the device and troubleshoot the issue. The Remote Control (RDC) feature is applicable only to the enrolled and approved devices.

With the Remote Control feature, the Administrator can perform the following tasks:

- Remotely view device screen (applicable to all the devices).
- Remotely control the device.

  Note:

  Only for the KNOX supported devices, the Administrator can have complete control of the device.

- Take screenshots of the remote device screen. The screenshot taken by the Administrator is saved on the local system.

The Remote-Control tab shows the following options:

Options	Description
Start RDC	Helps the Admin to start the RDC session and take control of the remote device.
Screenshot	Helps the Admin to take screenshot of the remote device.
Back	Helps the Admin to visit the previous screen on the device.
Home	Helps the Admin to visit the Home screen of the device.
Recent Apps	Helps the Admin to visit the recent apps on the device.

Stop RDC	Helps the Admin to stop the RDC session.

Note:

- The remote control (RDC) feature is applicable to Android OS 5.0 or later versions.
- The remote control feature is supported on MDM Client 1.5 and later versions.
- The functionality to take screenshot in RDC session is applicable for all the devices.
- Functionalities like moving back, visiting Home screen or visiting recent apps is applicable only to the KNOX supported devices.

Remotely controlling the device

In the remote control session, the Admin can completely control the device. This functionality is applicable only to the Samsung Knox supported devices.

To remotely view or control the user's device, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. In the Devices list, select the device to take its control and click the **Edit** icon.
3. In the Device Details page, click the **Remote Control** tab.
4. To view the device screen, click **Start RDC.**

   In Activity log you can see the status of RDC session.
5. The device user has to accept and provide the consent.
   - For MDM prompt on the device, the user must tap **Start Now**.
   - For system prompt, the user must tap **Allow**.
6. As the user accepts the consent, the Admin gets the visibility of the remote device screen on MDM portal and the remote session starts.

   Note:

   - For normal device and ADO enabled devices, the Admin can only view the remote screen of the device.
   - For KNOX supported devices, the Admin can take complete control of the remote device, perform actions remotely, and trouble shoot the issue.

   - To stop the remote session, click **Stop RDC**.

Important point to remember for seamless RDC connection:

- Device must have good Internet connectivity without any network fluctuations.
- Upon network switch (Wi-Fi to mobile or vice versa), the remote connection will be disconnected and the MDM Admin has to re-initiate the RDC.

- In case of fluctuations in mobile/Wi-Fi connection, remote connection will be disconnected and MDM Admin has to re-initiate the RDC.
- We may observer some delay (based on network speed) in screen appearance during RDC if network connection is slow.
- When the Admin requests for remote access, device user has to accept the RDC request, then RDC connection will established.
- Device should have consistent 400 kbps network speed for smooth remote connection.
- Device should have minimum 150 kbps network speed for establishing remote connection.

Activity

This section helps you to check out the various actions performed on the device. You can view the device actions that were performed on the selected device. You can also view the status of the action such as Pending, Notified, Expired, Success, Cancelled, Failed, and In progress. You can view the date and time when the action was performed on the device, the IP address of the device and the owner of the device. This section shows policy and configuration applied along with their name, version, and status. The Activity section includes Admin, Compliance Report, and Scan Report of the actions performed.

Admin

With the Admin option, you can view all the actions that were performed on the device. You can also view the status of the action such as Pending, Notified, Expired, Success, Cancelled, Failed, and In progress. You can view the date and time when the action was performed on the device, the IP address of the device, and the owner of the device.

Activity Status

Following are the various statuses of the activities:

- **Pending**: This status appears when the command/policy/configuration has not yet reached the device. The Cancel option is provided to end the request if you do not want the command to be executed.

  Note:

  In case the command is in pending state and you want to send the command again, you have to cancel that command or send the command again from the Device Actions list.

- **Notified**: This status appears when the command/policy/configuration has reached the device, but its status has not yet been received by the server.
- **In Progress**: This status appears when the command/policy/configuration is reached to the device and it is in a continued state. This status is applicable to locate, trace on, scan, and wipe process.

- **Failed**: This status appears when the command/policy/configuration was not able to reach the device due to unavailability of Internet connection or if the phone is switched off or any other reasons. You can view the reason for the failure so that you can act accordingly.
- **Cancelled**: This status appears when the FCM server is unable to communicate with the device and the command gets cancelled. You can view the reason for the cancellation so that you can act accordingly.
- **Expired**: This status appears when the command/policy/configuration has reached the set timeout and has not reached the device. After the request has expired, the Retry link appears. Clicking Retry will send the same request again to the device.
- **Success**: This status appears when the command/policy/configuration has been successfully executed on the device. You can view the policy/configuration version so that you can know the version number that is applied to the device.

Searching activity logs

To search the activity logs, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices**.
2. On the Devices page, select the device and click **Edit** icon > **Activity**.
3. In the Admin section, select the days or the date range to search the activity logs and click **Search**.

   Activity logs are displayed.

Compliance Report

The Compliance Report section shows the non-compliance report for the device. If report is not displayed, then you can send the sync command to fetch the latest reports.

Clicking **View Report** will show the Non-compliance report. This report includes the non-compliance report for policy non-compliance, configuration non-compliance, and device communication non-compliance.

Scan Report

The Scan Report option shows the scanned report of the device. The scan reports are displayed with the View Report link in front of each report.

To view the report, click **View Report**.

The device scan report shows:

- **Scan summary**: Shows the report type (what type of reports are generated) and the number of threats detected.
- **Threat details**: Shows the threat icon, name, type, location, threat installed date, action on the detected threat, and the date on which the action was taken on the threat.

Note:

The scan report is generated only when the virus is detected.

Importing devices

Seqrite MDM provides an option to import multiple devices with ease. In one instance, maximum of 1000 devices can be imported.

To import the devices, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices** > **Import**.
2. Select the CSV file, which is to be imported and click **Select File**.

   To know about the CSV file format, click **Download CSV sample format**.
3. Click **Import**.

   Devices are imported successfully.

Exporting devices

When there is a requirement, you can export the devices and their information. The device details can be exported in the CSV or PDF format. The exported devices' details show complete information about the devices present in Seqrite MDM.

To export devices and its details, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Devices** > **Export**.
2. Select the file format in which the devices are to be imported; CSV or PDF.

   Devices are exported successfully.

Deleting devices

Devices can be deleted using any of the either options:

- On Devices list page, select a single device and click the **Delete** icon in Actions column.
- On Devices list page, select single or multiple devices. The **With selected** option is displayed. Select **Delete** and then click **Submit**.

Groups

The Group option helps you to add a group, view the group information, add devices to the group, and assign a policy. The policies and configurations applied to a group will be applied automatically to multiple devices in that group. You must create a group and add devices to that group to apply the same type of restrictions. After adding the group, you can edit the group information whenever required. When you create a new device, a default group is created, and the default policy is applied to the user.

Group QR Code

The Group QR Code option provides the facility to enroll multiple devices of any group in a single instance. The devices enrolled using Group QR Code option will be added to MDM portal as per the group name with incremental numbering. For example; if the group name is QR Group, then the devices added to the MDM portal will have the nomenclature as QR Group-1, QR Group-2 and so on.

To enroll the devices using Group QR Code, a group owner has to be assigned, who will receive all the information about the QR code via email. Other than the group owner, you can also send this QR code details any other user as well. When the device user scans the QR code created for a group, the device will be assigned to that group and the policy applied to the group will be automatically applied to the device on approval. The validity of generated QR Code can be set to 7 or 15 or 30 days.

Note:

When generating the QR code, by default, the Auto Approval check box is not selected on the MDM portal. If it is selected, then after scanning the QR code, all the devices of a group will be automatically approved.

Advanced Search for Groups

The Advanced Search option allows you to perform an advanced search of the devices in the groups. The categories to search groups include the following options:

To search groups with Advanced Search option, follow these steps:

1. Log on to Seqrite MDM portal and click **Manage** > **Groups** > **Advanced Search**.
2. Select the search categories:
   - **Select Policy**: Helps you to search groups of a particular policy.
   - **Select Created By**: Helps you to search groups by the creator name.
3. Click **Search**.

   To change the search categories, click **Reset**.

Groups List Page

The Groups list page displays all the available groups on the Seqrite MDM portal. The table displays information of all the groups. If an exclamation mark symbol is shown next to the Group Name, it indicates that there are non-compliant devices in that group. The Delete option is not available for the default group, as the default group cannot be deleted.

With selected Options for Groups

The With selected list appears when single or multiple groups are selected. The With selected options for groups are as follows:

- **Delete**: Helps you to delete the single or multiple selected groups.
- **Export CSV**: Helps you to export a list of single or multiple selected groups in .csv format.
- **Export PDF**: Helps you to export a list of single or multiple selected groups in .pdf format.
- **Apply Configuration**: Allows you to apply the configuration on the single or multiple selected groups. The configurations include Anti-Theft, Web Security, Wi-Fi, Schedule Scan, App Configuration, and Network Usage.
- **Apply Policy**: Allows you to apply the policy to the single or multiple selected groups.
- **Apply Fence Configuration**: Allows you to apply the fence configuration on the single or multiple selected groups.
- **Broadcast Message**: Allows you to send a message to the single or multiple selected groups. After broadcasting the message to a group, it will send messages to all the devices of that group. To know how to broadcast messages, see Broadcasting Message.
    - Select the required With selected option and sub-option (if any) and click **Submit**.

Adding a group

Groups can be added by the Admin.

To add a new group, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Groups** > **Add**.

   The Add Group page is displayed.

2. Enter the mandatory fields; Group Name and Assigned Policy. Select the required Fence Config, App Configuration, and Description.

   To know more about policies, see Policies.

3. Select the **Default** check box to make this group as the default group. All the newly added devices will be added to the default group.

4. Click **Save**.

   The group is created successfully.

Viewing the group information

After the new group is created with the Seqrite MDM portal, the Group Details page is displayed.

To navigate directly to the Group Details page, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Groups.**
2. On Groups page, select the group and click the **Edit** icon.

   The Group Details page is displayed. The following options are available:

   - **Overview**: This option helps you to view the entire information of the group. You can view the Group Name, Assigned Policy, Fence Config, App Configuration, Total devices, Description, and Default, and whether it is a default group or not. It also displays recently added devices to the group. To view all the devices added to the selected group, click **Show all**.
   - **Edit**: Allows you to edit the group information. The Edit tab includes Edit details, Devices, and Group QR Code sections.

Editing group information and adding devices to the group

With this option you can edit the group information and also, view all the added devices and if required add new devices.

To edit the group information, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Groups**.
2. On Groups page select a group and click **Edit** icon > **Edit** tab > **Edit details**.
3. Edit the following information such as the Group Name, Assigned Policy, Fence Config, App Configuration, and Description and click **Save**.

   To export the group details, click **Export**.
4. Click the **Devices** section and then click **Add device to Group**.

   The Add device to Group dialog is displayed.
5. Select the devices that you want to add to the selected group.
6. Click **Add Devices**.

   Devices are added to the selected group.

Generating QR Code for the group

All the devices of any group can be enrolled in a single instance using the Group QR Code option. To enroll the devices of the group, you need to generate the QR code.

To generate a QR code and to enroll multiple devices of a group, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Groups** > select the group > click **Edit** icon > click **Edit** > click **Group QR Code**.

2. To enable other sections on the Group Details page, select the **Generate QR Code for the Group** check box.
3. Assign owner to the group by clicking **Assign Owner** button.
4. Select the validity of the QR code by selecting the number of days from the list.
5. Click **Generate QR Code**.

   An email will be sent to the group owner with the respective QR code details.

   - The QR code is generated. To generate new QR code, you can click the **Try new QR code** link.
   - The group QR Code is generated with the details such as; Company Code, OTP, Enrollment URL, Expiry date, Group Owner, Group name, Auto Approval.
6. Other than the group owner, you can send the QR code to other users by entering multiple comma-separated email IDs. Add the email address in the **Send Email** text box and click **Send**.

   - To update the QR code details, click **Update QR Code**.
   - To cease the QR code at any instance, click **Terminate QR Code**.

Importing groups

In one instance, maximum of 1000 device groups can be imported.

To import the groups, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **Groups** > **Import**.
2. In Import Groups dialog, select the file that is to be imported.

   To view the sample format of CSV file to import the groups, click the **Download CSV sample format** link.
3. Click **Import**.

   The groups are imported successfully.

Exporting groups

When you use the export groups option you get information of all the available groups of Seqrite MDM. The groups can be exported in PDF or CSV format. The exported file shows the following group information such as group name, description, is the group default, applied policy to the group, creator of the group, and number of devices assigned to the group.

To export the groups, from Groups list page, click **Export**, and select the output file format.

Deleting groups

Groups can be deleted using any of the either options:

- A single group can be deleted by clicking the **Delete** icon on Groups list page.

- On Groups list page, select single or multiple groups. The **With selected** option is displayed. From the list, select **Delete** and then click **Submit**.

User Roles

The User Roles menu helps you to view all the admin role types of the Seqrite MDM portal. You can use the option to assign the User Role type. You can assign administrator privileges to a normal user by making the user an Administrator to manage the MDM portal. You can assign or remove user roles whenever required. By default, there are five user roles (Administrator types): Super Admin, Admin, Advanced, Standard, and Basic. You can edit the user roles and privileges as well. However, you cannot edit or delete the default user roles. You can create new Administrator roles and assign privileges if required.

The Super Administrator is the main administrator of the Seqrite MDM portal. The Super Administrator can create the Admin by assigning the user roles and privileges to any existing user.

Types of user roles

The user roles are based on privileges.

Super Admin

The Super Admin role is created at the time of Seqrite MDM company creation. For the entire MDM portal, a single Super Admin is assigned. The Super Admin can create multiple Admins with administrator role. The Super Admin has all the privileges such as read, create, update, delete, assign/unassign, approve/disapprove, perform basic, advance, and critical actions, for all the modules of Seqrite MDM. The Super Admin also has the privilege to set up services such as APNS, and IMEI number.

Assigning Super Admin role to an Admin

In many instances, the Admin may be responsible to perform all or similar activities of Super Admin. With Seqrite MDM, the Super Admin can assign any Admin, a Super Admin privilege. This functionality helps to allocate and utilize the resources effectively. When an Admin is assigned a Super Admin role, the Admin gets the privilege to make changes to all the Setup Services settings. Thus, such Admin can view the Settings option on MDM portal and perform all the Super Admin responsibilities.

Admin

The Admin can access all the users of the Seqrite MDM portal and have all the privileges similar to Super Admin. The Admin can create indefinite Admins to manage the MDM portal.

Advanced

The Advanced user role type has all the privileges except the delete privilege. In addition, this user role doesn’t have any privilege to create, update, assign/unassign, and delete user role. Also, cannot upgrade or renew the license.

Standard

The Standard user role type has all the privilege such as update, assign, and unassign.

The Standard user role cannot:

- Create or delete users, departments, groups, policies, configurations. Also, cannot renew or upgrade the license.
- Create/delete/update/assign/unassign any user role.
- Create/delete/approve/disapprove devices.
- Perform any advance action such as wipe/lock/unlock/uninstall/Push policy or configuration.
- Delete the notifications.

Basic

The Basic user role type has only the Read-Only privileges. The Basic user role can export the data and view the privileges, but cannot assign any privileges to the user.

The table below helps you to understand the privileges assigned to the user role. These are the default privileges with the following indications:

- ✓: User has the permission
- ×: User does not have the permission

Privileges	Entity / User Roles				
	Basic	Standard	Advanced	Admin	Super
User					
Read	✓	✓	✓	✓	✓
Create	×	×	✓	✓	✓
Update	×	✓	✓	✓	✓
Delete	×	×	×	✓	✓
Send enrollment request	×	×	✓	✓	✓
Department					
Read	✓	✓	✓	✓	✓
Create	×	×	✓	✓	✓
Update	×	✓	✓	✓	✓
Delete	×	×	×	✓	✓
Assign/Unassign	×	✓	✓	✓	✓
User Role					
Read	✓	✓	✓	✓	✓

Privileges	Entity / User Roles				
	Basic	Standard	Advanced	Admin	Super
Create	✗	✗	✗	✓	✓
Update	✗	✗	✗	✓	✓
Delete	✗	✗	✗	✓	✓
Assign/Unassign	✗	✗	✗	✓	✓
Device					
Read	✓	✓	✓	✓	✓
Create	✗	✗	✓	✓	✓
Update	✗	✓	✓	✓	✓
Delete	✗	✗	✗	✓	✓
Assign/Unassign	✗	✓	✓	✓	✓
Approve/Disapprove	✗	✗	✓	✓	✓
Basic Action (Ring/locate/trace/scan/sync)	✗	✓	✓	✓	✓
Advanced Action (wipe/lock/unlock/uninstall/Push policy or configuration)	✗	✗	✓	✓	✓
Critical Action (Wipe/uninstall/disconnect/exit launcher)	✓	✓	✓	✓	✓
Group					
Read	✓	✓	✓	✓	✓
Create	✗	✗	✓	✓	✓
Update	✗	✓	✓	✓	✓
Delete	✗	✗	✗	✓	✓
Assign/Unassign	✗	✓	✓	✓	✓
Policy					
Read	✓	✓	✓	✓	✓
Create	✗	✗	✓	✓	✓
Update	✗	✓	✓	✓	✓
Delete	✗	✗	✗	✓	✓
Apply/Revoke	✗	✓	✓	✓	✓

Privileges	Entity / User Roles				
	Basic	Standard	Advanced	Admin	Super
Configuration					
Read	✓	✓	✓	✓	✓
Create	×	×	✓	✓	✓
Update	×	✓	✓	✓	✓
Delete	×	×	×	✓	✓
Apply/Revoke	×	✓	✓	✓	✓
Export					
Export	✓	✓	✓	✓	✓
Licensing					
Read	✓	✓	✓	✓	✓
Renew	×	×	×	✓	✓
Upgrade	×	×	×	✓	✓
Report					
Read	✓	✓	✓	✓	✓
Create	×	×	✓	✓	✓
Delete	×	×	×	✓	✓
Update	×	✓	✓	✓	✓
App Control					
Read	✓	✓	✓	✓	✓
Create	×	×	✓	✓	✓
Update	×	✓	✓	✓	✓
Delete	×	×	×	✓	✓
App Repository	×	×	✓	✓	✓
Assign/Unassign	×	✓	✓	✓	✓
Notification					
Read	✓	✓	✓	✓	✓
Delete	×	×	×	✓	✓

* You can change the privileges as per your requirement. Else, you can assign the default privileges.

Advanced Search for user roles

The Advanced Search option allows you to perform an advanced search for different User roles. To search user roles with advanced search option, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **User Roles** > **Advanced Search**.
2. From the Select Created By list, select the desired creator name and click **Search**.

   The result gets displayed.

User Roles List Page

The User Roles list page displays all the available user roles in Seqrite MDM portal. The table shows the information about all the user roles.

With selected options for user roles

The With selected list appears on the User Roles page when you select single or multiple user roles. The available options in the With selected list are:

- **Create Copy**: Helps to create a duplicate copy of a single or multiple selected user role.
- **Delete**: Helps to delete a single or multiple selected user role.

  Note:

  - You cannot delete the default user roles.
  - You cannot delete a user assigned to a user role.

    - Select the required options and click **Submit**.

Adding User Role

To add a new user role, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **User Roles** > **Add**.

   The Add User Role page is displayed.
2. Enter the User Role Name. Select the User Role Type from the list.

   After you select the User Role Type, the default privileges assigned to the user role type appears.
3. Modify the privileges and click **Save**.

   The new user role is created.

Overviewing user role

After you create a new user role, you can view the information of the user role and add the users to any particular role type. You can edit the newly created user roles, change the

privileges, and assign the newly created user roles to the users. You cannot edit the default user role types.

Note:

The editing of the user role type depends on the selected user role.

For example, if you select Standard user role type, then the User Role Details page will be displayed to edit Standard user role type.

To navigate directly to the User Role Details page, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **User Roles**.
2. On the User Roles page, select the user role and click the **Edit** icon.

   The User Role Details page is displayed. The following options are available:

   - **Overview**: Helps you to view the user role details and the privileges assigned to it. You can view the user Role Name and No. of Users. You can also view all the privileges, which are assigned to different user role types.
   - **Edit**: The Edit tab includes Edit details and Users sections.

Editing user role

This section allows you to edit the User Role name, Type, and Privileges. You can view all the privileges assigned to the user role.

To edit the user role details, follow these steps:

1. Log on to the Seqrite MDM portal and click **Manage** > **User Roles**.
2. On the User Roles page, select the user role and click the **Edit** icon > **Edit** tab > **Edit details**.
   - You can edit the user role name, user role type, and turn on/off the privileges.

Note:

You cannot change the privileges for default created user roles such as (Super Admin, Admin, Advanced, Standard, and Basic). You can simply view them.

3. Click **Users** section.

   You can view the added users to the user role type.

   Tip:

   You can assign user role to the users through the Privileges option on the User Details page.

Deleting user roles

The user roles can be deleted using any of the either options:

- On User Roles list page, select a single user role and click the **Delete** icon in Actions column.

  The default user roles cannot be deleted and so Delete icon is not available in the table for such default user roles.
- On User Roles list page, select single or multiple user roles. The **With selected** option is displayed. From With selected list, select **Delete** and then click **Submit**.

Chapter 7

Profiles

The Profiles option allows you to create and apply policies and configurations on the mobile devices enrolled with your Seqrite MDM account. This option provides a platform to create new policies, configurations, and perform various actions.

This chapter includes the following sections.

Policies

The Policies option allows you to assign policies to the group and manage the devices in that group. You can apply policies to the single or multiple groups to secure the devices from losing the crucial information. You can assign or unassign the policies, edit, and remove the policies.

Note:

- KNOX-supported policies are applicable to all the KNOX-supported devices.
- Some Samsung devices may not indicate that they are KNOX-supported, but may show a prompt to accept the KNOX/Samsung agreement. If the user accepts the KNOX/Samsung agreement, then the KNOX policies are applied to the device.

Advanced Search for Policies

The Advanced Search option allows you to perform an advanced search for different policies. To search policies, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Policies** > **Advanced Search**.
2. From the Select Created By list, select the desired creator name and click **Search**.

   The search result gets displayed.

Policies List Page

The Policies list page displays all the available policies in Seqrite MDM. The table shows the information about the policies.

With selected options for policies

The With selected list appears on the Policies list page when you select single or multiple policies. The With selected options are as follows:

- **Create Copy**: Helps you to create a duplicate copy of a single selected policy. You can create a copy of a single policy, whereas you cannot create copy of multiple policies.
- **Delete**: Helps you to delete single or multiple selected policies.

  Note:

  You cannot delete a policy which has a group assigned to it.

  - Select the required option from the list and click **Submit**.

Adding a policy

To add a new policy, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Policies** > **Add**.
2. Enter Policy Name and Description.
3. Select the **Default** check box to make this policy as the default policy. This default policy will be applied to all the newly added devices.
4. Click **Next** to apply the policies.

   The Add Policy page is displayed.

   The Edit Policies tab includes different policies divided in sections such as; All, Password Policies, Device, Device Applications, and App Security. To know more about policies, see Policy Details.
5. To inherit the policy from already created policies, select the policy from the **Inherit From** list.
6. To turn on (enable) the policy, click in the red circle. This policy gets active and applies restriction on the device.
7. Click **Save and Publish**.

   New policy is created successfully.

Viewing a policy

After you create a new policy, you can view the policy, edit the policy information, and add the groups to the policy. You can also view the version number of the policy. Editing the policies will change the current version of the policy.

To view the policy information, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Policies**.
2. On Policies list page, select the policy and click the **Edit** icon.

   The Policy Details page is displayed. The Overview tab displays the following policy information; Policy Details and Recently applied to groups.

   - **Policy Details**: Shows the Policy Name, No. of Groups, Description, and Default.
   - **Recently applied to groups**: Shows the date and time when the policy was created and also view the recently added groups.

     The Show all option helps you to view all the groups to which the policy has been applied. Clicking **Show all**, will navigate you to view all the added groups to the policy.

Editing policy details and groups

The Edit tab includes the Edit details and Groups sections. The Edit details section allows you to make changes to the policy name and policy description. From Groups section you can view the policy that is assigned to the group and also, apply the selected policy to more number of groups. You can also add the selected policy to the new groups and devices.

Note:

Editing the policy will change the current version of that policy.

To edit the policy information, follow these steps:

1. Log on to the Seqrite MDM portal and navigate to **Profiles** > **Policies** > **Edit** icon > **Edit** > **Edit details**.
2. You can edit the information such as; Policy Name and Description.

   To make this policy as the default policy, select the **Default** check box.

   Note:

   The default policy will be applied to the newly added device.

3. Click **Save**.
4. Click the **Groups** section and then click **Add groups to policy.**

   The Apply Policy to Group dialog is displayed. You can search the groups or select the groups from the list.

5. Select the group that you want to add to the policy and click **Add Group**.

   The groups are added to the devices.

Editing the policy

You can edit the selected policy and apply the policies to the group. You can turn on the selected policy to apply the restrictions on the device.

To edit a policy, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Policies** > **Edit** icon > **Edit Policies**.

   A policy is divided into different sections such as All, Password, Devices, Device Applications, and App Security Policies.

   Sign indicators on policy page are as follows:

   - Tick mark in green circle: The parameter is part of that policy.
   - Multiplication mark in red circle: The parameter is not part of the policy. To apply that parameter, click in the circle.
   - Grey multiplication mark: The parameter does not apply to that specific operating system.

     To know more about policies, see Policy Details.

2. Click **Save and Publish**.

   All the edited policies are displayed.

   Enter the comments about the changes in the description box and click **Confirm**.

   Note:

   A new version number is generated whenever changes are made to the policy.

Policy Details

To know the types and details of the policies, navigate to the Edit Policies tab, which includes All policies. The policies are also differentiated into different sections for better understanding such as: Password, Device, Device Application, App Security, ADO Security, and KNOX Security.

Sections	Description
All	This section shows all the policies available in Seqrite MDM. Shows all the policy options available in the Seqrite MDM portal. Options include Password, Device, Device Applications, and App Security. You can choose any of the policies listed here. The All policies section includes the Inherit From option to inherit a policy from the drop-down list of already created policies. Select this option to inherit the policy from earlier created policies. • Click the **Select All** option on the right side of the Edit Details tab if you want to select all the policies. It includes all the policies related to Password, Devices, Device Applications, and App Security. To know more about these policies, see Password Policy, Device policy, Device Application policy, App Security policy, ADO Security, and KNOX Security. • **Inherit From**: Allows to inherit the password policy from already created policies. While creating a new policy, you can select the **Inherit From** list to inherit the policies from already created policies.
Password	Shows all the policies related to the password criteria. You can turn on the policies as per your requirement.
Device	Lists the policies related to the device. You can turn on the policies as per your requirement.
Device Applications	This policy lists the policies related to the device applications. You can turn on the policies as per your requirement.
App Security	The App Security policy is related to the security of the apps. You can turn on the following policy as per your requirement.
ADO Security	The ADO policy is applicable to those devices where Seqrite MDM client is the device owner. • All the ADO policies are superscripted with “D” for easy identification. • This policy is applicable to the devices where the MDM client is the device owner. Also, check on the Seqrite MDM portal the specific OS versions of the devices to which this policy can be applied.
KNOX Security	The KNOX policies are applicable to the Samsung KNOX-supported devices. • All the KNOX policies are superscripted with “K” for easy identification.

Seqrite MDM supports following policies:

Requires Password

This policy applies a screen lock and sets the type of the password on the device. Password type are Low, Medium, and High. After applying this policy on the device, the user has to set the password as per the type of the password suggested. If the user has not applied this policy, the device will be shown as the Non-compliant device.

The following are the three values of the password:

- Low: A less secure option. You can set the Pattern, Pin, or Password for the device screen lock.
- Medium: A secure option. You can set the Pin or Password for the device screen lock.
- High: The most secure option. You can set only the Password for the device screen lock.

Password Minimum Length

To set the length of the password, turn on the Password Minimum Length policy. This policy is dependent on the Requires Password policy. After applying this policy on the device, the user must set the password as per the recommended password length.

- If the password type is Low, then the password length must be in between 4 to 16.
- If the password type is Medium, then the password length must be in between 6 to 16 alphanumeric letters.
- If the password type is High, then the password length must be in between 8 to 16 letters. The user has to set the password with at least one character, one numeric, and one special character.

 Note:

The user must apply settings as per the policy. Otherwise, the device will be shown as Non-compliance device.

Password Age

To set the age limit of the password, turn on the Age policy. You can apply an age limit till a specific period. This policy is dependent on the Requires Password policy. After applying this policy on the device, the user has to set the age of the password. The age of the password can be 15 Days, 30 Days, 45 Days, and 90 Days. After the specified time expires, the user should reset the password. Otherwise, the device will be shown as a Non-compliant device.

Device Autolock

To lock the device automatically after a preset idle time, turn on the Autolock policy. This policy is dependent on the Requires Password policy. After applying this policy on the device, if the device screen remains idle for the selected time, then the device will be automatically locked. The time can be 15 Sec, 30 Sec, 1 Min, 2 Min, 5 Min, 10 Min, and 30 Min.

Password History

To maintain a history of old passwords and to restrict the user from using the old passwords, turn on the Password History policy. After applying this policy, the device saves the selected number of old passwords given in the list. The values given in the list are 2, 3, 4, and 5. This policy is applicable only on iOS devices.

Block USB Connection

To block the device from connecting to other devices through USB, turn on the Block USB Connection policy. After applying this policy on the device, the user will not be able to connect to any device through USB. If the user tries to connect to any device through USB, then the device will be locked and the device password will get reset.

If this policy is applied to the KNOX devices, the device user would not be able to detect or transfer the data through USB connection.

Note:

- This policy is dependent on the Require Password policy.
- This policy may or may not be applicable to some of the devices.
- For ADO devices, this policy is applicable only when the device OS version is 6 or later.
- This policy is applicable to the non-ADO devices with OS 6 and earlier versions.

Block Safe Mode

To restrict the access to the Safe Mode on the selected device, turn on the Block Safe Mode policy. This policy is dependent on the Requires Password policy. After applying this policy on the device, the user device will be blocked and asked to set the password as per the password policy. After setting the password, the user will not be able to access the safe mode. The access to safe mode will be permanently blocked. If you do not want to block the Safe Mode access for a specified user, then revoke the policy for that user.

If this policy is applied to the KNOX devices, the device user would not be able to access the Safe Mode.

Note:

- To apply this policy, it is mandatory that the Requires Password type must be set to Medium or High.
- For ADO devices, this policy is applicable only when the device OS version is 6 or later
- For non-ADO devices, this policy is applicable only when the device OS version is 6 or earlier versions.
- This policy may or may not be applicable to some of the devices.

Block Camera

To block the use of camera, turn on the Block Camera policy. After applying this policy on the device, the user cannot use the camera on the device. If the user tries to launch the device camera, the Seqrite MDM will automatically close it.

Block Face Time

To block the use of Face Time app on iOS devices, you can enable this policy. It is dependent on Block Camera policy.

Block Factory Reset from Device Setting

This policy disables the Factory Reset option on the device. Thus, the device user cannot factory reset the device. The Restrict Factory Reset policy is applicable only to the devices where Seqrite MDM Client is the Device Owner and also to the Samsung KNOX supported devices.

 Note:

This policy is applicable to non-ADO Android devices with OS 6 or earlier versions.

Block Bluetooth

To block the usage of the Bluetooth, turn on the Block Bluetooth policy. After applying this policy on the device, the user cannot switch on the Bluetooth mode on the device. If the user tries to use Bluetooth on the device, then the Seqrite MDM will automatically close it for security. The Block Bluetooth policy is applicable to the KNOX devices and also to the Android ADO devices where MDM client is the device owner.

Block the user to Configure Bluetooth

The Blok the user to Configure Bluetooth policy can be enabled only when the Block Bluetooth policy is turned off. To restrict the user from configuring the Bluetooth on the device, turn on the Restrict Bluetooth Configuration policy.

If this policy is applied, the user cannot pair with new Bluetooth devices, but can connect with already paired devices.

This policy is applicable to KNOX devices as well as to the ADO devices where MDM client is the device owner.

Block Wi-Fi

To block the usage of Wi-Fi, turn on the Block Wi-Fi policy. After applying this policy on the device, the user cannot switch on the Wi-Fi. If the user tries to use the Wi-Fi on the device, Seqrite MDM will automatically close it.

Block Open Wi-Fi

To prevent the user from connecting to the available open Wi-Fi networks, turn on the Block Open Wi-Fi policy. After applying this policy on the device, the user will not be able to connect to any open Wi-Fi network.

Block Mobile Hotspot

To block the usage of the Mobile Hotspot, turn on the Block Mobile Hotspot policy. After applying this policy on the device, the user cannot switch on the Mobile Hotspot. If the user tries to use the Mobile Hotspot on the device, Seqrite MDM will automatically close it.

Note:

This policy is applicable only to the Samsung devices that support KNOX.

Block NFC

To block the usage of the NFC, turn on the Block NFC policy. If this policy is applied on the device, the NFC option gets disabled.

Note:

This policy is applicable only to the Samsung devices that support KNOX.

Block Mobile Data while Roaming

To restrict the user from accessing the mobile data while roaming, turn on Block Mobile Data while Roaming policy. When this policy is applied on the device, the user cannot turn on their mobile data in roaming.

Note:

This policy is applicable to KNOX devices and the devices where MDM Client is the device owner and the device OS version is 7(Nougat) or later.

Block Auto-Sync while Roaming

After applying this policy on the device, the user cannot auto-sync the mobile data in roaming. The auto-sync option will be disabled for the user if this policy is applied.

Note:

This policy is applicable only to the Android devices.

Block Outgoing Call in Roaming

To block the voice roaming or outgoing calls when the user is in roaming, turn on the Block Outgoing Call in Roaming policy**.** After applying this policy on the device, the user cannot make the outgoing calls or voice roaming during roaming. If the user tries to use the Voice Roaming or Outgoing calls on the device while roaming, then Seqrite MDM will not allow the user to make the calls.

Note:

This policy is applicable only to the Android devices.

Location Service (GPS)

This policy helps to enable or disable the location services option on the device. You can apply this policy as follows:

- **Always ON**: To allow the device user to use the location services continuously, select this option.
- **Always OFF**: To completely block the device user from using the location services, select this option.

Note:

- This policy is applicable to the Android devices.
- This policy is applicable to both ADO and KNOX supported devices.

Sync Frequency

To set the frequency of the reports from the server, turn on the Sync Frequency policy. After applying this policy on the device, the device will send reports (scan /non-compliance reports) to the server at the selected intervals. The frequency intervals are 4 hours, 8 hours, 16 hours, 24 hours, and 48 hours. If the user turns off this policy, then the server will send reports only in 24 hours.

Note:

This policy is applicable only to the Android devices.

Block Certificate

To block the unwanted downloads of certificates on the device from the untrusted websites, turn on the Block Certificate policy. This policy is device specific as follows:

- **iOS device**: In iOS devices, this policy blocks untrusted TLS certificate.
- **Windows device**: In Windows device, this policy blocks manual installation of certificates.

Block Screen Capture

To block screen capturing on the device, turn on the Block Screen Capture policy. After applying this policy on the device, the user cannot capture any screenshots.

Note:

This policy is applicable only to the ADO and KNOX supported devices.

This policy is not applicable to the non-ADO devices with OS 6 and earlier versions.

Block Text Copy and Paste

To block the copy and paste of the text on the device, turn on the Block Text Copy and Paste policy. After applying this policy on the device, the user will not be able to copy and paste the text on the device.

Note:

This policy is applicable only to the Android devices.

Block Pop-ups for Safari

To block the pop-ups on the iOS device for Safari browser, turn on the Block Pop-ups for Safari policy. The user will not receive any Safari browser pop-ups.

Block Fraud Warning from Safari

To block any fraud warnings on the iOS device from the Safari browser, turn on the Block Fraud Warning from Safari policy. After applying this policy on the device, the user will not be able to access the phishing websites for the Safari browser on the device.

Accept Cookies for Safari

To store cookies in Safari browser, turn on the Accept Cookies for Safari policy. After applying this policy on the iOS device, the cookies are stored for Safari on the user's device. To store the Safari browser cookies, you can use the following options:

- **Never**: If you select this option, the cookies are never stored on the device from the Safari browser.
- **From Visited Sites**: If you select this option, then the cookies are stored from the visited websites for the Safari browser on the device.
- **Always**: If you select this option, then the cookies are always stored in the Safari browser on the device.

Block iTunes App

To block the iTunes app on the iOS device, turn on the Block iTunes App policy. After applying this policy on the device, the user will not be able to access the iTunes app on the device.

Block App Store

To block the app store on the iOS device, turn on the Block App Store policy. The app store will be blocked and the user will not be able to download from the App store for iOS devices.

Set Google Account

To configure a Google account on the user's Android device, turn on the Set Google Account policy. After applying this policy, the user must configure the Google account manually on the device. If the user does not configure the Google account, the device will go in non-compliance mode.

Block Primary Microphone

To block the primary microphone on the user's Android device, turn on the Block Primary Microphone policy. After applying this policy, the user will not be able to use the microphone on the device.

Note:

This policy is applicable to the ADO and KNOX supported devices.

This policy is not supported by Lenovo devices.

Block Siri

To block Siri application on the iOS device, turn on the Block Siri policy. After applying this policy on the device, the user will not be able to delegate any request or action to Siri. You can select the available options to block Siri: Always and When Locked.

- **Always**: With this option, Siri will be entirely blocked on the users' device.
- **When Locked**: With this option, Siri will be blocked only when the device is locked.

Device Time-out

This policy is to ensure that the device remains connected to the server when the device is not communicating with the server for the specified number of days, then the device will be in the non-compliance mode. Select the number of days from the available options; 1, 2, 3, 5, and 7 days. After you select the days, the device will remain disconnected for the specific duration and after that, the device will go into the non-compliance mode. This policy is applicable to the Android and iOS devices.

Set Auto Time Zone

To set automatic date, time, and time zone on the user Android device, turn on the Set Auto Time Zone policy. After applying this policy, if the user sets the time and date or time zone manually, then the device will go into the non-compliance mode.

- If this policy is applied to the devices with KNOX operating system, the device user would be restricted from editing or updating the time zone or date and time on the device.
- If this policy is applied to the ADO devices where MDM Client is the device owner, the device user would be able to turn it off, but within 30 seconds the auto time zone is turned on automatically by MDM app.

Block the user to Switch Profile

At times, the user may have multiple user profile on a single device and can easily switch between the profiles. To restrict the user from switching to different user profiles, turn on the Restrict Profile Switch policy.

Note:

This policy is applicable to the ADO and KNOX supported devices.

Device Accessibility Service & App Usage

To notify the user to apply the accessibility and app usage services within the defined time, turn on the Device Accessibility Service & App Usage policy. This policy is required for the following:

- Accessibility Service: This service is required for functioning of Web security configuration.
- App Usage: This service is required for MDM to manage its app control configuration.

After enrolling the device, if this policy is not applied, the app usage screen is displayed on the device and the user has to enable the app usage service. If the user does not enable the app usage service, then the screen is displayed every 30 seconds. In such scenario, the device user will not be able to use the default browser or Chrome browser if the accessibility service is not enabled.

Note:

If app usage service access is not provided to MDM Client app, the app blocking or uninstalling functionality will not work.

When this policy is applied then the accessibility and app usage services are managed through server. To apply this policy, you should configure the following options:

- **Strict**: This is a default setting. When this option is selected, the device user will be forced to apply the accessibility and app usage service within the defined time. A blocked screen is displayed and the user will be forced to enable the accessibility and app usage service.
- **Notify**: This option is used if the admin does not want the device users to forcefully apply the accessibility and app usage services. If this option is selected, the device user will receive the notification on the device. When the user taps the services notification, the user will be navigated to Admin Messages screen with the message to enable App Usage. The user should tap the message to navigate to the apps screen, and turn on the Seqrite MDM.

  Note:

  To manually enable the App Usage for Seqrite MDM, the user can navigate as follows; Device Settings > Security (Lock Screen and security) > Apps with usage access > turn on Seqrite MDM.

Block the User to Modify Accounts

To restrict user from modifying any user profile, turn on the Restricts User Accounts Modification policy. When this policy is applied on the device, the user will not be able to make

any changes to the user profile. This policy is applicable only to the ADO supported devices where Seqrite MDM Client is the device owner.

Block USB Debug Mode

To restrict the user from accessing the debug mode when the device is connected to the system, turn on the Block USB Debug Mode policy. If this policy is applied, the user will not be able to use the USB Debug Mode on the device.

Note:

This policy is applicable to both, the KNOX Samsung devices and ADO supported devices where the MDM Client is the device owner.

Block App Control

To restrict the user from installing or uninstalling the apps on their device, turn on the Block App Control policy.

Note:

This policy is applicable to the ADO supported devices where the MDM Client is the device owner.

Block the User to Add User Profile

To restrict the user from creating new user profile, turn on the Block the User to Add User Profile policy. This policy is applicable to all ADO supported devices.

Block the User to Delete User Profile

To restrict the user from deleting any user profile, turn on the Block the User to Delete User Profile policy. If this policy is applied on the device and the user tries to delete the user profile, the device will go in non-compliance mode.

Note:

This policy is applicable to both, the KNOX Samsung devices and ADO supported devices where the MDM Client is the device owner.

Block the user Configure Network Setting

To restrict the user from configuring the mobile network on the device, turn on the Block the user Configure Network Setting policy. This policy is applicable to the ADO supported device where MDM Client is the device owner.

Block Outgoing Calls

To restrict the user from making any outgoing call, turn on the Block Outgoing Calls policy.

Note:

This policy is applicable to both, Samsung KNOX and the ADO supported devices where the MDM Client is the device owner.

Block Mount Physical Media

To restrict the user from mounting any physical media on the device, turn on the Block Mount Physical Media policy.

Note:

This policy is applicable to the Samsung KNOX supported devices.

Wi-Fi On Sleep Mode

To keep the Wi-Fi on even in sleep mode, turn on the Wi-Fi On Sleep Mode policy. If this policy is applied, the user cannot change the Wi-Fi settings and it will be kept on in sleep mode. To do more customization with this policy, following options are available:

Always: Select this option to access Wi-Fi continuously.

Never: Select this option to completely block with Wi-Fi usage.

Only When Plugged In: Select this option to allow Wi-Fi only when the device is plugged in to the charger.

Note:

This policy is applicable to both, Samsung KNOX and the ADO enabled devices.

Block App Installation from Unknown Sources

To restrict the device user from installing any app from unknown sources, turn on the Block App Installation from Unknown Sources policy.

Note:

This policy is applicable to both, Samsung KNOX and the ADO supported devices where the MDM Client is the device owner.

Block Notification Area

To restrict the device user from viewing any notifications and block the notification area on the device, turn on the Block Notification Area policy.

Note:

This policy is applicable to both, ADO and KNOX supported devices. For ADO devices, it is applicable where the MDM Client is the device owner and OS of the device is Marshmallow (6.0) or later.

Block Cellular Data

To restrict the apps and services, on user device, from using cellular data to connect to the Internet, turn on the Block Cellular Data policy. When this policy is applied, the device user cannot access Internet using Cellular Data.

Note:

This policy is applicable to the Samsung KNOX supported devices.

Block Mock Location

Mock Locations allow the device users to show the fake location of their device with the help of GPS and network operator. To restrict device user to create the mock location of their device, turn on the Block Mock Location policy.

Note:

This policy is applicable to the Samsung KNOX supported devices.

Block Outgoing MMS and SMS

To restrict the incoming or outgoing MMS and SMS on the user device, turn on the Block Outgoing MMS and SMS policy.

Block Airplane Mode

Airplane Mode disconnects call and SMSs and, in some devices, it also disables Wi-Fi and Bluetooth. Thus, to restrict the device user from accessing Airplane Mode on the device turn on the Block Airplane Mode policy.

Note:

This policy is applicable to the Samsung KNOX supported devices.

History

The History tab on the Policy Details page allows you to view the history of the created policies. You can also view the history of all the versions of the created policies.

To view the history of a policy, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Policies** > **Edit** icon > **History**.

   The policy history list is displayed with the information about the version, created on, created by and action on the policy. The available action item is View (eye-shaped icon). This action helps you to view the entire details of the policy.

   - Clicking the View icon will navigate you to the Policy History page. The Policy History page shows Versions list, the policy created date, created by, comments and all the policy details.

Importing a policy

All the policies can be imported to get the details. Only one policy can be imported in a single instance. When performing the import action, a specific file format is required. To know more about the file format, click the **Download XLS sample format** link. The imported file shows the information about the policy name, applied to (Android and iOS), and name of the dependent policies.

To import a policy, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Policies** > **Import**.
2. In Import policy dialog, select the file to be imported and click **Import**.

   Policy file is imported successfully.

Configurations

Seqrite MDM provides the following configurations; Anti-theft, Web security, Wi-Fi, Schedule Scan, and Network Usage. Also, you can create your own configurations and apply them to the device or the device group. The Anti-Theft and Web Security configurations are created by default when the company is registered. Thus, the anti-theft and web security configurations are applied by default to the newly added devices.

Advanced Search for Configurations

The Advanced Search option allows you to perform an advanced search for the devices.

To search configurations with advanced search option, follow these steps:

1. Log on to Seqrite MDM portal and click **Profiles** > **Configurations** > **Advanced Search**.
2. Select the search categories:
   - **Select Configuration type**: Select this option to search configurations according to the configuration type.
   - **Select Created By**: Select this option to search the configurations by creator name.
3. Click **Search**.

   To change the search categories, click **Reset**.

Configurations List Page

The Configurations list page displays the default and created configurations. The table displays the information about all the configurations added to MDM portal.

With selected Options for Configurations

The With selected option appears when you select single or multiple configurations. The With selected options for configurations are as follows:

- **Delete**: You can delete single or multiple selected configurations with this option.

- **Apply to Groups**: Helps to apply the selected configuration to the selected groups.
- **Apply to Device**: Helps to apply the selected configuration to the selected devices.

Note:

You cannot apply multiple configurations of one type on the groups or device at the same time, whereas you can apply multiple Wi-Fi configurations.

From the available options, select the option and sub-option (if any).

- Select **Delete** and then click **Submit**.
- If Apply to Group or Apply to Device is selected, you need to select the groups or devices and then click **Apply**. On confirmation screen, click **OK**.

Wi-Fi Configuration

The Wi-Fi configuration helps you to enable Wi-Fi on the user's device without sharing the Wi-Fi credentials. You can revoke Wi-Fi configuration whenever it is not required. This helps you to create Wi-Fi configurations and later apply to the device.

Adding Wi-Fi Configuration

To add Wi-Fi- configuration, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Configurations** > **Add** > **Wi-Fi**.

   The Add Wi-Fi Configuration page is displayed.

2. Enter Network SSID and select the Security option for the company. The security options include WEP, WPA/WPA2 PSK, and None.
   - If you select WEP, the Password Type appears. There are password types such as ASCII, and Hexadecimal.
   - In case of WPA/WPA2 PSK, the Password text box is displayed.
3. Select the security option and enter the password and click **Save**.

   The Wi-Fi configuration is applied successfully.

Note:

WEP type is supported only on the Android devices.

You must collect the SSID, Security Option, and Password Type details from IT Administrator of the organization.

Overviewing Wi-Fi Configuration

After the Wi-Fi configuration is created, the Wi-Fi Configuration Details page is displayed.

To navigate directly to the Wi-Fi Configuration Details page, follow these steps:

1. Log on to the Seqrite MDM portal.

2. Click **Profiles** > **Configurations** > select a configuration > click **Edit** icon.

   The Wi-Fi Configuration Details page is displayed. The following options are available.

   Note:

   To edit any Wi-Fi configuration, you must click the Edit icon available next to the Wi-Fi configuration only.

   - **Overview**: Helps you to view the Wi-Fi configuration details. You can view the Network SSID, Security Option, Updated on, and Total Devices. You can also view recently added devices. To display all the devices added to the selected configuration, click **Show all**.
   - **Edit**: Helps you to edit the Wi-Fi configuration details and assign the default configurations.

Editing Wi-Fi Configuration

The Edit tab includes Edit details and Devices sections.

- **Edit details**: Lets you edit the information of the Wi-Fi configuration (Network SSID and security options) added to the Seqrite MDM portal.
- **Devices**: Lets you view the number of added devices to the Wi-Fi configuration. You can also add the devices to the Wi-Fi configuration.

  Note:

  If the configuration is edited, the current version of the configurations will be changed.

To edit the configurations and apply configurations on the device, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Configurations** > select a configuration > click **Edit** icon > **Edit** tab > **Edit details**.
2. You can edit the configuration details such as Network SSID, Security Option, change password type for WEP, and edit password for WPA/WPA2 PSK. Then click **Save**.
3. Click **Devices** section and then click **Apply configuration to device**.

   The Apply configuration to devices dialog is displayed.
4. Select the devices that you want to add to the configuration and click **Apply**.

   Configurations are applied to the device.
   - To remove the applied Wi-Fi configuration from any device, go to Devices section and select the check box available in front of the device name and click **Remove**.

Anti-Theft Configuration

The anti-theft configuration helps you to block the device and trace the device in case of loss or theft. The default anti-theft configurations are created when you add a new device at the time

of approval. With the help of this option, you can create the Anti-Theft configuration and can apply them to the device.

Adding Anti-Theft Configuration

To apply Anti-theft configurations, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Configurations** > **Add**.
2. In the Add list, select the **Anti-Theft** option.

   The Create Anti-Theft Configuration page is displayed.
3. Enter the Configuration Name and the mobile number of the Admin and click **Add**.

   The mobile number gets displayed in Admin Mobile Numbers list.

   Note:

   In this section, you have to add contact numbers of the other MDM Admins. You can add up to nine mobile numbers and these numbers will be displayed on the blocked screen of the device for the user to contact the Admin.
4. Enter the message in the **Block Screen Message** text box that should be displayed when the device gets blocked.

   Note:

   The blocked screen message is displayed whenever the user device gets blocked. A default blocked screen message is already displayed in its text box. However, you can edit this message if required.
5. Select the **Lock device on Airplane Mode** check box. This is optional.

   This option helps to lock the mobile when the mobile device is in the airplane mode. The device gets locked on the airplane mode only if the password is set on the device as per the password policy criteria.

   Note:

   If the Lock device on Airplane Mode is applied, the lock screen appears.
6. If SIM is changed, you can take appropriate action on the device. Thus, select the required action from the **Action on SIM change** list.
   - **Lock device on SIM Change**: This option helps to lock the mobile if the SIM is changed by any unauthorized user or the device is stolen. Select the **Lock device on SIM Change** check box to enable this option. When the Lock device on SIM Change option is selected, the Notify admin on SIM Change check box gets visible. If required, you can select this option.

The Lock device on SIM Change option is based on three categories:

- If the password is not set on the device, then the device is blocked on SIM change.
- If the password is set on the device as per the password policy criteria, then the device is locked on SIM change.
- If the password is set on the device, but not as per the password policy criteria, then the device is blocked on SIM change.

Note:

To avoid blocking of the device, ensure to apply the password on the device as per the policy.

- **Notify admin on SIM Change**: With this option, you can send a notification to the alternate numbers of the Admin, when the SIM is changed. If the user of the device changes the SIM, then a notification message will be sent to the alternative numbers (mentioned in anti-theft alternative contact number list). If the user of the device unlocks or unblocks the device within five minutes, then the notification message will not be sent to the Admin.

Note:

The Notify admin on SIM Change check box is dependent on the Lock device on SIM Change. If Lock device on SIM Change option is selected, then only you can view the Notify admin on SIM Change check box.

- **Block device on SIM Change**: When you select this option on the MDM portal and if the device user inserts a new SIM in the device, the device will be blocked. This option is beneficial when you do not want the device user to use any new SIM in the device.

Note:

When the device is blocked and the device user removes the newly inserted SIM, the device will be unblocked.

7. Select the **Default** check box to make this configuration as default. The default configuration will be applied to the newly added device automatically.
8. Click **Save**.

The Anti-Theft configuration is created successfully.

Note:

The Anti-Theft configuration is applicable only to the Android devices.

Overviewing Anti-Theft Configuration

After the Anti-Theft configuration is created, the Anti-Theft Configuration Details page is displayed.

To navigate directly to the Anti-Theft Configuration Details page, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Configurations** > select a configuration > click **Edit** icon.
2. To view the anti-theft configuration, click the **Edit** icon available next to the anti-theft configuration only.

   The Anti-Theft Configuration Details page is displayed. The following options are available.

   - **Overview**: Helps you to view the Anti-Theft configuration details. You can view the Setting Name, Updated On, Total Devices, and Default status. You can also view recently added devices. To display all the devices added to the selected configuration, click **Show all**.
   - **Edit**: You can edit the Anti-Theft configuration details and assign the default configurations from this section.

Editing Anti-Theft Configuration

The Edit tab includes the Edit details and Devices sections.

- **Edit details**: Lets you edit the Anti-Theft Configuration added to the Seqrite MDM portal.
- **Devices**: Lets you view the number of devices to which the Anti-Theft configuration is applied. You can also add more devices to the Anti-Theft configuration.

  Note:

  If the anti-theft configuration is edited, the current version of the anti-theft configuration will be changed.

To edit the configuration details and apply configuration on the device, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Configurations.**
2. Select the anti-theft configuration to be edited and click the > **Edit** icon > **Edit** tab > **Edit details**.

   The Anti-Theft Configuration Details page is displayed.
3. You can edit the configuration details such as the Setting Name, Administrator Mobile Numbers, Block Screen Messages, and notification options such as Lock device on SIM Change, Notify admin on SIM Change, Block device on SIM Change, and Lock device on Airplane Mode.
4. Select **Default** check box to make the Anti-Theft configuration as the default configuration, and click **Save**.

5. Click **Devices** section and then click **Apply configuration to device**.

   The Apply configuration to device dialog is displayed.

6. Select the devices to which you want to apply the configuration and click **Apply**.

   The configuration is edited and applied to the selected devices.

   To remove the anti-theft configuration from the devices, click the Devices section and select the check box available in front of the device name and click **Remove**.

Web Security Configuration

The Web Security configuration helps you to restrict the Web access of the user's device by blocking website-based categories, black listing URLs, black listing certain URLs of a website irrespective of the domain, blacklisting or whitelisting keywords, and protecting the device from phishing and malicious websites. The default Web Security configurations are created, when you add a new device. With the help of this option, you can create the new Web Security configurations and later, they can be applied to the device.

Adding Web Security Configurations

To create new Web Security configurations, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Configurations** > **Add.**
2. In the Add list, select **Web Security**.

   The Create Web Security Configuration page is displayed.

3. Enter Configuration Name, select the Security Settings options by selecting the Browsing Protection, Phishing Protection, and Web Protection check boxes.
4. To make the web security configuration default, select the **Default** check box.

   Note:

   Selecting the Default check box, will mark this web configuration as default and will be applied automatically to the newly added devices.

5. Click **Next**.

   The Web Categories section is displayed. The Web Categories page includes a list of options to select the categories.

6. To block any of the Web category, select the check boxes as per your requirement. To choose all the Web categories, select the **Select All** check box. Select **Default** to select the default Web categories.
7. Click **Next**.

   The Blacklist/Whitelist URLs section is displayed.

8. Enter a URL in the **Please enter keyword or URL** text box and click **Add**.

9. The keyword or URL gets added to the Blacklist. To move the blacklisted URL into the whitelist or vice-versa, double-click the keyword or URL. You can add any keyword or URL to the blacklist or whitelist. You can also block keywords, URLs, or domains by adding specific keywords. Also, add the keywords from URL or domain name to blacklist or whitelist.
   - To move all the blacklisted Keywords or URLs to Whitelist, click **Whitelist All**.
   - To move all the whitelisted Keywords or URLs to Blacklist, click **Blacklist All**.
10. Click **Save**.

    Web Security configuration is created successfully.

    Note:

    On the device, the Web Security configuration will work only on the Google Chrome Browser.

Overviewing Web Security Configuration

After the Web Security configuration is created, the Web Security Configuration Details page is displayed.

To navigate directly to the Web Security Configuration Details page, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Configurations** > select a configuration > click **Edit** icon.

   The Web Security Configuration Details page is displayed. The following options are available.

   Note:

   To view and edit the Web Security configurations, you must click the **Edit** icon available next to the Web Security configuration only.

   - **Overview**: This section helps to view the entire Web Security configuration details. You can view the Web Security Details such as Setting Name, Browsing Protection, Phishing Protection, Web Protection, Total Devices, and Default status. You can also view recently added devices. To display all the devices added to the selected configuration, click **Show all**.
   - **Edit**: With Edit, the Web Security configuration details can be edited and the default configurations can be assigned.

Editing Web Security Configuration

The Edit tab includes Edit details, Web Categories, Blacklist/Whitelist URLs, and Devices.

Edit details

With this option, you can edit the Web Security configuration added to the Seqrite MDM portal.

Editing web security configuration details

To edit the configurations, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Configurations.**
2. Select the Web security configuration, which is to be edited and click the **Edit** icon > **Edit** tab > **Edit details**.
3. You can edit the configuration name and security settings such as Web categories and Blacklist/Whitelist URLs.
4. You can edit the configuration name and security settings such as Browsing Protection, Phishing Protection, and Web Protection.
5. Select the **Default** check box to make the configuration as the default Web Security configuration.

   Note:

   The default Web Security configuration will be applied to the newly added device.

6. Click **Save**.

   The Web Security configuration details are edited successfully.

Web Categories

This section helps you to select and block the Web categories and to stop the user from accessing blocked websites.

Blocking Web Categories

To block the Web categories, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Configurations**.
2. Select the configuration to be edited and click **Edit** icon > **Edit** tab > **Web Categories**.

   The Web Security configuration details page is displayed.
3. Select the check boxes of the Web categories, which are to be blocked.
4. If required, select the following options:
   - **Select All**: Helps you to select all the Web categories check boxes.
   - **Reset**: Helps you to reset the Web categories configuration.
   - **Default**: Helps you to remove the customized settings and apply the default settings of Seqrite MDM.
5. To save the configuration, click **Save**.

   The Web categories are blocked successfully.

Blacklist/Whitelist URLs

In this section, you can edit the black listed or white listed keyword or URL.

Blacklisting or whitelisting the URLs

For details to black list or white list any URLs or keywords follow the steps mentioned in Adding Web Security Configurations section, the 8th step.

Devices

The Devices section helps you to view the number of devices to which the Web Security configuration is applied. You can also add more devices to apply the Web Security configuration.

Applying Web Security configuration to the devices

To apply configurations on the device, follow these steps:

1. Log on to the Seqrite MDM portal and navigate to **Profiles** > **Configurations**.
2. Select the Web Security configuration and click **Edit** icon > **Edit** tab > **Devices** > **Apply configuration to device**.

   The Apply configuration to devices dialog is displayed.
3. Select the devices to which you want to apply the configuration and click **Apply**.

   The Web security configuration is applied successfully.

Note:

In Web Security, the URL blocking works for Android devices on Chrome browser only.

Schedule Scan Configuration

With the Schedule Scan option, you can scan all the enrolled devices of MDM at fixed intervals. The scan can be scheduled at the following intervals such as Daily, Weekly, Fortnightly, and Monthly. The schedule scan configuration also provides an option for virus definition database update on Seqrite MDM client app only when the device is connected to the Wi-Fi. If the Update Virus definition database on client app via Wi-Fi only check box is not selected, then the virus definitions will be updated when the device is connected to the Internet via any network.

By default, Seqrite MDM checks the Internet connectivity and updates the virus definition database. But the Schedule Scan Configuration provides an option to update the virus definition database on client app via Wi-Fi only.

Note:

Schedule Scan configuration is applicable only to the Android devices.

Adding schedule scan configuration

To schedule a scan, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Configurations** > **Add.**
2. From the configurations list, select **Schedule Scan**.

   The Schedule Scan Configuration page is displayed.
3. Enter Schedule Scan Configuration Name and select the schedule scan type such as Quick or Full.
   - **Quick scan**: Lets you scan all the apps installed on the devices.
   - **Full scan**: Lets you scan the entire device such as external SD card, internal memory, and apps, etc.
4. Select a scan cycle to perform a scan at fixed intervals such as daily, weekly, fortnightly, or monthly.
5. Select the **Update Virus definition database on client app via Wi-Fi only** check box to update the virus definition database using the available Wi-Fi.

   Note:

   If the Update Virus definition database on client app via Wi-Fi only check box is not selected on the Seqrite MDM portal, the virus definition database on the client app will be automatically updated when the device gets connected to the Internet.
6. Click **Save**.

   The schedule scan is configured successfully.

Overviewing schedule scan configurations

After the Schedule Scan configuration is created, the Schedule Scan Configuration Details page is displayed.

To navigate directly to the Schedule Scan Configuration Details page, follow these steps:

1. Log on to the Seqrite MDM portal, and click **Profiles** > **Configurations.**
2. On the Configurations page, select the Scheduled Scan configuration which is to be viewed and click the **Edit** icon.

   The Schedule Scan Configuration Details page is displayed. The following options are available.
   - **Overview**: This option helps you to view the Schedule Scan configuration details. You can view the Setting Name, Schedule Scan Type, Schedule Scan Cycle, and Total Devices. You can also view recently added devices. To display all the devices added to the selected configuration, click **Show all**.

- **Edit**: Allows you to edit the Schedule Scan configuration details and assign the default configurations.

Editing Schedule Scan configuration

The Edit tab includes Edit details and Devices.

Note:

Editing the Schedule Scan Configurations will change the current version of the configuration.

- **Edit details**: With this option you can edit the information of the Schedule Scan configuration added to the Seqrite MDM portal.
- **Devices**: Helps you to view the number of devices to which the Schedule Scan configuration is applied. You can also apply the schedule scan configuration to more devices.

To edit the schedule scan configuration, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Configurations.**
2. On the Configurations list page, select the schedule scan configuration to be edited and click **Edit** icon > **Edit** tab > **Edit details**.

   You can edit the configuration details such as the Schedule Scan Configuration Name, Schedule Scan Type, and Schedule Scan Cycle. You can also select the option to update the virus definition database on client app using Wi-Fi.
3. Click **Save**.
4. Click **Devices** section and then click **Apply configuration to device**.

   The Apply configuration to device dialog is displayed.
5. Select the devices to which you want to apply the configuration and click **Apply**.

   The scheduled scan configuration is edited and applied to the device successfully.
   - To remove the Scheduled Scan configuration from any device, go to **Devices** section and select the check box available in front of the device name and click **Remove**.

Network Usage Configuration

With the Network Usage configurations, you can monitor the Internet data usage with respect to Wi-Fi, Mobile Data, and in Roaming status. You can create the new network configurations and apply the configurations to any particular device or any group. This configuration helps you to monitor the usage of Internet across all the devices enrolled with Seqrite MDM. You can monitor mobile data usage and Wi-Fi usage (MDM configured or all available Wi-Fi networks) as required. You can send alert notifications to the user when the user mobile data usage reaches the pre-configured limit and when the Wi-Fi data usage exceeds the daily limit. This option helps you to monitor data usage and across MDM network.

Adding Network Usage configuration

To create a new network usage configuration, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Configurations** > **Add**.
2. From the configurations list, select **Network Usage**.

   The Create Network Usage Configuration page is displayed.
3. Enter Configuration Name and configure Mobile Internet Plan by adding the following details:
   - Billing Cycle Start Date: Helps you to select the billing cycle start date.
   - Number Of Days: Helps you to add the billing period; such as 28 days or 30 days or 31 days.
   - Mobile Data Plan Limit (in MB): Helps you to set the mobile data plan limit.
   - Alert Notification At: Helps you to set the percentage of mobile data usage limit and to send the alert notification to the user when the set percentage is reached.
4. Configure Wi-Fi Settings by adding the following details:
   - Wi-Fi Daily Usage Limit (in MB): With this option, you can set the daily Wi-Fi usage limit and send the user an alert when the set daily Wi-Fi usage is exceeded.
   - Monitor wifi usage: This options helps to monitor all the Wi-Fi or MDM configured Wi-Fi network.
     - Monitor all Wi-Fi: This option monitors Wi-Fi data usage of Android devices across all SSIDs.
     - MDM Configured Wi-Fi Networks Only: This option will monitor Wi-Fi data usage for SSIDs configured through the MDM portal. It is mandatory to have at least one latest SSID configured and pushed to the device for data usage monitoring.
5. Click **Save**.

   The network usage setting is configured successfully.

Note:

After you apply the Network Usage configuration, the MDM app installed on the device will start monitoring the Internet data usage of the devices and send the details to the server.

Overviewing Network Usage Configuration

After the Network Usage configuration is created, the Network Usage Configuration Details page is displayed.

To navigate directly to the Network Usage Configuration Details page, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Configurations.**

2. On the Configurations page, select the network usage configuration to be viewed and click the **Edit** icon.

   The Network Usage Configuration Details page is displayed. The following options are displayed.

   - **Overview**: Helps you to view the Network Usage configuration details. You can view the date and time when the configuration was created, Configuration Name, Updated On, Billing Start Date, Number Of Days, Wi-Fi Daily Usage Limit, Mobile Data Plan, and Alert Notifications. The page also shows the recently added devices to a particular configuration. To view the devices added to the particular configuration, click **Show all**.
   - **Edit**: Helps you to edit the Network Usage configuration details and assign the default configurations if required.

Editing Network Usage Configuration

The Edit tab includes Edit details and Devices.

- Edit details: Lets you edit the Network Usage configuration.
- Devices: Lets you view the number of devices to which the Network Usage configuration has been applied.

To edit the network usage configuration details and apply it to the devices, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Configurations.**
2. On the Configurations page, select the network usage configuration to be edited and click the **Edit** icon > **Edit** tab > **Edit details**.

   You can edit the configuration details such as Configuration Name, Mobile Data settings, and Wi-Fi data settings.

3. Click the **Devices** section and then click **Apply configuration to device**.

   The Apply configuration to device page is displayed, which consists of the list of the devices added on the MDM portal.

4. Select the devices to which you want to apply the Network Usage configuration and click **Apply**.

   The network usage configuration is edited and applied to the devices successfully.

   - To remove the Network Usage configuration from the devices, go to **Devices** section and select the check box available in front of the devices name and click **Remove**.

Deleting configurations

The Default anti-theft and Web security configurations cannot be deleted. The customized configurations can be deleted. The customized Wi-Fi, schedule scan, Network Data Usage configurations can be deleted if those configurations are not applied to any devices.

To delete any customized configurations, follow these steps:

1. Log on to the Seqrite MDM portal and click **Profiles** > **Configurations**.
2. On the Configurations page, select the configurations which are not applied to any devices.
   - To delete multiple configurations in a single instance, follow these steps:
     i. On Configurations list page, select the check boxes in front of the configuration names which are to be deleted.

        The With selected option is displayed.
     ii. From the With selected list, select **Delete** and then click **Submit**.
     iii. On confirmation dialog, click **OK**.
   - To delete a single configuration, follow these steps:
     i. On Configurations list page, select the configuration which is to be deleted and click the **Delete** icon available in the Action column.
     ii. On the confirmation dialog, click **OK**.

Chapter 8

Apps

The Apps option lets you manage all the installed apps on the device. With the help of the Apps option, you can add new apps to the device, block the apps partially or fully, and activate the Launcher on the device. App management includes App Repository and App Configuration.

This chapter includes following sections:

Repository

The App Repository is the place where all the apps installed on the enrolled devices are stored. You can manage apps and add new apps to the App Repository. You can tag a label to the recommended apps and the apps that are to be uninstalled.

You can add the multiple versions of the application to the repository. You can upload the multiple versions of the application when you add the application via Custom URL and Custom APK options.

When the app is added to the app repository following information is collected from the newly added app.

App Status

In Seqrite MDM following app statuses are found:

- **Recommended apps**: The apps that are suggested to install on users device.
- **Apps to Uninstall**: The apps that are restricted to install on the users device.

App Type

Seqrite MDM categorizes the apps as follows:

- **Downloaded**: These apps are downloaded by the user. Only the downloaded apps can be deleted.

- **System**: These apps are inbuilt in the mobile.
- **Suggested**: These apps are suggested by the Admin.
- **Restricted**: These apps are restricted by the Admin.

Source Type

The Source Type shows the options from where the MDM apk. is downloaded and installed.

- Google Play
- Custom App URL
- Upload Custom APK

Category

All the apps on the Seqrite MDM portal are categorized in different categories such as; unknown, Books and References, Business, Comics, Communication, Education, Entertainment, Finance, Health and Fitness, Libraries and Demo, Lifestyle, Live Wallpaper, Media and Video, Medical, Music and Video, Medical, Music and Audio, News and Magazines, Personalization, Photography, Productivity, Shopping, Social, Sports, Tools, Transportation, Travel and Local, Weather, and Game.

Advanced Search for Apps

The Advanced Search option allows you to perform an advanced search for different apps. To search apps, follow these steps:

1. Log on to the Seqrite MDM portal and click **Apps** > **Repository** > **Advanced Search**.
2. Following search categories are displayed:
   - **Select App Type**: Select this option to search apps according to the app type.
   - **Select OS**: Select this option to search the apps according to the operating system.
   - **Select Category**: Select this option to search the apps according to the app category.
3. Select the required search options and click **Search**.

   The result gets displayed.

App Repository List Page

The App Repository page displays all the available apps of Seqrite MDM console. The table displays the information of all the apps such as OS, package ID, device count, status, type, source type, category etc.

With selected options for App Repository

The With selected list is beneficial to delete multiple selected apps. The following With selected options are available for App Repository.

- **Mark as suggested**: With this option you can recommend the user to install the selected apps on the user's device. You can suggest single or multiple selected apps at the same time. After you mark the selected apps as suggested, the status of the selected app will be changed to Suggested.
- **Mark as restricted**: This option helps you to mark the selected apps as restricted to uninstall them on the user's device. You can tag single or multiple selected apps to be uninstalled from the devices. After you mark the selected apps as restricted, the status of the selected app will be changed to Restricted.
- **Clear Status**: Helps you to clear the current status of an app. You can clear the tags: Suggested and Restricted.
- **Delete**: Helps you to delete a single or multiple selected apps.

  Note:

  - You can delete single or multiple selected apps only if the app is not associated with any device or app configuration.
  - When the app that is not associated with any device is deleted, its network data usage information is also deleted.

- **Upgrade**: With this option, you can upgrade the selected application.

  Note:

  Only the Android applications that are uploaded via a custom URL or custom APK can be upgraded.

To use the With selected options for App Repository, follow these steps:

1. Log on to the Seqrite MDM portal and click **Apps** > **Repository** > select a single or multiple apps.

   The With selected option is displayed.

2. Select the required option from With selected list and click **Submit**.

   The selected action is carried out on a single or multiple selected apps.

Adding Apps via App Repository

The Add option on the upper-right side of the App Repository page helps you to add a new app to the repository. This helps you whenever you want to recommend the app in case the app is not present in the app repository. Seqrite MDM provides the following options to add apps to the repository: From Google Play, Custom App URL, and Upload Custom APK.

You can also upload the latest version of the app, which is already there in the repository.

Note:

After adding the apps to the App Repository through the given options, you can configure these apps to install, block, or uninstall on the user devices.

Adding apps via Google Play Store

With this option you can add a new app to App Repository from Google play store. This is applicable only to the Android device users.

To add a new app through Google Play store, follow these steps:

1. Log on to the Seqrite MDM portal and click **Apps** > **Repository** > **Add** > **From Google Play Store**.

   The Add app from Google play store dialog is displayed.

2. Enter Google Play Store URL of the app in the given text box. You can refer to the example of the URL given in the dialog.
3. Click **Add**.

   A new app is added to the app repository.

Adding apps using Custom App URL

You can add a new app to the App Repository using the Custom App URL option. This option is applicable only to the Android device users. You can also add the other versions of the app via Custom App URL.

To add a new app using Custom App URL, follow these steps:

1. Log on to the Seqrite MDM portal and click **Apps** > **Repository** > **Add** > **Custom App URL**.

   The Add Custom App URL dialog is displayed.

2. Enter the App Name, Package Id, Version Name, Version Code, and APK URL in the respective text boxes.

   Note:

   - Ensure to provide the correct version name and version code of the custom app.
   - Only HTTP, HTTPS, FTP, and SFTP URLs are supported and the URL should direct to the APK file.

3. Click **Add** or click **Add and Publish** to add the application to the repository and publish on the user device.

   A new app is added to the app repository.

Adding App using Upload Custom APK

The Upload Custom APK option helps you to add a new app to the App Repository. This option is applicable only to the Android device users. You can also upload the other versions of the app to the app repository via Upload Custom URL.

To add a new app using Upload Custom APK, follow these steps:

1. Log on to the Seqrite MDM portal and click **Apps** > **Repository** > **Add** > **Upload Custom APK**.

   The Upload Custom APK dialog is displayed.

2. Select the .apk file that you want to add to the app repository.

   Note:

   Maximum file size of APK can be up to 50 MB and only the files with APK extension are allowed.

3. Click **Upload**.

   The new app is uploaded to the App Repository.

Configuration

The app Configuration option lets you control and apply app restrictions on the device. You can create new app configurations and apply the configurations on the devices. You can block access for any newly installed apps on the Android devices and block the apps based on the selected app categories that are available in Seqrite MDM. You can apply restrictions to block apps for the full time. You can also recommend apps for installation on the user devices. You can add a particular version or multiple versions of the apps as suggested, restricted, fully blocked, or whitelisted.

Additionally, you can also restrict and limit the usage of the apps by configuring Launcher. With the App Launcher option, the user will be able to see and access only the selected active apps. After App Launcher is configured on a particular device, the Launcher screen will be activated and then the user can view only the selected apps and configure only the selected settings on the device.

Note:

If the user tries to access other apps, then the Launcher will block the app.

Advanced Search for App Configurations

The Advanced Search option allows you to perform an advanced search for different app configurations.

To search app configurations, follow these steps:

1. Log on to the Seqrite MDM portal and click **Apps** > **Configuration** > **Advanced Search**.

2. Following search category is displayed:
   - **Select Created By**: Select this option to search configurations as per creator name.
3. Select the creator name and click **Search**.

   The search result gets displayed.

App Configurations List Page

The App Configurations list page displays all the created app configurations. The table displays the information of all the available app configurations, such as configuration name, type, number of devices, created on, last updated etc.

With selected options for app configurations

The With selected list appears on the App Configurations page when you select a single or multiple user role. The available options in the With selected list are:

- **Delete**: Helps you to delete the single or multiple selected app configurations.
- **Apply to Groups**: Helps you to apply the selected app configuration to the groups. You can apply the single configuration to multiple groups at the same time.
- **Apply to Device**: Helps you to apply the selected app configuration to the multiple selected devices.

 Note:

After you apply a new App Configuration to a group, it will overwrite the old App Configuration that was already applied.

1. Select the option from the With selected list and follow the steps mentioned below;
   - Select **Delete** and click **Submit**. Or
   - Select **Apply to Groups** or **Apply to Devices** > select the groups or devices to apply the configuration > click **Apply**.

   The selected action is carried out on a single or multiple selected apps.

Adding app configuration and activating the Launcher

The Add button on the upper-right side of the App Configuration page lets you create a new app configuration. With the help of this app configuration, you can block access to newly installed apps, block apps based on their categories, recommend an app or restrict an app from uninstalling. You can also block an app fully as per your requirement. Also, you can configure Launcher to restrict and limit the usage of the apps on the user's device.

App configuration provides many useful features to manage the apps as follows:

App Categories

Seqrite MDM provides App Categories section to help block different categories to which the applications belong. The app category blocking is applicable only to the Android devices. You can select either a single or multiple or all the app categories.

Whitelisted Apps

With this option, you can white list the apps. The white listed apps are accessible, even if their category is blocked. You can also add particular versions of the app to the white list. Only the selected, white listed versions of the application will be accessible to the user and other versions would be blocked. You can remove single or multiple versions of the app from the whitelist.

App Restriction

App Restriction feature applies restriction on apps in the following ways:

Apps to Uninstall

If you want the user to uninstall all the versions of the app, then select the entire package to uninstall all the versions. You can also add the particular version of the app to the uninstall apps list. The selected single or multiple app versions will be blocked and the other app versions will be accessible. This functionality is only applicable to the Android devices.

Fully Blocked Apps

Fully Blocked Apps option helps you to add the particular version of the app to the block list. The selected single or multiple app versions will be blocked and the other app versions will be accessible. If you want the user to block all the versions of the app, then select the entire application. You can fully block the apps of Android mobile devices.

- The Apps to uninstall and Fully Blocked Apps lists are not visible to the ADO and KNOX supported devices.

Recommended Apps

Recommended Apps functionality helps the user to add the apps to the recommended list and view the list. You can select the entire app or a specific version of the app and add to the recommended list. The selected app version will be recommended and the other app versions will be blocked. If you want the user to access all the versions of the app, then select the entire app and add to the recommended list. If the Restrict new app installation on ADO & Knox Enabled Devices check box is selected in the app configuration settings, then you will receive a prompt to clear the check box and then recommend the apps.

Note:

The device user will not be able to uninstall, force stop, and clear cache for the recommended apps on the KNOX devices.

System Kiosk Mode

System Kiosk Mode is applicable to the ADO enabled devices where Seqrite MDM Client is the device owner and also to the Samsung KNOX supported devices. At times if both Kiosk Modes (System Kiosk Mode and Launcher Kiosk Mode) are enabled, then System Kiosk Mode will have the priority. Thus, System Kiosk Mode setting will be applied on the device. But for Non-ADO devices, Launcher Kiosk Mode will be applied.

In System Kiosk Mode, you can add only one app to the ADO-supported devices. The user can access only the app added in the System Kiosk Mode. The app will be auto launched whenever the System Kiosk Mode is applied on the device or user restarts the device or if the user locks and unlocks the device. In case, if the Restrict new app installation on ADO & Knox Enabled Devices check box is selected in the app configuration, then you must first clear the check box and then add an app to System Kiosk Mode.

Launcher

Seqrite Launcher gives the experience of customized style and function of your mobile device. The Launcher tab helps you to activate the Seqrite Launcher.

Launcher Setting

In this section, you can configure Seqrite Launcher, Primary Settings, and Device Settings.

Seqrite Launcher

After the Launcher is activated on the device, the user must enable the Accessibility Service on the device. If the Accessibility Service is not enabled on the user device, the device will be blocked. To enable the accessibility service on the device, the user must select **Enable Service**. If the accessibility service of the device is disabled, then the Launcher may not work properly on the device. After activating Launcher, only the active apps will be visible on Seqrite Launcher and other apps will not be accessible.

If any app configuration with the Launcher is activated on the device, then the Launcher configurations will have the highest preference and all the other app configurations will be overridden. In case, you have deactivated the Launcher, then the App Configurations will be activated on the device by overriding the Launcher configurations.

At times, if the Restrict new app installation on ADO & Knox Enabled Devices check box is selected, you will receive a prompt to clear the check box and then recommend an app for Launcher setting.

Also, you can configure the exit launcher duration from the Launcher section.

Primary Settings

Settings	Description
Block Device Notification	Blocks all the notifications on the launcher screen. After blocking, the user will not be able to access the notification area on the device.

Allow Call & SMS	Allows call and text messaging apps on the device when the launcher is activated. If you do not want call and text messaging apps to be visible on the device, clear this option.
Set Password	Helps you to set the password on the device. If this setting is enabled, the device user can set or change the password on the device.
Location Service (GPS)	Allows the user to turn on the location, network, Wi-Fi services to get the device location on the launcher screen.
Disable App Request	Helps you to disable the app request option on the user request. If this setting is enabled, then the device user cannot send the request for the app.
Allow Device Hard Keys	Allows the user to use the hard keys of the device. If these settings are enabled, you can access the device power, volume, and menu keys. The menu key will be disabled to block the recent applications list. If the user is on the launcher screen, then the user can access volume and power keys. The user can change the volume of the device using hard volume keys, but you can revert the change to the volume that has been set and the user will be notified with a message that the change of the volume is blocked.
Allow Camera	Allows the user to use the camera on the device. If this setting is enabled, the user can use the camera app on the launcher screen.
Device Settings App	Allows the user to access the system settings on the device. If this setting is enabled, the user can access the device system settings.

Device Settings

The Device Settings help to manage and control the following aspect of the device such as brightness, volume, Wi-Fi, data network, auto rotate, Bluetooth, air plane mode, and sound.

Active Apps

If the apps added to the Active Apps list are installed on the user's device then only these apps will be visible and accessible on the launcher. In case, the added apps are not installed on the device then the apps will be added to the recommended list on the user's device and the user must install the recommended apps on the device.

The Active Apps section includes Normal mode and Kiosk mode.

- **Normal Mode**: In this mode, you can add apps to the Active apps list. This list includes the apps that you want the user to access on the device when the launcher is activated.
- **Kiosk Mode**: In this mode, you can add only one app to the active apps list of Kiosk mode. The user can access only the app added in the kiosk mode. The app will be auto launched when the kiosk mode is applied on the device, user restarts the device, or if the user locks and unlocks the device.

Note:

Whenever the Launcher Kiosk Mode settings are applied and System Kiosk Mode settings are also active, then System Kiosk Mode settings will be applied on the ADO supported devices.

Also, make sure the **Restrict new app installation on ADO & Knox Enabled Devices** check box is not selected in app configuration.

Branding

The Branding option is helpful in changing the company name, company logo, and wallpaper on Launcher. These Launcher Setting override all the custom settings at company level (Admin settings).

Adding new app configuration and activating the Launcher

To add new app configuration, follow these steps:

1. Log on to the Seqrite MDM portal and click **Apps** > **Configuration** > **Add**.

   The Create App Configuration page is displayed.

2. In Edit Details section, enter the configuration name in **App Configuration Name** text box.
3. To restrict the user from using the newly installed apps on ADO and KNOX supported devices, select the **Restrict new app installation on ADO & Knox Enabled Devices** check box.

   - If you do not want to block the new app installation on ADO and KNOX devices, clear the check box.

   Note:

   If you are recommending the apps, adding app to the Launcher, or adding app to System Kiosk Mode, then you will receive a prompt to clear the **Restrict new app installation on ADO & Knox Enabled Devices** check box. Then either use the check box or the App Configuration settings.

4. To make this app configuration a default configuration, select the **Default** check box.
5. Click **Next**.

   The Edit Configurations tab displays App Categories, App Restrictions, Recommended Apps, and System Kiosk Mode sections.

6. In App Categories section, you can take the following steps:

   i. Select the app categories check boxes which are to be blocked.

   ii. To select all the available app categories, you can select the **Select All** check box.

   iii. To exclude any app from the blocked category, you can add that particular app to the Whitelisted apps list by clicking **Add Apps**.

In Add apps to whitelist dialog, you can perform an advance search to view the downloaded, system, suggested, and restricted apps. Also, white list particular version of an app.

7. Click **Next**.
8. In App Restrictions section, you can restrict the apps by adding the apps to the **Apps to uninstall** list and **Fully Blocked Apps** list.

   Note:

   Apps added to **Apps to uninstall** and **Fully Blocked Apps** lists are not visible to ADO and KNOX supported devices.

   i. To add apps to uninstall list, click **Apps to uninstall**. Click the **Add Apps** button. In new window, select the apps. Add Apps button gets visible. Click **Add Apps**.

   ii. To add apps to fully blocked list, click **Fully Blocked Apps**. Click the **Add Apps** button. In new window, select the apps. Add Apps button gets visible. Click **Add Apps**.

   When adding apps to uninstall or fully blocked list, you can also perform an advanced search to view the separate list of downloaded, system, suggested, and restricted apps.

9. Click **Next**.
10. In Recommended Apps section, to recommend any Android app or app version, click **Add Apps**. In new window, select the apps. Add Apps button gets visible. Click **Add Apps**. Make sure the **Restrict new app installation on ADO & Knox Enabled Devices** check box is not selected in app configuration.

    Note:

    - User will not be able to uninstall, force stop, and clear cache for recommended apps on Samsung KNOX devices.
    - Custom Apps in recommended list will be silently installed on the ADO and Samsung KNOX devices.

11. Click **Next**.
12. In System Kiosk Mode section, you can recommend a single app in Kiosk mode for ADO supported devices.

    i. In System Kiosk Mode for ADO devices page, click **Add Apps**.

    ii. In Add Apps for Kiosk Mode page, select the app, and click **Add Apps**.

    Make sure the **Restrict new app installation on ADO & Knox Enabled Devices** check box is not selected in app configuration.

13. Click **Next**.

A confirmation to enable the ADO Kiosk mode is displayed.

14. Click **OK**.

    You are directed to the Launcher settings section.

15. In Launcher Setting section, you can turn on the device Launcher. After enabling the Launcher, on the confirmation screen, click **Activate**.

    The Restrict new app installation on ADO & Knox Enabled Devices check box must be cleared before recommending an app for Launcher.

    Note:

    - The Launcher configuration will always have the highest preference as compared to app configurations. If Launcher is activated, only the Launcher configuration will work on the device and app configurations will not be applicable. When the Launcher is deactivated, all the app configurations will be applied again on the device.
    - If the Seqrite Launcher option is turned OFF, the Launcher will get deactivated from the device. The device user will not receive any prompt to uninstall the Launcher.

    When the Launcher activates, you can configure the following things:

    - **Launcher reminder**: Use this option to set the time and send a prompt to the user to activate the Launcher on the device. The available options are 1 minute, 2 minutes, 3 minutes, 5 minutes, 10 minutes, and 30 minutes.
    - **Launcher Exit Duration**: You can configure the time to exit the Launcher. Enter the time in the Launcher Exit Duration field to allow the user to exit the Launcher for a limited period. The user of the device must enter the passcode to exit the launcher. The default time to exit the launcher is 30 minutes.
    - **Primary Settings**: Configure the primary settings to access the selected settings on the device Launcher screen. To know more about primary settings, see Primary Settings.
    - **Device Settings**: Configure the device settings options to access the selected device settings on the Launcher screen.

16. Click **Next**.

    The Active Apps section is displayed.

17. Select either the Normal Mode or Kiosk Mode. For more information about normal and kiosk mode, see Active Apps.

    i. To add apps to the Active Apps list in Normal Mode and Kiosk Mode, click **Add Apps**. The Add apps on launcher dialog is displayed. Select the apps that you want to view on the Launcher and click **Add Apps**.

Note:

- In Kiosk Mode, you can add only one app to the Active Apps list. This Launcher Kiosk Mode is applicable to the non-ADO devices.
- If the System Kiosk Mode settings are active with Launcher Kiosk Mode, then System Kiosk Mode settings will be applied on the ADO supported devices.
- Only the selected app versions are visible on the Launcher.
- Make sure that the apps added to the Active Apps list are installed on the user's device.

18. Click **Next**.

    You are directed to the Branding section, where all the fields would be dimmed/disabled. You can make following changes to the Launcher setting.

19. On the Branding page, select the **Enable Launcher Branding** check box.

    All the other fields on the page get enabled, where you can change the **Company Name**, **Company Logo**, and **Launcher Wallpaper.**

    i. Change the Company logo and Launcher Wallpaper by clicking the **down arrow** > **Upload** > selecting the image. For best logo and wallpaper image experience, you must use the following image resolutions:
       - Company logo: Between 300 X 300 pixels to 1000 X 1000 pixels.
       - Wallpaper: 1080 x 1920

20. Click **Save**.

    The changes are reflected on the Launcher.

    The app configuration is created successfully.

    You can export the details of the configuration in PDF format.

Note:

The changes done to company name and logo, and launcher wallpaper, from this section (Launcher Setting) will override all the company and launcher settings of Custom Settings.

Overviewing and editing app configuration and Launcher

After the app configuration is added to the Seqrite MDM portal, the App Configuration page is displayed. You can edit configuration details.

To overview and edit the app configurations, follow these steps:

1. Log on to the Seqrite MDM portal and click **Apps** > **Configuration** > **Edit** icon.

   Overview of the app configuration is displayed.

   The Overview page informs about the configuration created date, setting name, number of devices to which the configuration is applied, version of the configuration, if the

configuration access is blocked for newly installed apps or if the configuration is marked as default. Also, it lists the devices to which the configuration was applied.

2. Click the **Edit** tab.

   Edit details and Device options are displayed.

3. In Edit details section, you can edit the configuration details; such as configuration name, mark it as default or block the configuration access to the newly installed apps.

4. Click the **Devices** tab.

   List of devices to which the configuration is applied is displayed.

5. To apply the configuration to any device, click **Apply configuration to device**. In the new screen, select the devices and click **Apply**.

6. Click the **Edit Configuration** tab. In this section,

   - In App Categories section, you can block the category or remove category blocking by selecting or clearing the check boxes. Also, white list the apps or app versions.
   - In App Restrictions section, you can edit the uninstall list or fully blocked list.
   - In Recommended Apps section, you can add apps or app versions to the recommended list.
   - In the System Kiosk Mode, you can add or remove the app that will be visible on ADO supported devices in Kiosk mode.

   To get more information, see Adding new app configuration and activating the Launcher.

7. Click the **Launcher** tab.

   In this section, you can change the Launcher settings and edit the Active Apps list as follows:

   - Turn on or off the Launcher, or change the alert time, or change the Launcher exit duration.
   - You can change primary settings or device settings.
   - You can edit the active apps list.
   - With respect to branding, you can add or change the company logo and wallpaper that will be displayed on the Launcher.

8. To save the edited configuration, click **Save**.

Deleting App Configurations

The app configurations can be deleted using any of the either options:

- On App Configurations list page, select a single app configuration and click the **Delete** icon in Actions column.
- On App Configurations list page, select single or multiple devices. The **With selected** option is displayed. Select **Delete** and then click **Submit**.

Chapter 9

Fencing

With the rise in the number of mobile devices, securing the confidential data has become crucial. Seqrite MDM upholds a very strong feature of fencing for securing the confidential data. The Fencing feature acts as a virtual boundary.

Fencing allows you to setup rules to allow or to restrict the user by applying the profiles or app configurations to the user device.

Seqrite MDM defines the safe areas for the devices. The fence triggers and sends alerts when the device leaves the assigned boundaries. The virtual barrier allows you to know the user device entry or exit of defined boundaries. You can set up the triggers when the device meets the defined boundaries. The fencing technique uses geographical locations, Wi-Fi SSIDs, and time as boundaries.

After the fence is created, apply the restrictions on the device. The configurations must be applied on the device to limit the usage of the features on the device.

This chapter includes the following sections:

Fences

The Fences option helps you to add new fences and modify the details of the fences. You can create a boundary of the fencing and apply the fence restrictions on the device. Seqrite MDM provides the following fences: Wi-Fi Fence, Geo Fence, and Time Fence.

Advanced Search for Fences

The Advanced Search option allows you to perform an advanced search for different fences created in Seqrite MDM.

To search fences, follow these steps:

1. Log on to the Seqrite MDM portal and click **Fencing** > **Fences** > **Advanced Search**.

   Following search category is displayed:

- **Select Configuration type**: Select this option to search fences of a particular configuration types including Wi-Fi, Geo, and Time.

2. Select the required configuration type and click **Search**.

   The result gets displayed.

Note:

Fencing is applicable only to the Android devices.

Fences List Page

The Fences list page displays all the configured fences. You can change the look of Fences list page either as a map or in the table format.

- **Map**: On Fences list page if Map is clicked, all the fences and their details are displayed on the map. To view the details of the fence, you have to locate the fence and click on it.
- **Table**: If Table is clicked, all the fence configuration details are displayed in table format.

With selected options for Fences

When you select single or multiple fences, the With selected option appears on the Fences list page.

- Select **Delete** and then click **Submit**. The selected action is carried out on the selected fences.

Fences

Seqrite MDM helps you to create virtual boundaries for your devices with the help of fences.

Seqrite MDM supports the following fence types.

Wi-Fi Fence

The Wi-Fi fencing is a technique that uses Wi-Fi SSID to define the fence. Whenever the user device gets connected to the defined SSID, the Wi-Fi fence triggers and then the selected restrictions in that Wi-Fi fence are applied on the device. While creating a Wi-Fi fence, you can provide any Wi-Fi SSID, and in addition you can select only the existing SSID from Wi-Fi configuration list.

Note:

The new SSID which is added while creating a Wi-Fi fence, will not be the part of Wi-Fi Configuration. The Wi-Fi fence will be triggered only after the authentication process.

Geo Fence

The Geo fencing helps to create the fence with restrictions in a geographical area. This option lets you allow or restrict the usage of the features within a specific area by tracking the device via GPS (global positioning system). Whenever the device enters the defined location, then the Geo fence triggers on the device and all the restrictions are applied on the user's device. This fencing allows to create a virtual barrier around a location on a map. This option helps to detect entry or exit of the device from the defined perimeter. You can draw a circle on the map to define the boundaries. You can add a new geo fence by defining radius or length on a geographical location of a map.

When multiple Geo fences are added in an organization, then the details of each Geo fence is important and should be handy. So, Seqrite MDM facilitates to import the Geo fence details. On Fences list page, the **Import Geo Fence** button is available to import the Geo fence details. In single instance, maximum of 1000 Geo fences details can be imported.

Time Fence

The Time fencing helps you to setup the time-based rules to be applied on the user devices. This option helps to limit the users of Seqrite MDM by defining the time as the boundary. You can define a particular time and particular dates to define the fencing. Whenever the defined time is executed on the device, then the fence triggers on the device and the restrictions are applied on the device. If you want to execute time fencing on particular days within the defined time range, you can select the days that you want to execute fencing. You can also exclude executing the fencing on a particular date from the defined fencing period.

Defining Fence

The Add option on the upper-right side of the Fencing page helps you to add a new fence. This helps you to add different types of fences that complies the requirement.

Adding Wi-Fi Fence

To add a Wi-Fi fence, follow these steps:

1. Log on to the Seqrite MDM portal and click **Fencing** > **Fences** > **Add** > **Wi-Fi Fence**.

   The Add Wi-Fi page is displayed.

2. Enter the name of the Wi-Fi and then select **Wi-Fi SSID**. If the Wi-Fi SSID is a new one, then enter SSID. If you want to use existing SSID from Wi-Fi configuration, then select **Existing Wi-Fi SSID**. After selecting existing Wi-Fi SSID, all the configured Wi-Fi SSIDs of Wi-Fi configuration are displayed.

3. Click **Add**.

   A new Wi-Fi fence is added.

Adding Geo fence

To add Geo fence, follow these steps:

1. Log on to the Seqrite MDM portal and click **Fencing** > **Fences** > **Add** > **Geo Fence**.

   The Add Geo Fence page is displayed.

2. Enter the place name to select the location and define the boundaries. The place name you entered will show the exact location on the map or will help to locate the place.
3. Click **Add Geo Fence**.

   The Save Geo Fence dialog is displayed.

4. Enter the Fence Name, radius in meters, and then click **Save**.

   The Geo Fence is created successfully and a red circle with defined boundary length is displayed on the map. You can create multiple Geo fences from the same map by selecting locations. If you want to see all the created Geo fences, click **Show All Geo Fences**.

Note:

- The radius of the location must be at least 100 meters.
- Please be noted that the Geo fence triggers only when you select High Accuracy mode location service.

Importing Geo fence

The feature to import geo fence is beneficial to import multiple fences in a single instance and get all the geo fence details. This feature shows valuable data of geo fence, which helps the Admin to make appropriate changes to the geo fences. The imported geo fence details provide information about fence name, location, latitude, longitude, and radius of the fence. In one instance, you can import maximum of 1000 fence details.

To import geo fence, follow these steps:

1. Log on to the Seqrite MDM portal and click **Fencing** > **Fences** > **Import Geo Fences**.
2. Select the CSV file in which fence details are added and click **Import**.

   To get more information about the CSV file format, click **Download CSV sample format**.

Adding Time Fence

To add a new time fence, follow these steps:

1. Log on to the Seqrite MDM portal and click **Fencing** > **Fences** > **Add** > **Time Fence**.

   The Add Time Fence page is displayed.

2. Enter the name of the time fence, select **Set Time Fence on** option. The Set Time Fence on option includes two types: Date Range and Recursive on Days.

- **Date Range**: Select the Date Range option to define a particular date range. The fencing is executed on the selective date range.
- **Recursive on Days**: Select this type to execute fencing on the selected days.

3. Set the **From Time** and **To** time to define the time period.
4. In case you want to exclude the fence on certain dates, select the dates and then click **Save**.

   The time fence is added successfully.

Overviewing and editing fence information

After you add a new fencing to the Seqrite MDM portal, you can view and modify the fencing details as required. This option helps you to edit the details of the fencing, which you have entered at the time of creating a new fence. You can also view the information of a selected fencing.

To navigate directly to the Fencing Details page, follow these steps:

1. Log on to the Seqrite MDM portal and click **Fencing** > **Fences**.
2. Select the fence which is to be viewed or edited and then click the **Edit** icon from Actions column.

   Tip:

   To edit the time fence, click the Edit icon in front of the Time Fence only. Similarly, to edit the Geo or Wi-Fi fence, click the Edit icon in front of Geo or Wi-Fi fence only.

3. The Fence overview page is displayed with fence details.

   The fence details change according to the type of fence selected.
4. Click **Edit** tab.
   - For Wi-Fi and Time fence, in Edit details section, you can edit the fence information.
   - For Geo fence, in Edit tab a map is displayed with the fence balloon. To edit the geo details, click the balloon. In Save Geo Fence dialog, make the required changes.
5. To save the edited fence configurations, click **Save**.

   To get the complete detail of the fence configuration, click the **Export** button.

Deleting Fences

The Fences can be deleted using any of the either options:

- On Fences list page, select a single fence and click the **Delete** icon in Actions column.
- On Fences list page, select single or multiple devices. The **With selected** option is displayed. Select **Delete** and then click **Submit**.

Configurations

The fencing configurations allow you to map with the defined fences and implement the applied restrictions on the devices. With the help of fencing configurations, you can configure the profiles and app configurations on the device.

The Fencing Configuration option lets you control and apply restrictions on the device. The restrictions include policies, configurations, and app configurations. You can create new fencing configurations and apply the configurations on the devices. You can block access to the device if GPS, Wi-Fi, and Automatic Date and Time are disabled on the device to ensure the fence triggers as per the defined fence conditions.

You can add new configurations, add fence group, and define a new fence if required.

Advanced Search for Fence Configuration

The Advanced Search option allows you to perform an advanced search for different fence configurations.

To search fence configurations, follow these steps:

1. Log on to the Seqrite MDM portal and click **Fencing** > **Configurations** > **Advanced Search**.
2. Following search category is displayed:
   - **Select Created By**: Select this option to search the fence configuration according to the creator name.
3. Select the creator name and click **Search**.

   The search result is displayed.

Fence Configuration List Page

The Configurations list page displays and provides information of all the fence configurations available in Seqrite MDM.

With selected Options for Fence Configuration

The With selected option appears on the Fence Configurations page when you select single or multiple fence configurations. The available options in the With selected list are:

- **Delete**: Deletes the selected fence configurations. You can delete a single or multiple selected apps.
- **Apply to Groups**: Helps you to apply the selected fence configuration to the groups. You can apply the single fence configuration to multiple selected groups.

1. Select the required option and follow either steps:
   - Select **Delete** and click **Submit**. Or
   - Select **Apply to Groups** > click **Select Groups** > select the groups to apply the configuration > click **Apply**.

Add fence configuration

The Add option on the upper-right side of the Fence Configuration page helps you to add a new fence configuration. This helps you to add the fence configuration according to the requirement.

When creating fence configuration, you need to understand:

Fence Group

Fence group includes the list of fences, actions, policies, and restrictions that have to be applied on the device when the device meets the defined fence condition. You can select the actions and restrictions to be applied on the device. You can create multiple fence groups in one fence configuration. The multiple fence groups help to apply restrictions on the device based on the defined fence conditions. The fence group is applied as per the priority. The first priority is given to the latest fence group created. You can edit the name of the fence group and delete the fence group if required.

Define Fence

The define fence option helps to create new fence for Geo, time, and Wi-Fi.

Adding and defining fence configuration

1. Log on to the Seqrite MDM portal and click **Fence** > **Configurations** > **Add**.

   The Add Fence Configuration page is displayed.
2. Enter the name of the configuration and description.
3. Select the following required check boxes:
   - **Compel the user to enable Location Service on device**: Select this check box to force the user to enable GPS on the device. It ensures that the Geo fence triggers as per the defined fence conditions.
   - **Compel the user to set automatic date/time on device**: Select this check box to force the user to configure automatic time on the device. It ensures that the Time fence triggers as per the defined fence conditions.
   - **Compel the user to enable WiFi on device**: Select this check box to force the user to enable Wi-Fi on the device. It ensures that the Wi-Fi fence triggers as per the defined fence conditions.
4. Select either options:
   - **Add Fence Group**: Select this option to apply restrictions on the already defined fences.
   - **Define Fence**: Select this option to define a new fence.
5. To create a new fence, follow these steps:
   i. Click **Define Fence**. The Define Fence page is displayed.

ii. Select the fence type such as Geo, Wi-Fi, and Time fence and create the new fence as required. To know how to create different types of fences, see Add Fences.

iii. After the new fence is created, click **Add Fence Group** to apply restrictions on the defined fences. The Fence Group section is displayed.

6. Select the Geo Fence, Time Fence, and Wi-Fi Fence that you want to apply on the device.
7. Set the Fence Relation option to AND or OR as required.
   - If you select AND, the fence triggers only when all the defined fence conditions are met.
   - If you select OR, the fence triggers when any of the defined fence conditions meet.
8. Select any **Set Trigger on** option:
   - **Fence In**: If you select the fence In, the restrictions will be applied on the device when the device goes into the defined fences (Geo, Time, Wi-Fi) fence.
   - **Fence Out**: If you select Fence Out, the restrictions will be applied on the device when the device goes out of the defined fences (Geo, Time, Wi-Fi).
9. Select Action/Alert/Restriction to be performed when the fence configuration is applied on the device.
   - **Define Actions**: When the device comes in the defined fence, the defined actions will be carried out on the device such as Block, Trace, and Notification. The MDM Admin will get the notifications.
   - **Alerts**: If this option is selected, the user will receive SMS notification when the fence is triggered.
   - **Apply Restriction**: Helps to apply restriction on the device when the fence configuration is applied on the device. The restrictions include Policies, Web Security configurations, and App configurations.
10. Click **Save**.

    The new fence configuration is created.

Note:

- You can reorder the fence groups to change their priority.
- If GPS is blocked in any policy then it will not map with Geo Fence. If Wi-Fi is blocked in any policy then it will not map with Wi-Fi Fence.

Overviewing and editing fence configurations

After the fence configuration is created, the fence Configuration Details page is displayed.

To navigate directly to the Fence Configuration Details page, follow these steps:

1. Log on to the Seqrite MDM portal and click **Fencing** > **Configurations.**

2. On Fence Configurations page, select the configuration and click **Edit** icon.

   The Fence Configuration Details page displays the following:

   - **Overview**: This page shows the fence configuration details. You can view the Name, Version, Description, and number of groups assigned to the configuration. You can also view recently added groups. To display all the groups added to the selected configuration, click **Show all**.

3. To edit the fence configuration details, click **Edit** tab.

   The Edit tab includes Edit details and Groups sections.

4. In **Edit details** section, you can edit the configuration and fence group details.

5. Click **Save**.

6. Click **Groups.** In this section you can add the groups or remove the groups from the fence configuration.

   Note:

   If the configuration is edited, its current version will be changed.

7. Click **Add Groups to Fence Configuration**.

   The Apply Fence Configuration to device group dialog is displayed.

8. Select the groups to which the fence configuration is to be applied and click **Add Group**.

   Configuration is applied to the selected groups.

   - To remove the applied fence configuration from any group, go to **Groups** section, select the groups and click **Remove**.
   - To get the details of fence configuration, click **Export**.

Chapter 9

Reports

Seqrite MDM provides an extensive report for different types of modules. These reports are very useful for analyzing and solving specific issues and formulating official policies.

This chapter includes the following sections:

Standard Reports

Standard reports help you to get the detailed reports on Infection Status, Network Data Usage, and App Non-Compliance. You can also get reports of particular date range and export these reports in CSV and PDF formats.

Note:

- You must filter the options to view the reports.
- The Export button appears only when a report is selected.

The following types of standard reports are available on Seqrite MDM:

- Infection Status
- Network Data Usage
- App Non-Compliance

Infection Status

The infection status report displays the detailed information related to the threats and infected devices. Infection Status displays two types of reports based on your search.

- Infection status report for device
- Infection status report for threats detected

Viewing infection status report for devices

The infection status report for devices include the list of devices that were infected. You can also search for the devices that are infected in a particular date range, view the name of the device, type of threat detected, number of threats detected, and details of the threats detected.

To view the infection status reports related to the devices, follow these steps:

1. Log on to the Seqrite MDM portal and click **Reports** > **Standard Reports**.

   The Reports page is displayed. Select appropriate filter criteria to view the reports.

2. In Report Type list, select **Infection Status**.
3. In Select Type list, select **Device** and then select the **Date Range** and click **Search**.
4. The list of infected devices, which are infected in the selected date range, is displayed. The device report shows the following details; Device name, Threat Type, Threats detected, and View Details.

   Note:

   If any particular date is not selected, a list of all the infected devices is displayed.

5. To get more information about a particular device and the threats detected, click **View Details**.

   The Threats Detected dialog is displayed. You can view the following details; Threat Name, Threat Type, and Date.

6. To go back to the Reports page, click **Close**.

Viewing infection status report for threats detected

The infection status report for threats detected includes the list of threats detected on the device. You can also view the details of the threats detected in a particular date range. You can view the following information; Threat name, Threat Type, Device Count, and View Details.

To view the status reports for the threats detected, follow these steps:

1. Log on to the Seqrite MDM portal and click **Reports** > **Standard Reports**.

   The Reports page is displayed. Select appropriate filter criteria to view the reports.

2. In Report Type list, select **Infection Status.**
3. In Select Type list, select **Threat Name** and **Date Range**, and then click **Search**.

   The list of detected threats for the selected date range, is displayed. The threat report shows details about Threat Name, Threat Type, Device Count, and View Details.

 Note:

If any particular date is not selected, a list of all the threats that were detected is displayed.

4. To know more about a particular threat and the infected devices, click **View Details**.

   The Device Count dialog is displayed. You can view the following details; Device Name, Threat Type, and Date.

5. To go back to the Reports page, click **Close**.

Network Data Usage

The network data usage report includes the usage of network data by the devices and apps. You can search standard reports of network usage by the apps and devices for a selected date range. The report displays the detailed information of the network data usage of devices and apps with respect to Mobile Data, Wi-Fi, and in Roaming status. Network Data Usage displays two types of reports based on your search:

- Network data usage by devices
- Network data usage by apps

You can export these reports in CSV and PDF formats.

Viewing network data usage by devices

This search gives the report for the devices that utilized the network data in a particular date range within the MDM network. You can also view the report of data usage with respect to Mobile, Wi-Fi, and in Roaming status.

To view the network usage report for the device within the MDM network, follow these steps:

1. Log on to the Seqrite MDM portal and click **Reports** > **Standard Reports**.

   The Reports page is displayed. Select appropriate filter criteria to view the reports.

2. In Report Type list, select **Network Data Usage**.
3. In Select Type list, select **Device**. Select the **Date Range** and then click **Search**.

   The list of devices that utilized network data for the selected date range, is displayed. The report shows details about Id, Device Name, Mobile Data (in MB), Wi-Fi Data (in MB), and roaming.

    Note:

   If any particular date range is not selected, usage for all the devices is displayed.

4. To go back to the Reports page, click **Close**.

Viewing network data usage by apps

This search gives the report for the apps that utilized the network data in a particular date range within the MDM network. You can also view the report of data usage by the individual app with respect to Mobile, Wi-Fi, and Roaming.

To view the network usage report for an app, follow these steps:

1. Log on to the Seqrite MDM portal and click **Reports** > **Standard Reports**.

   The Reports page is displayed. Select appropriate filter criteria to view reports.

2. In Report Type list, select **Network Data Usage**.
3. In Select Type list, select **Apps** and then select the **Date Range** and click **Search**.

   The list of the apps that utilized the network data in the selected date range is displayed. The report includes the app icon and shows details about the App Name, Mobile Data (in MB), Wi-Fi Data (in MB), and Roaming.

   Note:

   If any particular date range is not selected, then the usage for all the apps is displayed.

4. To go back to the Reports page, click **Close**.

App Non-Compliance Report

The standard reports of app non-compliance display the detailed information about non-compliant apps. The report is generated as per the status of the app such as Installation pending, Upgradation pending, Downgrade pending, and Uninstallation pending. You can export these reports in CSV and PDF formats.

- If you have recommended the app to install on the user device and the installation is pending, then the app will go into non-compliance mode and a report is generated.
- If you have asked the user to uninstall a particular app on the user's device and the uninstallation is pending, then the app will go into app non-compliance mode and a report is generated.
- If an update of the MDM app is available and the users have not upgraded the app, then the app will go into non-compliance mode and a report is generated. If you recommend the higher or lower version of the app which is already installed on the device, and the user has not upgraded or downgraded the app, then that app will go in app non-compliance mode.

Viewing app non-compliance reports for devices

To view app non-compliance reports for devices, follow these steps:

1. Log on to the Seqrite MDM portal and click **Reports** > **Standard Reports**.

   The Reports page is displayed. Select appropriate filter criteria to view the reports.

2. In Report Type list, select **App Non-Compliance Report**.
3. Select the app name, app version, and then click **Search**.

   The non-compliance report of the app is displayed. The report shows the following details; Device id, Device Name, Device Group, Device Owner, App Version, and App Non-Compliance Reason.

   Note:

   If any particular application is in compliance mode, then no report will be generated.

Exporting standard report

All the available standard reports can be exported in PDF or CSV format.

- On Standard Reports list page, select the required search criteria and click **Export**.

Custom Reports

The custom report assists you to create reports on your own and customize them according to the requirement. Select the entities to build custom reports from scratch to suit the exact needs of your requirement and the way it should be displayed. The selected entities are highlighted in yellow to help you understand the entities selection. You can change the header names as per your requirement. You can create custom reports based on specific devices, user groups, date ranges, file preferences or profiles. These reports are centralized within the Seqrite MDM portal.

The custom report can be exported in CSV file format when you click the View or Export icon on the Custom Reports page. When the custom report result generates a huge data, the report cannot be viewed and it gives a warning message. In such scenario, if any date fields are available in the report, you can use them to filter the columns and generate the custom report.

Advanced Search for Custom Reports

The Advanced Search option allows you to perform an advanced search of the custom reports.

To find custom reports with the Advanced Search option, follow these steps:

1. Log on to the Seqrite MDM portal and click **Reports** > **Custom Reports** > **Advanced Search**.

   The advanced search parameter is displayed.

   - **Select Created By:** Select this option to search custom reports according to the creator name.

2. Click **Search**.

   The search result is displayed.

Viewing reports

You can view the custom reports created as per your requirement. The custom reports can be viewed in the following formats.

- **Data table**: Displays the set of rows and columns in the tabular format. The table gives a clear understanding and observation of each and every column and row.
- **Pivot table**: Summarizes, analyzes, explores, and displays the data as per your requirement. You can simplify the complexity of any table and organize your table by using the Pivot table. This table helps you to generate a table that has column and row headers, which is devoid of blank rows. You can click any cell in the range of cells or table. A pivot table can automatically sort, count, total or display the average of the data stored in one table or spreadsheet and displays the results in a second table showing the summarized data. Pivot table helps to create unweighted cross tabulations. You can customize the table by dragging and dropping the fields graphically.

To view the custom report, follow these steps:

1. Log on to the Seqrite MDM portal and click **Reports** > **Custom Reports** > click **View (Eye-shape)** icon.

   The Custom Report page is displayed.

2. The report will be generated in data table format (by default). The Admin can choose Pivot Table if required to change the report preview.

   Note:

   - You can view other reports by selecting the report name from the Select report list and then click Generate Report.
   - When creating a report, if any date field is selected in the selected entities then when the report is generated, a **Select date field** list is displayed with a calendar to select the date range.

3. If any date field is available in the created report, then select the option from **Select date** field list, and click the calendar and select the date range.

   If different dates are selected when providing a date range, a warning message is displayed. Make sure to select a continuous date range.

4. Click **Generate Report**.

   The report gets generated for the given date range.

   - To export the report, click **Export**.

Note:

- If the report generates huge data, then the error message is displayed at the time of export and the report cannot be exported.
- When trying to export the report by clicking the Export icon on Custom Report list page and the generated report shows huge data, a warning message is displayed.

Generating custom report

You can generate the custom report by selecting the multiple entities.

To generate custom report, follow these steps:

1. Log on to the Seqrite MDM portal and click **Reports** > **Custom Reports**.

   The reports page is displayed. If reports are not available, then the Reports page will be empty.

2. Click **Add**.

   The Create Report page is displayed.

3. Enter Report Name, and then select the Root entity as per your requirement.

   The root entities include User, Department, Device, Device Group, User Role, Policy, App Repository, Configurations, and Fence Configurations.

   Note:

   Only one entity should be selected from the Root entity list.

   After you select the Root entity, all the entities related to the selected root entity are displayed.

5. Click the sub-entities as per your requirement.
6. After the entities are selected, they are displayed under the **Selected Entities** section. Click the entity from the list; the relevant columns of the selected entity are displayed.
7. Select all or few columns of the selected entity that you want to include in the report. The selected columns are displayed in the lower-half section of the Report Details page.

   Note:

   When creating the custom reports, maximum of 15 columns can be included. The report should not exceed the set limit of 15 columns.

   The Report Details page includes the following columns:

Options	Description
Entity	Displays the selected entity. The entities include User, Department, Device, Device Group, User Role, Policy, App Repository, Configurations, and Fence Configuration.
Field	Displays the selected fields of the entity.
Is visible	Displays the type of the fence: Wi-Fi fence, Geo fence, and Time fence.
Caption	Allows you to change the name of the column header as per your requirement.
Search Criteria	The Select Criteria column includes two sections such as Select Where Operator and Filter parameter. • Select Where Operator: Helps to select the operator as per the requirement. You can precise your data in Custom Report by using Where Operator while creating and editing the report. The operators include Less than, Greater than, Equals, Less than equal, Greater than equal, Not equal, In, Not In, Contains, Does not contain, Starts with, and Ends with. You can use the following operators with the respective data type: • String data: Supported operators for string data are Equals, Not equal, Contains, Does not contain, Starts with and Ends with. For example: Device Name, App Name, Device Status, etc. • Numeric data: Supported operators for numeric data are Less than, Greater than, Equals, Less than equal, Greater than equal, Not equal, In, Not in, Like, and Between. For example: Device ID, User ID, etc. • Boolean data: Supported operators for Boolean data are Yes, and No. For example: Is Compliant, Is Seqrite Launcher activated, etc. Time stamp data: Supported operators for time stamp data are Less than, Greater than, Equal, Less than equal, Greater than equal, Not Equal, and Between. For example: Device creation date, User creation date, Device Group creation date, etc.  • Please be noted that you must enter inputs as zero or one, true or false and yes or no to search Boolean data. • You must enter the date in DD-MM-YYYY format to search time stamp data. • You cannot use Like operator for string type data with predefined values. For example: Device status.

Options	Description
Search Criteria	• Filter parameter: To filter the parameter as per your requirement. After selecting the Where Operator, enter any parameter to generate the report matching to the filtered criteria.
Group By	Group By functionality is used to group rows that have similar values. It gives the summary of the database.
Aggregate functions	Aggregate function allows you to perform calculation on multiple rows of a single column of a table and give a single value. The aggregate functions include: • COUNT: The COUNT aggregate function gives the total number of values in a field. • AVG: The AVG aggregate function gives the average of the values in a specified column. It is applicable only for numeric data. • SUM: The SUM aggregate function gives the sum of the values in a specified column and is applicable only for the numeric data. • MAX: The MAX aggregate function gives the largest value from the specified table field. • MIN: The MIN aggregate function gives the smallest value from the specified table field.
Reorder	To rearrange the rows as per your requirement. You can drag and drop the columns.

8. Click **Save**.

The report is generated successfully. The Custom Reports list page is displayed with all the available custom reports.

The custom reports page table shows the following information about the custom reports.

Columns	Description
Id	Displays the Id of the generated custom report.
Name	Displays the name of the custom report.
Created By	Displays the name of the report creator.
Action	The action items include few icons: • **View**: Helps you to view the selected report. • **Download**: Helps you to download the selected custom report. • **Edit**: Helps you to modify the selected custom report. • **Delete**: Helps you to delete the selected report.

Columns	Description
With selected	The With selected option appears on the Custom Reports page when you select single or multiple reports. The available action in With selected list is: • **Delete**: Helps you to delete the single or multiple selected reports. To delete the report, select the reports. The With selected option is displayed. Select **Delete** and then click **Submit**.

Editing custom reports

This option helps to make changes to the generated custom reports.

To edit the custom report, follow these steps:

1. Log on to the Seqrite MDM portal and click **Reports** > **Custom Reports**.
2. On the Custom Reports page, select the custom report and click **Edit** icon.

   The Create Report page is displayed.
3. You can make changes to the report name, entities, and columns as required and click **Save**.

   You will be directed to the Custom Reports page.
   - To just view the report, click the **View** (eye icon).
   - To download the report in CSV format, click the **Download** icon.

Chapter 9

Admin

The Admin option lets you configure the Setup Services, APNs, Registering IMEI number for auto approval, and MDM Upgrade Setting. The Admin option includes Setup Services, Activity Logs, Action Logs, and License sections. You can also configure the settings, view the activity logs, and can view license details of the Seqrite MDM portal.

This chapter includes following sections:

Setup Services

The Setup Services section lets you register cloud services for the Android devices. These setup services allow the communication between client and server. It is a one-time activity to be done on the Seqrite MDM portal. The service helps you to send messages from the server to the enrolled devices. This acts as an interface between the client and server. The Setup Services include Apple Certificate, Register IMEI, MDM and Launcher Upgrade Setting, and Custom Settings.

Note:

The Setup Services section is visible to Super Admin and to the Admin with the Super Admin privilege.

Register IMEI

The Register IMEI option helps to auto approve the enrollment request of devices added through IMEI number. Select the **Auto Approve** check box to approve the devices automatically for which IMEI number is added to the list. You can also import and export the registered IMEI

numbers in CSV format. You can download the sample CSV file format for reference. You have to add the IMEI number of a device to validate and auto approve it.

This option helps you to auto approve the enrollment request for the devices added through IMEI numbers. You need to add IMEI numbers of the devices, which are to be registered with the MDM console. After the enrollment is completed on the device, the request comes to the MDM server for approval. The device will be auto approved (which IMEI number is added) if the **Auto Approve** check box is selected.

IMEI List Page

If the IMEI number of multiple devices are added, then all the IMEI information will be displayed in the table format as follows:

Column	Description
IMEI Number	Displays the IMEI number.
Added on	Displays the date on which IMEI number was registered.
Last Modified On	Displays the latest modified date of IMEI number.
Action	The action item includes: • **Edit**: Helps you to edit the IMEI number. Click the **Edit** icon and change the IMEI number and click ✓ symbol to save it. • **Delete**: Helps you to delete an IMEI number. Click the **Delete** icon to delete the IMEI number.

With selected option for IMEI

The With selected option is displayed when you select a single or multiple IMEI numbers.
To use the With selected options for IMEI, select a single or multiple IMEI numbers. The With selected option is displayed. Select **Delete** and then click **Submit**.

Adding IMEI number

To add IMEI number, follow these steps:

1. Log on to the Seqrite MDM portal and click **Admin** > **Setup Services** > **Register IMEI** > **Add**.

   The Add IMEI Number dialog is displayed.

2. Enter IMEI Number and click **Save**.

   Your IMEI number is successfully registered.

4. To approve the device enrollment request automatically, you can select the **Auto Approval** check box. If you do not want to auto approve the device, clear the Auto Approval check box.

5. Click **Save**.

   The new IMEI number is added to the list.

Client Upgrade

The Upgrade Setting section gives you information about sharing the updated versions of Seqrite MDM client app and Seqrite Launcher client app using different app source types.

MDM Upgrade

The MDM Upgrade setting helps you to send the updated version of the MDM client app from the server to the user's device. Keeping the MDM client app updated gives you access to the latest features and improves the device security. This setting provides different sources to download and install the updated version of the MDM client app.

Before you proceed to send the update of the client app to the users, you must enable the Upgrade MDM Notification option. In addition, you must set the frequency to send the upgrade MDM alert. The Upgrade MDM alert helps to send the prompt to the users to update the MDM app to the latest version at the selected frequency.

The App source type includes Default Location, Custom URL, and Upload MDM.

Default Location for MDM

The Default Location option helps you to update the version of the MDM app using Seqrite App Store. All the MDM app users can download the client app from the Default Location of MDM app and install it on the device.

Updating MDM app via Default Location

To update the MDM app via Seqrite App Store, follow these steps:

1. Log on to the Seqrite MDM portal, and click **Admin** > **Setup Services** > **Client Upgrade** > **MDM Upgrade**.
2. Turn ON the **MDM Upgrade Notification** and select the **Alert To Upgrade MDM** duration in hours.
3. Select the App Source Type as **Default Location**.

   The Package ID option will be pre-filled.
4. Click **Save**.

Custom URL for MDM

With the Custom URL option, you can download the MDM client app from the custom URL on your own company's Cloud. After you upload the MDM client app on Cloud, the user receives a prompt about the availability of the update of the MDM client app. Thus the user can download and install the updated MDM client app from the company's Cloud URL.

Downloading MDM client app from custom URL

To upload custom URL on Cloud, follow these steps:

1. Log on to the Seqrite MDM portal and click **Admin** > **Setup Services** > **Client Upgrade** > **MDM Upgrade**.
2. Turn ON the **MDM Upgrade Notification** and select the duration from the **Alert To Upgrade MDM** list.
3. Select the App Source Type as **Custom URL**.

   The Custom URL section is displayed.
4. Enter Version Name, Version Code, Package Id, and URL of apk. file in the respective text boxes.
5. Click **Save**.

   The Custom URL setting is saved successfully and the user will receive a prompt to download and install the updated MDM client app.

Upload MDM App

With this option, you can upload the APK on Seqrite MDM Cloud. After the APK is uploaded on the Seqrite MDM Server, the MDM client app will be downloaded to the device and user needs to install it on the device.

Uploading APK on Seqrite MDM Cloud

To upload APK on MDM server, follow these steps:

1. Log on to the Seqrite MDM portal and click **Admin** > **Setup Services** > **Client Upgrade** > **MDM Upgrade**.
2. Turn ON the **MDM Upgrade Notification** and select the duration from the **Alert To Upgrade MDM** list.
3. Select the App Source Type as **Upload MDM App**.

   The Package ID option will be pre-filled.
4. Select the APK file and click **Save**.

   If an older version of MDM client is installed on the device, then as soon as the device syncs with the server, the APK will be downloaded automatically on the device and the user will be promoted to install the new version of the MDM client.
5. On the device, tap the **Install** button to install the latest MDM client.

Launcher Upgrade

The Launcher Upgrade setting helps you to send the updated version of the Launcher client app from the server to the users' device. The updated Launcher client app gives you the access to

the latest features and improves the device security. The new launcher version can be downloaded and installed from Default Location, custom URL, or APK.

To send the update of the Launcher client app to the users, you must enable the Launcher Upgrade Notification option. In addition, you must set the frequency to send the user the alert to upgrade the Launcher application.

Default Location for Launcher

With this option, you can send the updated version of the Launcher app via Default Location. All the Seqrite Launcher users can download the app from the default location of Launcher App and install it on the device.

Updating Launcher client app via Default Location

To update the Launcher using the default location, follow these steps:

1. Log on to the Seqrite MDM portal, and click **Admin** > **Setup Services** > **Client Upgrade** > **Launcher Upgrade**.
2. Turn ON the **Launcher Upgrade Notification** option and select the frequency, in hours to send the alert to the user to upgrade the Launcher.
3. From the App Source Type list, select **Default Location**.

   Package ID is pre-filled.
4. Click **Save**.

   If the old version of Launcher is installed on the device, as soon as the device syncs with the server, the APK will be downloaded automatically on the device. The user will be prompted to install the new version of the Launcher client app.

Custom URL for Launcher

The custom URL option is helpful to you to download the Launcher client app from the custom URL on your own company's Cloud. After you upload the Launcher client app on Cloud, the user receives a prompt about the availability of the update. The user can download and install the updated Launcher client app from the company's Cloud URL.

Downloading Launcher client app from custom URL

To upload the custom URL on Cloud, follow these steps:

1. Log on to the Seqrite MDM portal and click **Admin** > **Setup Services** > **Client Upgrade** > **Launcher Upgrade**.
2. Turn ON the **Launcher Upgrade Notification** option and select the frequency, in hours. This will help you to send an alert to the user to upgrade the Launcher client app.
3. From the App Source Type option, select **Custom URL**.
4. Enter Version Name, Version Code, Package Id, and URL of apk. file.
5. Click **Save**.

The Custom URL setting is saved successfully and the user will receive a prompt to download and install the updated Launcher client app.

Upload Launcher App

With this option you can upload the Launcher APK on Seqrite MDM Cloud. After the APK is uploaded on the Seqrite MDM Server, the Seqrite Launcher app will be downloaded to the device and the user needs to install it on the device.

Uploading Launcher APK on Seqrite MDM Cloud

To upload the Launcher APK on MDM server, follow these steps:

1. Log on to the Seqrite MDM portal and click **Admin** > **Setup Services** > **Client Upgrade** > **Launcher Upgrade**.
2. Turn ON the **Launcher Upgrade Notification** option and select the frequency, in hours. This will help you to send an alert to upgrade the Launcher client app.
3. From the App Source Type option, select **Upload Launcher App**.

   The Package ID option will be pre-filled.
4. Select the file from your computer to upload the APK and click **Save**.

   If the old version of Launcher is installed on the device, then as soon as the device syncs with the server, the APK will be downloaded automatically on the device. The user will be prompted to install the new version of the MDM client app.
5. On device, tap the **Install** button to install the latest Seqrite Launcher client app.

Custom Settings

With the Custom Settings, you can edit the company name, logo, Launcher wallpaper, QR code validity of the logged in tenant, and email setting for non-compliance reports.

Company Settings

In this section, as soon as you update the company name, it gets reflected on the MDM portal, About screen of MDM client app, and on the Launcher app. The Company Logo option is to edit the company logo on the Launcher. Whenever, the device syncs with the server, the updated logo reflects on the Launcher.

Editing company name and logo

To edit the company name and logo, follow these steps:

1. Log on to the Seqrite MDM portal and click **Admin** > **Setup Services** > **Custom Settings** > **Company Settings**.
2. In Company Settings section, click the company logo.

   Camera icon is displayed.
3. Click the arrow next to the camera.

- To add a new company logo, click **Upload**.
- To remove company logo, click **Delete**.

Note:

You can also change the company name and logo from Launcher Settings section of app configuration. If any change is done to the Launcher Settings (app configuration), then it will override the Company Settings.

Launcher Wallpaper Setting

To have a good user experience, the Launcher wallpaper can be edited. You can upload the Launcher wallpaper from the server console and this wallpaper reflects on Seqrite Launcher Home screen. The updated wallpaper reflects on the device when the device syncs with the server or the Admin sends a sync command. The functionality to set the Launcher wallpaper is applicable to the Launcher 1.1.44 and later versions.

Note:

- The Launcher wallpaper image resolution must be between 320 x 533 to 1080 x 1920.
- The Launcher wallpaper reflects on the device when the device syncs with the server or the Admin sends a sync command.
- There is a provision to change the launcher wallpaper from Launcher Settings section of app configuration. The Launcher Settings (app configuration) override the Launcher Wallpaper Setting (Custom Setting).

Editing Launcher wallpaper

To edit the Launcher wallpaper, follow these steps:

1. Log on to the Seqrite MDM portal and click **Admin** > **Setup Services** > **Custom Settings** > **Launcher Wallpaper Setting**.
2. Click inside the Launcher wallpaper space. The Camera icon is displayed.
3. Click the arrow next to the camera.
   - To add a new Launcher wallpaper, click **Upload**.
   - To remove the Launcher wallpaper, click **Delete**.

Other Setting

In this section, you configure the QR code settings and the settings for non-compliance report.

QR Code Setting

This option helps to set the OTP validity for the overall QR codes generated in an organization. The QR code OTP expires after the set time period.

Setting QR code validity

To set the QR code validity, follow these steps:

1. Log on to the Seqrite MDM portal and click **Admin** > **Setup Services** > **Custom Settings** > **Other Setting**.
2. Enter the QR Code Validity and click the **tick** mark.

Email Settings for Non-Compliance Reports

This email setting is helpful to notify the admins about the non-compliance status of the devices. If the Send Email to Below Admins check box is selected, then the admins receive the notification about the non-compliant devices every 24 hours. You have the privilege to add in maximum of five, comma-separated, email IDs of the admins.

For any non-compliance report, the admins receive an email with details and following reasons of non-compliance; policy non-compliance, app configuration non-compliance, launcher configuration, and device inactivity.

If you are logged on to the MDM portal and in the email, if you click the device name, you are directed to the Device page.

Sending non-compliance reports to the admins

To send the non-compliance reports to the assigned admins, follow these steps:

1. Log on to the Seqrite MDM portal and click **Admin** > **Setup Services** > **Custom Settings** > **Other Setting**.
2. In Email Settings for Non-compliance Reports section, select the **Send Email to Below Admins** check box.
3. Add comma-separated email IDs in the text field, and click **Save**.

   Maximum of five email IDs can be added.

Activity Logs

The Activity Logs section helps you to keep a track of the actions performed by all the Admins. The activity logs are created when any of the Admin perform any action on the Seqrite MDM portal. You can search the Admin activity using different search criteria and also export the activity logs.

The Activity Logs page shows all the available activity logs and the table gives the following information:

Columns	Description
Date	Displays the date and time of the activity performed.
User	Displays the name of the user who performed the activity.
Action	Displays the type of the action that is performed.

Context	Shows the context of the activity.
Action On (Id: Name)	Displays the ID and name of the individual component on which the activity is performed.
Field Type	Displays the updated field on which the activity is performed.
New Value	Displays the new value of the component on which the activity is performed.
Old Value	Displays the old value before making the changes.
Date	Displays the date and time of the activity performed.

Advanced Search for Activity Logs

The Advanced Search option on the upper-right side of the Activity Logs page allows you to perform an advanced search of the users' activity logs.

To find activity logs with the Advanced Search option, follow these steps:

1. Log on to the Seqrite MDM portal and click **Admin** > **Activity Logs** > **Advanced Search**.

   Advanced search parameters are displayed.

   The search parameters are as follows:

   - **Select Entity**: Select this option to view the activity logs according to the entities such as User, Department, Devices and so on.
   - **Select Change Log Context**: Select this option to view the activity logs for a change log context.
   - **Select Change Log Action**: Select this option to view a list of activity logs for a change long action.
   - **Select days**: Select this option to view the activity logs for a particular number of days.
2. Click **Search**.
   - To reset the selected criteria, click **Reset**.
   - To get the complete details of the search result in CSV format, click **Export**.

Exporting Activity Logs

To export the activity logs, you can use the advanced search criteria. This helps to keep the documented record of all the admin activities. The activity logs are exported in CSV file.

To export the activity logs, follow these steps:

1. Log on to the Seqrite MDM portal, and click **Admin** > **Activity Logs** > **Advanced Search**.

   Search criteria are displayed.
2. Select the entities, change log context, and change log action.
3. Select the number of days or date range and click **Export**.

Tip:

Exported data will be based on the selected search criteria, so choose the search criteria properly.

4. On confirmation screen, click **OK**.

Action Logs

The Action Logs section helps you to keep a track of the device actions executed on the devices by the Seqrite MDM portal. You can also export the action logs by clicking Export. To know more about device actions, see Device Actions.

Action Logs List Page

The Action Logs list page shows all the action logs available in Seqrite MDM portal. The information on the list page shows the following details:

Options	Description
Id	Displays the Id of the action performed on the device.
User	Displays the name of the user who performed the action.
Type	Displays the type of the action that is performed.
Performed On	Shows the date and time when the action took place.
Total	Displays the count of the devices on which the activity is performed.
Completed	Displays the count of the devices on which the action is completed.
Action	The action item includes; • View: Helps you to view the status of the action performed on the device. On clicking the View icon, you will be navigated to the Action Details page.

Advanced Search for Action Logs

The Advanced Search option on the upper-right side of the Action Logs page allows you to perform an advanced search of the device actions.

To find action logs with the Advanced Search option, follow these steps:

1. Log on to the Seqrite MDM portal and click **Admin** > **Action Logs** > **Advanced Search**.

   Advanced search parameters are displayed.

   The search parameters are as follows:

   - **Select Action Type**: Select this option to view the action logs of a particular action performed on the device.

- **Select Date:** Select this option to view the action logs for a particular date.

2. Click **Search**.
   - To reset the selected criteria, click **Reset**.
   - To get the complete details of the search result in CSV format, click **Export**.

Action Details

The Action Details section helps you to know the detailed status of the execution of the action performed on the device. You can view the type of the task performed, action Id, and percentage of the task completed.

The Action Logs page includes the following:

Column	Description
Device Id	Displays the Id of the device on which the action is performed. To know more details of the device, click the **Device Id**. You will be redirected to the Device Details page.
Device Name	Displays the name of the device.
Status	Displays the activity status of the action performed.
Description	Shows the description of the action performed.
Last updated	Shows the last updated date and time of the action performed.
Refresh	Helps to refresh the Action Details page.

Exporting Action Logs

To export the action logs, you can use the advanced search criteria. The action logs are exported in CSV file.

To export action logs, follow these steps:

1. Log on to the Seqrite MDM portal and click **Admin** > **Action Logs** > **Advanced Search**.

   Search criteria are displayed.

2. Select the action type and then select the action days or date range, and click **Export**.

   Tip:

   Exported data will be based on the selected search criteria, so choose the search criteria properly.

3. On confirmation screen, click **OK**.

   The action logs are exported.

License

The License section lets you view the license details of the product. You can view the details of the owner of the licensed copy.

- **Overview:** With Overview, you can view the Company Name, Company Code, Product Name, Product Type, Product Key, License Valid till, Number of Devices, Contact Name, Contact Email, and Contact Number. In addition, you can edit the Contact Name, Contact Email, and Contact Number whenever required.
  - Click **Refresh License Details** to refresh the details of the license.
- **History:** The History tab lets you view the details of the product license. The history of the license stores all the changes that have been done to the product license such as Registration, Update, Addition, and Renew.
  - The License History table shows the following information:

Columns	Description
Action	Displays the action that is performed on the product license. The actions can be registration of the license, updating the license, renewing, and the addition of the devices to the MDM account. The actions include Registration, Update, Addition, and Renew.
Action Date	Displays the date on which the action was performed on the product license.
License Type	Displays the type of the license.
Product Key	Displays the product key of the license.
Total Devices	Shows the total number of the devices enrolled for a product license.
Duration	Shows the duration of the license.
Expiry Date	Displays the liable expiry date of the license.
Contact Email	Displays the email id of the Super Admin.
Contact Name	Displays the contact name of the Super Admin.
Contact No.	Displays the contact number of the Super Admin. Note: Whenever the Admin is changed, you can edit the Contact Name, Contact Email, and Contact Number.

Chapter 10

Help

Seqrite MDM provides various methods to help you and resolve the issues. The bottom section includes the support center, privacy policy, license agreement, share feedback, and release notes of the Seqrite MDM current version.

Support

This section helps you to view the Online Help, read FAQs, and the contact details of the Seqrite support. To view the available support options, follow these steps:

1. Log on to the Seqrite MDM portal.
2. In the extreme lower section of the portal, click **Support**.

   The Support option includes the following options:

   - **Contact**

     This option helps you to know the various ways to contact Seqrite support. It includes the following support facilities such as Email Support, Live Chat Support, and Phone Support.

     - **Email Support**

       If you have a query and want to submit a ticket to us, you can visit our Email Support system. Here you can submit a ticket with the issues. Our experts will revert soon with appropriate inputs.

       - To submit a ticket, click **Submit** ticket.

       You can also share feedback about the Seqrite MDM portal.

       - To share your feedback, click **Share Feedback**.

     - **Live Chat Support**

       To get a live technical support or answers to the issues, you can chat with our technical experts.

       - To avail of live chat, click **Chat Now**.

     - **Phone Support**

You can call us at the following numbers: +91 927-22-12-121 between 09:30 AM to 06:30 PM IST (India Standard Time) between Monday to Saturday.

- **Frequently Asked Questions**

  This option helps you to know the answers to the frequently asked questions (FAQ) related to the Seqrite MDM portal.

  - To refer FAQs, click **FAQ**.

- **Online Help**

  This option includes the Administrator's Guide of the Seqrite MDM portal.

  - To view Online Help, click the **Click Here** link. You are redirected to the online help where you can know about the features.

Privacy Policy

This section helps you to view the privacy policies of the Seqrite MDM portal.

License Agreement

This section helps you to view the complete license agreement of the Seqrite MDM portal.

Share Feedback

The Share Feedback option is a simple approach for you to reach us. You can share feedback on the Seqrite MDM portal with us. To share your feedback, click **Share Feedback**.

You can also share your feedback with the help of the Support option.

Release Notes

This option includes the release notes of the current version. Click the version number on the lower left of the Seqrite MDM portal to navigate to the release notes where you can find the detailed information of corrections, changes or enhancements of Seqrite MDM and the known issues of the new version of Seqrite MDM.

Head Office Contact Details

Quick Heal Technologies Ltd.

(Formerly Known as Quick Heal Technologies Pvt. Ltd.)

Reg. Office: Marvel Edge, Office No. 7010 C & D, 7th Floor,

Viman Nagar, Pune 411014.

Telephone: +91 20 66813232

Official Website: www.quickheal.com

Email: info@quickheal.com

Index

A

B

C

D

E

F

G

H

I

L

M

N

P

R

S

U

W