Seqrite
Enterprise Mobility Management

SEQRITE

Administrator's Guide

v3.4

www.seqrite.com

Copyright & License Information

About This Document

This manual covers all the information required to install and use Seqrite EMM. 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 box, 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.
Administrator	Administrator is the company or organization that enrols mobile devices.
Client agent	Client agent is the device user and is also known as the tenant.

Contents

Seqrite EMM Features for Android and iOS

Feature list for Android and iOS devices:

	Feature	Android	iOS
Features	**Enrollment**		
	Enrollment	✓	✓
	Antivirus		
	Real-Time Protection, Scheduled Scan, Remote Scan, Seqrite EMM App auto upgrade	✓	✕
	Action on device		
	Sync, Locate, Block, Unblock, Fetch Logs, Locate, Reset Password, Broadcast Files(s) / Message	✓	✓
	Scan, Exit Launcher, Trace Device, Push Fence Configuration, Disconnect, Uninstall, Call/SMS Monitoring	✓	✕
	Remote Buzz	✓	✓
	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	✓	✕
App Management	**App Management**		
	Restrict access to newly installed apps	✓	✕
	Whitelist App	✓	✕
	Recommend app to install, Apps to Remove	✓	✓
	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	✓	✕

Seqrite EMM policies for Android and iOS devices

Policy Name	Android	iOS
Requires Password, Password Minimum Length, Password Age, Device Autolock	✓	✓
Password History, Block Voice Dialing from Lock Screen	✗	✓
Block USB Connection, Block Safe Mode	✓	✗
Block Camera	✓	✓
Block Face Time	✗	✓
Block Factory Reset from Device Setting	✓	✓
Block Bluetooth, Block Configuring Bluetooth, Block Wi-Fi, Block Open Wi-Fi, Block Mobile Hotspot, and Block NFC	✓	✗
Location Service (GPS), Sync Frequency	✓	✗
Block Certificate	✗	✓
Block Screen Capture	✓	✓
Block Text Copy and Paste	✓	✗
Block iTunes App, Block App Store	✗	✓
Set Google Account, Block Primary Microphone	✓	✗
Block Siri	✗	✓
Device Time-out, Set Auto Time Zone	✓	✓
Block Profile Switch, Device Accessibility Service & App Usage	✓	✗
Block Accounts Modify	✓	✓
Block USB Debug Mode, Block App Control, Block Adding New User Profile, Block Deletion of User Profile, Block Configuring Mobile Data Setting, Block Outgoing Calls, Block Mounting Physical Media, Wi-Fi On in Sleep Mode, Block App Installation from Unknown Sources, Block Notification Area, Block Cellular Data, Block Mock Location, Block Outgoing MMS & SMS, Block Airplane Mode	✓	✗
Block Notification on Lock Screen, Block Control Center on Lock Screen, Block Safari, Block App Uninstallation, Block iMessage, Block Apple Books, Block In-app Purchase, Block Backup to iCloud	✗	✓

Seqrite EMM supports Android OS version 5.0 to 9, and iOS 10 and later versions on mobile.

1. Introducing Seqrite Enterprise Mobility Management

In the present era, organizations allow their employees to bring smartphones, tablets, and handheld devices to the office and use the mobile devices for official tasks. In such a scenario, it is important to monitor mobile devices to the protect data of the organizations.

Seqrite Enterprise Mobility Management (EMM) console is a turnkey solution that empowers organizations to remotely monitor, manage, and track all types of mobile devices to implement compliance policies on the digital devices and ensure that the corporate data is secure.

Advantages of Seqrite Enterprise Mobility Management

Following are the advantages of Seqrite EMM:

- Monitor the mobile devices if they comply with the policy of the organizations.
- Implement the required security on mobile devices including Android and iOS devices.
- Secure the data of the organizations.
- Monitor resources to enhance productivity.
- Maintain instant communications with the employees.
- Perform console administration functions.
- Monitor network data usage and call/SMS.
- Manage the device app with app configuration.
- Generate customized reports.
- Remotely access the enrolled mobile device.

How does Seqrite Enterprise Mobility Management work?

Seqrite EMM works on the Agent-Server architecture where the console is hosted on Cloud to manage the mobile devices. The agents are installed on all the systems of mobile platforms (Android, iOS). Seqrite EMM Admin gets full control of the device to manage, monitor, or track the device.

Seqrite EMM allows the administrators to deploy and enroll Seqrite EMM Agent on the mobile devices remotely, and apply required policies and configurations such as App Configuration, Web Security Configuration, Anti-theft, Network Data usage, Fence Configuration and so on, on the mobile devices.

Seqrite EMM Agent acts on the mobile devices silently and applies most of the restrictions without user intervention. Seqrite EMM Agent has built-in antivirus that keeps the devices safe from any virus attack.

Seqrite EMM variants

Seqrite EMM comes in different variants: Standard and Advance.

- Standard: Standard Seqrite EMM comes with a limited set of features.
- Advance: Advance Seqrite EMM includes all features.

Features included in different variants

The following table describes complete information about the features included in the Standard and Advance Seqrite EMM variants.

Features	Variants	
	Standard	Advance
Device Management	✔	✔
Application Management	✔	✔
Security Management	✔	✔
Real Time Malware Protection	✔	✔
Network Data Monitoring	✔	✔
Launcher Mode	✔	✔
Call & SMS Monitoring	✖	✔
Device Lockdown	✖	✔
Virtual Fencing (Geo, Wi-Fi, Time based)	✖	✔
Remote Device Control and file management	✖	✔
Reporting	Basic	Custom
Logs and Reports	1 month	3 months

Tenant and data retention policy on Cloud

- The Trial and Standard license tenants will be completely deleted from the Seqrite EMM server after one month since the license expires. As a result of this, all the user data will be deleted and cannot be recovered.

- The Advance license tenant will be deleted after three months since the license expires. In such a scenario, user data will be deleted and cannot be recovered.

- Every tenant Admin will get prior notification before the tenant is deleted from the Seqrite EMM database as per the following schedules.

- Trial and Standard license user: 7 days, 15 days, and 25 days.

- Advance license user: 15 days, 30 days, 45 days, 60 days, and 75 days.

- Seqrite will maintain a limited set of logs and reports on the server based on user license type.

- For Trial and the Standard license tenants, only 1-month data will be kept on the server. Data older than 1 month will be automatically deleted from the server. This action is irreversible.

- Notifications, device action logs, and activity logs will be maintained only for 1 month for Standard variant and 3 months for Advance variant. No historical data will be maintained after the above-mentioned periods.
- For Advance license tenants, data of 3 months will be saved on the server. Data older than 3 months will be automatically deleted from the server. This action is irreversible.

Seqrite Workspace

Seqrite Workspace is a container-based application that can be installed on Android mobile devices. After Seqrite Workspace is installed on a mobile device, a Workspace environment is created where the user can perform various functions. However, the data from the secure Workspace cannot be shared outside. Thus, it eliminates the risk of leaking business data.

At the same time, the employees have uninterrupted access to their personal sections on the same mobile device.

Advantages of Seqrite Workspace

- A separate Work profile is created on the mobile devices where business data and corporate-approved apps remain secure.
- Admin can install corporate-approved apps in the Work profile.
- Creates a separate Workspace environment on the mobile device of the users yet restricts sharing of the business data outside.
- Allows the users uninterrupted access to the personal sections.
- Supports bringing your own devices (BYOD) to the office and allows official tasks on personal mobile devices.
- Allows access to your corporate emails and contacts on the go.
- Access or share the important documents that you receive in the vault repository.

2. Getting started

To install Seqrite EMM, ensure that you comply with the following requirements:

Prerequisites

System requirements

Prerequisites

Before installing Seqrite EMM on your device, follow these guidelines:

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

System requirements

To use Seqrite EMM, your browser and mobile devices must meet the following requirements.

Mobile device specifications	• Android 5.1 to 12.0 OS versions. • iOS 12 and later versions.
Browser requirements	Administrator Web panel, Google Chrome (latest versions), Firefox (latest version), and EDGE (latest versions)
Terminology	**User**: An employee who enrolled the device with Seqrite EMM.
	Administrator: A user with access to the Seqrite EMM console to manage the devices.

System requirements are subject to change from time to time. To check for the latest system requirements, visit our website at www.seqrite.com.

3. Registration and installation

Administrators are the owners of the Seqrite EMM console. They must register their companies with the Seqrite EMM console.

To function with the Seqrite EMM console, the following steps are involved.

[Registering with the Seqrite EMM console](#)

[Installing the Seqrite EMM agent on the mobile devices](#)

Registering with Seqrite EMM

To register with the Seqrite EMM console, follow these steps:

1.   Go to https://cloud.emm.seqrite.com/

2.   On the Sign In page, click **Try Now**.

        The Trial Sign-up page appears.

3.   On the Registration page, enter the **Contact Information**, **Company Information**, and **Verification Code** in the corresponding text boxes.

4.   Select the Terms of agreement and Privacy Policy options and click **Register**.

        You will receive a confirmation email from Seqrite EMM that includes the product key and **Sign Up** link.

5.   In the confirmation email, click the **Sign Up** link.

        The Sign Up page is displayed.

6.   On the Sign Up page, enter the required information such as First Name, Last Name, Mobile Number, Email, Confirm Email, Product key, Password, and Confirm Password.

7.   Click Sign-up Account.

        On registering with Seqrite EMM console successfully, users can log on to the EMM console.

Installing Seqrite EMM agent on mobile devices

The administrators can [add the mobile devices](#) of the employees to the Seqrite EMM console and [enroll the devices](#) to manage them.

Note: Seqrite EMM agent app is now available on Google Play Store. (Applicable for Android Enterprise Enrollment devices only.)

4. Dashboard

Dashboard is the default page that is displayed after you Log on to Seqrite EMM console. The dashboard gives a glimpse of the status on various factors such as if any devices do not comply with the company policy, if any restricted apps are installed or required apps are removed without permission from the administrator, there is any virus attack on a device, or there is any policy violation.

The dashboard helps to navigate easily to all the features or components of the Seqrite EMM console. However, access to the features or components is based on the license type that you buy.

The dashboard includes the following information.

Section	Description
Overview	
App Non-Compliance Devices	This tile shows the devices that are app non-compliant. It lists those devices that are not compliant with allowed app configuration settings. App is either in pending state for installation/un-installation or Launcher is in a pending state for activation/deactivation.
Policy Non-compliance Devices	This tile shows the devices that are not compliant with policy. It lists those devices that violate the policy compliance and do not follow the allowed policy rule.
Agent Vulnerable Devices	Displays the number of devices that are vulnerable to uninstallation of the Seqrite EMM agent app from the devices. This happens when Device Administrator permission is revoked from a device.
Agent Unauthorized Removal	This tile shows the number of the devices from which the Seqrite EMM Agent was removed without the permission of Seqrite EMM Administrator.
Anti-theft Locked Devices	Displays the count of the devices that are blocked by the Seqrite EMM Administrator.
Rooted / Jailbroken Devices	Displays the number of enrolled devices that are rooted or jailbroken. The operating system of such devices is tampered, and the devices are compromised.
Total Devices	Shows the total number of devices added to the Seqrite EMM console.

Section	Description
Toggle Bar	Click the toggle bar and choose the OS of your device. • Android Devices: Shows the total number of Android devices and their Agent versions in the Seqrite EMM console. • iOS Devices: Shows the total number of iOS devices and their Agent versions in the Seqrite EMM console.
Device Enrollment Status	
Idle	Shows the number of devices added in the console but the enrollment request is not sent to the devices.
Pending	Shows the number of devices that are pending for enrollment and the Administrator has sent enrollment request to the devices. However, the device user is yet to enroll the device.
Approval Pending	Shows the number of devices for which enrolment request is pending for approval. The Administrator needs to approve the request of the devices.
Enrolled	Shows the number of devices on which the Seqrite EMM Agent is successfully installed and the device is enrolled with the Seqrite EMM console.
Uninstalled	Shows the number of devices from which the Seqrite EMM app has been uninstalled.
Device Last Synced	Displays the total number of devices that synced with Seqrite EMM server for a particular period. The number of days when the last sync occurred is shown as: 0-1 day, 2-7 days, 8-15 days, 16-30 days, and 30+ days.
Data Subscription Usage in GB	Displays the amount of data used by the users while performing the transactions such as downloading custom APK, performing RDC session, or uploading or downloading any file in the RDC session. The heading displays the data used and the total allotted data to the tenants. The chart shows the percentage of data used for each type of transaction.
Device Statistics	
Available Storage	This pie chart shows the available storage on different devices.
Available Battery	This pie chart shows available battery on different devices.
Device Manufacturer	This pie chart shows the name of the manufacturers of the devices.

Section	Description
Malware Statistics for the last 7 days	Displays if any virus infections are detected on the devices enrolled with the Seqrite EMM console. If you hover over the graph, the names of the viruses detected, and the number of devices infected on a particular date are displayed. This shows the status of infection detected in the last 30 days. You can view the 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**: Allows you to 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 Malwares for the last 7 days	Displays if there is any malware attack on the devices.
Data Usage	
Data Usage Statistics	The graph displays the status of the network usage for all the devices. 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: Last 7 days, Last 30 days, Last 15 days, and current month. $\boxed{i}$ Note: 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.
Max Data Usage Devices	Displays the list of the devices that consume more 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.

Section	Description
Max Data Usage Apps	Displays the list of the apps that consume more data. 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.
Most Popular Apps	Displays the list of apps that are installed by most of the users. You can view the name of the app, the category of the app, and the count of the devices on which the app is installed. On clicking the app count, you are directed to the Devices dialog box that gives complete information about the devices that have the specific app installed. • To exclude the recommended standard apps, select the **Exclude recommended apps** check box on the right side of the Top Installed Apps section. • To view the App Repository page and view all the installed apps within the Seqrite EMM network, click **View Details.**
Workspace	
Total Devices	Shows the number of devices enrolled with Seqrite Workspace.
Toggle bar	**OS Version**: Shows the device's OS version. **Agent Version**: Shows the Seqrite EMM Workspace version on the device.
Device Enrollment Status	**Pending**: Shows the number of devices on which the Workspace app activation is pending. The device user has to activate the app. **Enrolled**: Shows the number of devices on which the Workspace app has been activated. **Uninstalled**: Shows the number of devices from which the Workspace app has been uninstalled.
App Non-Compliance Devices	Shows the devices that are app non-compliant. The app is either in a pending state for installation/un-installation in the Work profile.
Web Violation in last 30 days	Shows the number of devices that have violated the Workspace web policies in the last 30 days.

Notifications

Notifications are the communications generated from the Seqrite agents installed on the mobile devices and sent to the administrator. The Seqrite agents send notifications to the administrator for several reasons.

Enrollment Notification: When a new device is enrolled successfully with The Seqrite agent.

Alert Notification: There is an alert regarding non-compliance of the policy on a mobile device, upgrade failure, or scan report.

Info Notification: This notification is related to importing the allowed data like user or device list, when a new device is added to the fencing safety, or if there are any battery or Seqrite EMM Agent log issues.

App Request Notification: This notification is sent if there is a request for an app and so on.

Workspace Notification: This notification is sent if there is an incident related to Workspace.

The administrator verifies the notifications and needs to take action whenever required to resolve the issue.

User Profile

The User Profile section on the upper right corner of dashboard shows the name of the registered user. When you click the logged on user name, the following options are displayed: User Management, Setup Services, License Management, Change Password, Share Feedback, Contact Us, Administrator Guide, Help Articles, and Release Notes.

Menus

Menus show different features of Seqrite EMM console.

Menus	Description
Users	Allows to create and manage users.
Departments	Allows to create and manage departments.
Devices	Allows to add and manage devices.
Groups	Allows to create and manage groups.
Profiles	Allows to apply policies and configurations to groups and devices.
Workspace	Allows to create and apply policies and profile to the Android and iOS device container.
Apps	Allows to create an app repository and app configurations for the devices.

Fencing	Allows to restrict the devices and app usage with the help of a digital fence. The Administrator can configure and apply the fence to different groups.
Reports	Allows to generate reports for infection status, network data usage, and app-compliance. The Administrator can also create a customized report as per requirement.

5. Notifications

Notifications are the communications generated from the Seqrite agents installed on the mobile devices and sent to the administrator.

The administrator can view the notifications by clicking the notification icons available on the upper right-hand side available next to the admin user profile. If there are new and unread notifications, this is indicated by the count on the notification icon.

Viewing notifications

You can view the notifications in the following ways.

Click the notification link: When you click the notification link from any of the notification icons, the notification page for the relevant notifications appears. The notification table shows the following information.

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. After taking an action on a notification, the administrator can delete the notification.

On the notification table, click the notification that you want to check in detail. In some cases, you may need to take action to resolve the issues. You may also remove the notifications if you do not need them in the future.

Search by browsing: On the main page of notifications, you can change the options for your search such as Enrollment Notification, Alert Notification, Info Notification, App Request Notification, and Workspace Notification, and their respective types.

Search by keywords: If the list of notifications is long and you are familiar with the type of notifications, you can search the notifications of your interest by entering the relevant keywords in the search text box.

Viewing notifications

To view a notification, follow these steps:

1. Log on to Seqrite EMM console and click any of the notification icons.

2. The relevant notification page appears.

    If required, you can take an action.

    You can also change your search options to view notifications for other reasons.

3. To change your search option, select either of the following notification types on the notification page.

    ▪ Enrollment Notification and its sub-types Enrollment Notification, Agent Vulnerable Notification, Accessibility Permission Revoked.

    ▪ Alert Notification and its sub-types Scan Report, Non-compliant Report, App Upgrade Failure Notification.

    ▪ Info Notification and its sub-types Import Notification, Fence Notification, Battery Notification, Messages from Seqrite, Log Notification.

    ▪ App Request Notification

    ▪ Workspace Notification

4. Select the period for which you want to view the notifications.

5. Click **Search**.

    The search result is displayed.

    Note:

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

Search for Notifications

The search option is available for all notifications that allow you to search the notifications of your interest.

Searching notifications

To search the notifications using the advanced search option, follow these steps:

1. Log on to Seqrite EMM console and click any of the notification icons.

2. In the notifications dialog box, click **View all Notifications**.

3. On the Notifications page, select the following search parameters.

    Notifications can be searched using the following parameters:

- **Select Notification Type**: Select one of the following notifications: Enrollment Notification, Alert Notification, Info Notification, App Request Notification, and Secure Workspace Notifications.

- **Select Report Type**: Depending on the selected notification type, the report type list is displayed. Select the required report type.

- **Select limit from**: Select the period for which the notifications are required such as Today, Last 7 days, and Last 15 days.

  ⓘ 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.

Taking an action on Notifications

Take Action is an option that helps you take an appropriate action on the notifications. This option is available for all notifications.

For notification, you have one action that is you can delete a notification. Make sure you do not need the notifications that you delete.

Deleting a notification

To delete a notification, follow these steps:

1. When you are on the notification page, select a notification.

   The Take Action list appears.

2. Select **Delete** and then click **Submit**.

Notifications for the following reasons are generated:

[Enrollment Notification](#)

    [Enrollment Notification](#)

    [Agent Vulnerable Notification](#)

    [Accessibility Permission Revoked](#)

[Alert Notification](#)

    [Scan Report](#)

    [Non-compliant Report](#)

    [App Upgrade Failure Notification](#)

[Info Notification](#)

    [Import Notification](#)

    [Fence Notification](#)

    [Battery Notification](#)

    [Messages from Seqrite](#)

    Seqrite EMM Agent [Log Notification](#)

[App Request Notification](#)

[Workspace Notifications](#)

Enrollment Notification

Notifications related to the device enrolment are found under this category. Click the mobile device icon on the upper right-hand side available next to the admin user profile. This notification includes the following enrolment notification types.

Enrollment Notification

These notifications are related to the status of the device enrollment such as the devices requesting for approval and those devices that have been approved to be enrolled, and so on.

As an administrator, you can approve or disapprove the device enrollment directly from the enrollment notification section. When the device enrollment request is approved by clicking **Approved**, the approval command is sent to the device.

Viewing Enrollment Notification

To view the device enrollment alert, follow these steps:

1. Log on to Seqrite EMM console and click the mobile icon for enrollment notifications.

2. Click View all Notifications.

    The relevant notification page appears.

3. For **Enrollment Notification**, select **Enrollment Notification** from the following notification types:

    - Enrollment Notification

    - Agent Vulnerable Notification

    - Accessibility Permission Revoked

4. Select the period for the notification and click **Search**.

    All the notifications for the selected search options are displayed.

Approving or disapproving device enrollment request

To approve or disapprove a device enrollment request, follow these steps:

1. Log on to Seqrite EMM console and click the mobile icon for enrollment notifications.

    On the enrollment notification page, the requested enrollment notification shows the **Approve** and **Disapprove** options.

2. To approve the request, click **Approved**. The approval command is sent to the device.

3. To disapprove the request, click **Disapproved**.

    When the device enrollment request is disapproved, the Seqrite EMM Agent will be uninstalled from the device. You can directly disapprove the device enrollment request from the notifications page or send an SMS to disapprove the device enrollment.

    A check box **Disapprove device by sending SMS** is available on the confirmation screen. If the mobile number of the device is not available, this check box is not available and appears in grey. When the mobile number of the device is available, you can send the device disapproval using the SMS option.

Agent Vulnerable Notification

At the time of installation, the Seqrite EMM Agent app asks for device accessibility permission. With this permission, the Seqrite EMM Agent is restricted from getting uninstalled. However, when the device accessibility permission is revoked because of any reason, the Seqrite EMM Agent becomes vulnerable to uninstallation. To alert about this to the administrator, an Agent Vulnerable Notification is generated.

Viewing Agent Vulnerable Notification

To view the agent vulnerability notification, follow these steps:

1. Log on to Seqrite EMM console and click the mobile icon for enrollment notifications.

2. Click View all Notifications.

    The relevant notification page appears.

3. For **Enrollment Notification**, select **Agent Vulnerable Notification** from the following notification types:

    ▪ Enrollment Notification

    ▪ Agent Vulnerable Notification

    ▪ Accessibility Permission Revoked

4. Select the period for the notification and click **Search**.

    A list of notifications is displayed with the device name from where the applied device policy has been removed and the Seqrite EMM Agent has become vulnerable.

Accessibility Permission Revoked

You get this notification when the accessibility permission for Seqrite EMM and Launcher app is disabled or disconnected. The web security and app control functionalities would not ensure excepted security.

*   To fix this problem, you should contact the device user to enable the accessibility service. If the device shows the accessibility permission is turned ON, the device user needs to turn it **OFF** and again turn it **ON** to reflect the change. If this issue persists, ask the device user to restart the device.

*   If the problem persists even after restarting the device, then re-enroll the device.

*   When the issue is resolved, you can close this notification.

Viewing Accessibility Permission Revoked

To view the accessibility permission revoked from the devices, follow these steps:

1. Log on to Seqrite EMM console and click the mobile icon for enrollment notifications.

2. Click View all Notifications.

    The relevant notification page appears.

3. For **Enrollment Notification**, select Accessibility Permission Revoked from the following Notification Types:

    ▪ Enrollment Notification

    ▪ Agent Vulnerable Notification

    ▪ Accessibility Permission Revoked

4. Select the period for the notification and click **Search**.

    All the notifications for the selected search options are displayed.

    The notification list is displayed with the device names on which the Accessibility Permission for Seqrite EMM and launcher app has been removed.

Alert Notification

This notification sends alert messages that need immediate attention. The alert message may be reports on scans, non-complaint devices, and any failed attempt for app upgrade.

Scan Report

The scan report gives information about the threats detected, threat information, and if any action has been taken. If no virus is detected, only the information about the scan is displayed in the report.

Viewing device scan report

To view the device scan report, follow these steps:

1. Log on to Seqrite EMM console and click the bell icon for alert notifications.

    The relevant notification page appears. To see the details of a notification, click the **View Report** link under a notification.

2. For **Alert Notification**, select **Scan Report** from the following notification types:

    ▪ Scan Report

    ▪ Non-Compliant Report

    ▪ App Upgrade Failure Notification

3. Select the period for the notification and click **Search**.

    All the notifications for the selected search options are displayed.

    To see the details of a notification, click the **View Report** link under a notification.

4. The Device Scan Report shows the following information:

    ▪ Report Type: Shows the type of the report, Real-time protection.

    ▪ Threats detected: Shows the total number of threats detected.

    ▪ Table shows the threat information:

        o Icon: Shows the icon of the diagnosed threat.

        o Name: Shows the name of the threat.

        o Threat: Shows the type of threat. For example, adware, Potentially Unwanted Programs.

        o Type: Shows the type of threat. For example; application and file.

        o Location: Shows the location of the threat.

        o Installed on: Shows the date when the threat was installed on the device.

        o Action: Shows if any action has been taken on the threat.

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

Non-compliant Report

The non-compliance report is generated when the device does not comply with the policies or expected security configurations. If you do not find a report for a device in the notifications, 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 Seqrite EMM console and click the bell icon for alert notifications.

   The relevant notification page appears. To see the details of a notification, click the **View Report** link under a notification.

2. For **Alert Notification**, select **Non-Compliant Report** from the following notification types:

   - Scan Report

   - Non-Compliant Report

   - App Upgrade Failure Notification

3. Select the period for the notification and click **Search**.

   All the notifications for the selected search options are displayed.

   To see the details of a notification, click the **View Report** link under a notification.

4. 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:

     o Policy: Shows the name and type of the policy.
     o Reason: Shows the reason for device non-compliance with respect to the policy.
     o Reported Date: Shows the date when the device was non-compliant with the policy.
     o Resolved Date: Shows the date when the policy non-compliance was resolved.
     o Status: Shows the status of the policy.

   - The configuration table shows the following information:

     o Configuration Type: Shows the type of the configuration.
     o Name: Shows the name of the configuration.
     o Reason: Shows the reason of device non-compliance with respect to configurations.
     o Reported Date: Shows the date when the configuration non-compliance occurred.
     o Resolved Date: Shows the date when the configuration non-compliance was resolved.
     o Status: Shows the status of the configuration.

5. Click **Close**.

App Upgrade Failure Notification

Whenever there is an upgrade for the Seqrite EMM Agent, the administrator sends a push upgrade notification to the device user. The device user needs to upgrade the Seqrite EMM Agent. However, if the upgrade fails, a notification is sent to the administrator. The administrator then can take appropriate action.

Viewing the App Upgrade Failure Notification

To view the app upgrade failure notification report, follow these steps:

1. Log on to Seqrite EMM console and click the bell icon for alert notifications.

   The relevant notification page appears. To see the details of a notification, click the **View Report** link under a notification.

2. For **Alert Notification**, select **App Upgrade Failure Notification** from the following notification types:

   ▪ Scan Report

   ▪ Non-Compliant Report

   ▪ App Upgrade Failure Notification

3. Select the period for the notification and click **Search**.

   All the notifications for the selected search options are displayed. To see the details of a notification, click the **View Report** link under a notification.

   You can take an appropriate action to fix the issue.

Info Notification

This notification gives information about functionalities such as import, fence, battery, message, and app log notification.

Import Notifications

These notifications are displayed when an import action is started or completed. The notification includes the name of the item imported, import status, date, time, and Admin name of who started the import action.

Viewing Import Notification

To view the import notifications, follow these steps:

1. Log on to Seqrite EMM console and click the info notification icon.

2. Click View all Notifications.

    The relevant notification page appears.

3. For **Info Notification**, select **Import Notification** from the following notification types:

    - Import Notification
    - Fence Notification
    - Battery Notification
    - Messages from Seqrite
    - Log Notification

4. Select the period for the notification and click **Search**.

    All the import notifications for the selected search options are displayed.

Fence Notification

The fence notifications show information about the device and device user, the date and time when the device entered the defined fence, and the successful application of fence restriction.

Viewing Fence Notification

    To view the fence notifications, follow these steps:

1. Log on to Seqrite EMM console and click the info notification icon.

2. Click View all Notifications.

    The relevant notification page appears.

3. For **Info Notification**, select **Fence Notification** from the following notification types:

    - Import Notification
    - Fence Notification

- Battery Notification

- Messages from Seqrite

- Log Notification

4. Select the period for the notification and click **Search**.

All the fence notifications for the selected search options are displayed.

Battery Notification

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

Viewing Battery Notification

To view the battery notifications, follow these steps:

1. Log on to Seqrite EMM console and click the info notification icon.

2. Click View all Notifications.

The relevant notification page appears.

3. For **Info Notification**, select **Battery Notification** from the following notification types:

- Import Notification

- Fence Notification

- Battery Notification

- Messages from Seqrite

- Log Notification

4. Select the period for the notification and click **Search**.

All the battery notifications for the selected search options are displayed.

Messages from Seqrite

The EMM Administrator receives notifications from Seqrite about different Seqrite announcements, upgrades, license information, and so on. These notifications are displayed as push notifications and once read, they are listed in the messages from Seqrite notification list.

Viewing general messages

To view the general messages, follow these steps:

1. Log on to Seqrite EMM console and click the info notification icon.

2. Click View all Notifications.

The relevant notification page appears.

3. For **Info Notification**, select **Messages from Seqrite** from the following notification types:

    ▪ Import Notification

    ▪ Fence Notification

    ▪ Battery Notification

    ▪ Messages from Seqrite

    ▪ Log Notification

4. Select the period for the notification and click **Search**.

    All the general messages for the selected search options are displayed.

Log Notification

The Seqrite EMM App generates logs for various incidents.

Viewing Log Notification

To view the EMM App Log Notification, follow these steps:

1. Log on to Seqrite EMM console and click the info notification icon.

2. Click View all Notifications.

    The relevant notification page appears.

3. For **Info Notification**, select **EMM App Log Notification** from the following notification types:

    ▪ Import Notification

    ▪ Fence Notification

    ▪ Battery Notification

    ▪ Messages from Seqrite

    ▪ Log Notification

4. Select the period for the notification and click **Search**.

    All the general messages for the selected search options are displayed.

App Request Notifications

When the device user requests to install an app on the device via App Launcher, this notification is sent to the administrator. You can accept or reject the app request sent by the device user. To know more about the Launcher, see Seqrite Launcher.

Viewing app requests

To view the app request notifications, follow these steps:

1. Log on to Seqrite EMM console and click the Note icon.

2. Select the notification types, if available, and the period for the notification, and then click **Search**.

    All the notifications for the selected search options are displayed.

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.

Accepting or rejecting the app request

To accept or reject the app requests, follow these steps:

1. Log on to Seqrite EMM console and click **Alerts**.

2. In the Alert dialog box, click **App Request.**

    The details of app request are displayed with the **Accept** and **Reject** options.

    - **Accept**: Click this button to accept the app request received from the user.

    - **Reject**: Click this button to reject the app request received from the user. Enter the rejection reason and then click **Reject**.

Workspace Notifications

In this section, all the Workspace related notifications are received. You receive notifications for the following reasons.

- Workspace Enrollment: This notification is generated when the Workspace app is enrolled on a device.

- Workspace Uninstallation: This notification is generated when the Workspace app is uninstalled from a device.

- Workspace Time-bomb Trigger: This notification is generated when the Workspace app is removed from a device. This is considered alarming.

- Workspace Locked: This notification is generated when the Workspace app is locked from a device for a specified time due to invalid login attempts.

Viewing Workspace notifications

To view Workspace notifications, follow these steps:

1. Log on to Seqrite EMM console and click the Workspace notification icon.

   Notifications related to Workspace are displayed.

2. To view all the Workspace notifications, click **View All Workspace Notifications**.

3. In the Select Notification Type list, click **Workspace Notifications**.

4. In the Select Report Type list, select the required notification type.

5. Select the time duration to view the notifications and click **Search**.

   All the notifications related to Workspace are displayed.

6. User Profile

This chapter includes the following sections:

User Management

Setup Services

License Management

Change Password

Share Feedback

Contact Us

Administrator Guide

Help Articles

Release Notes

User Management

The User Management option helps you to create a user with an admin role and assign the privileges according to the requirement. Such users can play their roles to carry out various responsibilities. You can change the privileges of a user as per requirement at any point in time. When you assign the rights, the privileges are inherited from pre-defined settings. However, you can change some of the privileges.

By default, there are four admin roles (Administrator types): Super Admin, Admin, Help Desk, and Read Only. You cannot change the privileges of the default admin roles. The Super Administrator is the main administrator or owner of the organization who registers an account with the Seqrite EMM console.

Types of admin roles

The following are the admin roles based on different privileges.

Super Admin

The Super Admin is the main administrator and is created by default when you register a new account with the Seqrite EMM console. For the entire Seqrite EMM console, a single Super Admin is assigned.

The Super Admin has all the privileges for all the modules of the Seqrite EMM console. The Super Admin can set up services such as APNS, Agent upgrade, Agent preference and can customize the reports as per requirement. The Super Admin can create multiple admins with administrator roles, so they can help the Super Admin carry out several responsibilities.

Assigning Super Admin role to an Admin

In many instances, the Admin may be responsible for performing all or similar activities of the Super Admin. With Seqrite EMM, 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 the Seqrite EMM console and perform all the Super Admin responsibilities.

Admin

The Admin can access those users that are assigned to a particular department and have all the privileges similar to Super Admin. The Admin can create multiple administrators with restricted or complete access to all the privileges in the Seqrite EMM console.

Help Desk

The Help Desk role has all the privileges except the delete privilege for the assigned department only.

Read Only

This admin role type has Read-Only privileges, with restricted visibility of the Seqrite EMM console. This admin can export the data and view the privileges but cannot assign any privileges to the user.

Group-wise visibility for EMM console

With restricted visibility, the Admin gets the privilege to manage only the assigned group and gets access to the devices, users, app configurations, and other entities of that particular group.

When such a restricted user with an Admin role creates a department, then a group is also created automatically with the same department name. Thus, the devices associated with that group are visible and the respective administrator can manage them. If any configuration is applied on the device, then such configuration is also visible to the Administrator. With restricted console visibility, the Administrator receives only those notifications that are limited to a specific group. Only the Super admin can generate the custom reports and other admins can generate and schedule the standard report.

Advanced Search for Admin roles

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

1. Log on to Seqrite EMM console and hover over the setting icon of the logged-in user,

available in the upper right corner. Click **User Management.**

2. On the User Management page, click **Advanced Search**.

3. From the Select Created By list, select the desired creator name and click **Search**.

    The result gets displayed.

Creating an admin role

To create a new admin role, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **User Management.**

2. On the User Management page, click **Add** available on the upper right corner.

    The Create Admin Role page appears.

3. In the **Admin Role Name** field, type a role name.

4. In the **Inherit from** list, select one of the admin role types.

    ▪   Admin

    ▪   Help Desk

    ▪   Read Only

    The Inherit list is a predefined set of privileges. When you select an Inherit list, the default privileges assigned to the admin role type appear. Verify if all the privileges are right for the admin role that you are creating. You may modify some of the default privileges, if required.

5. To save your settings, click **Save**.

    The new admin role is created.

    You can edit the newly created admin role, change its privileges, and add users to the admin.

Adding a user to the admin role

After you create a new admin role, you can add users to an admin role type. This admin will carry out the responsibilities for all the assigned users. To know about how to add a user to an admin role, see Add a user.

Taking an action on admin roles

Take Action is an option that helps you take an appropriate action on the admin roles.

For admin roles, you can create a copy of the admin role or delete an admin.

Creating a copy of an admin role and deleting an admin role

To delete an admin role, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **User Management.**

2. On the User Management page, select an admin role.

   The Take Action list appears.

3. Select **Create Copy** to create an admin role with the same privileges or select **Delete** to remove the admin role.

4. Click **Submit**.

   [i] Note:

   o   You cannot delete the default admin roles.
   o   You cannot delete a user assigned to an admin role.

Editing an admin role

You can edit the Admin Role name, Type, and Privileges. You can view all the privileges assigned to the admin role for the specific department.

To edit the Admin role details, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **User Management.**

2. On the User Management page, select an Admin role and click the **Edit** icon.

3. Click the **Edit** tab and then click the **Edit details** tab.

4. Edit the admin role name, admin role type, and turn on/off the privileges as required.

   [i] Note:

   You cannot change the default admin role privileges such as (Super Admin, Admin, Advanced, Standard, and Basic). You can simply view them.

5. Click the **Admins** tab.

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

   [Tip icon] Tip:

   You can assign an admin role to the Admin through the Privileges option on the User Details page.

Setup Services

The Setup Services section lets you register cloud services for the Android and iOS devices. These setup services allow communication between the Agent and the server. It is a one-time activity to be done on the Seqrite EMM console.

This service helps you to send messages from the server to the enrolled devices. This acts as an interface between the Agent and the server.

> **ℹ Note:**
>
> The Setup Services section is visible to Super Admin and to the Admin with the Super Admin privilege.

The Setup Services include the following services:

Enterprise Account Enrollment

Apple Certificate

Agent Upgrade

Agent Preference

Company Branding

Notification Preference

SMS Settings

Custom Account Settings

Flash Enrollment

Enterprise Account Enrollment

Android Enterprise Account Enrollment helps you to enroll your company for Android Enterprise Management and integrate the Android devices into the enterprise mobility management solutions. The enrolled Android Enterprise account details are displayed when you click the Enterprise Account Enrollment tab.

> **💡 IMPORTANT:** If you change the admin email address, you need to enroll the devices again with the new email address.

To enroll Seqrite EMM account with Android Enterprise, follow these steps.

1. Log on to Seqrite EMM console, and in the left pane, click **Setup Services**.

    You are redirected to the Setup Services page.

2. In Enterprise Account Enrollment section, click **Enroll** to register your company using   the

company Gmail account.

You are redirected to Google Play page.

3. On the Google Play page, click **Get Started** to login with the Gmail account.

4. Enter the organization name in the Business name field and click **Next**.

5. Enter the contact details such as Name, Email Address and Phone of company's Data Protection Officer and EU Representative. Select the check box to agree to the Google Play terms.

6. Click **Confirm**. You are redirected to the Set up complete page. Click **Complete Registration**.

You are redirected to the Setup Services page in your EMM console.

7. After Android Enterprise is enrolled to the EMM account, the admin can initiate Android Enterprise Enrollment in the following ways:

- **Users** > Select one or more Users > From the Take Action list, select **Enrollment Request>For Device Management>Using Android Enterprise>For Device Management>Android Enterprise Enrollment Using AMA.**

- **Devices** > Select one or more Devices > From the Take Action list, select **Enrollment Request** > F**or Device Management>Android Enterprise Enrollment Using AMA.**

- **Devices** > Device Details > Overview > **Android Enterprise Enrollment Using AMA.**

- **Groups** > Group Details > Bulk Enrollment > Select Enrollment Preference as **Android Enterprise Enrollment Using AMA.**

Apple Certificate

Apple Push Notification Service (APNS) helps you to configure cloud services for iOS devices. Customers must have an Apple ID for configuring APNS certificate and use their Apple Certificate to send the push notification to the devices.

To upload the Apple Certificate, follow these steps.

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, follow these steps:

   ▪ Download a Certificate Signing Request (CSR), signed by Quick Heal Technologies Ltd.

   ▪ Go to the Apple Push Certificate Portal and upload the CSR and download the Push Certificate.

   ▪ Upload the Apple Certificate.

   ▪ Upload the Apple Push Certificate file.

3. Click **Upload**.

> ℹ️ Note:
>
> To help you know how to download the CSR, create and upload Apple Certificate, instructions are given on the right-hand side.

Upgrade

The Upgrade Setting section gives you information about how to share the updated versions of Seqrite EMM Agent app and Seqrite Launcher Agent app using different app source types.

Agent Upgrade

The Agent Upgrade setting helps you to send the updated version of the Seqrite EMM Agent from the server to the user's device. This setting provides different sources to download and install the updated version of the Seqrite EMM Agent.

Before you send the update of the Agent app to the users, you must enable the Agent Upgrade Notification option.

The App source type includes Default Location, Custom URL, and Upload Agent.

Default Location

The Default Location option helps you to update the version of Seqrite EMM app using Seqrite App Store. All the users can download the Agent app from the Default Location of Seqrite EMM app and install it with an in-built wakeup app on the device.

Updating Seqrite Agent app via Default Location

To update the Seqrite EMM app via Seqrite App Store, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Upgrade** and then, click Agent **Upgrade**.

3. Turn on the Agent Upgrade Notification and select the App Source Type as Default Location.

    The Package ID option will be pre-filled.

4. Click **Save**.

Custom URL

With the Custom URL option, you can make the Seqrite Agent app available from your own company website to the users. After you upload the Seqrite Agent app on your website, the user receives a prompt about the availability of the updated Seqrite Agent app. The user can then download the latest version of Seqrite Agent and in-built wakeup app from the company URL.

Uploading custom URL on Cloud

To upload custom URL on Cloud, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Upgrade** and then, click **Agent Upgrade**.

3. Turn on the **Agent Upgrade Notification** and select the App Source Type as **Custom URL**.

    The Custom URL section is displayed.

4. Enter Version Name, Version Code, Package Id, and URL where the apk. file is available.

5. Enter App MD5 hash.

6. Click **Save**.

    The Custom URL setting is saved successfully, and the user will receive a prompt to download and install the updated Seqrite EMM Agent.

Upload Agent

With this option, you can upload the APK file of the Agent app on Seqrite EMM Cloud. After the APK is uploaded on the Seqrite EMM Server, the Agent with in-built wakeup app will be downloaded on the device and the user can install it.

Uploading APK on Seqrite EMM Cloud

To upload APK on Seqrite EMM server, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Upgrade** and then click **Agent Upgrade**.

3. Turn on the EMM Upgrade Notification and select the App Source Type as Upload EMM App.

   The Package ID option will be pre-filled.

4. Enter App MD5 hash.

5. Select the APK file and click **Save**.

   If an older version of Seqrite EMM Agent is installed on the device, then as soon as the device syncs with the server, the .apk file will be downloaded automatically on the device and the user will be promoted to install the new version of the Seqrite EMM Agent.

   Important: The user needs to tap the **Install** button to install the latest Seqrite EMM Agent.

Launcher Upgrade

The Launcher Upgrade setting helps you to send the updated version of the Launcher Agent from the server to the users' device. The new launcher version can be downloaded and installed from Default Location, custom URL, or Upload Launcher App.

To send the update of the Launcher Agent to the users, you must enable the Launcher Upgrade Notification option.

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 Agent via Default Location

To update the Launcher using the default location, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Upgrade** and then, click **Launcher Upgrade**.

3. Turn on the Launcher Upgrade Notification option.

4. From the App Source Type option, select **Default Location**.

   Package ID is pre-filled.

5. 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.

   Important: The user needs to tap the **Install** button to install the latest Launcher app.

Custom URL for Launcher

With the Custom URL option, you can make the Launcher Agent available from your own company website to the users. After you upload the Launcher Agent app on your website, the user receives a prompt about the availability of the updated Launcher Agent app. The user can download the latest version of Launcher Agent and in-built wakeup app from the company URL.

Downloading Launcher Agent from custom URL

To upload the custom URL on Cloud, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Upgrade** and then click **Launcher Agent**.

3. Turn on the Launcher Upgrade Notification.

4. From the App Source Type option, select **Custom URL**.

5. Select App MD5 hash.

6. Enter Version Name, Version Code, Package Id, and URL where the apk. file is available.

7. Enter App MD5 hash.

8. Click **Save**.

   The Custom URL setting is saved successfully, and the user will receive a prompt to download and install the updated Launcher Agent.

   Important: The user needs to tap the **Install** button to install the latest Launcher app.

Upload Launcher App

With this option, you can upload the .apk file of the Launcher Upgrade on Seqrite EMM Cloud. After the .apk file is uploaded on the Seqrite EMM Server, the Launcher Upgrade with in-built wakeup app will be downloaded on the device and the user can install it.

Uploading Launcher APK on Seqrite EMM Cloud

To upload the Launcher APK on Seqrite EMM server, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user,

available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Upgrade** and then click **Launcher Upgrade**.

3. Turn on the Launcher Upgrade Notification option.

4. From the App Source Type option, select **Upload Launcher App**.

   The Package ID option will be pre-filled.

5. Enter App MD5 hash.

6. Select the APK file 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 Seqrite EMM Agent.

   Important: The user needs to tap the **Install** button to install the latest Launcher app.

Workspace App Upgrade

With Workspace App Upgrade option, you can send the updated version of the Workspace app from the server to the user's device. The upgrade can be downloaded and installed from the default location or Workspace app APK.

To send the updated Workspace app to the users, you must enable the upgrade notification option.

Default Location for Workspace app

With this option, you can send the updated version of Workspace app using the 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 Workspace app from default location

To update the Workspace app using the default location, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Upgrade** and then click **Workspace App Upgrade**.

3. Turn on the Workspace App Upgrade Notification option.

4. From the App Source Type option, select **Default Location**.

   The Package ID is pre-filled.

5. Select App MD5 hash.

6. Click **Save**.

   The update app is uploaded to the default location.

Upload Workspace App

With this option, you can upload the Workspace app APK on the Seqrite EMM Cloud. After the APK is uploaded on the Seqrite EMM Server, the Workspace app will be downloaded on the devices and the users must install it.

Uploading Workspace APK on Seqrite EMM Cloud

To upload the Workspace APK on Seqrite EMM server, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Upgrade,** and then click **Workspace App Upgrade**.

3. Turn on the Workspace App Upgrade Notification option.

4. From the App Source Type option, select **Upload Workspace App**.

    The Package ID option will be pre-filled.

5. Select the APK file and click **Save**.

    If the old version of Workspace app is installed on the device, then as soon as the device syncs with the server, the new APK will be downloaded automatically on the device. The user will be prompted to install the new version of the Workspace app.

Important: The user needs to tap the **Install** button to install the latest Workspace app.

Agent Preference

The Agent Preference option gives you the privilege to choose the default or custom build of EMM Agent to be installed on Android devices in the network of your organization.

Selecting the Agent preference is a one-time activity. Make sure all the devices in your network have the same Agent app preference. If you wish to change the Agent app preference, uninstall all the devices from the console, and enroll the devices with the required Agent preference again.

Changing the Agent preference

To change the Agent app preference, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Agent Preference**.

3. In the App Preference section, select either Default or Custom app, as per your requirement.

   - Default App: Choose this option if you wish to use the default EMM app from Seqrite.
   - Custom App: Choose this option if you have customized the app as per requirement.

4. Click **Save**.

Company Branding

Using the Company Branding option, you can customize the company name, logo and favicon, and personalize the device wallpaper.

Company Name

In this section, you can enter your own company name to reflect in the Seqrite EMM console, in the About page of Seqrite EMM Agent app, and on the Launcher app. The Company Logo option lets you edit the company logo on the Launcher. Whenever the device syncs with the server, the updated logo reflects on the Launcher.

Customizing the company name

To customize the company name, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user,

available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Company Branding,** and then click **Company Name**.

3. Enter the company name and then click **Save**.

![i]Note:

You can also change the company name and logo from Launcher Settings section of app configuration. If any change is made to the Launcher Settings (app configuration), it will override the Company Settings.

Console Personalization

In this section, you can change the company logo and favorite icon.

Along with the personalized company name, all these changes will reflect in the Seqrite EMM console, in the About page of Seqrite EMM Agent app, and on the Launcher app.

The Company Logo option lets you edit the company logo on the Launcher. Whenever the device syncs with the server, the updated logo reflects on the Launcher.

Customizing the Console

To customize the console, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Company Branding,** and then click **Console Personalization**.

3. Enter the company logo and favicon and then click **Save**.

![i]Note:

You can also change the company name and logo from the Launcher Settings section of app configuration. If any change is made to the Launcher Settings (app configuration), this change will override the Company Settings.

Device Personalization

You can add a company logo to customize the Seqrite EMM Agent app installed on the devices and even add a wallpaper for the devices. This personalization will help you create a brand image of your organization as both the Seqrite EMM Agent app and device wallpaper will have the same company logo.

Note:

- o The wallpaper image resolution must be 1080 x 1920.
- o Wallpaper is supported on the devices that are ADO and KNOX supported with OS 6 or later versions.
- o The device wallpaper reflects on the device when the device syncs with the server or the Admin sends a sync command from the console.
- o There is a provision to change the launcher wallpaper from Launcher Settings section of app configuration also. The Launcher Settings (app configuration) override the Launcher Wallpaper Setting (Custom Setting).

Customizing the device wallpaper

To customize the wallpaper, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Company Branding** and then click **Device Personalization**.

3. Hover over the device wallpaper space. The Camera icon is displayed.

4. Click the arrow next to the camera.

   - To add a new device wallpaper, click **Upload**.

   - To remove the device wallpaper, click **Delete**.

5. To save your settings, click **Save**.

Notification Preference

With Notification Preference, you as an admin can select the reasons for which you want notifications to be received on the Seqrite EMM console. Notifications are the messages that bring to your notice the incidents happening in the Seqrite EMM console and devices where the Seqrite EMM Agent is installed.

By default, certain notifications are selected. However, you can select your own preference, if required.

Setting Notification Preference

To set notification preference, follow these steps:

1. Log on to Seqrite EMM console and in the upper right corner, click the logged on User name > click **Setup Services** > **Notification Preference**.

2. Log on to Seqrite EMM console and hover over the setting icon of the logged in user,

available in the upper right corner. Click **Setup Services.**

3. On the Setup Services page, click **Notification Preference**.

4. For each notification type, you can select whether you want to receive the notification on the Seqrite EMM console or as an email sent to the configured email address or both.

    If you select for email notification, make sure that you also add an email address in the appropriate field.

5. To save your settings, click **Save**.

SMS Settings

In this section, you must configure the SMS gateway to send and receive SMS notifications to the devices.

SMS Gateway Integration

You must configure the SMS gateway to successfully send and receive SMS notifications about incidents related to the devices.

Configuring SMS Gateway

To configure the SMS gateway, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **SMS Settings,** and then click **SMS Gateway Integration**.

3. Enter the SMS Server URL, Sender Id, Mobile No Key, and the Message Key.

4. To save your settings, click **Save**.

SMS Battery Notification

In this section, you can configure the notification to be sent when the battery level goes below 15%.

Configuring SMS for battery notification

To configure SMS Battery Notification, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **SMS Settings,** and then click **SMS Battery Notification**.

3. Select the Send SMS for battery below 15% check box.

4. Add an admin mobile number.

    You can add up to three mobile numbers, separate by commas.

5. To save your settings, click **Save**.

Custom Account Settings

In Custom Account Settings, you can configure the settings for IMAP/POP email services for receiving emails, and the protocols for Contacts and Calendar.

Email (IMAP/POP) Settings

In Email (IMAP/POP) Settings, you can configure the email account settings for IMAP and POP services. The Internet Email (IMAP/POP) policy in Workspace will work, only if you have configured the email account settings.

Configuring Email (IMAP/POP) Settings

To configure Email (IMAP/POP) Settings, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Custom Account Settings**.

3. For Email (IMAP/POP) Settings, select either IMAP or POP service for email communication. Each has similar settings.

4. Configure Incoming mail server, Port and Encryption Type, Outgoing mail server (SMTP), and Port and Encryption Type.

   Make sure that you set the correct information in each field, else the email communication will fail.

5. To save your settings, click **Save**.

Contacts (LDAP/CARDDAV) Settings

In Contacts (LDAP/CARDDAV) Settings, you can configure the settings for LDAP and CardDAV protocols to import contacts from different sources on your mobile phones.

Configuring Contacts (LDAP/CARDDAV) Settings

To configure Contacts (LDAP/CARDDAV) Settings, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Custom Account Settings**.

3. In Contacts (LDAP/CARDDAV) Settings, select the Account Type. You can select LDAP or CARDDAV protocols.

   - If you select LDAP, configure LDAP Host, Port and Encryption Type, Login Attribute, Base DN, and User Filter.

   - If you select CARDDAV, configure Server URL and Port.

4. To save your settings, click **Save**.

Calendar (CALDAV) Settings

In Calendar (CALDAV) Settings, you can configure the settings for CALDAV protocol to synchronize calendar with the email account services such as Outlook, GSuite, and others.

Configuring Calendar (CALDAV) Settings

To configure Calendar (CALDAV) Settings, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Custom Account Settings**.

3. In Calendar (CALDAV) Settings, configure **Server URL** and **Port**.

4. To save your settings, click **Save**.

Flash Enrollment

The Flash Enrollment allows bulk enrollment without manual interference for individual device. The Admin imports device IMEI on the Seqrite EMM console and the device gets enrolled automatically with the Seqrite EMM Agent. This enrollment is done without the need for OTP or Scan QR code for the enrollment.

If you prefer Flash Enrollment, you must import device IMEI, group name and device user Email id in CSN format. Post IMEI import, you can set preference to assign device name using IMEI number, MAC address, phone number or system generated name.

i Note:

Flash mEnrollment will not work on the devices with Android OS version 10.

Enrolling device with Flash Enrollment

To enroll the device with flash enrollment process, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Setup Services.**

2. On the Setup Services page, click **Flash Enrollment**.

3. Click Import Details.

    In this section, you can import details such as IMEI number of the devices, the group name in which the user should be added, and the user email address.

4. Click in the blank field or click **Select File** and browse for the csv. file and click **Open**. Then

click **Import**.

If you want to see the reference csv. file, click **Download sample CSV file format** link.

- Export: Use this option to export the IMEI details.

- Delete: Use this option to delete all the IMEI details exported till date.

5. Click **Device Name Preference** and from the Select Device Name list, select the required option.

- As System Generated: Select this option to have a default nomenclature for the devices.

- As IMEI Number: Select this option to name the device as per IMEI number.

6. Click **Save**.

To enroll the device, the device user needs to download and install the EMM Agent App and it will auto-enroll with mapped group and owner. Device users will not require to Scan QR Code or enter OTP/Company Code.

$\boxed{i}$ Note:

Flash mEnrollment works on Android 9 or later versions only.

License Management

The License section lets you view the license details of the product. This helps you know when your license is going to expire, so you can renew it on time.

Viewing the license details

To view the license details, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **License Management.**

The license page appears with the license details.

You can change the contact name, email address, and contact number if required.

You can even renew your license. If you have renewed your license but the license details do not reflect the new license expire date, you can update the license information.

Under History, you see the duration from when you are using the Seqrite EMM console and other information.

Buy Subscription

When you have a trial version of Advance Seqrite EMM software, you can buy Seqrite EMM by using Buy Subscription option. This option is visible in the License section as well as on the Seqrite EMM dashboard header when the license is about to expire.

To purchase Seqrite EMM, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner.

2. Click License Management and then click Buy Subscription.

    A purchase success prompt appears. The purchase request is sent to the sales executive with Seqrite EMM. The sales executive will contact the Administrator of Seqrite Enterprise Mobility Management (customer) for further processing.

Renew

When you have a Standard or Advance license of Seqrite EMM, and it is about to expire, then you can renew your product license.

To renew Seqrite EMM software, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner.

2. Click **License Management** and then click **Renew**.

    A renewal success prompt appears. The renewal request is sent to the sales executive with Seqrite EMM. The sales executive will contact the Administrator of Seqrite Enterprise Mobility Management (customer) for further processing.

Change Password

With this option, you can change the password of EMM console.

Changing the password in EMM console

To reset the password in Seqrite EMM console, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Change Password**.

2. In the Change Password dialog box, enter the current password, new password, and confirm the new password.

3. Click **OK**.

Share Feedback

The Share Feedback option is a simple approach for you to reach us. You can share your feedback with us and help us to make the product better.

To share your feedback, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner. Click **Share Feedback** and share your feedback.

2. Click **Submit**.
   For any technical queries, you can write to us to mdm.support@seqrite.com.

Contact Us

With this option you can contact the Seqrite Support in multiple ways.

To see our contact details, follow these steps:

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner.

2. Click Contact Us.

   It includes the following support facilities:

   ▪ Email Support: Using this option, you can submit a ticket for your query.

   ▪ Live Chat Support: To connect with us directly, use this option.

   ▪ Phone Support: To make a call, use the phone numbers given.

   ▪ FAQ: If you have any query, you can visit our [FAQ portal](#) and check an answer to your query.

   ▪ Online Help: To check information about how to configure the settings of a feature, you can check our [Online Help](#). Alternatively, you can click the Help icon available on each

feature. This will help you open the relevant Help page. You can also browse to other sections from any Help page.

Phone Support

For telephonic support, you can call our India-based support center at:

1800 212 7377

Monday – Saturday : 9:00 AM to 9:00 PM (IST)

You can also 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 9:00 AM to 9:00 PM (IST).

Documentation

Administrator Guide

To know about how to configure the settings of a feature, you can check our Administrator guide. Our Administrator guide is oriented towards helping you carry out configuration independently in the easiest way.

Alternatively, you can click the Help icon available on each feature. This will help you open the relevant Help page. Although you can browse to other sections from any Help page.

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner.

2. Click Administrator Guide.

Help Articles

Under this section, you find help articles you perform certain actions on your own. You can get information related to how to enroll devices, activate the device owner mode, how to enable supervised mode iOS, and other kinds of information.

Release Notes

This option includes the release notes of the current product version. The release notes include the details of new features, enhancements of the product and the known issues of the new version of Seqrite EMM.

1. Log on to Seqrite EMM console and hover over the setting icon of the logged in user, available in the upper right corner.

2. Click Release Notes.

7. Users

The Users option allows you to add users to the Seqrite EMM console and manage them.

Advanced Search for Users

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

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

1. Log on to Seqrite EMM console and in the left pane, click **Users**.

2. On the Users page, click **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.

3. 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 Admin Role**: Select the option from the list to search the Admin according to their Admin role.

4. Click **Search**.

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

Adding a user

To add a new user, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Users**.

2. On the Users page, click **Add User** > **Add** available on the right-hand side.

   The Add User page is displayed.

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

4. Click **Save**.

   The user is added successfully.

   After a user is added, you must assign privileges, visibility restriction, and send an enrollment request to a device.

   With privileges, a user can play certain roles, and with visibility restriction, the user can access the assigned entities.

Importing users

Prerequisites: To import users, keep the csv file containing the list of users ready on your device.

To import users, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Users**.

2. On the Users page, click **Add User** > **Import** available on the right-hand side.
   The Import Users dialog box is displayed.

3. Browse and select the file containing the list of users.

4. Click **Import**.

   The users are imported into Seqrite EMM.

Editing User Details

To edit the user details, follow these steps,

1. Log on to Seqrite EMM console and in the left pane, click **Users**.

2. On the Users page, select the user and click the edit icon for which you want to edit the details.

3. On the User Details page, click the **Edit** tab.

4. Update the details as required and click **Save**.

Assigning Privileges to a user

To assign privileges to a user, follow these steps:

1. When you log on to Seqrite EMM console, make sure you are in the Privileges section on the Users page.

2. Select Allow admin access.

3. From the **Admin Role** list, select an admin role.

    The Privileges are displayed.

    Admin roles are available as per your own organization structure.

4. Click **Save**.

Assigning Visibility Restriction to a user

To assign visibility restriction to a user, follow these steps:

1. When you log on the Seqrite EMM console, make sure you are in the Visibility Restriction section on the Users page.

    A description about Visibility Restriction is visible.

    Read the restriction carefully.

    In the **Assign visibility for all groups**, turn On or Off as per requirement.

Exporting User Details

To export the user details, follow these steps,

1. Log on to Seqrite EMM console and in the left pane, click **Users**.

2. On the Users page, select the user and click the edit icon for which you want to export the details.

3. On the User Details page, click the **Export**.

    The user details are exported in a PDF format.

Enrollment

Device Enrollment is the process of enrolling the mobile device with the Seqrite Enterprise Mobility Management console. After enrollment, the mobile device users become members of the Seqrite Enterprise Mobility Management console. When you complete the enrollment, you can manage the device functionality, configurations, and perform the actions remotely. The device can be enrolled using Email/SMS, QR Code, Android Enterprise Enrollment, Enrollment with ADO Enablement or Enrollment with COPE Enablement. Both the Android and iOS can be enrolled.

Note: Both Android and iOS devices can be enrolled under **Users** tab only.

Enrollment for Android

You can enroll your device in the following ways using Seqrite Enterprise Mobility Management for device management option:

   a. Enrollment using QR Code, Email or SMS

   b. Device Owner Enrollment (Enrollment using ADO enablement)

   c. Android Enterprise Enrollment using AMA

   d. Work Profile for personal device

   e. Work Profile for corporate device

Enrollment using QR Code, Email or SMS

In this process, the admin generates a QR Code on the EMM console and scans the generated QR code on the console through the EMM app on the device. The QR code is also mailed to the user and can also be sent through SMS. Alternatively, the generated QR code can be printed and shared with the users for scanning through the device.

1. To submit the request for enrollment on the Seqrite EMM console, navigate to the **Users** tab in the left pane and select the user from the list.
   From the Take Action list, select **Enrollment Request** > **For Android Devices** > **QR Code, Email or SMS** and click **Submit**.
2. After sending the enrollment request, the device user will receive the enrollment details (Company Code and OTP) through email and SMS as shown below.
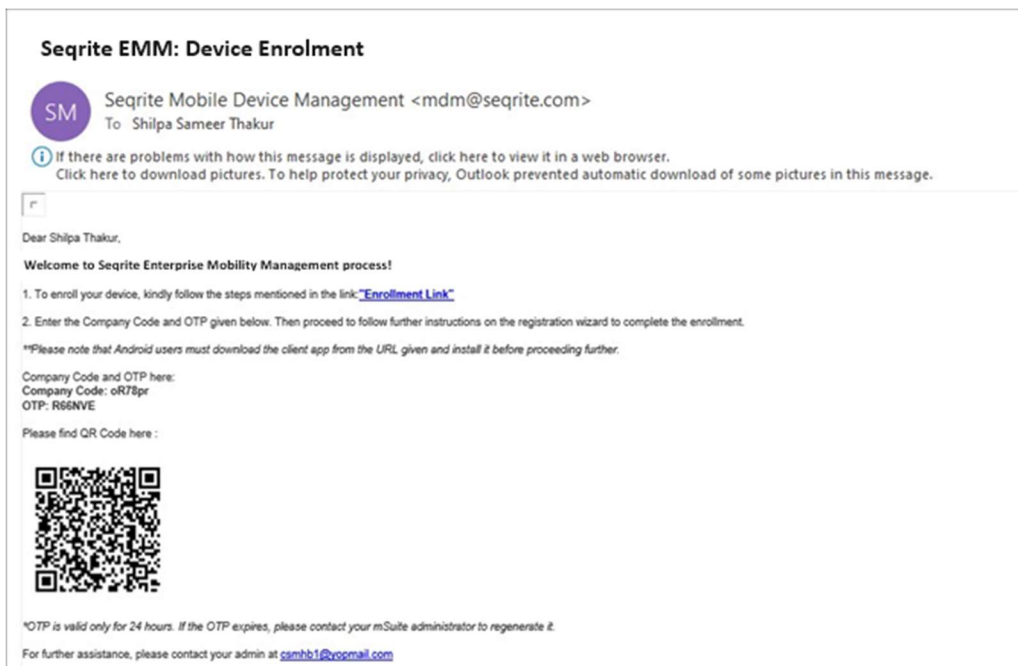
3. Tap the enrollment link, you are navigated to the Seqrite App store.

4. Click **Download**. The file is downloaded onto your device. Tap the downloaded file to start the app installation. The License Agreement screen is displayed.

5. On the License Agreement screen, tap **I Agree**.

6. On the Permission required screen, tap **OK.**

7. Tap Allow to   grant   the   app   permission   to   manage   phone   calls.
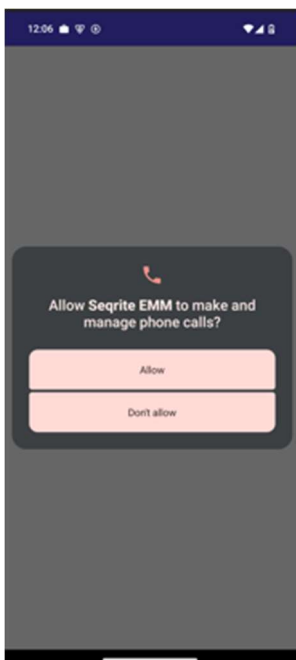
8. Tap **Proceed** to grant device admin permission.

9. Enter the displayed captcha verification code, which may appear only on some devices. On certain devices, you may see only the Activate option.
Tap **Activate**.
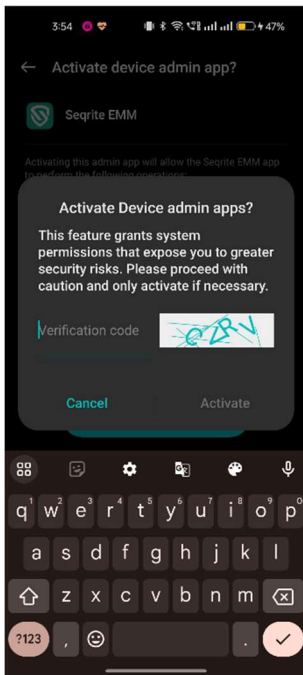
10. Tap **Activate** on the Activate device admin app screen.

11. Enter the enrollment details that the user received in the email and tap **Enroll** or use the Scan QR Code option to scan the QR code received in email.
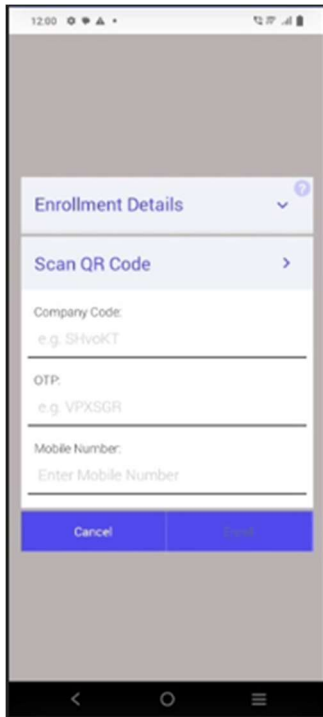
12. Tap **Proceed** to grant Android Runtime Permission.
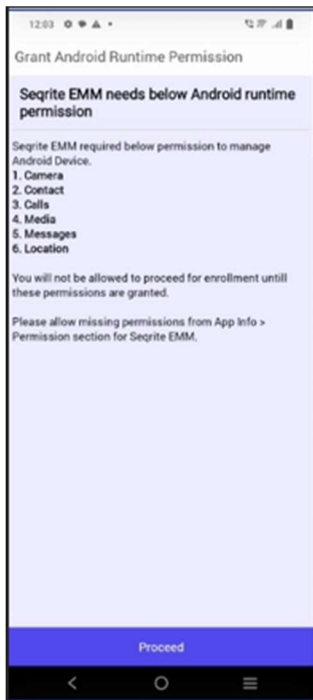
13. To allow Seqrite EMM to take pictures, record video and audio, tap **While using the app.**
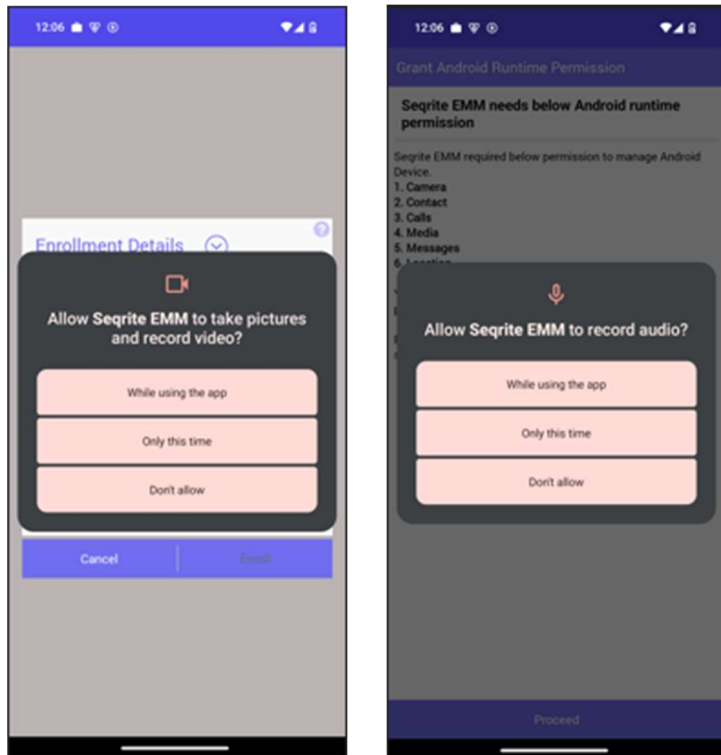
14. To allow Seqrite EMM to access phone logs, contacts and determine nearby devices, tap **Allow.**
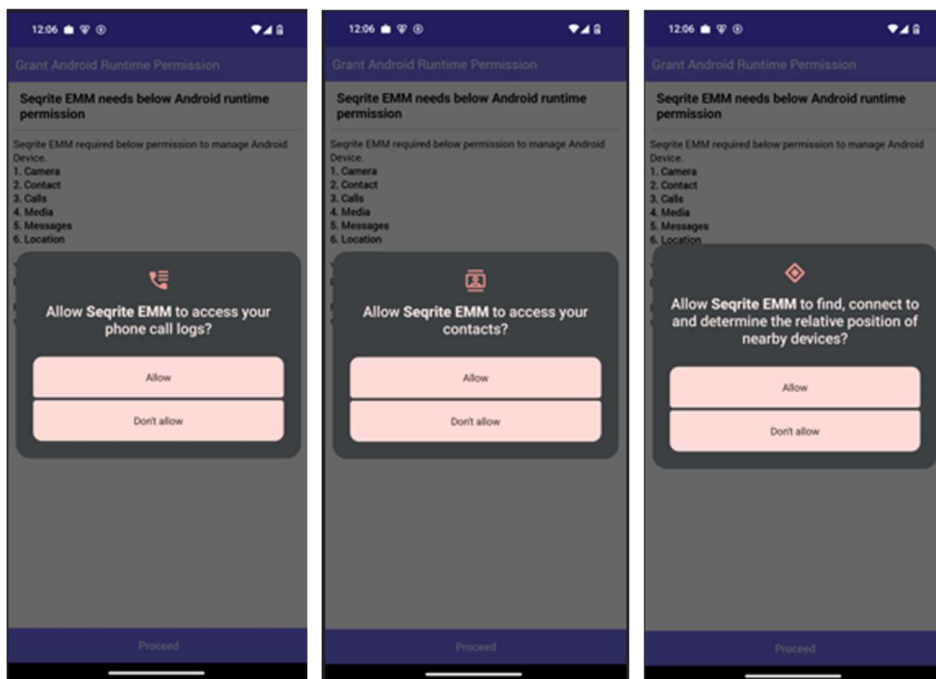
15. Tap **Settings** to allow installation of the app.
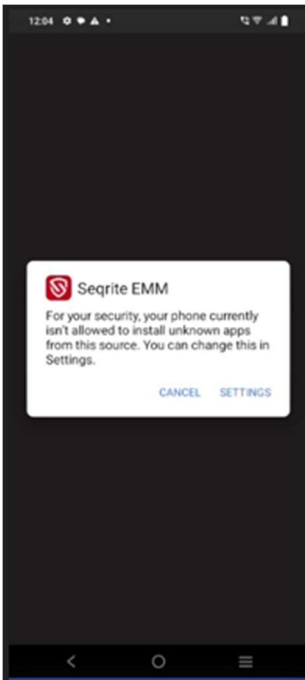
16. Enable the toggle to allow installation of apps from this source.
17. Tap **OK** to grant background location permission to the Seqrite EMM app.
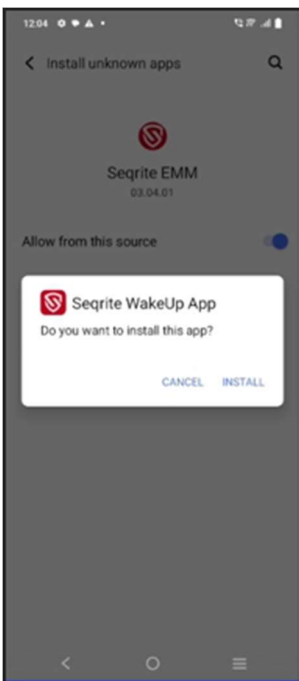
18. Tap **Permissions** on App Info screen.
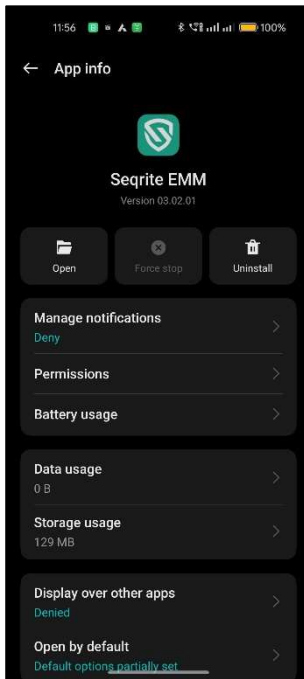
19. Tap the back arrow and navigate to Location Permission. On the Location Permission screen select **Allow all the time**.
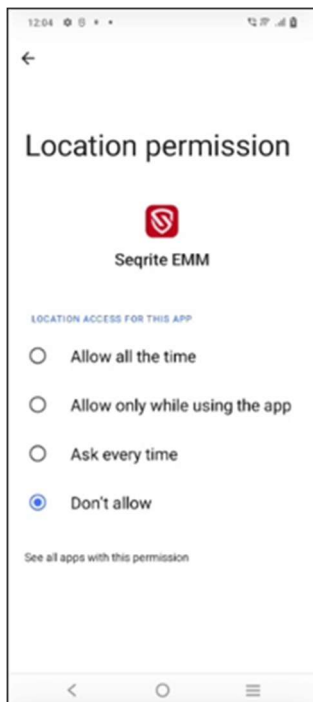
20. Tap the back arrow and enable the option to allow notifications.
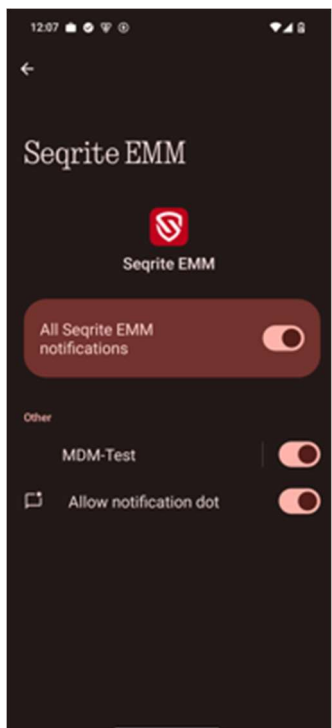
21. Tap the back arrow and enable the option to allow modify system settings.
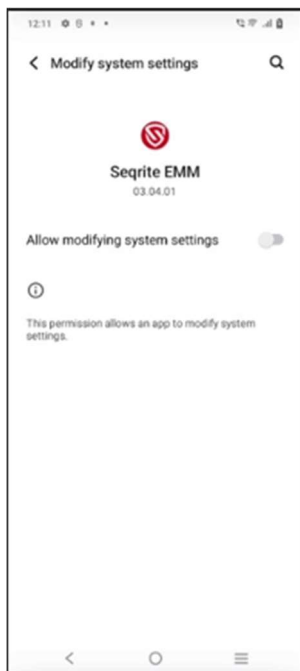
22. Tap the back arrow and select **Seqrite EMM** on the Display over other apps screen.
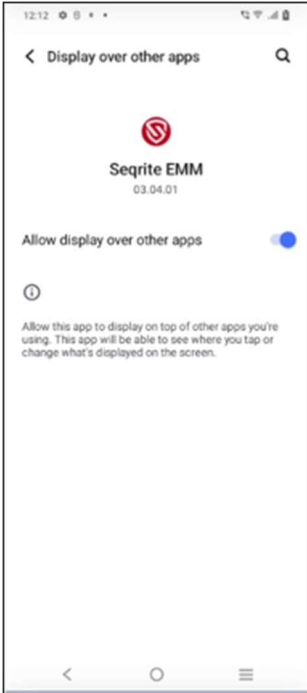
23. Enable the toggle to allow Seqrite EMM app to display over other apps.
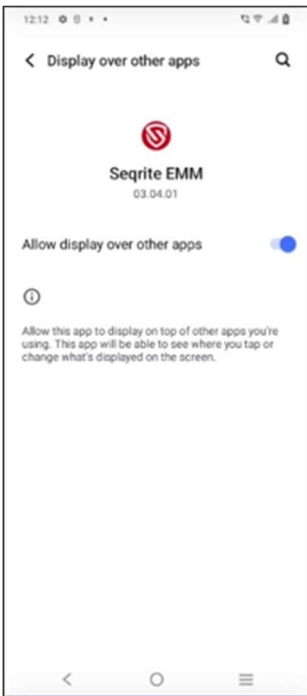
24. Tap the back arrow and select Seqrite EMM on the **Usage access** screen.
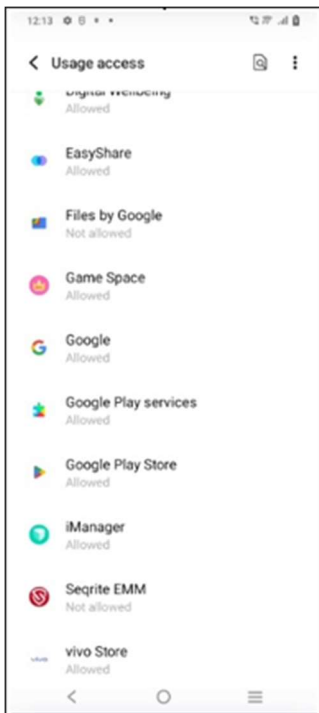
25. Tap back arrow and enable the toggle to **Permit usage access** for Seqrite EMM app.
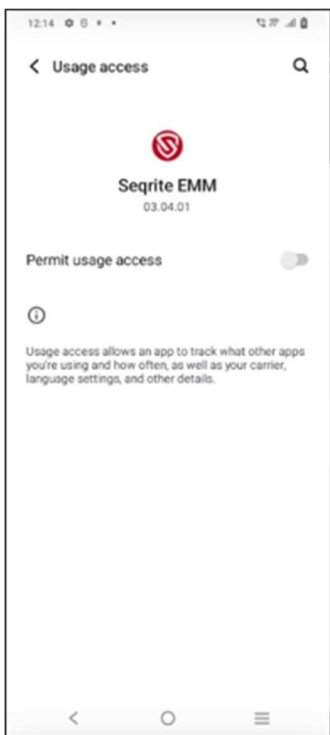
26. Tap the back arrow and select Seqrite EMM on **Do Not Disturb** screen.

27. On the Do Not Disturb screen enable the toggle **Allow Do Not Disturb** and tap **Allow.**

28. The Seqrite EMM app home screen is displayed.
29. Tap the icon in the center of the screen to grant device accessibility permission.
30. Tap **Seqrite EMM** to enable accessibility permission for the Seqrite EMM app.

31. Tap **Allow** to let the Seqrite EMM app always run in the background.
Seqrite EMM app is enrolled.
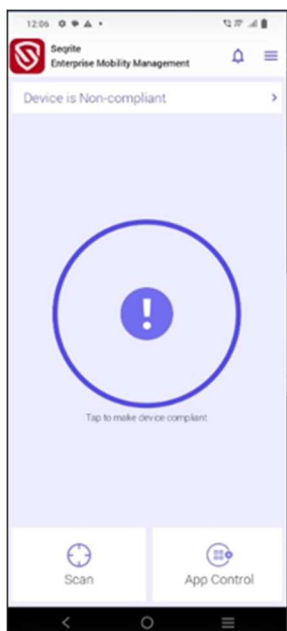
Device Owner Enrollment (Enrollment using ADO enablement)

You can enroll company owned devices using this enrollment type where device will be completely controlled or managed by the configuring and applying policies.
You can enroll company owned devices using this enrollment type and control or mange the corporate data by configuring and applying policies.
You can do enrollment using ADO in the following two ways:

- Using QR codes
- Using ADB (Android Debug Bridge).
  The ADB is a command tool that allows communication between a computer and a connected Android device.

ADO Enrollment using QR Codes
For enrollment using ADO enablement, you can either use a new device or you need to perform a factory reset on your device.
Note: When you perform a factory reset, all the data on the device is permanently deleted. Ensure that you take a backup of your data.

A. Performing a factory reset on your phone

1. On the device, tap **Settings > System > Reset**. Please note that the terminology in your device may differ.
2. Tap **Reset Phone**.
   A Welcome screen is displayed after a factory reset of the device.

Next, you need to do ADO enrollment of your device using a QR Code.

B. Enrollment of a device using QR code
The admin or the end user can both enroll the device.

- If you (admin) are enrolling the device, you can use the QR codes displayed on the Seqrite Enterprise Mobility Management console during the enrollment process in the following way.

  o Navigate to the Users tab in the left pane and select the user from the list.
    From the **Take Action** list, select **Enrollment Request** > **For Android Device** > **Device Owner Enrollment** and click **Submit**.
    QR codes are generated on the Seqrite Enterprise Mobility Management console that need to be scanned later on the device.

- If the user is performing the enrollment, the user can scan the QR codes that are shared by admin with the user.

  1. On the Welcome screen, tap 6-7 times below the word Welcome. Devices may show "Welcome", "Hi" or "Hello" as per the device models. A QR code scanner appears.
     If the scanner does not appear, you may need to connect to the Internet and download a QR code scanner application.
  2. Scan the **first** QR code (ADO Enablement QR Code) displayed on the Seqrite EMM console. Alternatively, the end user performing the enrollment process can scan the QR code shared by admin or received by email.
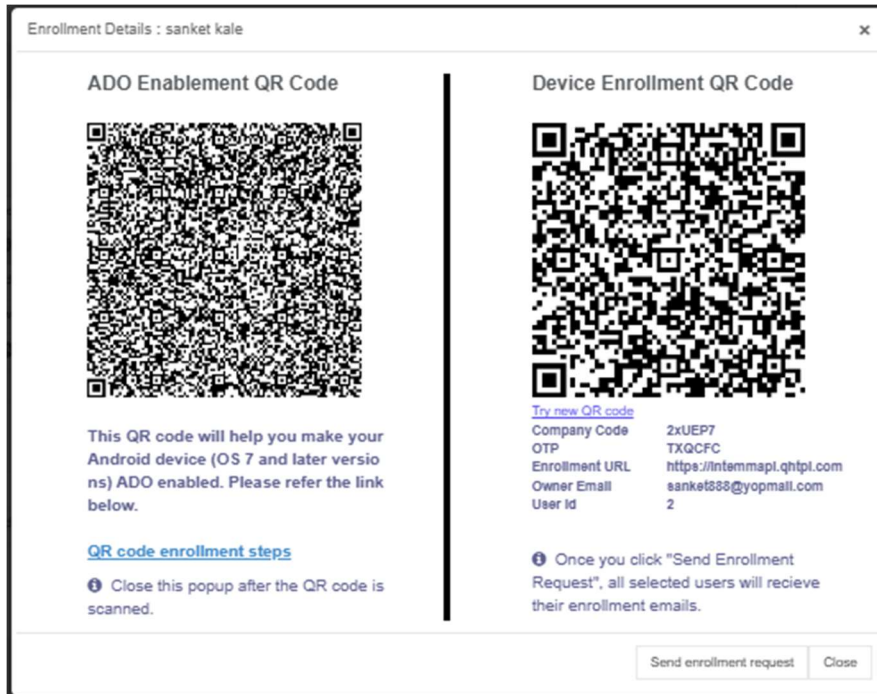
3. Next, choose the appropriate option to connect to the Internet. You are redirected to Set Up Your Device screen. Tap **ACCEPT & CONTINUE**.
   The Seqrite EMM app is downloaded on your device and displayed on the Home screen.
4. Tap **Seqrite EMM** app. You are redirected to the license agreement screen.
5. Tap **I Agree.** You are redirected to the permission required dialog box.

6. Tap **OK**.
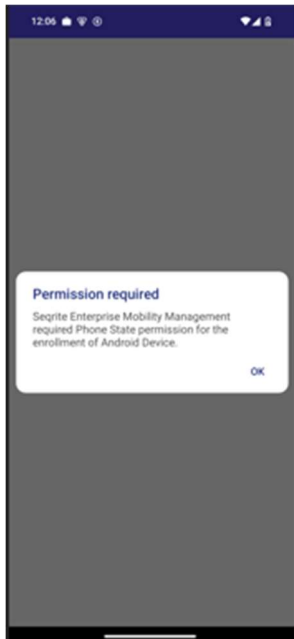
7. Tap **Allow** to allow Seqrite EMM to manage phone calls.
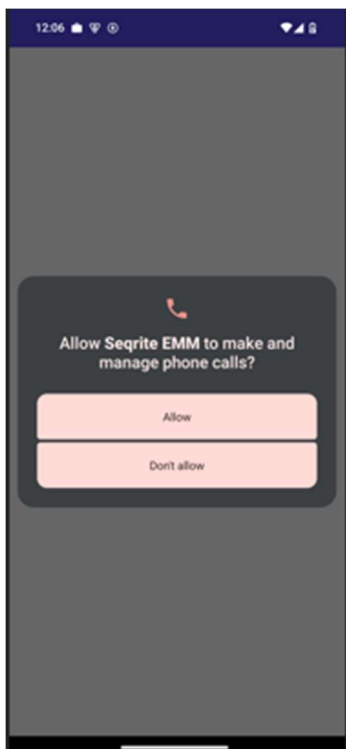
8. On the Enrollment Details screen, tap **Scan QR Code**.
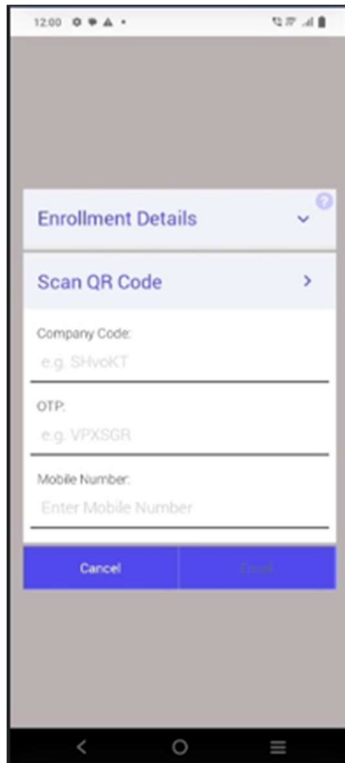
9. Scan the **second** QR code displayed on the Seqrite EMM console.
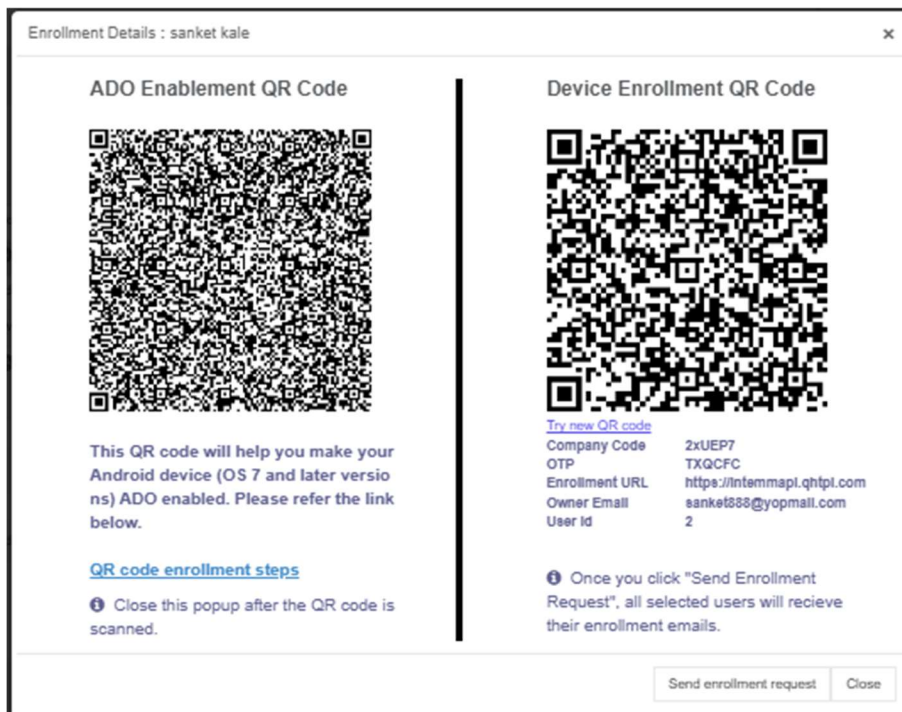
10. Tap **Allow** to allow Seqrite EMM to take pictures and record video. You are redirected to Device Enrollment screen.
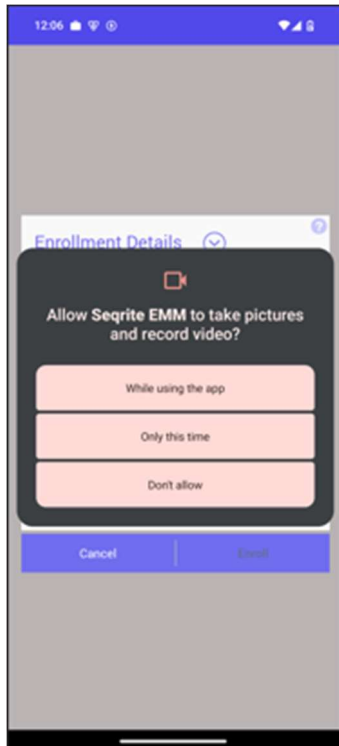
11. Tap **Proceed** to grant Android runtime permission.
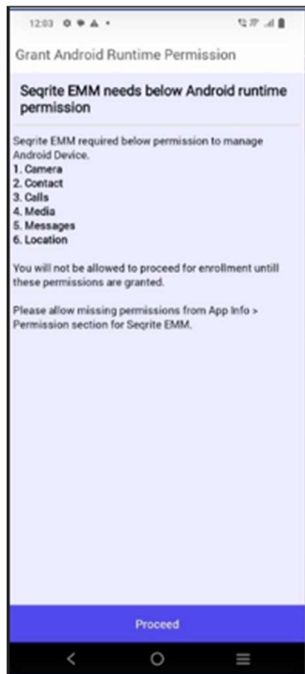
12. To allow Seqrite EMM to send message, and access your phone call logs, tap **Allow.**
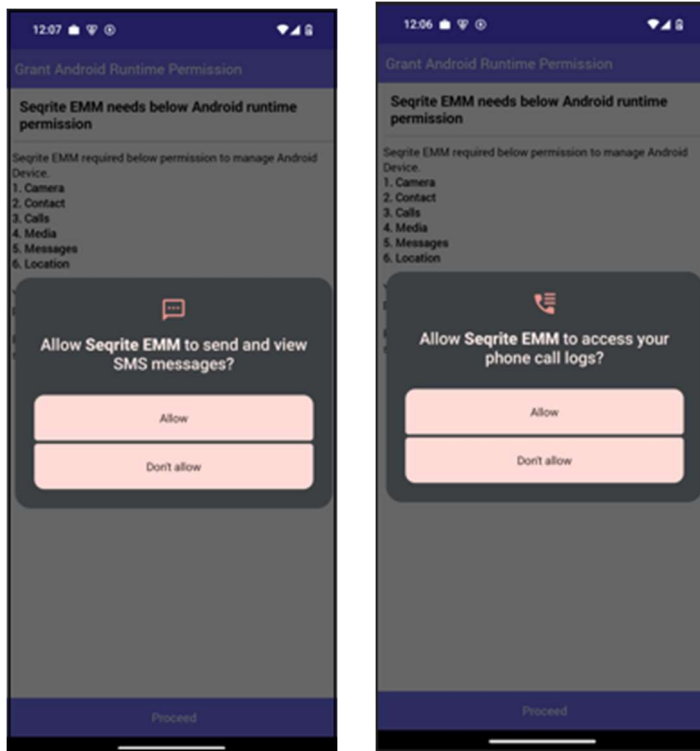
13. Enable the toggle on modify system settings screen.
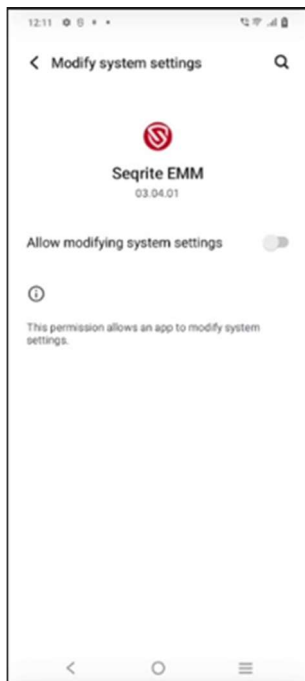
14. Tap back and select Seqrite EMM on **Apps with usage access** screen.
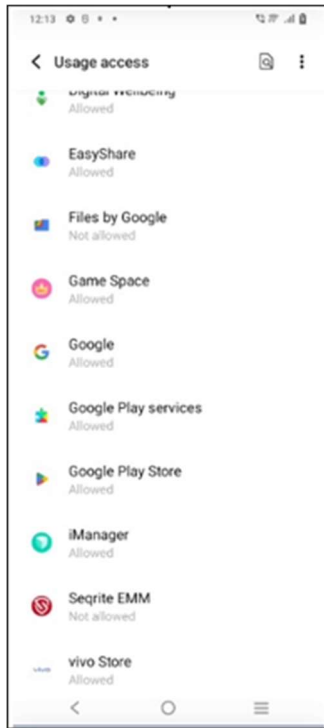
15. Enable the toggle to Permit usage access.
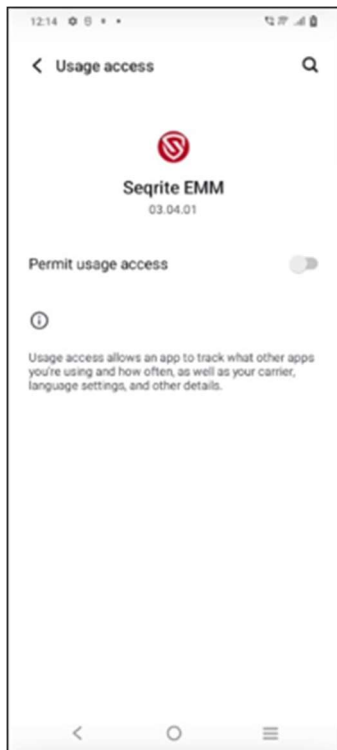
16. Enable the toggles for Seqrite EMM and Seqrite WakeUp App on the Autostart screen. Seqrite Enterprise Mobility Management app is enrolled.
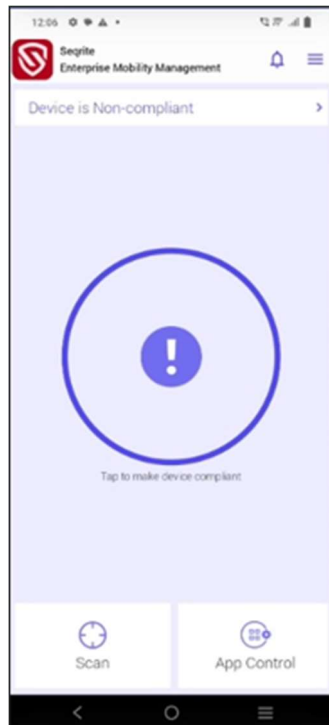
ADO Enrollment using ADB

Activating Device Owner Mode

Android Debug Bridge (adb) is a command line tool that allows communication between a computer and a connected Android device. This method is recommended for Device Owner provisioning only when the device cannot be provisioned using Scan QR Code for ADO.

This method uses Android Debug Bridge (or ADB) to provision devices as Device Owner and is applicable for Android devices 5.0 or later versions.

Prerequisites

- Ensure you do not have any Google account setup on your device.
- Android Debug Bridge (ADB) binary must be downloaded and installed on your computer.
- When trying to open the ADB zip file, if the platform tool folder is not visible, then use the Windows explorer to open the zip folder.
- When installing ADB, its environment variable path should be defined on the same computer where the ADB is to be configured and device owner is to be enabled.
- The Device Owner enrollment is applicable only to the devices that have Android devices 5.0 or later versions.

Activating Device Owner Mode using ADB

Step 1

Download and install the latest Seqrite EMM application on your Android device.
URL:https://dlupdate.quickheal.com/seqrite_msuite/mdmprod/builds/cloud/mSuite_Agent.apk

Short URL: https://www.seqrite.com/app-store/

For downloading and installing steps, see Installing Seqrite Enterprise Mobility Management on device.

Step 2

Download and install the Android Debug Bridge (ADB) binary on your computer.
Windows: https://dl.google.com/android/repository/platform-tools-latest-windows.zip
Mac: https://dl.google.com/android/repository/platform-tools-latest-darwin.zip
Linux: https://dl.google.com/android/repository/platform-tools-latest-linux.zip

Step 3

You can use either of the steps to access the command window to run commands.

- After the ADB Zip file is downloaded, extract the files to your PC drive.
- Copy the directory path of the file up to adb.exe file in the platform-tools folder.
- On your computer, right-click **MyPC/MyComputers > click Properties > Advance System settings**.
- In System Properties dialog, click Environment Variables.
- In System Variables section, click **Path > Edit** > add the selected path in the path section.
- Enter adb in command prompt. If "adb" command is not recognized, try restarting your computer or try installing the drivers for the specific devices.

Step 4

Go through the setup wizard WITHOUT adding a Google account. If you accidently added an account, simply remove the account from the Settings app once you finish the setup wizard.
Connect your device to the computer with USB (it is considered that the device USB drivers are already installed on your computer).
Your device might prompt you with a trust dialog. Click **Accept**.

To enable the Developer option on your device:

1. Go to **Device > in device Setting**, enable USB debugging option from Developer option. Make sure the Device setting has the Developer option.
2. Go to **About device** (Steps may differ by models), and to turn on the Developer option, click the Build number field 7 times.
3. Go back to **Settings > Developer > enable USB debugging.**
4. Plug the device to the computer. Your device may prompt you with a trust dialog. Click Accept.
5. Further the device asks for the trusted connection, select the Always allow from this computer check box.

Step 5

On your computer, open the command prompt and run the following command to initialize ADB:

Command

c: UsersUser>adb devices

Result

List of devices attached

3100875ea5ec6300 device

Note: Every device will have a unique device name.

After this command, the connected devices would be displayed on your command prompt window.

If it is a new device, go through the setup wizard without adding a Google account.

If it is an old device, then remove the Google account or any other account from your devices Settings.

Step 6

Run the following command to set the Seqrite Enterprise Mobility Management app as the device owner of the device:

Command

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

Result

Device owner set to package com.seqrite.client

Active admin set to component

{com.seqrite.client/com.seqrite.client.components.receivers.MainDeviceAdminReceiver}

- This result shows that the ADO enablement is successfully completed.
- Repeat the above-mentioned steps for all the devices.
- After Seqrite Enterprise Mobility Management is setup as the device owner, the device enrollment screen is displayed and with successful enrollment, the user will be able to access the Seqrite Enterprise Mobility Management app dashboard.

Troubleshooting

Google or any account is present on the device.

The following screen is displayed when the device has the User account or Google account, or any other account configured on it. Even after removing the accounts, if you are still getting the same error, then try performing a Factory Reset of the device.

Seqrite Enterprise Mobility Management client is already a device owner.

The following screen is displayed when the Seqrite Enterprise Mobility Management client application is already provisioned as a Device Owner.

Device name not listed at the time of installation.

If your device is not getting listed when you enter the adb devices command in command prompt, then try to install the specific drivers for that device.

Device ownership is assigned to a third-party application.

If the issue persists, then the device may have been already provisioned as device owner by the OEM provider (manufacturer) and hence the device cannot be provisioned again with Seqrite Enterprise Mobility Management client. In this case, you can enroll the Seqrite Enterprise Mobility Management client with regular enrollment process by enabling Device Administrator.

Android Enterprise Enrollment

You can enroll company owned devices using this enrollment type where the device will be managed by Google API.

Prerequisites
- Wi-Fi connection is a must for enrollment.
- Devices having Android versions 7 and above can only be enrolled using AMA.
- These devices should not be enrolled previously on Seqrite Enterprise Mobility Management.
- You can enroll the device to the Seqrite Enterprise Mobility Management console through either of Users, Groups, or Devices options.
- Once the device is added to the Seqrite Enterprise Mobility Management console, configure the required policies and app configurations to the device

    Note:
    Before getting devices enrolled, ensure that

    o **Android Kiosk Mode** is not selected in Android app management.
    o Setting for **Disable Apps Installation** is not set to enabled.
    o The enrollment process may take time depending upon the speed of the network connection.

To prepare the mobile device for AMA enrollment, you need to follow these steps:
1. Perform a factory reset of your phone
2. Android Enterprise Enrollment of a device using QR code
3. Setting Device admin and system permissions

Performing a factory reset on your phone
You can either use a new device or you need to perform a factory reset on your device. When you perform a factory reset, all the data on the device is permanently deleted. Ensure that you take a backup of your data.
1. On the device, tap Settings > System > Reset. Please note that the terminology in your device may differ.
2. Tap Reset Phone.
A Welcome screen is displayed after a factory reset of the device.
Next, you need to do Android Enterprise enrollment of your device using a QR Code.

Android Enterprise Enrollment of a device using QR code

The admin or the end user can enroll the device.

- If you (admin) are enrolling the device, you can use the QR code displayed on the Seqrite Enterprise Mobility Management console during enrollment.
- If the device user is performing the enrollment, the user can use the QR code that is sent to the email address.

1. On the Welcome screen, tap 6/7 times below the word Welcome. Devices may show "Welcome", "Hi" or "Hello" as per the device models. Based on the device model, scenarios either **A** or **B** or **C** will follow. Follow the steps as applicable.

A: QR Code scanner is displayed	B: QR Code scanner is not displayed	C: QR Code scanner is not displayed (Applicable to some devices only
i. Scan the QR code displayed on the Seqrite Enterprise Mobility Management console. Alternatively, the end user performing the enrollment process can scan the QR code received on the email address specified earlier. ii. Next, choose the appropriate option to connect to the Internet. You are redirected to **This device belongs to your organization screen**. iii. Tap **Next**. You are redirected to **Let's set up your work device** screen.	i. Tap **START** on the Welcome screen > **Connect to mobile network** screen is displayed. ii. Insert SIM card > **Connect to Wi-Fi** screen. iii. Select the Wi-Fi network from the list. Tap **Accept & Continue** on the **Privacy and software updates** screen. iv. On **Copy apps and data** screen, tap **Next**. The **Google Sign in** screen is displayed. v. Enter the email address as **afw#setup** and tap **Next**. vi. On **This device belongs to your organization** screen, tap **Next**. The QR code scanner is displayed. vii. Scan the QR code displayed on the Seqrite Enterprise Mobility Management console or scan the QR code received on your email address. You are redirected to **Let's set up your work device** screen.	i. Connect to the Internet and the *QR code scanner* is automatically downloaded on the device. ii. Scan the QR code displayed on the Seqrite Enterprise Mobility Management console or scan the QR code received on your email address. iii. You are redirected to **Let's set up your work device** screen.

2. Tap **Accept** & **continue** on the Let's set up your work device screen.
   You are redirected to **This device isn't private** screen.
3. Tap **Next**.
   You are redirected to **Updating device** screen and after that to the **Registering**

device screen.

Note: This process may take some time as apps are updated to the latest version from the factory version.

4. Next, depending on the password and app configurations policy configured by default, follow the steps as applicable.

- If the default password and app configuration policies are configured, follow these steps:

  i. You are redirected to the screens for setting the password and installing the apps. Follow the instructions for setting up the screen lock as required.
  Tap **Install** for installing Seqrite Enterprise Mobility Management and the recommended apps that are configured through the default app configuration.

     Note: Installation of apps may take time depending upon the network connection.
  ii. You are redirected to the **Google services** screen. Proceed to step 5 and further.

- If the default password and app configuration policies are not configured, you are redirected to the Updates Privacy and Software screen.

  i. Tap Accept & continue.
  ii. On the Google services screen, tap Accept.

5. You are all set/Your device is ready to go! screen is displayed.
6. Tap Done. Seqrite Enterprise Mobility Management app is now installed on the device.

   Note: At this point, on the Device Details page, the device Enrollment Status is shown as **AMA Enrolled** as the procedure is partially completed. Next, you need to set the System permissions after which the enrollment process is completed.

Setting System permissions
You need to complete the further steps after which the device Enrollment Status is displayed as **Enrolled** on the Device Details page.
1. On your device, tap the **Seqrite Enterprise Mobility Management** app. You are redirected to the **License Agreement** screen.
2. Tap **I Agree**.You are redirected to the **Seqrite Enterprise Mobility Management Permissions** screen.
3. Tap **Continue**.
   You are redirected to the **All File Access** dialog box.

4. Tap **I ACCEPT** .
   You are redirected to the **All files access** screen.
5. Enable the toggle button **Allow access to manage all files** and tap the **Back** icon.
6. Tap **I ACCEPT** on **Accessibility Settings** dialog box.
   You are redirected to **Seqrite Enterprise Mobility Management** screen.
7. Enable the toggle buttons **Use Seqrite Enterprise Mobility Management** and **Seqrite Enterprise Mobility Management shortcut** and tap the Back icon.
8. Tap **I ACCEPT** on Device Location dialog box.
   You are redirected to App info screen.
9. Tap **Permissions** and select Location permission.
10. On the Location permission screen select the permission as required. Enable the toggle button to **Use precise location** and tap Back icon.
11. Tap **Yes** on the Phone dialog box.
    You are redirected to **Seqrite Enterprise Mobility Management Permissions** screen.
12. A green tick mark indicates that the permissions are granted by the user. A red exclamation mark indicates that the permissions are not granted by the user.
13. Tap **Continue**.
    Device Enrollment proceeds to enroll the device.
14. The device user should grant Seqrite Enterprise Mobility Management device access permissions by enabling the toggle buttons for the following or choose to grant permissions later:

- Do Not Disturb
- Modify System Setting
- Overlay
- App Usage Access
- Autostart
  A green tick mark indicates that the permissions are granted by the user. A red exclamation mark indicates that the permissions are not granted by the user.

15. A prompt appears asking confirmation to allow Seqrite Enterprise Mobility Management to run in the background.
16. Tap **Yes**.
    A prompt appears requesting permission for app to always run in the background.
17. Tap **ALLOW.**
    The device is enrolled. You can view the Enrollment Status on the Device Details page on Seqrite Enterprise Mobility Management console displayed as **Enrolled**.

Enrollment of Work Profile for Personal Device

You can enroll personal devices (Bring Your Own Device) using this enrollment type and ensure that both the corporate data are secure while keeping the personal information private.

Prerequisites
- Set one Gmail account on EMM console
- Internet connection on device
- Seqrite EMM Workspace License and login credentials
- Supported Android devices version 7 and above

Setting up Enterprise Account Enrollment
First, you need to get a Google Account, and a Seqrite EMM Workspace License. Next you need to set up your Enterprise account in Seqrite EMM.
Refer to the following link for steps to setup your company Enterprise Account on Seqrite EMM:

Set Up Enterprise Account in Seqrite EMM

Seqrite Workspace (Work Profile)
Seqrite Workspace allows organizations to create a virtual container on an employee-owned device to manage and protect corporate data without compromising user privacy. This virtual container ensures isolation of the company data and resources even though used on the end user's device. The Seqrite EMM administrator can limit the apps that the employee can install and use in the corporate Workspace profile. The administrator can add/move/import the users to the desired group and apply the associated policies.

Note: Workspace enrollment can be done only through the **Users** tab.

Enrollment of device using Email address
1. Log on to Seqrite EMM with your credentials.
2. Navigate to **Users**, select user.
   Note: Users can be imported through Seqrite CSM and synced to Seqrite EMM portal.
3. In **Take Action** drop-down select **Enrollment Request** > **For Android Devices** > **Work Profile for Personal device.**
4. Click **Submit**. An Enrollment email is sent to the email address.

5. On the device, open the received email and click on the Enrollment Link given in the mail. Setup of work Profile starts.
6. Tap **Next**.
7. Tap **Accept and Continue**.
8. Tap **Next.** The Updating device and Registering Profile process follows.
9. On the Work Check list screen, under Install Work Apps, tap **Install**.
   Seqrite Workspace app starts downloading.
10. Tap **Setup** under Seqrite Configure Workspace App to configure the app.
    The License Agreement screen is displayed.
11. Tap **I agree** to agree to the terms and conditions. The Enrollment process starts.

The **Seqrite Workspace permissions** screen is displayed.
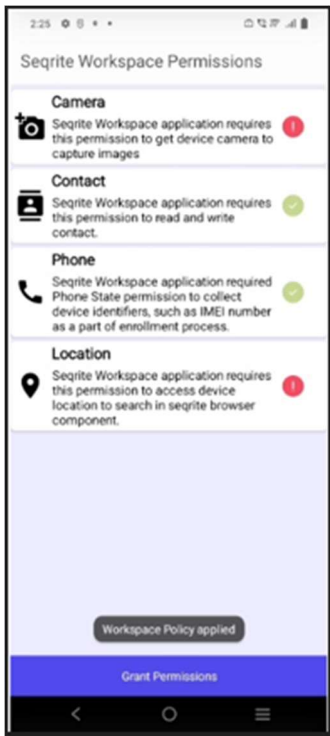
12. Tap **Grant Permissions** to grant the required permissions.
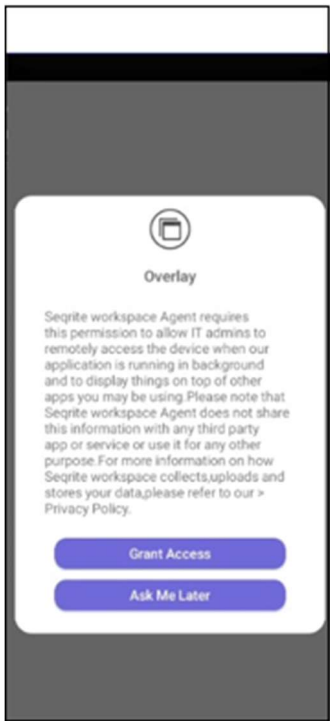
Grant the permissions as required.
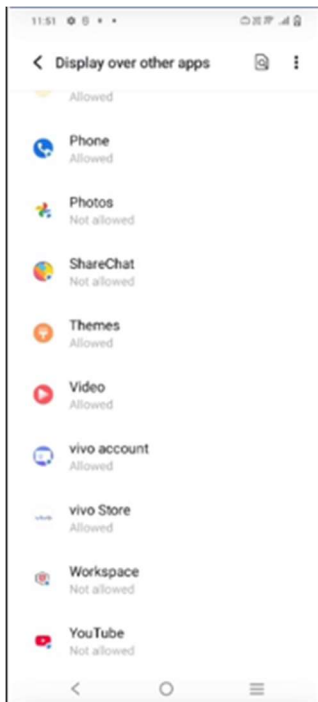
The Seqrite Workspace login prompt is displayed.

13. Enter password and confirm password.
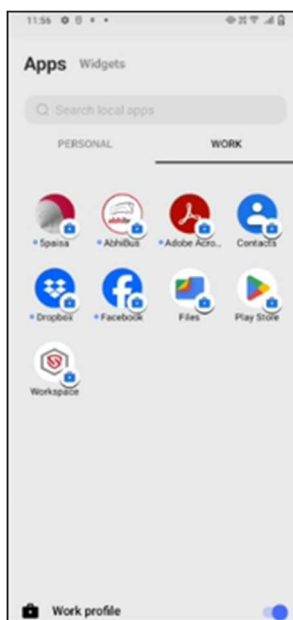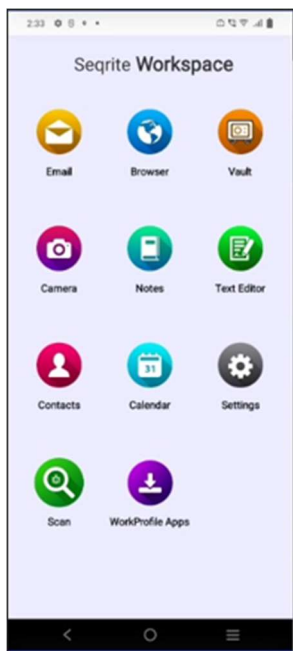
Seqrite Workspace is activated, and a Work profile is created on the device. The pre-configured applications are downloaded and displayed.

Note: The apps are installed on the User device automatically if the **Install Silently** option is enabled for the apps.

All the policies that are assigned to the group for that user will be applied to the enrolled device.

Enrollment of devices using QR code

1. Log on to Seqrite EMM with your credentials.
2. Navigate to **Users**, select user.

   Note: Users can be imported through Seqrite CSM and synced to Seqrite EMM portal.

3. In Take Action drop-down select **Enrollment Request > For Android Work Profile > Using QR Code**.
4. Click **Submit**.
   The QR Code is displayed on the console.
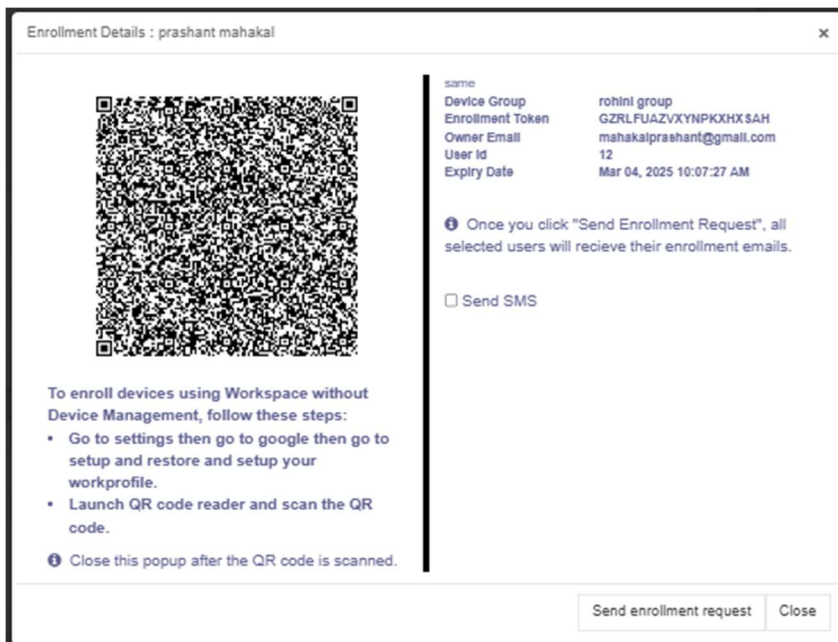
5. On the device, go to the **Settings > Google Accounts > Setup a Device > All Services > Setup and Restore > Setup your Work Profile**.

Tap **Setup & Restore** and then tap **Setup your work Profile**.
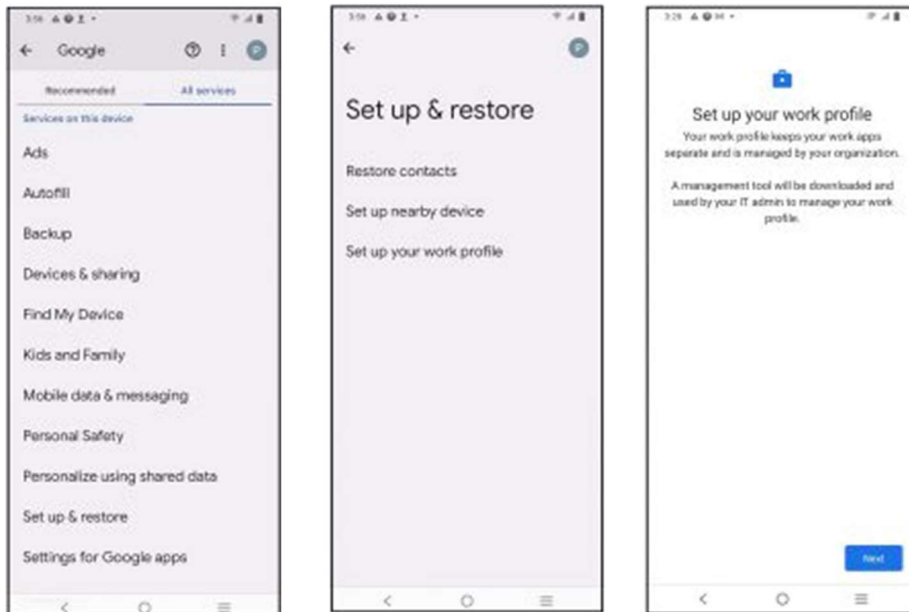
6. Tap **Next**. The enrollment process starts with downloading the required files.
   Grant permission as required. On the Enroll this device screen, tap the camera icon.
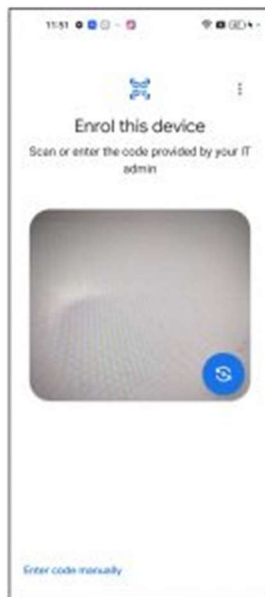
7. Scan the QR code generated on the Seqrite EMM console earlier.
8. Tap **Accept and Continue** on the device. Your work profile is being setup.

9. Tap **Next**.

10. On the Work Check list screen, under Install Work Apps, tap **Install**.
    Seqrite Workspace app starts downloading.
11. Tap **Done**. The Seqrite Configure Workspace App option is displayed.
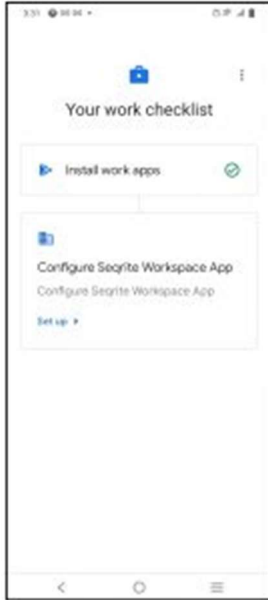
12. Tap **Setup** under Seqrite Configure Workspace App to configure the app. The License Agreement screen is displayed.

13. Tap **I agree** to agree to the terms and conditions. The Enrollment process starts.

The Seqrite Workspace permissions screen is displayed.
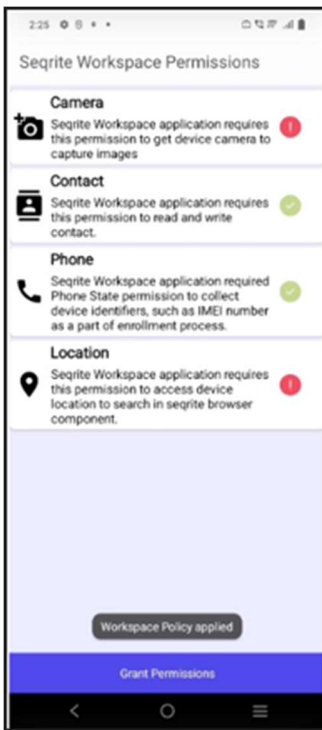
14. Tap **Grant Permissions** to grant the required permissions.
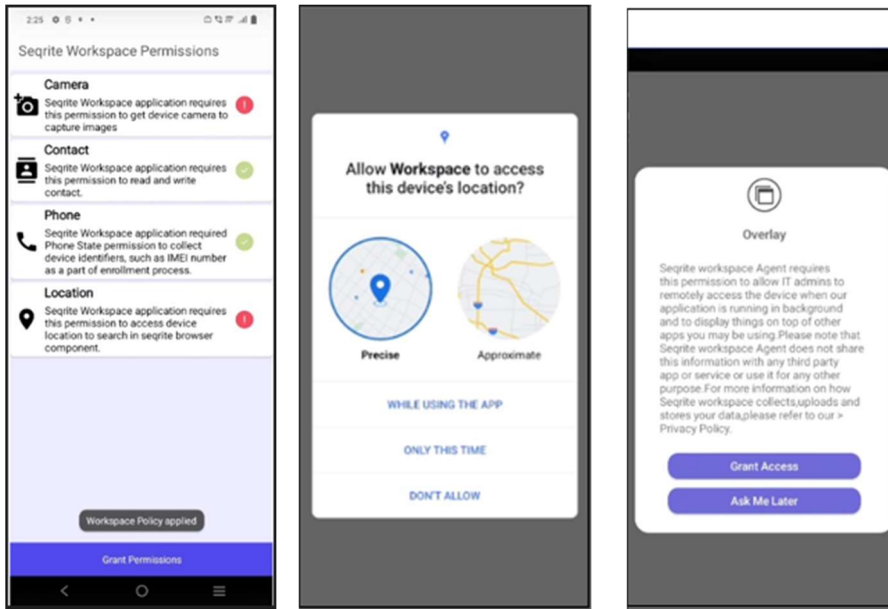
15. Grant the permissions as required.
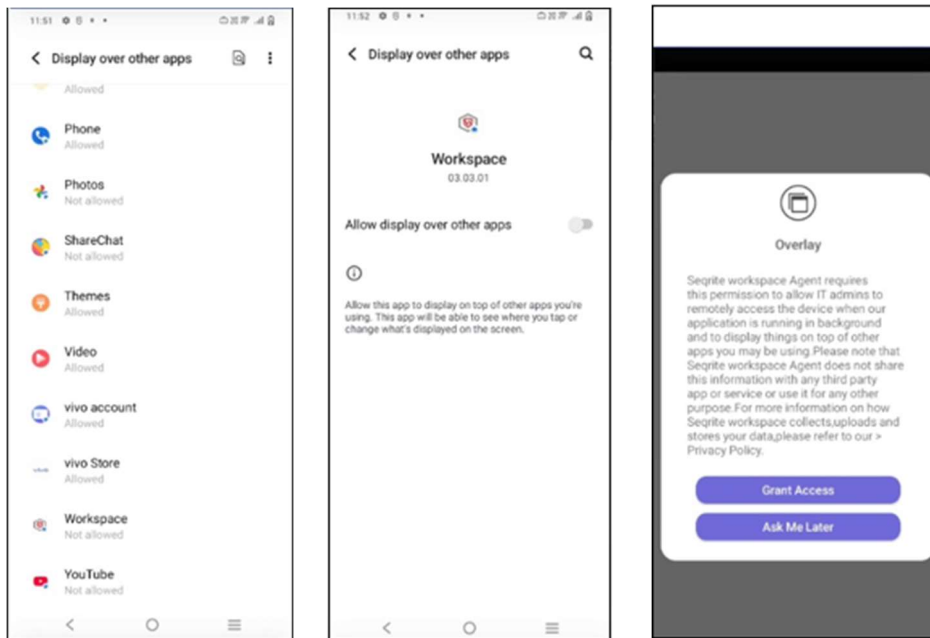
The Seqrite Workspace Login prompt is displayed.

16. Enter password and confirm password.
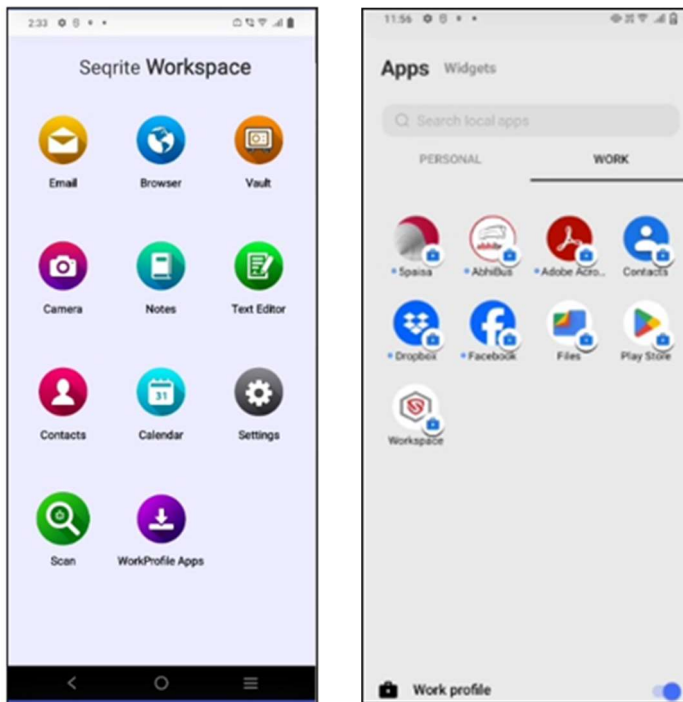
Seqrite Workspace is activated, and a Work profile is created on the device. The pre-configured applications are downloaded and displayed.

Note: The apps are installed on the User device automatically if the Install Silently option is enabled for the user.

All the policies that are assigned to the group for that user will be applied to the enrolled device.

Enrollment of Work Profile for Corporate Device

You can enroll company owned devices using this enrollment type and control or manage the corporate data by configuring and applying policies.

Prerequisites
- Wi-Fi connection is a must for enrollment
- Devices having Android versions 11 and above can only be enrolled using COPEs
- IMEI number of devices should not be enrolled previously on Seqrite EMM
- You can add the device to the Seqrite EMM console through User.
- Once the device is added to the Seqrite EMM console, configure the required policies and Work Profile to the device.

Note: The enrollment process may take time depending upon the speed of the network connection.

To prepare the mobile device for COPE enrollment, you need to follow these steps:
1. Performing a factory reset on your phone
2. Enrollment of Work Profile for Corporate device using QR code
3. Setting up system permissions

Performing a factory reset on your phone

You can either use a new device or you need to perform a factory reset on your device. When you perform a factory reset, all the data on the device is permanently deleted. Ensure that you take a backup of your data.

1. On the device, tap Settings > System > Reset. Please note that the terminology in your device may differ.
2. Tap Reset Phone

After a factory reset of the device, a Welcome screen is displayed. Next, you need to do Work Profile for Corporate device enrollment of your device using a QR Code.

COPE Enrollment of a device using a QR code

Admin or the end user can enroll the device.
- If you (admin) are enrolling the device, you can use the QR code displayed on the Seqrite EMM console during enrollment.
- If the device user is performing enrollment, the user can use the QR code that is sent to the email address.

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

1. On the Welcome screen, tap 6 to 7 times below the word Hi. Devices may show "Welcome, Hi, or Hello" as per device models.
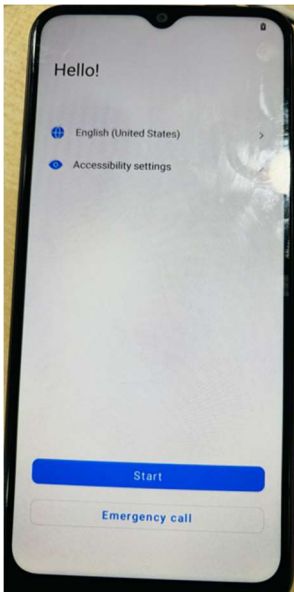
2. Scan the QR code displayed on the Seqrite EMM console. Alternatively, the end user performing the enrollment process can scan the QR code received on the email address as specified earlier.
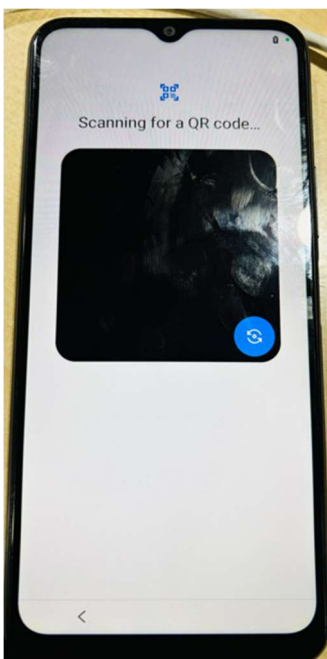
3. Choose the Wi-Fi connection and connect to the internet.
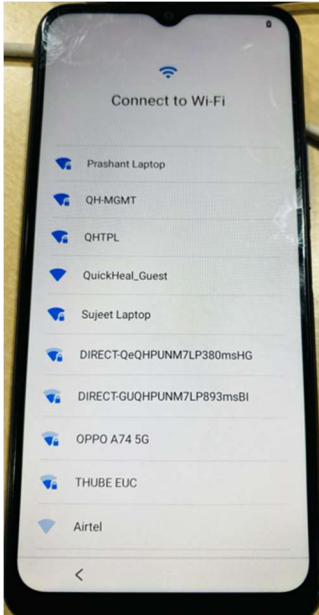
This device belongs to your organization screen is displayed.
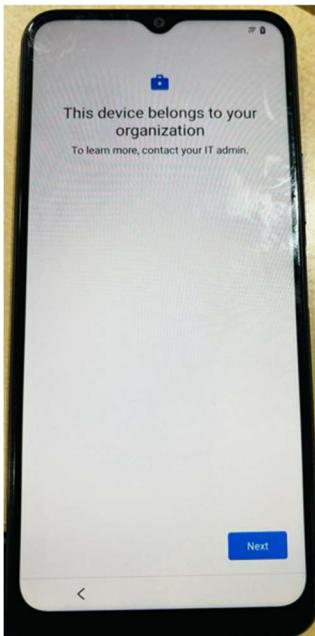
4. Tap **Next.**
   The **Let's setup your work profile** screen is displayed.
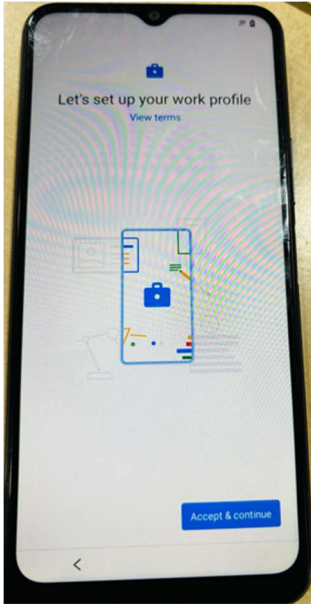
5. Tap **Accept & continue**.
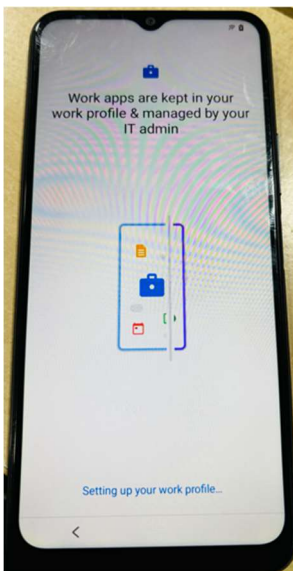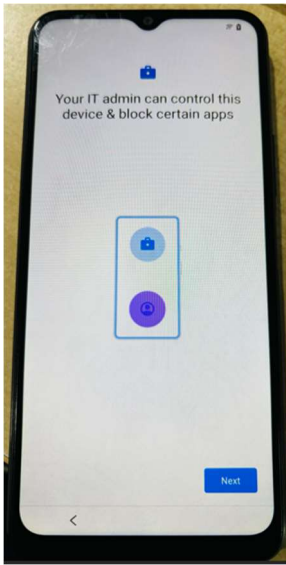
6. Tap **Next.**
    The **Updating device** Updating device and **Registering profile** screens are displayed.
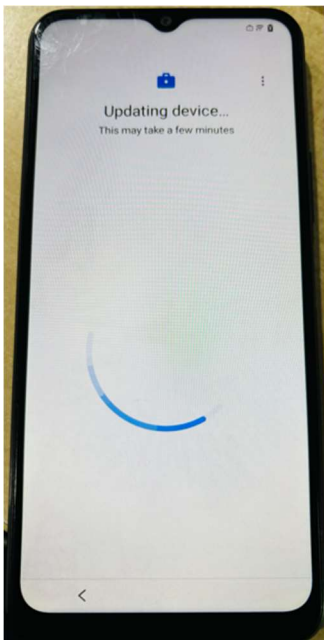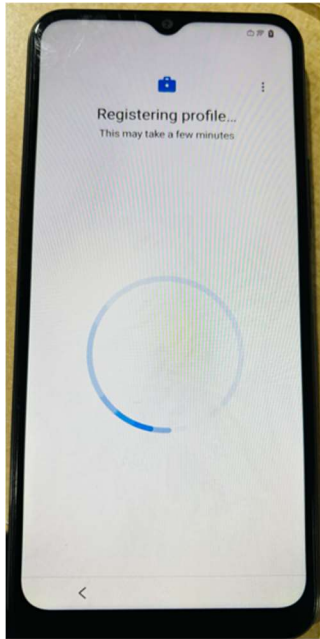
Note: This process may take some time as apps are updated to the latest version from the factory version.
Work profile is ready. You can add your personal Google account to access your app and content.
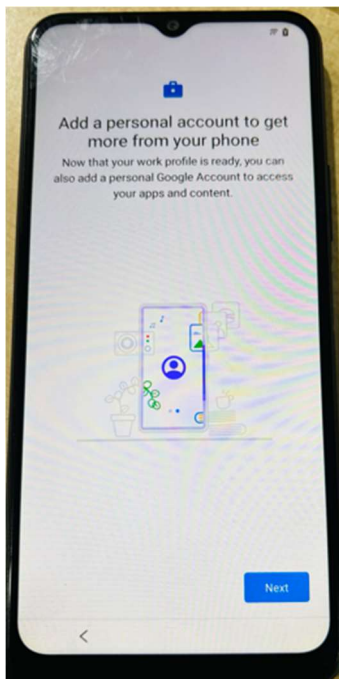
7. Tap **Next.**
8. Sign in with your personal account and tap **Next.**
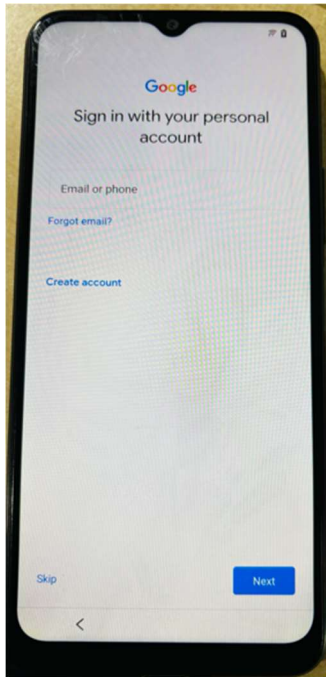
Google services screen is displayed.
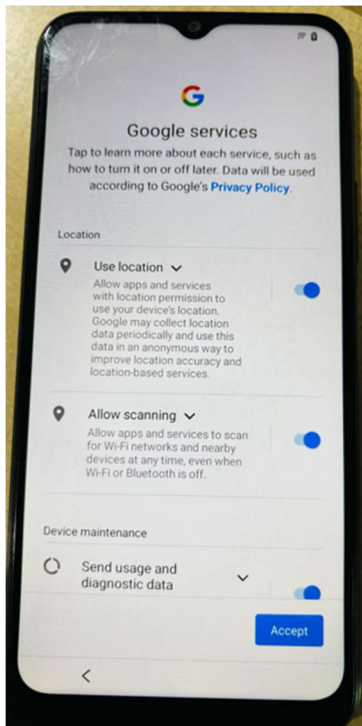
9. Tap **Accept.**
    The **Set up screen lock** screen is displayed.
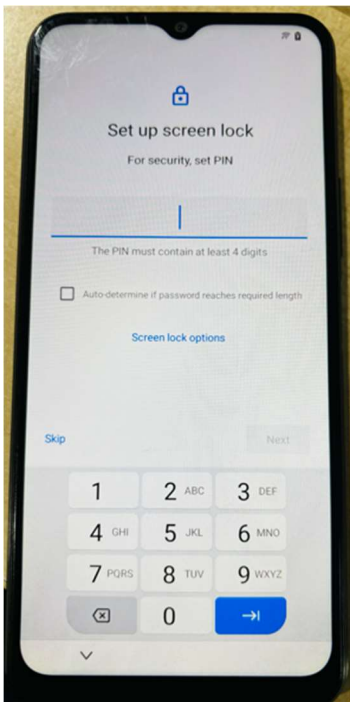
You can set up a security PIN or choose to skip this step.

10. Tap **Next**.
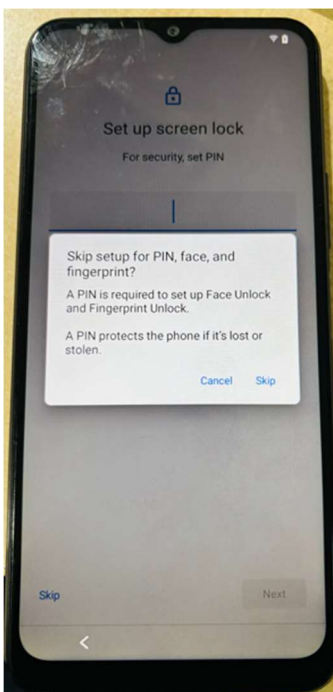
The **App widget** screen is displayed.
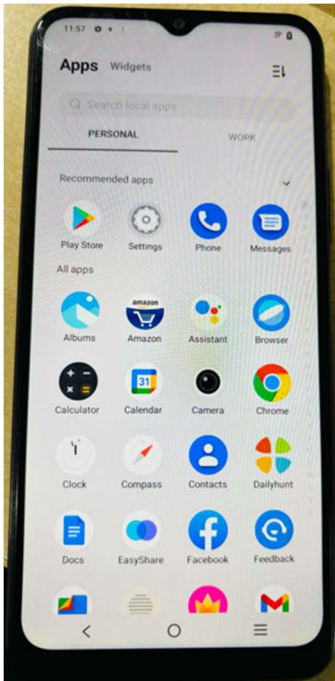
11. Tap the **WORK** container.
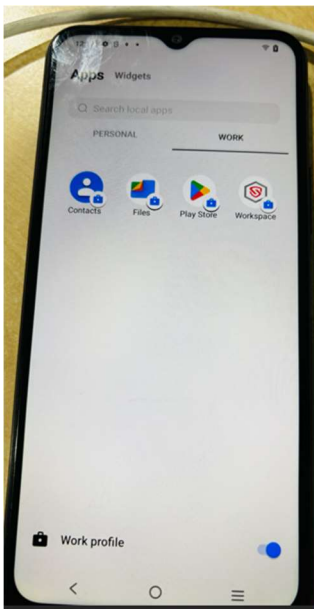
Setting up system permissions

You need to set up the system permissions to complete the device enrollment.

1. Tap **Workspace** under the **Work** container.
   The **License Agreement** screen is displayed.
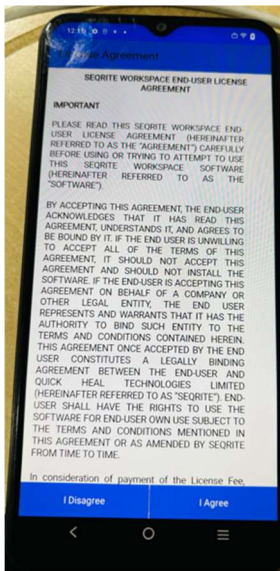
2. Tap **I Agree**.
   The **Seqrite Workspace Permissions** screen is displayed.
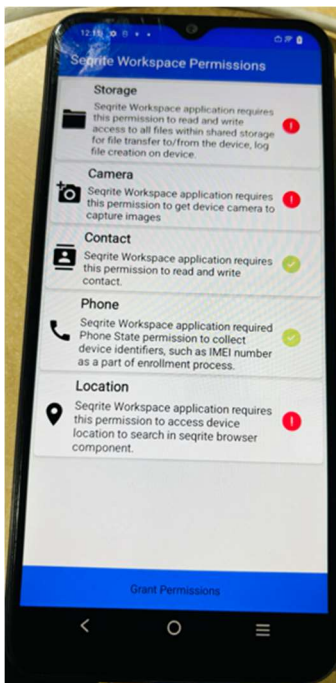
3. Tap **Grant Permissions** to grant the required permissions.
4. Tap **WHILE USING THE APP**.
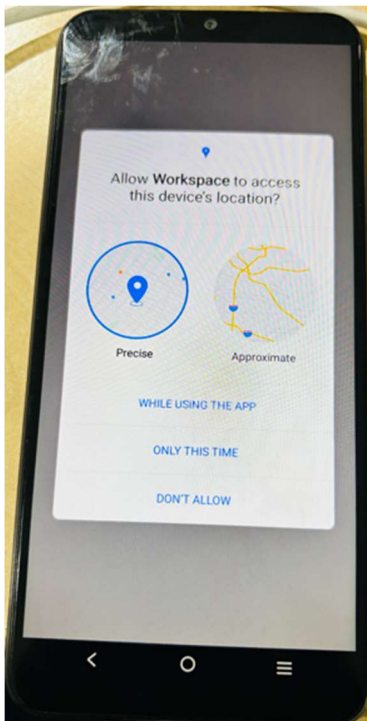
5. Tap **Grant Access**.
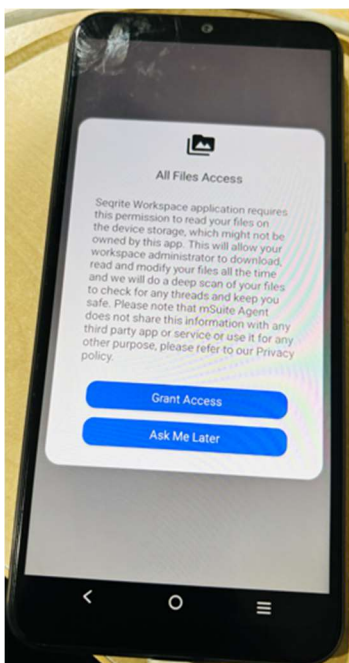
6. Turn on the **Allow access to manage all files** toggle key and then tap
   < (back).
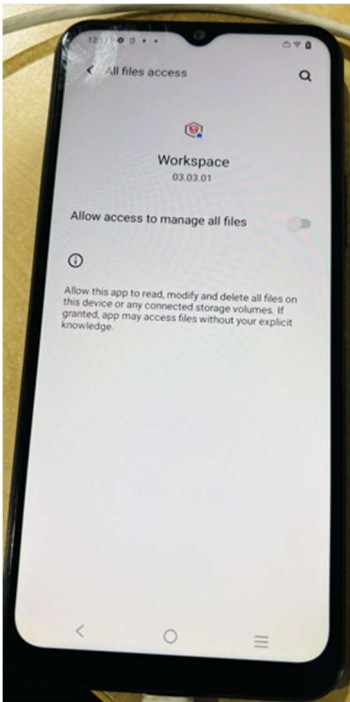
7. Tap **Grant Access**.
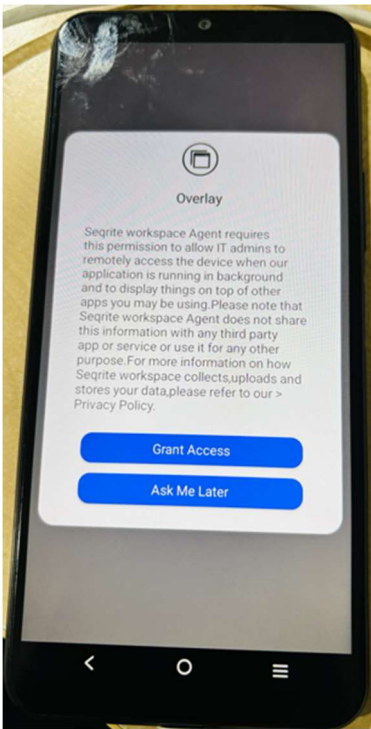
8. Turn on the Allow display over other apps toggle key and then tap **<** (back).
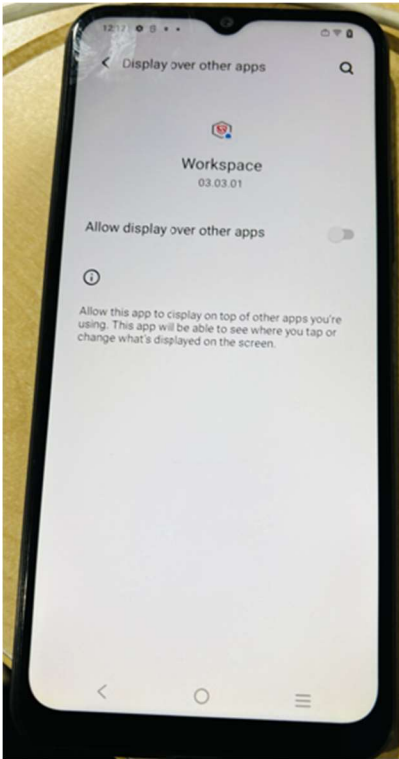
The **Seqrite Workspace** login screen is displayed.
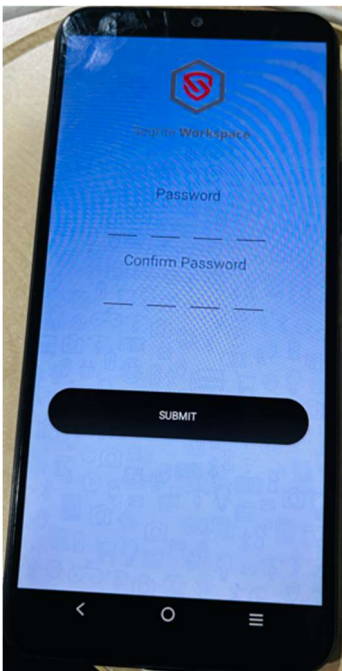
9. Enter password and re-enter password to confirm. Tap **Submit**.
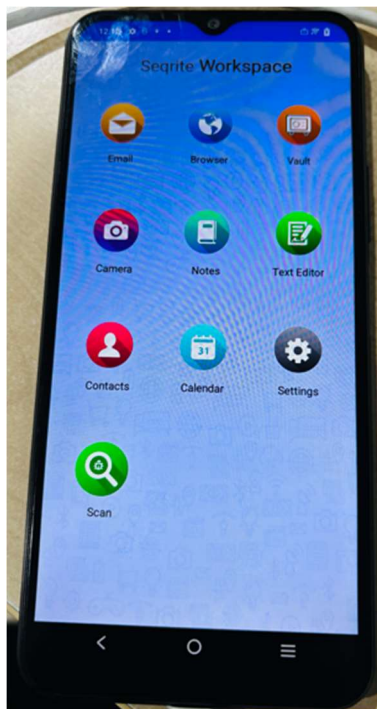
Seqrite Workspace is activated. The pre-configured applications are downloaded and displayed.
Note: The apps are installed on the user device automatically if the Install Silently option is enabled for the apps.

All the policies that are assigned to the group for that user will be applied to the enrolled device.

Enrollment for iOS

You can enroll your device in the following ways using Seqrite Enterprise Mobility Management for device management option:

1. Enrollment using QR Code, Email or SMS
2. Container Management for Personal Device
3. Device and Container Management

Enrollment using QR Code, Email or SMS

You can enroll both personal devices (Bring Your Own Device) and company owned devices using this enrollment type where device will be managed by applying policies.
In this process, the admin generates a QR Code on the Seqrite EMM console and scans the generated QR code on console through the Seqrite EMM app on the device. Alternatively, the generated QR code can be shared with the users for scanning through their devices.

To submit the request for enrollment on the Seqrite EMM console:
1. Navigate to the Users tab in the left pane and select the user from the list.
2. From the Take Action list, select **Enrollment Request** > **For iOS Devices** > **QR Code, Email or SMS** and click **Submit**.
A QR Code is generated and displayed on the Seqrite EMM console. You will need to scan this code while installing the Seqrite EMM app on the device.

Installing Seqrite Enterprise Mobility Management on iOS device

You must download and install the Seqrite EMM app on your device first before you can proceed with the enrollment process.

1. On your device, open the link in your browser, https://apps.apple.com/sa/app/seqrite-msuite/id1444868965
2. Download the Seqrite EMM app for iOS on your device.

3. Open the **Agent** app.
4. Tap **Agree** on the license agreement screen

Enrollment Details screen is displayed.

6. Tap **Scan QR Code** and scan the QR code displayed on the Seqrite EMM console or shared with user (as described earlier).
7. Tap **OK** to grant permission to Seqrite EMM to access the camera.
8. Tap **Allow** to download configuration profile on the device.
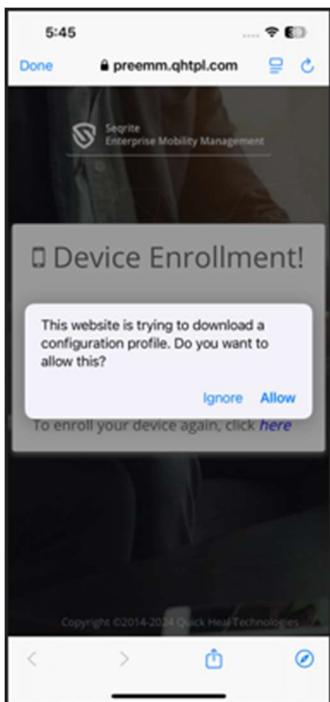
9. The profile is downloaded on your device.
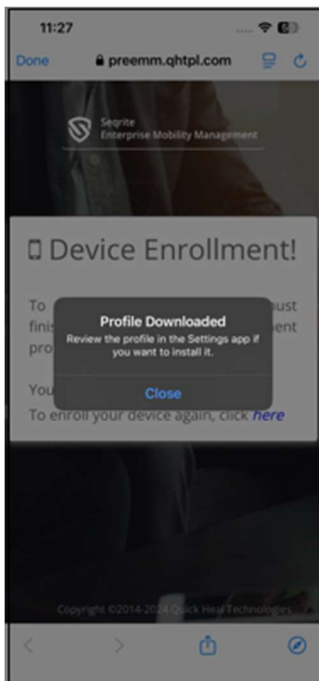
10. Go to **Settings General > VPN & Device Management**. Tap **Seqrite Enterprise Mobility Management Enrollment Profile**.
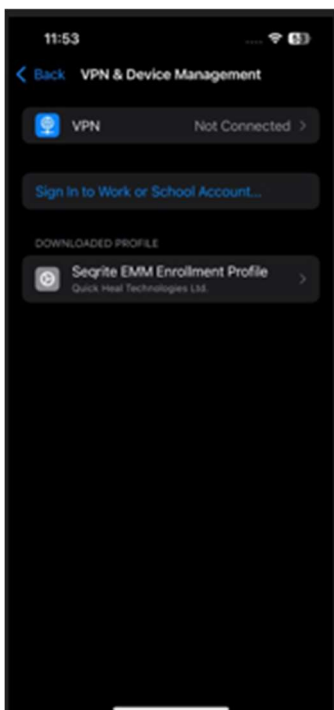
11. Tap **Seqrite EMM Enrollment Profile**.
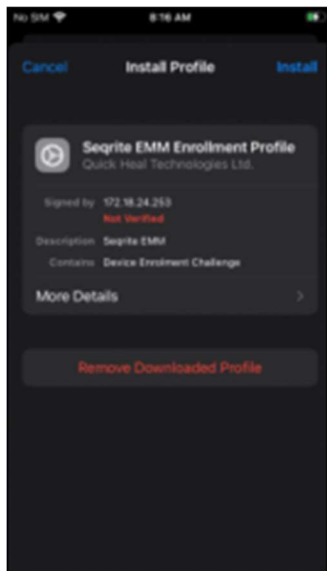
12. Tap **Install** to install the downloaded profile.
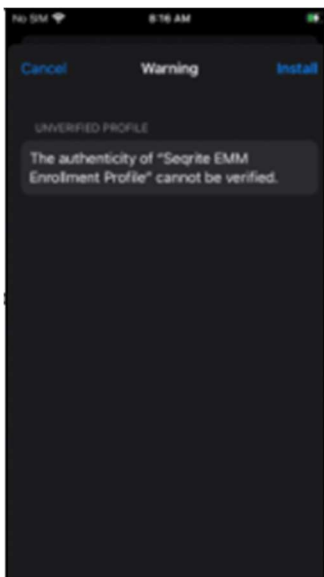
13. Tap **Install** again on the screen warning about the unverified profile. to download
    configuration profile on the device.
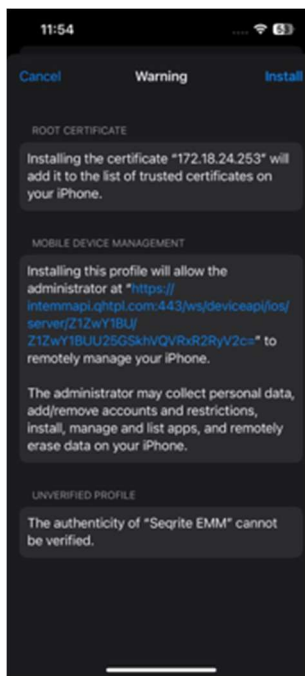
14. Tap **Install** again on the screen warning about the unverified profile.
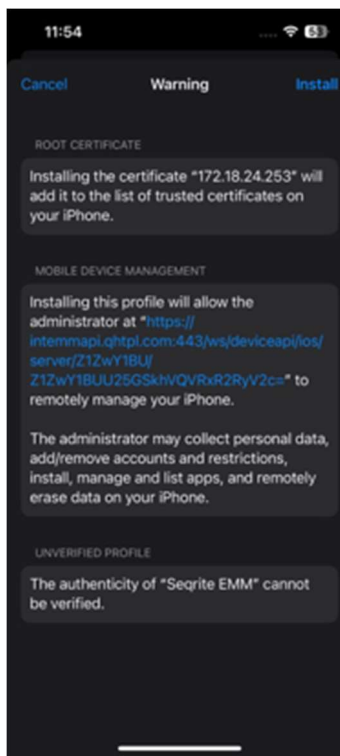
15. Tap **Trust** to enroll your device into remote management.
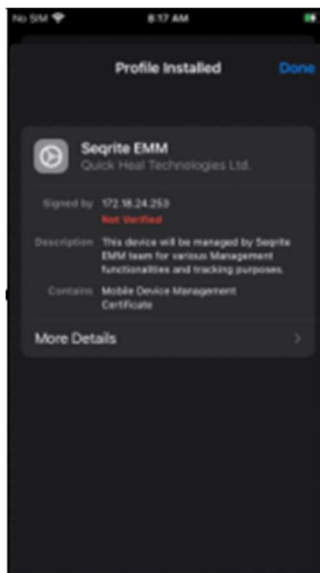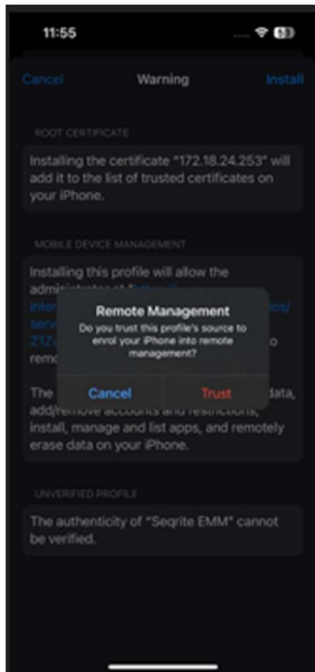
16. Tap **Done**.
17. Close the settings and open Agent App.
    Device enrollment screen will display.
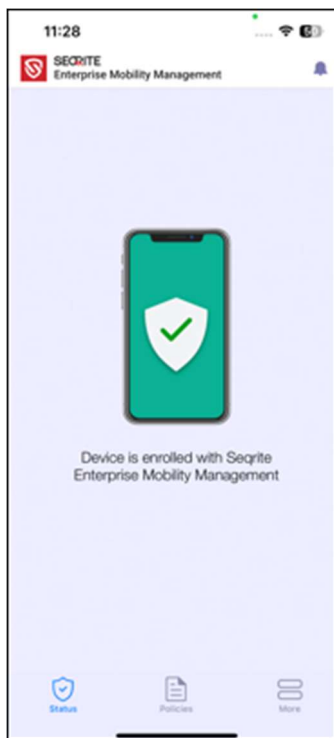
The device is enrolled with the Seqrite EMM console.

Container Management for Personal Device

You can enroll both company owned and personal devices where only corporate data will be managed by configuring and applying policy.

In this process, the admin generates a QR Code on the Seqrite EMM console and scans the generated QR code on console through the Seqrite EMM app on the device. Alternatively, the generated QR code can be shared with the users for scanning through their devices.

To submit the request for enrollment on the Seqrite EMM console:

1. Navigate to the Users tab in the left pane and select the user from the list.
2. From the Take Action list, select **Enrollment Request** > **For iOS Devices** > **Container Management for Personal Device** and click **Submit**.

A QR Code is generated and displayed on the Seqrite EMM console. You will need to scan this code while installing the Seqrite EMM app on the device.

Installing Seqrite Enterprise Mobility Management on iOS device

You must download and install the Seqrite EMM app on your device first before you can proceed with the enrollment process.

1. On your device, open the link in your browser, https://apps.apple.com/sa/app/seqrite-msuite/id1444868965
2. Download the Seqrite EMM app for iOS on your device.

3. Open the **Agent** app.
4. Tap **Agree** on the license agreement screen.

Enrollment Details screen is displayed.
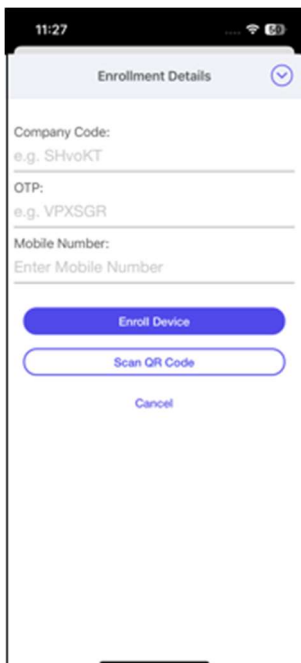
5. Tap **Scan QR Code** and scan the QR code displayed on the Seqrite EMM console or shared with user (as described earlier).
6. Tap **OK** to grant permission to Seqrite EMM to access the camera.
7. Tap **Allow** to download configuration profile on the device.
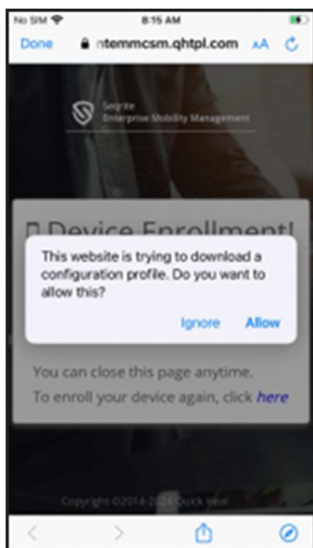
The profile is downloaded on your device.
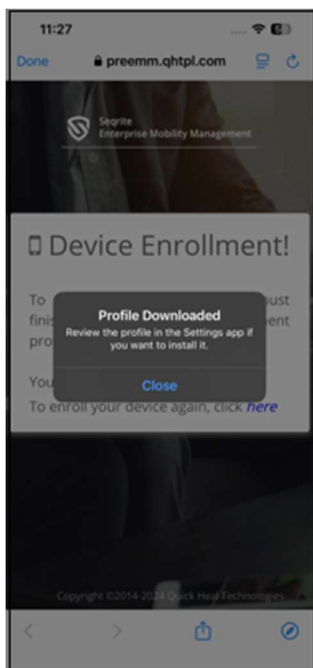
8. Go to **Settings General > VPN & Device Management**. Tap **Seqrite Enterprise Mobility Management Enrollment Profile**.
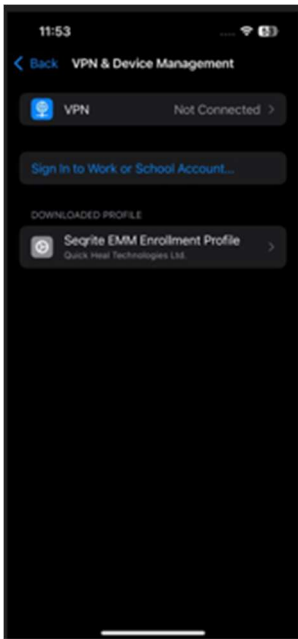
9. Tap **Seqrite EMM Enrollment Profile**.
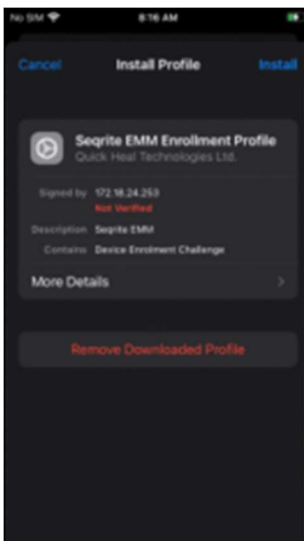
10. Tap **Install** to install the downloaded profile.
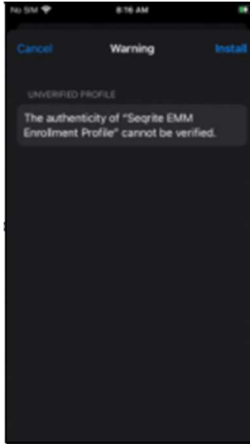
11. Tap **Install** again on the screen warning about the unverified profile. to download configuration profile on the device.
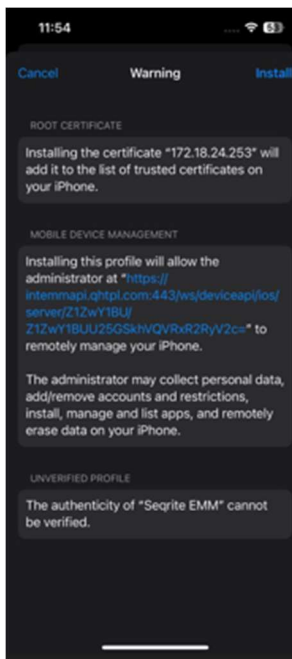
12. Tap **Install** again on the screen warning about the unverified profile.
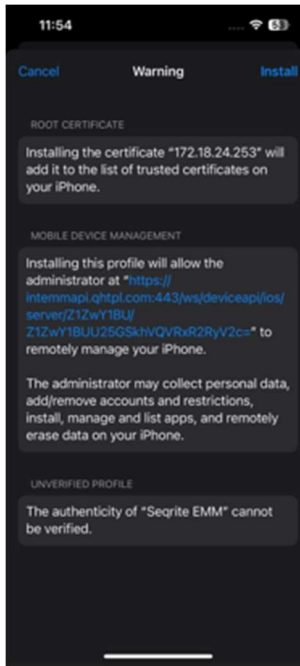
13. Tap **Trust** to enroll your device into remote management.
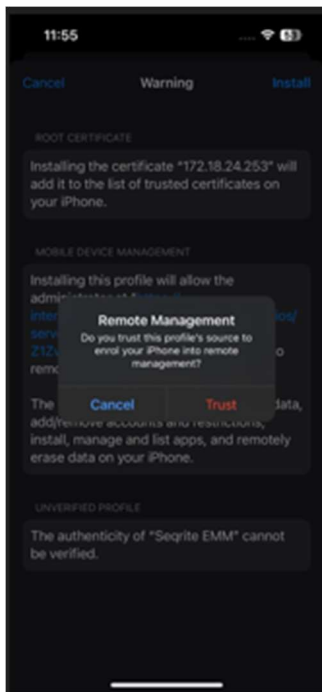
14. Tap **Done**.
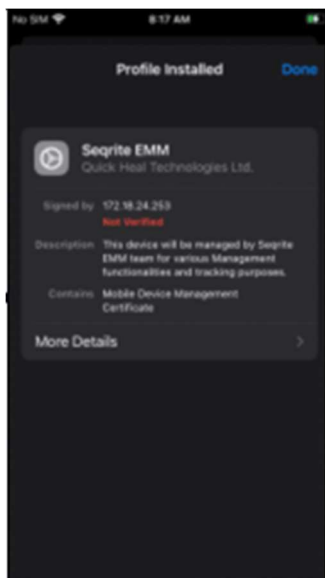
10. Close the settings and open Agent App.
    Seqrite workspace will be activated and ask you to set the PIN.
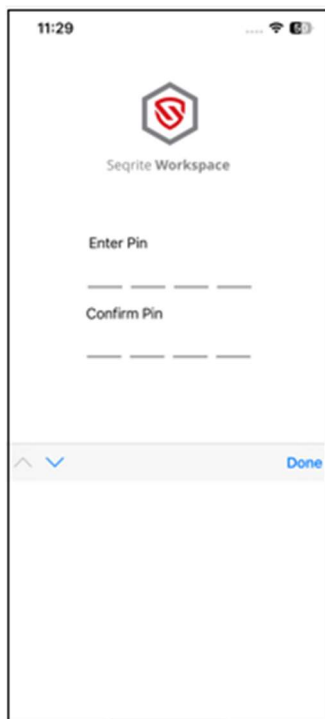
After setting PIN, device and container will be enrolled successfully.
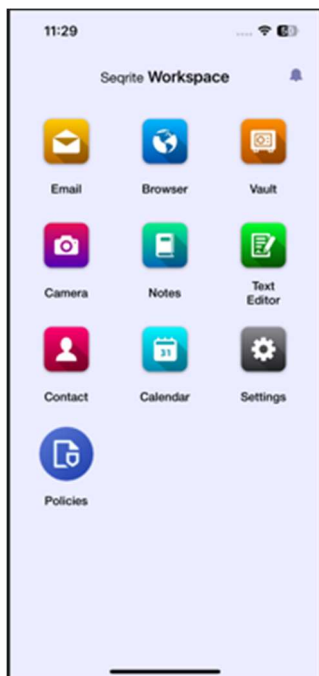
Device & Container Management

You can enroll both company owned and personal devices where both personal and corporate data will be managed by configuring and applying policy.
In this process, the admin generates a QR Code on the Seqrite EMM console and scans the generated QR code on console through the Seqrite EMM app on the device. Alternatively, the generated QR code can be shared with the users for scanning through their devices.

To submit the request for enrollment on the Seqrite EMM console:

1. Navigate to the Users tab in the left pane and select the user from the list.
2. From the Take Action list, select **Enrollment Request** > **For iOS Devices** > **Device & Container Management** and click **Submit**.

A QR Code is generated and displayed on the Seqrite EMM console. You will need to scan this code while installing the Seqrite EMM app on the device.

Installing Seqrite Enterprise Mobility Management on iOS device

You must download and install the Seqrite EMM app on your device first before you can proceed with the enrollment process.

1. On your device, open the link in your browser, https://apps.apple.com/sa/app/seqrite-msuite/id1444868965
2. Download the Seqrite EMM app for iOS on your device.

3. Open the **Agent** app.
4. Tap **Agree** on the license agreement screen.

Enrollment Details screen is displayed.
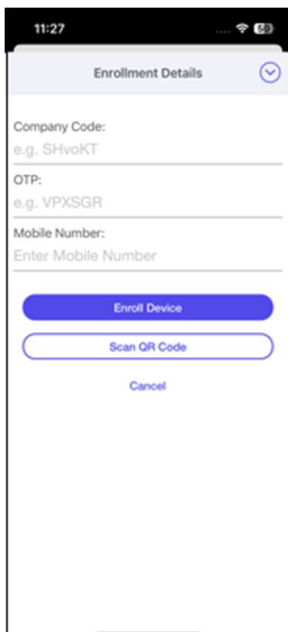
4. Tap **Scan QR Code** and scan the QR code displayed on the Seqrite EMM console or shared with user (as described earlier).
5. Tap **OK** to grant permission to Seqrite EMM to access the camera.
6. Tap **Allow** to download configuration profile on the device.
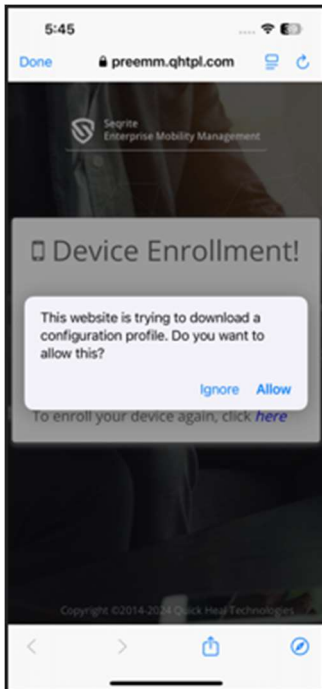
7. The profile is downloaded on your device.
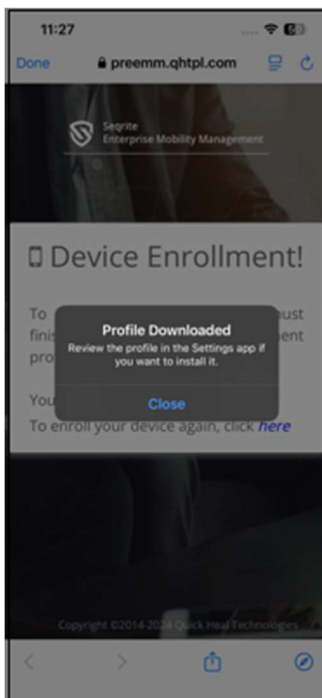
8. Go to **Settings General > VPN & Device Management**. Tap **Seqrite Enterprise Mobility Management Enrollment Profile**.
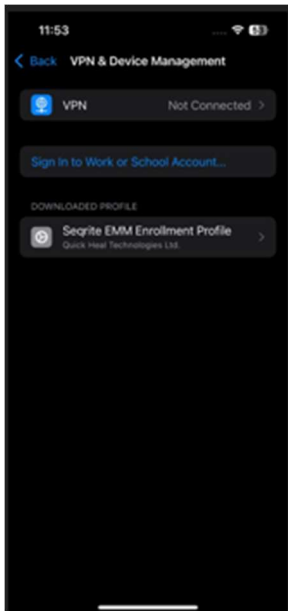
9. Tap **Seqrite EMM Enrollment Profile**.
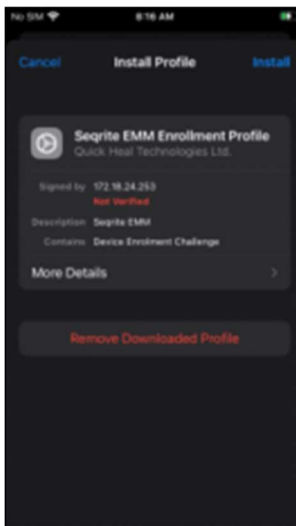
10. Tap **Install** to install the downloaded profile.
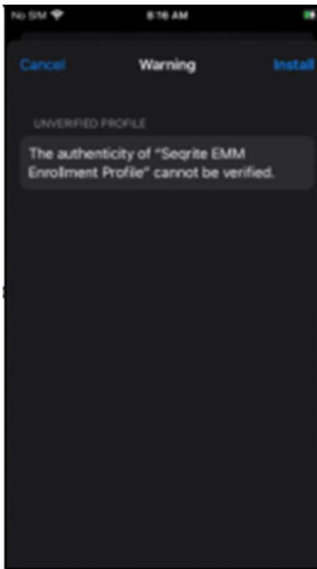
11. Tap **Install** again on the screen warning about the unverified profile. to download configuration profile on the device.
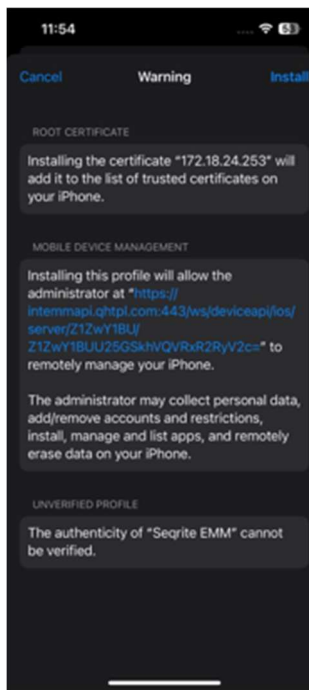
12. Tap **Install** again on the screen warning about the unverified profile.
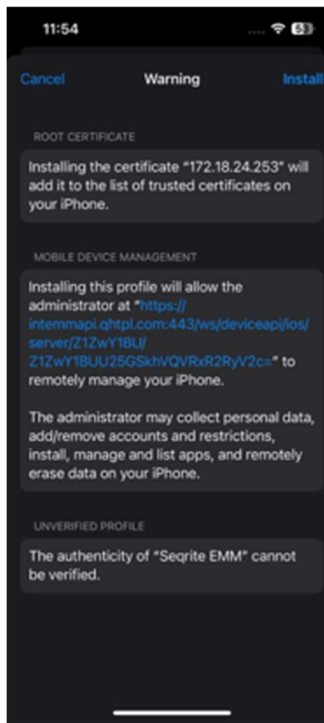
13. Tap **Trust** to enroll your device into remote management.
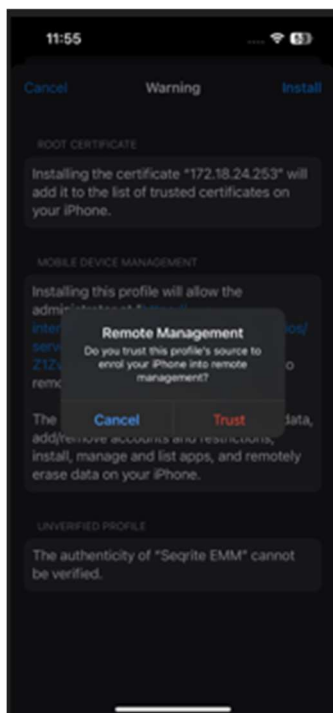
14. Tap **Done**.
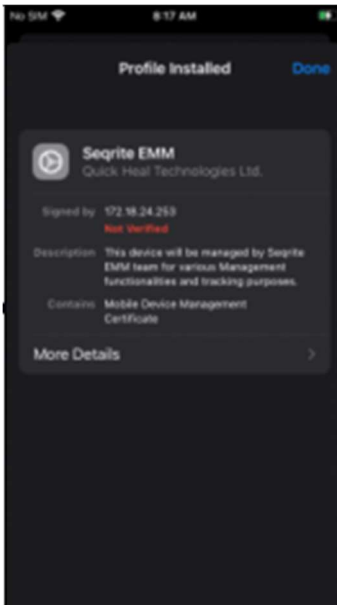
15. Close the settings and open Agent App.
    Device enrollment screen is displayed.
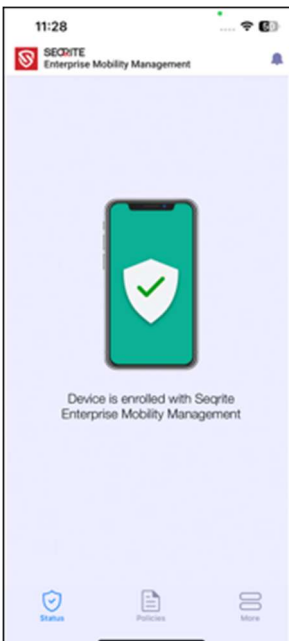
Seqrite workspace will be activated and ask you to set the PIN.
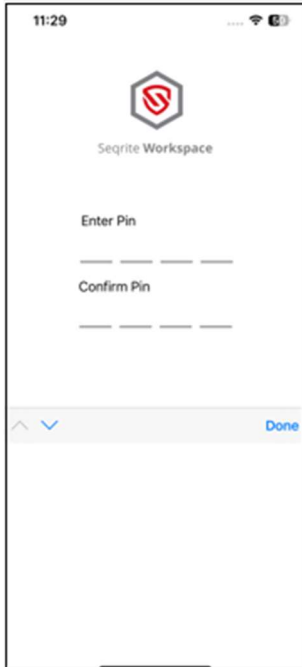
After setting PIN, device and container will be enrolled successfully.
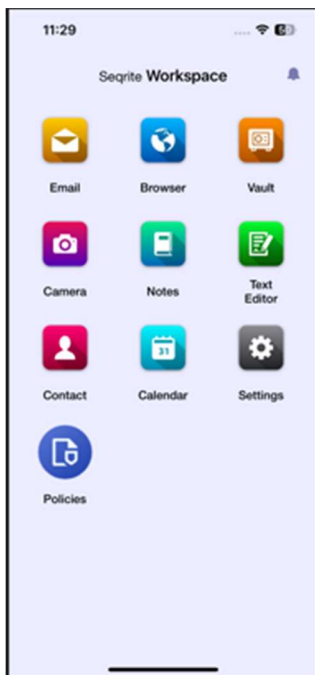
Taking an action on users

Take Action is an option that helps you take an appropriate action on the user.

Sending enrollment request or deleting a user

To send an enrollment request or delete a user, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Users**.

2. On the Users page, select a user.

    The Take Action list appears.

3. Select one of the following options:

    ▪ Select **Enrollment Request** to send an enrollment request to a user's device. There are two options for enrollments.

        o For Device Management: Enroll a device using Email/SMS, using QR code, using ADO enablement, or using [Android Management API](#).

        o Workspace Without Device Management: Enroll a device using Email/SMS or using QR Code

    ▪ Select **Delete** to delete the selected users.
      To know more about the enrollment, see [Enrolling a new device](#).

    ▪ Select **Export CSV to** export a list of users in the CSV format.

4. Click **Submit**.

Additional Actions

On the Users page, you can carry out the following actions as well.

Editing user information: You can edit the user details and change the department, the privileges, and the visibility restriction. Editing user information is similar to [adding user](#).

Importing users: You can import multiple users at one go. This is helpful if you have a long list of users.

Exporting users: You can export multiple users at one go. This is helpful if you have a long list of users and you need the list for some other purposes. To export users, select the users on the Users list. The option for Enrollment Request, Delete, and Export CSV are enabled. Select **Export CSV** and then click **Submit**.

8. Departments

The Departments option lets you add a new department to the Seqrite EMM console. After you create a department, you can add the users to the department, edit the department details, and create groups of the selected departments.

Advanced Search for Departments

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

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

1. Log on to Seqrite EMM console and in the left pane, click **Departments**.

2. On the Departments page, click **Advanced Search**.

    Advanced search parameters are displayed.

    ▪ Select **Parent Department**: Search departments by selecting parent department.

    ▪ Select **Created By**: Select this option to search the department by the creator name.

3. Click **Search**.

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

    ▪ To customize the categories of the Advanced Search, click **Modify**.

Adding a department

To add a new department, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Departments**.

2. On the Departments page, click **Add Department** and then click **Add**.

    You may import the departments you if have a long list of departments with you.
    The Add Department page is displayed.

3. On the Add Department page, enter the **Department Name**, **Parent Department**, and **Description**.

    The Parent Department may have multiple choices depending on your organization structure.

4. 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.

    You may add user to the department, if required.

5. Click **Save**.

    A new department is created along with a group name.

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

Adding users to the department

After you create a department, you should add users to the department so the user can perform actions according to the requirements.

To add users to a department, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Departments**.

2. On the Departments page, select a department and then click the **Edit** icon.

3. Click the **Edit** tab and then click the **Users** tab.

4. Click Add user to department.

    The user list appears.

5. Select the users that you want to add to the selected department.

6. Click Add Users.

    Users are added successfully to the selected department.

Taking an action for Departments

Take Action is an option that helps you take an appropriate action for the departments.

1. Log on to Seqrite EMM console and in the left pane, click **Departments**.

2. On the Departments page, select a department.

    The Take Action list appears.

3. Select one of the following actions:

   - **Delete**: Helps you to delete the selected departments.

   - **Export CSV**: Helps you export a list of the selected departments in the CSV format.

   - **Create Group**: Helps you create a group of for the selected departments.

4. Click **Submit**.

Additional Actions

On the Department page, you can carry out the following actions as well.

Editing department information: You can edit the department details, change the parent department, and add new users to the department. However, to remove a user from a department, you have to change the department of the user by editing the user details from the User option.

Importing departments: You can import multiple departments at one go. This is helpful if you have a long list of departments.

Exporting departments: You can export multiple departments at one go. This is helpful if you have a long list of departments and you need the list for some other purposes. To export departments, select the departments on the Departments list. The option of Delete, Export CSV, and Create Group is enabled. Select **Export CSV** and then click **Submit**.

Deleting departments: You can delete departments from the list at any point in time. To delete departments, select the departments on the Departments list. The option of Delete, Export CSV, and Create Group is enabled. Select **Delete** and then click **Submit**.

9. Devices

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

- Add a new mobile device, assign ownership, and assign owner and group to the device.
- 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

All the devices added to the Seqrite EMM console are recognized by their owners, IMEI, groups, and status.

Different device statuses include:

- **Idle**: Device is added to the Seqrite EMM console, but the enrollment request has not been sent to the device.
- **Pending:** Device added, however enrollment pending.
- **Approval Pending**: Device has requested the server for approval.
- **Disapproved**: Server has not granted permission for the device enrollment.
- **Enrolled**: Device is approved by the server.
- **Uninstalled devices**: Seqrite EMM has been removed from the device.
- **Disconnected**: Administrator has disconnected the device.

Advanced Search for Devices

The Advanced Search option allows you to perform searches of your interest. You can see if any devices are policy non-complaint, app non-complaint, or whether any of the devices are pending for approval or have been uninstalled, and so on.

To see the status of the devices, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Devices**.

2. On the Devices list, click **Advanced Search**.

   The search options for compliance status, device status, and groups appear.

3. Select one of the following compliance statuses:

   - Policy Non-Complaint

   - Configuration Non-Complaint

   - App Non-Complaint

   - Launcher Non-Complaint

   - Agent Unauthorized Removal

   - Device Fully Complaint

   - Agent Venerable

4. Select one of the following device status:

   - Idle

   - Pending

   - Approval Pending

   - Approved

   - Disapproved

   - Uninstalled

5. From the Select Groups list, select a group.

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

   - **Modify**: Help you to modify the search options. When you click the Modify option, the selected search option appears. You can change your search options.

   - **Reset**: Help to remove the selected search options and make the search again.

Taking an action on device

On the devices, you can push several actions from EMM.

To take an action, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Devices**.

2. On the Devices list, select a device.

   The Take Action list appears.

3. Take one of the following actions:

- **Enrollment Request**: Allows you to send enrollment request for EMM and Workspace to the devices.

- **Uninstall Device Management** Allows you to send notification for uninstalling EMM to a device.

- **Delete**: Allows you to delete devices from Seqrite EMM.

- **Export CSV**: Allows you to export the details of devices in the CSV format.

- **Send Messages / File(s)**: Allows you to send messages or files to the devices.

- **Push File on Device**: Allows you to push files on any device in your network. During this process, you can also customize the notification tone for the received file on the device.

- **Move to group**: Allows you to move the selected devices to the selected groups.

- **Workspace action**: Allows you to perform action on Workspace of multiple selected devices. The Workspace action includes Sync Workspace, Push Workspace Policy, Push Workspace Profile, Uninstall Workspace, and Push File into Workspace.

- **Device actions**: Allows you to perform device actions on the devices. The device actions include Update Virus Signature, Push Anti-Theft Configuration, Push Web Security Configuration, Push Wi-Fi Configuration, Push Schedule Scan Configuration, Push Data Usage Configuration, Location Tracking On, Location Tracking Off, Call/SMS Monitoring ON, Call/SMS Monitoring OFF, Scan, Locate, and Sync.

4. Click **Submit**.

   After you send an action order to the device, the device owner needs to take the appropriate action.

Adding devices

To add a new device, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Devices**.

2. On the Devices page, click **Add Device** available on the right-hand side. Click one of the following options.

   - **Add**: Click **Add** to add a device.

   - **Import**: Click **Import** to import a list of devices.

        The Add Device page is displayed.

3. Enter the Device Name and Ownership and then assign Owner and Group.

4. Click **Save**.

Zero-Touch Enrollment (ZTE) for Android Devices

Zero-touch enrollment is a feature on Android devices that automatically sets up your device with your organization's apps and IT policies. You may have received your Zero touch enabled device from your vendor. The device will automatically provision itself with the necessary apps and data for your organization upon first boot. This allows for a streamlined setup process without the need for complex configurations.

Advantages of Android Zero Touch Enrollment

- One-time setup and helps large scale enterprise device roll-out.
- Mandatory MDM management.
- Allows authorized Android device Resellers to add devices to Zero Touch portal, easing enrollment process.
- Admins can set up the device with necessary apps and profiles and it gets applied automatically on device activation.

Prerequisites for Zero Touch Enrollment

- Android Zero Touch Enrollment is supported for devices running Android 9.0 and later.
- Purchase the device either from a Zero-touch reseller partner , Google partner or Zero-Touch device reseller.
- A Zero-touch portal account needed that can be obtained by contacting your reseller.
- A zero-touch account created by an authorized zero-touch vendor that requires your Gmail address.

Follow the steps in given order to proceed with zero-touch enrollment.

1. Associating your Enterprise Google Account with zero-touch portal
2. Creating a configuration and enrolling devices to a group

Associating your Enterprise Google Account with zero-touch portal

Zero touch enrollment is applicable only for devices that are zero-touch provisioned and purchased from sellers listed in Android Enterprise Solutions Directory.

Note: Click here to view and purchase new devices from vendors provided by Android Enterprise.

1. Log on to Seqrite EMM with your credentials.
   The dashboard appears.
2. Navigate to the Setup Services option on the upper right corner.
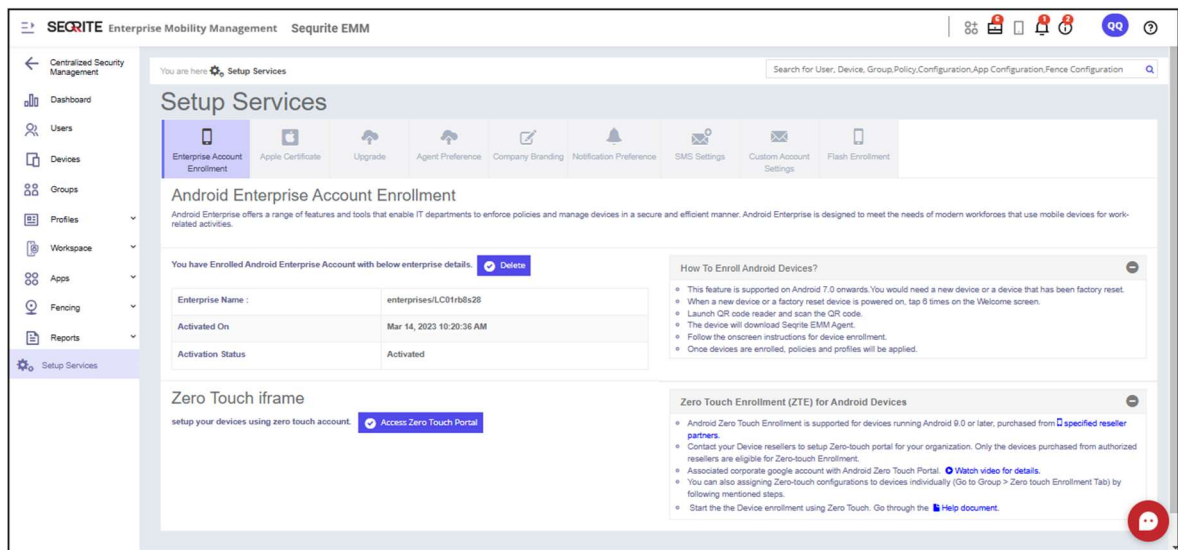
3. On the Enterprise Account Enrollment tab, click **Access Zero Touch Portal**.
   A linked company account will be displayed.
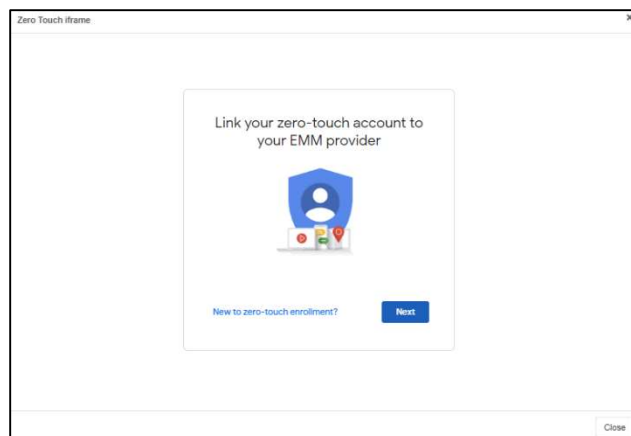
4. Click **Next**.

5. The page to sign-in appears, wherein you will need to provide your Zero-touch account credentials (shared by Device Reseller).
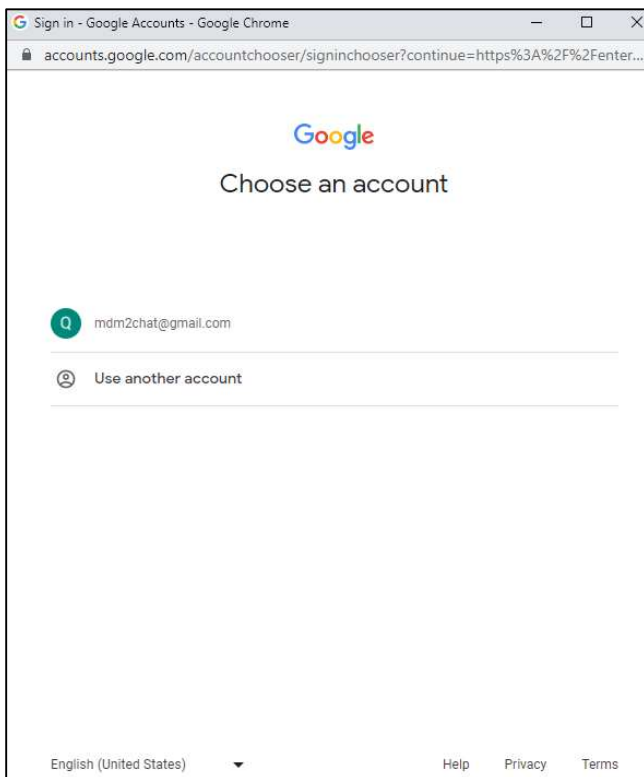
6. Select your company Enterprise Google account and click **Link**.

   Note: All purchased devices in this account will be displayed and linked to your EMM provider. If you are not able to link your account, then contact the device reseller to Configure/Setup your Zero Touch account against your Enterprise Google Account. For more details, click the [link](#).

   You can choose the accounts that contain the devices to be managed.
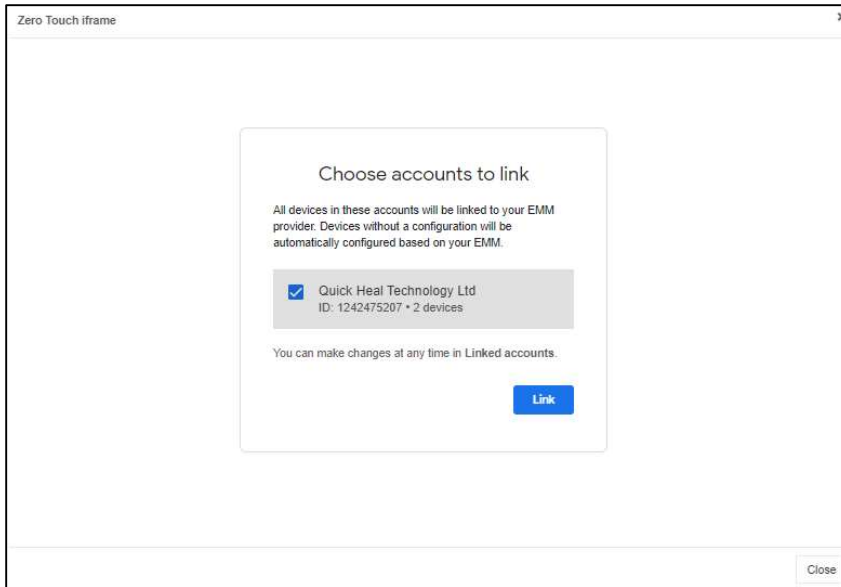
7. Default configuration if any will be applied to the devices. Click **Next**.
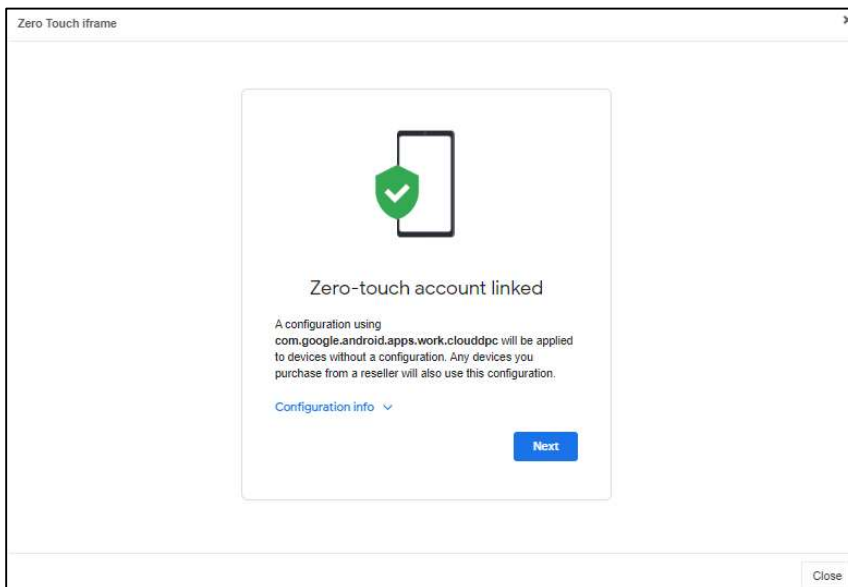
8. On the **Add support info** dialog box, provide your company's support details for employees to reach you in case of any issues during set up.
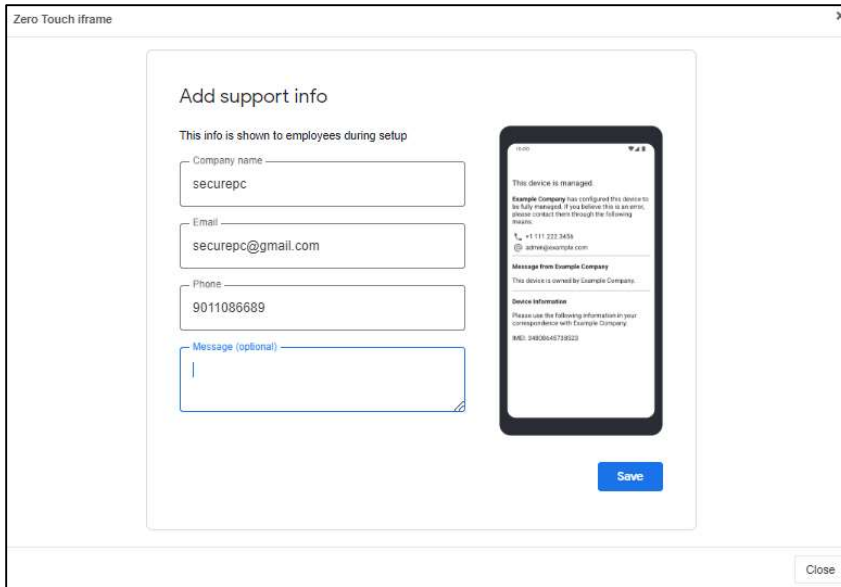
9. Click **Save.**
   Your company account name is linked to Zero Touch iframe.
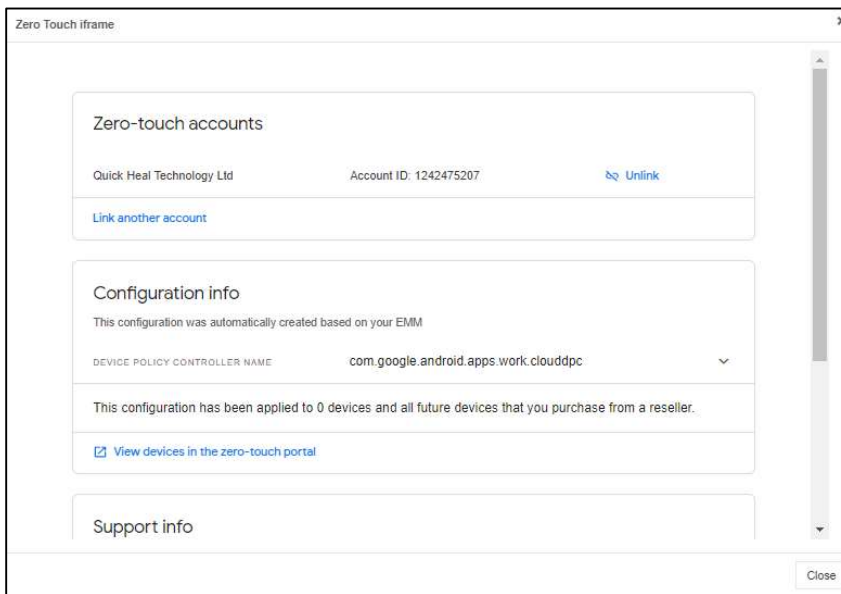
10. Click **View devices in the zero-touch portal** to view the devices purchased by your company.
    You are redirected to your company account on Zero Touch portal Configurations page.
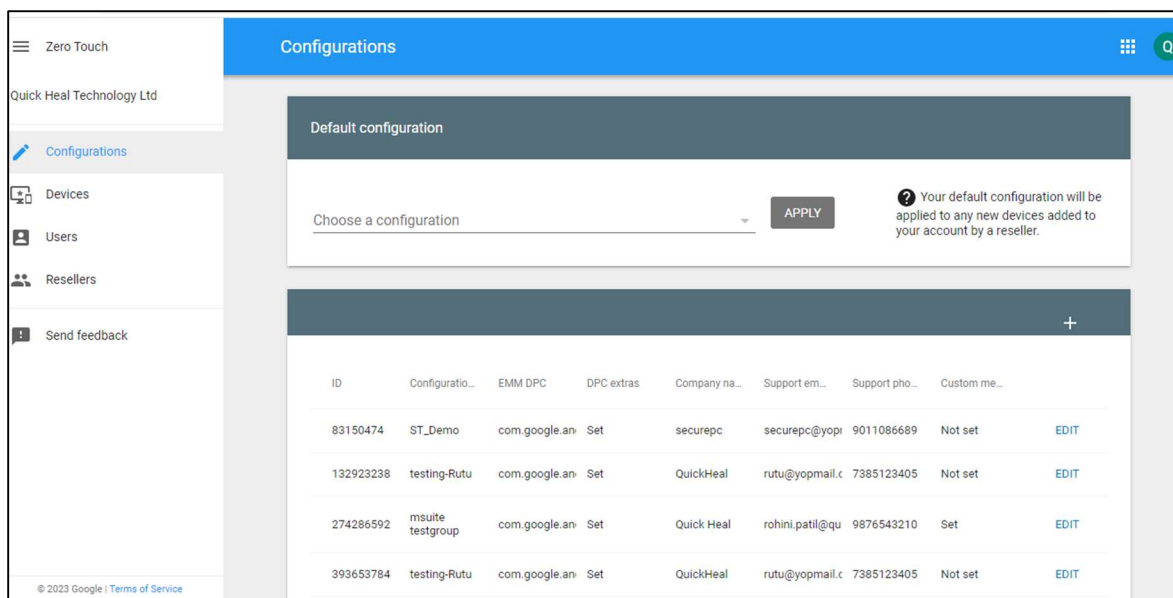
About Zero-touch portal

Zero-touch portal contains the details of the devices, resellers, MDM configurations and so on. You can refer the table for more details.

PARAMETER	DESCRIPTION
Configurations	If you have an updated setup, you are provided with Enterprise Default Configurations that cannot be modified. Else you can add, modify, and delete the MDM configurations here. You can also choose to assign MDM configurations by default, to the devices being added to the account.
Devices	You can view the list of devices added to the account here. You can select devices and assign the created configurations to these devices. Additionally, you can also choose to delete the added devices here.
Manage People	You can add, modify, and delete the users, who can manage and access the portal here.
Resellers	You can choose to add additional reseller details here.

Creating a configuration and enrolling devices to a group

You can create configurations to assign policies and app management for your devices. You can create configurations for different groups or a default configuration that you want to apply to devices that are enrolled via Zero Touch enrollment. A configuration contains the following:

- The EMM device policy controller (DPC) you want to install on the devices.
- EMM policies you want to apply to the devices.

Steps

1. Log on to Seqrite EMM portal.
2. Navigate to **Groups** in the left pane. Select the group to which you want to add the zero-touch devices.
3. Click **Edit**.
   The Group details page appears.

4. Click **Zero Touch Enrollment** tab.
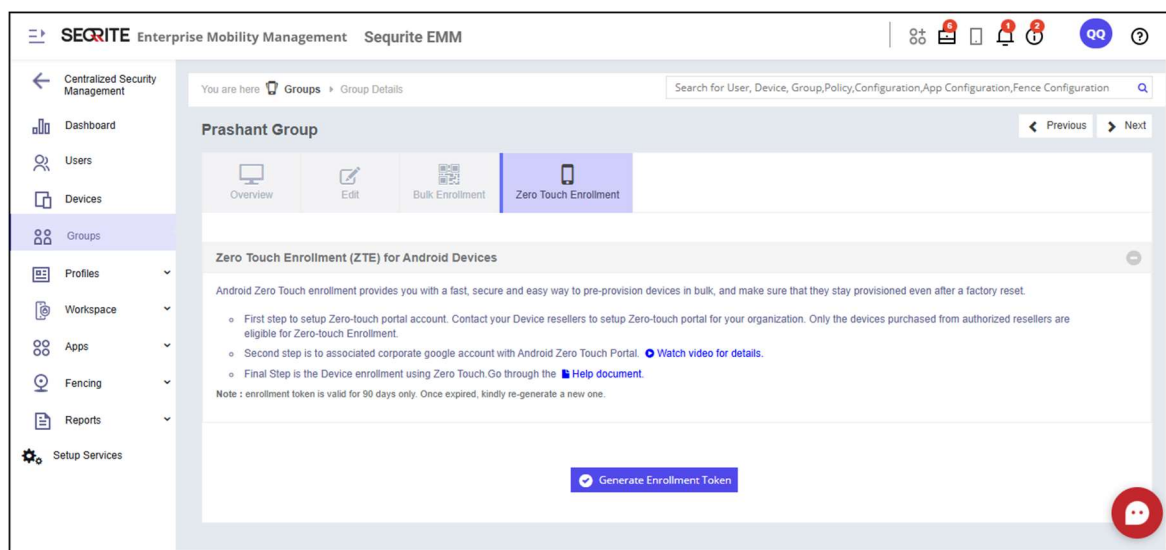
- If the group is newly created, click **Generate Enrollment Token** to generate token (JSON content) for enrollment.
- For existing groups, click **Copy text** to copy the token (JSON content) to the clipboard.
  Note: The enrollment tokens expire in 90 days. If expired, re-generate a new one.
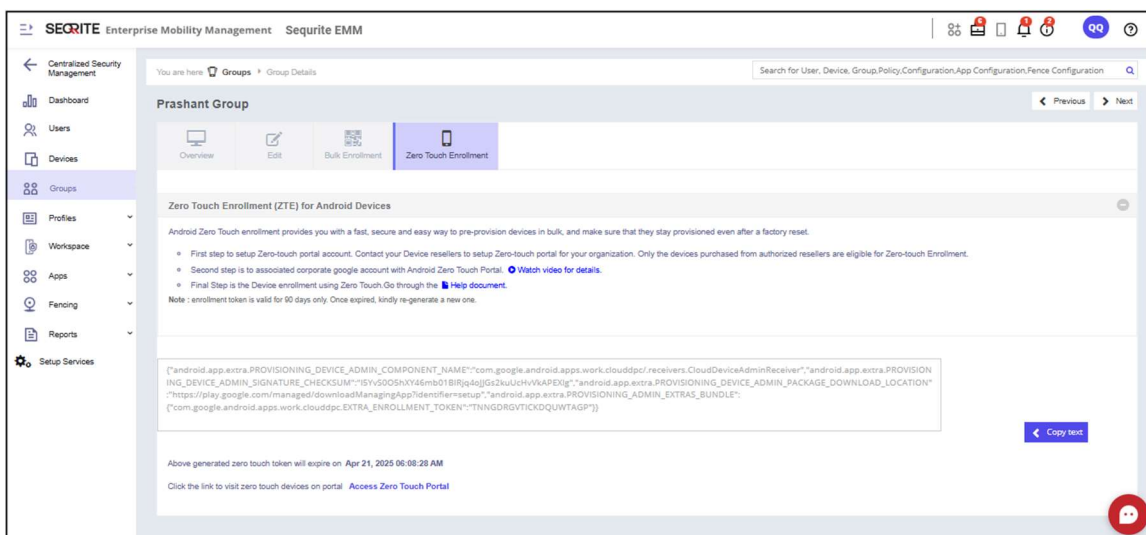
5. Click **Access Zero Touch Portal** link.
   You are redirected to your company account on the zero-touch portal.

Setting up Zero-touch portal using JSON configurations

If you are setting up Zero Touch portal using JSON configuration, follow the steps:

1. Login with the Google account associated with your corporate e-mail if need be.
2. Click Configurations present in the navigation panel and click the + button to add a new configuration.
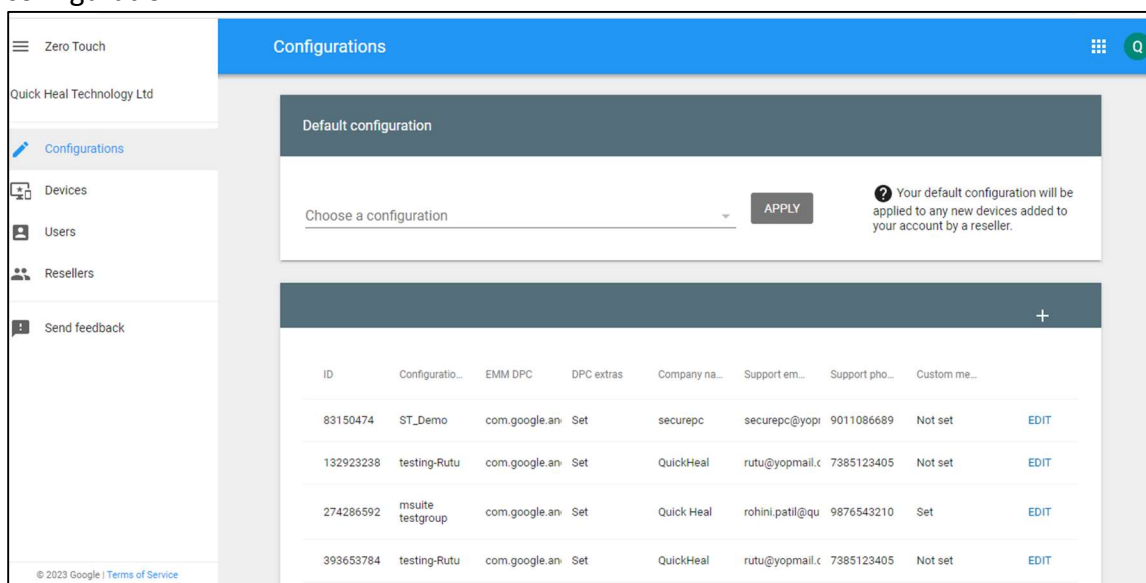
3. Enter the Configuration name and select the Android Device policy from the drop-down for EMM DPC.

4. In the **DPC extras** section paste the copied token(JSON content).
5. Enter the Company name, Support email address, Support phone number and Custom message.

6. Click **ADD**.
   The configuration for that group is added to your company account on the zero-touch portal.
7. Click **Devices** in the left pane.
   The Devices page appears. These devices are added to your account by your vendor after purchase.
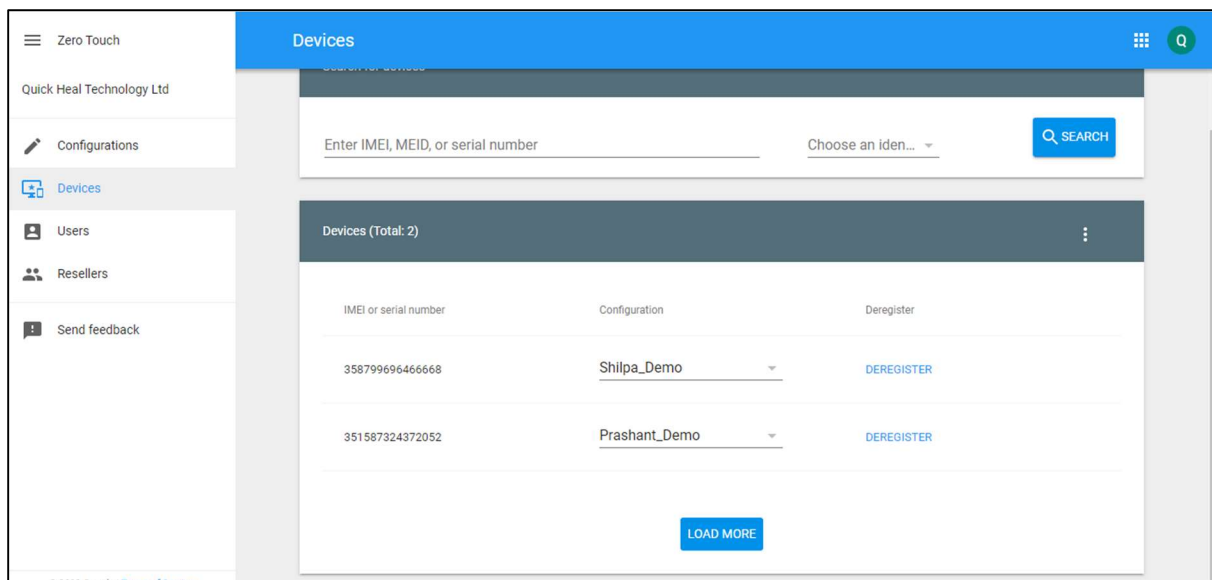
8. For each device, in configuration drop-down, select the group configuration (saved earlier) that you want to assign the devices to.

9. Ensure that you have performed the factory reset on the device before assigning configuration.
Note: For newly purchased device do not setup device until configuration is mapped to the device.

10. Click **Update**.

11. After you save the devices configuration, setup your devices. Your devices will be enrolled under respective groups that were used to create configuration.

    After completing the above procedure, when the user unboxes the new device and connects it to the Internet, the user will be prompted to accept the enrollment agreement and start the enrollment process with Seqrite EMM.

Additional Actions

On the Device screen, you can carry out several actions. To carry an action on a device, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Devices**.

2. On the Devices page, select a device and click the **Edit** icon.

   On the Device Details page, you can perform any of the following actions.

   ▪ Overview: Helps you to view the device details, hardware storage, perform enrolment for EMM and Workspace. To know about how to enroll a device, see Enrolling a new Android device.

   ▪ Edit: Helps you to edit device details such as device name, ownership, mobile number, device type, owner name, group name, and configure security settings for the device.

- Location: Helps you to trace the device on geo map.

- Apps: Helps you to view the app inventory of the device.

- Data Usage: Helps you to view data usage for the device. It gives a detailed view of the current data plan, how much data has been used, and how many apps are in use.

- Call/SMS Logs: Helps you to view call and SMS logs. This is helpful to know how many calls have been made and with whom.

- Remote Control: Helps you to access the device remotely and perform several actions. However, no action can be performed on the Mac devices, except mirroring of the device.

- Reports: Helps you to view reports on different activities carried out on a device, device compliance report, and scan report.

Overview

Under Overview, you can take actions for EMM and Workspace.

Select an Action for EMM

You can perform various actions for EMM on the devices. The actions are displayed as per the device status.

- If the device is in uninstalled or pending state, the **Select an Action** list displays the following options: Enrollment using Email/SMS, Enrollment using QR Code, Enrollment using ADO Enablement and Enrollment using [Android Enterprise Enrollment Using AMA](#).

- If the device status is in Approval Pending state, the Select an Action list shows three options: Approve, Disapprove, and Disconnect.

- If the device status is in Enrolled state, the Select an Action list shows the following options:

Device actions	Description
Sync	Helps you to sync the device with the Seqrite EMM server. After sending this command, the device will send the latest app details, scan, and compliance report to the server.
Locate	Use this command to fetch the current location of the Android device. This helps you know whether the device user is under the allowed geo location.
Scan	This command initiates virus scanning of the Android device and forwards the scan report to the administrator.
Remote Buzz	Use this command to play the ringtone on the selected Android device.

Device actions	Description
Block	Use this command to block the Android device completely and the user cannot access the device. This command should be used carefully.
Unblock	Use this command to unblock the blocked Android device.
Exit Launcher	EMM Launcher allows access to certain allowed apps on the device. Even if there are other apps installed on the device, they are hidden by the EMM Launcher. However, if there is some need to remove this restriction either temporarily or permanently, you can send this command. When you exit the launcher temporarily, you must enter time. As soon as the assigned time elapses, the restriction of the launcher will apply again.
Fetch Logs	Use this command to fetch the activity logs about the actions 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, and crash files.
Wipe	Use this command to wipe out the data from the device. The Wipe option includes Full Wipe, SD Card, Factory Reset, and Custom Wipe. Note: Full Wipe is not supported on devices that have Android 10 and above OS.
Reset Password	Use this command to reset the password of the selected device through Seqrite EMM.
Send Messages/Files	Use this command to broadcast a message or file URLs to the Android and iOS devices. To know more about Broadcast Message, see Broadcasting File and Message.
Push Anti-Theft Settings	Use this command to reapply the anti-theft settings on the selected device. You can use this command when previously applied anti-theft settings fail to execute on the device.
Push Web Security Configuration	Use this command to reapply 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.

Device actions	Description
Push Policy	Use this command to reapply the mapped policy on the selected device. You can use this command only when the previously applied policy fails to execute on the device.
Push App Configuration	Use this command to reapply the 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.
Push Wi-Fi Settings	Use this command to reapply the Wi-Fi settings on the selected device. You can use this command only when the previously Wi-Fi settings fail to execute on the device.
Push Schedule Scan Settings	Use this command to reapply the Schedule Scan Settings on the selected device. You can use this command only when the previously Schedule Scan Settings fail to execute on the device.
Push Data Usage Configuration	Use this command to reapply 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	Use this command to reapply a fence configuration on the selected device.
Disconnect	This command will disconnect the device from the Seqrite EMM server. After the command is executed on the device, the device cannot be managed by the Seqrite EMM console. Use this command cautiously.
Uninstall EMM	Use this command to remotely uninstall the Seqrite EMM Agent from the selected ADO/Knox devices.
Update EMM Virus Signature	Use this command to update the EMM Virus Signature on the selected device.
Reset Device Password	Use this command to remotely reset the password for a particular device.
Reboot	Use this command to remotely reboot a particular device.

i Note:

- The iOS devices support only the following commands: Sync, lock, clear passcode, un-install, disconnect, broadcast files and messages, locate, ring, and fetch location.

Select an action for Workspace

You can perform various actions for Workspace on the devices.

Device actions	Description
Sync	Helps you to sync the selected device with the Seqrite Workspace server. After sending this command the device will send the latest app details and compliance report to the server.
Reset Workspace Password	Use this command to reset the password of Seqrite Workspace.
Wipe Workspace Data	Use this command to delete the Workspace data.
Block Workspace	Use this command to block the Workspace application on a device.
Unblock Workspace	Use this command to unblock the blocked Workspace application.
Uninstall Workspace	Use this command to uninstall the Workspace application from the device.
Push Workspace Policy	Use this command to push any Workspace policy on the device.
Push Workspace Profile	Use this command to push any Workspace profile on the device.

Edit

The Edit tab allows you to edit the device details and its configurations. You can change configurations such as Wi-Fi, Anti-Theft, Web Security, 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 Seqrite EMM console and in the left pane, click **Devices**.

2. On the Devices page, select a device and click the **Edit** icon.

3. On the Device Details screen, click the **Edit** tab and then click **Edit details**.

4. Edit the required information such as Device Name, Ownership, Device Type, Owner, and Group.

5. Click **Save**.

   The device information is edited successfully.

Configuration

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

> **Note:**

> If the device is associated with any device group, to which the app configuration is applied, 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 Seqrite EMM console and in the left pane, click **Devices**.

2. On the Devices page, select a device and click the **Edit** icon.

3. On the Device Details screen, click the **Edit** tab and then click **Configurations**.

4. You can edit or update Wi-Fi, Anti-Theft, Web Security, Schedule Scan, Network Data Usage, and App Configurations as required.

   To know more about various configurations, see security profile [Configurations](#).

5. Click.

   The device information is edited successfully.

Location Save & Apply

Helps to locate the device on the geo map. This is helpful to see where the device users travel most of the time.

Note: If the device user denies the location permission, then the admin is unable to access the location of the device and locate/trace commands are bound to fail.

Turning on the 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 tracing location option is turned on, the activity log is in progress. When the task is completed, its status changes to complete.

To trace the device location, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Devices**.
2. On the Devices page, select a device that is to be traced and click the **Edit** icon.
3. On the Device Details screen, click the **Location** tab.
4. Turn on the **Trace** option.
5. On the Location Tracking Frequency dialog box, select the **Location tracking frequency** in minutes and click **Configure**.

    - The Trace On command is submitted successfully.

        [i] Note:

        To enable tracing of a device, make sure that the GPS option on the mobile device is always turned on.

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

        This command is applicable only to the Android device.

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

Options	Description
Locate	This command is to fetch the current location of the selected device. [i] Note: Location will be fetched only if the Location Services is enabled on the device.

Options	Description
Trace On	This command is to carry out the continuous trace for the selected Android 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.

Obtaining the device location

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

To locate the device location, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Devices**.
2. On the Devices page, select a device that is to be traced and click the **Edit** icon.
3. On the Device Details screen, click the **Location** tab.
4. Select one of the following periods for which you want to see the device location.

   You can view location history for Today, Since Yesterday, Last 7 days, Last 15 days, Last 30 days, Last 45 days, Last 60 days, and Last 90 days.
   Note: Location history will start being stored only after you select the options. By default, location history is stored only for 7 days.
5. Click the search icon.

   Device locations appear. You can import the locations in CSV or PDF format.

6. To send the device location by SMS, click the **Locate** button on the map.

   A confirmation screen appears.

7. Select the **Locate device by sending SMS** check box and then click **Locate**.

   $\boxed{i}$ Note:

   The Locate device command via SMS works only when the Android device has the SIM and the mobile number is updated.

Locate Multiple Devices

Locate Multiple Devices helps you to locate the devices enrolled in your network. You can see all the devices on a single map wherever they are.

This gives you the flexibility to know where your resources are, like if they are in the approved locations.

Locating devices

To locate the devices, follow these steps:

1. Log on to Seqrite EMM console.

2. Select any device. You may select multiple number of devices.

   A banner appears at the footer with the option **Show on Map**.

3. Click **Show on Map** available at the footer.
   However, if you want to locate all the devices on a single map, click **Show on Map** available as a tab on the upper right side.

Apps

Apps is a list of apps installed on mobile devices. If any command is pending with respect to app inventory; a small exclamatory icon is displayed on the App Inventory tab and on the app in the app list. When hovered over the icon, the pending command is displayed. The Apps tab for the iOS devices will be in read-only format and only the downloaded apps will be listed. However, it will not show any Android system apps. With the App Inventory option, you can perform multiple actions.

App Status

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

- **Installed**: This status is shown 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 the Admin 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

The Advanced Search option allows you to perform searches of your interest. You can see which apps have been downloaded, installed, blocked, or other status.

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

1. Log on to Seqrite EMM console and in the left pane, click **Devices**.

2. On the Devices page, select the device and click the **Edit** icon.

3. On the Device Details screen, click the **Apps** tab. Click **Advanced Search**.

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

    You can select all the options or only one.

5. Click **Search**.

    The Search result is displayed.

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

Installing the App Launcher

You can install the app launcher on the selected devices. This is helpful if you want to restrict the users to have access only to a certain number of apps allowed by you.

You can create a list of app inventory and initiate installing the app launcher on a mobile device. As soon as the app launcher is installed on a device, all the apps previously installed on the mobile will not be accessible, except the ones allowed by you.

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.

Activating the app launcher

To activate the launcher, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Devices**.

2. Select a device and then click the **Edit** icon.

3. On the Device Details page, click the **Install Launcher** button.

4. 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 the device, the launcher gets activated.

Exiting the launcher

To exit the launcher, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Devices**.

2. Select a device and then click the **Edit** icon.

3. On the Device Details page, select **Exit Launcher** from Select an Action list and then click **Submit**.

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

4. 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.

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

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

Data Usage

The Data Usage option lets you monitor Internet data usage applied to the selected device if the network usage configuration is applied on the device. After the Data Usage configuration is applied to the device, the Seqrite EMM 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 data 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 a 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 Seqrite EMM console and in the left pane, click **Devices**.

2. On the Devices page, select the device, click the **Edit** icon. Click the **Data Usage** tab.

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 detailed information of the mobile data and Wi-Fi usage in a selected range of periods. This data usage information is provided in MBs.

- 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 the **Settings** button.

> ℹ️ 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.

Parameters	Description
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, help 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. *i* Note: If the data plan is modified using this Setting icon, then the modified network usage configuration will have more preference and the changes will not be applied 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 MBs. Hover the mouse 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 consume 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 consume maximum Internet data in the selected date range. It gives the details of the Internet data usage by the user and helps 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 on 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 detailed quantifiable information on the Internet data usage daily. 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**.

Note:

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

The Usage Information option is visible only on the Android devices.

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 by the app.

Columns	Description
Roaming Data (in MB)	Shows the usage of data for apps in roaming status.

Call/SMS Logs

You can turn on monitoring for Calls and SMS and record logs. You can filter by log type, call type, and call log duration.

Call/SMS Logs Actions:

1. Navigate to Devices > Select device > Click Edit icon.
   You are redirected to Device Details page.
2. Click Call/SMS Logs tab. You can perform the following actions:

   - Turn ON or OFF Call/ SMS Monitoring.
   - Sync Logs from device to EMM.
   - Perform detailed search by filtering logs and clicking Advanced Search as required:
     - Log Type by Incoming, Outgoing, Missed, and Rejected.
     - Call/SMS by Call, Video Call, SMS, and MMS.
     - Duration (Call log history) by Today, Last 7 Days, Last 15 days, Last 30 days, Last 45 days, Last 60 days, and Last 90 days.
       Call log history will start being stored only after you select the options. By default, call log history is stored only for 7 days.
   - Export call logs to a file.

Remote Control

The Remote Control (RDC) feature helps the Seqrite EMM administrator to get the remote access of the user's device. It is helpful in case of emergency when the user is travelling or out of the office. In such a scenario, the Seqrite EMM 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. The administrator can take a maximum of two RDC sessions in a single instance. Even in case of network fluctuation, Seqrite EMM Agent tries not to disconnect the RDC session and automatically reconnects with the EMM console.

i Note:

By default, every EMM tenant is provided with certain data transaction usage limit. The process of remote device control and file handling is also part of this data transaction usage. If the limit exceeds, the user would not be allowed to take RDC of the device. Customer must buy/purchase additional transaction usage limit to take RDC of the device, and file upload and download in RDC session. If the transaction limit has exceeded, then the RDC tab will not be accessible.

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 (Android OS 7, 8, and later versions).
- Upload or download a file from the server to the device or from device to the server.

i Note:

Only for the KNOX supported devices, the Administrator can have complete control of the device. The Remote Control feature is applicable only for the Android devices.

- 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 you to start the RDC session and take control of the remote device.
Stop RDC	Helps you to stop the RDC session.
Resume	Helps you to resume the RDC session if it was stopped for any technical issue.
Back	Helps you to visit the previous screen on the device.
Home	Helps you to visit the Home screen of the device.
Recent Apps	Helps you to visit the recent apps on the device.
Screenshot	Helps you to take screenshot of the remote device.
File Handling	Helps you to view the files and folders structure on the device. Note: The admin can only access files if the device user authorizes it. If the user declines, the admin can try again by clicking retry (applicable only for android devices) to request access to the files. If device user doesn't authorize, then admin won't be able to view File Handling of the device.
Refresh	Helps you to refresh the files and folders structure on the device.
Create Folder	Admin can create new folder on Android device remotely and can perform action on the folder.
Download File	When in RDC session, it helps you to download a file from the device to the server. You can download maximum 30 MB file.
Upload File	When in RDC session, it helps you to upload a file from server to the device. You can upload maximum 50 MB file.
Delete	Helps to delete the file from the device.

⚞i⚟ Note:

- ○ The Remote Control (RDC) feature is applicable to Android OS 7, 8, and later versions.
- ○ The Remote Control feature is supported on Seqrite EMM Agent 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 are applicable only to the KNOX supported devices. For the Non-KNOX devices, the Admin can view only the mobile screen and cannot perform any action.

Remotely controlling the device

In the remote-control session, the Admin can completely control the device. This functionality is applicable only to all the devices with OS 7 and later versions.

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

1. Log on to Seqrite EMM console and in the left pane, click **Devices**.

2. In the Devices list, select the device to take its control and click the **Edit** icon.

3. On the Device Details page, click the **Remote Control** tab.

4. To view the device screen, click **Start RDC**. The RDC session starts in the new tab.

   In the Activity log, you can see the status of RDC session.

5. The device user has to accept and provide their consent.

   - For Seqrite EMM 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 Seqrite EMM console and the remote session starts.

   ⚞i⚟ Note:

   - For normal devices and ADO enabled devices, the Admin can only view the remote screen of the device with OS 6 and later versions.

   - For KNOX supported devices, the Admin can take complete control of the remote device, perform actions remotely, and troubleshoot the issue.

   - In case of Mac OS (iOS), the device can be viewed only but cannot be controlled.

   - To create new folder, click **Create Folder**.

- To get a file from the device, click **Download File**.

- To share a file from the server to the device, click **Upload File**.

- To delete any file or folder, select the file or folder in **File Handling** section and then click **Delete**.

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

Important points to remember for seamless RDC connection:

- Make sure that data transaction usage limit is not exceeded.

- Device must have good Internet connectivity without any network fluctuations.

Some delay may be observed (based on network speed) in screen appearance during RDC if network connection is slow.

- When the Admin requests for remote access, the device user has to accept the RDC request, then RDC connection will be established.

- Device should have consistent 400 kbps network speed for smooth remote connection.

- The device should have a minimum of 150 kbps network speed for establishing remote connection.

Reports

With Reports, you view the reports on all the actions that were performed on a device, compliance reports, and scan reports.

Activity

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 Seqrite EMM console and in the left pane, click **Devices**.

2. On the Devices page, select the device and click **Edit** icon.

3. On the Device Details page, click the **Reports** tab and click **Activity**.

4. From the period list, select the days or the date range to search the activity logs and click **Search**.

   Activity logs are displayed.

Device Compliance Report

The Device Compliance Report section shows a report on all non-compliant devices. If the report is not displayed, you can send the sync command to fetch the latest reports.

When you are on the Device Compliance Report page, all the non-complaint devices are displayed.

- To view more details of the report, click **View Report**.

Scan Report

The Scan Report option shows when a device was scanned. 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 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.

10.Groups

The Group option helps you to add a group, add devices to the group, and assign a policy to the group. The policies and configurations applied to a group are applied automatically to all the devices that belong to that group. You must create a group and add devices to that group to apply the same restrictions on all the devices. When you create a new device, a default group is created, and the default policy is also applied to the user.

Group QR Code

The Group QR Code option provides the facility to enroll multiple Android or iOS devices of any group in a single instance. The devices enrolled using Group QR Code option are added to the Seqrite EMM console as per the group name with incremental numbering. For example, if the group name is QR Group, the devices added to the Seqrite EMM console 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 must 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 to 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 the generated QR Code can be set to 30, 60, or 90 days.

> ⓘ Note:
>
> When generating the QR code, by default, the Auto Approval check box is not selected on the Seqrite EMM console. 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 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 EMM console and in the left pane, click **Groups.**

2. On the Groups page, click **Advanced Search**.

3. Select the following 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.

4. Click **Search**.

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

Taking an action on group

On the groups, you can take several actions.

To take an action, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Groups**.

2. On the Groups page, select a group.

    The Take Action list appears.

3. Take one of the following actions:

    ▪ **Delete**: Allows you to delete a group from Seqrite EMM console.

    ▪ **Export CSV**: Allows you to export the details of the groups in the CSV format.

    ▪ **Device actions**: Helps you to apply anti-theft actions on the devices that belong to the selected groups. You can perform actions such as assign anti-theft configuration, assign web security configuration, apply Wi-Fi configuration, assign schedule scan configuration, assign app configuration, assign data usage, assign policy, assign fence configurations, send messages/files, and push files on the device.

        o Location Tracking ON/OFF: This option enables the Seqrite EMM administrator to enable the location tracking on the devices in bulk. Administrator can select one or more groups from the Group list page and apply Location Tracking ON. It will send location tracking command to all the devices of the selected groups.

    ▪ **Workspace actions**: Helps you to perform different actions on Workspace for a single or multiple selected groups. You can send the commands and perform the actions such as sync Workspace, assign Workspace policy, assign Workspace profile, uninstall Workspace, and push file into Workspace.

4. Click **Submit**.

    After you send an action order to the device, the device owner needs to take the appropriate action.

Broadcasting files and messages to multiple devices in a group

When you want to broadcast the messages or files to a larger audience, you can use single or multiple groups to send the messages. This will help to communicate with larger audience with ease.

To broadcast files or message to multiple devices using groups, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Groups**.

2. On the Groups page, select the groups.

3. From the Take Action list, click Device actions.

4. In Apply Anti-Theft list, click **Send Messages / Files** and then click **Submit.**

   Send Messages / Files command will be executed only on the supported devices.

5. In the Message field, enter the message or file URL. You can enter comma-separated multiple URLs.

6. In the Broadcast Type list, select the required option.

7. In the Download Path field, enter the valid path where the file can be downloaded. Make sure you enter the valid download path, or the file will not be downloaded.

8. Click Broadcast.

9. On the confirmation popup, click **OK**.

   To check the status of the devices, refresh the page.

Adding a group

To add a new group, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Groups**.

2. On the Groups page, select **Add Group > Add**.

3. Enter the Group Name, assign a policy, select the required Fence Config, App Configuration, Workspace policy, Workspace profile, and add a description.

   To know more about policies, see Policies.

4. Select the **Default** check box to make this group a default group.

   $\boxed{i}$ Note:

   All the newly added devices will be added to the default group.

5. Click **Save**.

   The group is created successfully.

Editing group information and adding devices to the group

With this option, you can edit the group information and add new devices to the group.

To edit the group information, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Groups**.

2. On the Groups page, select a group and click **Edit** icon.

3. On the Group Details page, click the **Edit** tab and then click **Edit details**.

4. Edit the information that want to change. You can edit the Group Name, Assigned Policy, Fence Configuration, App Configuration, Workspace Policy, Workspace Profile, and Description, and click **Save**.

5. To add a device, click the **Devices** tab and then click the **Add device to group** button.

    The Add device to group list appears.

6. Select the devices that you want to add to the group.

7. Click Add Devices.

    The selected devices are added to the group.

Bulk Enrollment with Group QR Code

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.

While performing bulk enrollment using group QR code, for consistent nomenclature, you can use the device naming preference option. You can name the devices as per IMEI number, MAC address, phone address, or system generated number.

Generating group QR code

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

1. Log on to Seqrite EMM console and in the left pane, click **Groups.**

2. On the Groups page, select a group and click **Edit** icon.

3. On the Group Details page, click the **Bulk Enrollment** tab.

4. To enable other sections on the Group Details page, select the **Generate Group QR Code for the bulk enrollment** check box.

    This feature is applicable only to Android devices.

5. Assign the owner to the group by clicking **Assign Owner** button and select the owner.

6. Select an enrollment preference from EMM for Device Management, Workspace Without Device Management, Android Enterprise Enrollment using AMA and Enrollment using ADO Enablement.

7. To select the consistent naming convention for the devices, select the required option from

Select Device Name list from below-mentioned options.

[i] Note:

The naming convention is set as system generated by default for device when Android Enterprise Enrollment using AMA option is selected.

- As System Generated: Use this option for default nomenclature by the system.

- As IMEI Number: Use this option to name the devices according to the device IMEI number.

- As MAC Address: Use this option to name the devices by their MAC address.

- As Phone Number: Use this option to name the devices by their phone number.

8. Select the validity of the QR code by selecting the number of days from the list.

9. Click Generate QR Code.

   The QR code is generated with details such as Device Group name, Enrollment token, Expiry date, and Owner email address. An email is sent to the group owner with the respective QR code details.

   o To generate new QR code, click the **Try new QR code** link.

   o To cease the QR code at any instance, click **Terminate QR Code**.

   o To download the QR code, click **Download**. You can use this option to print the QR code and share on the notice board. Users can scan the QR Code and enroll the mobile devices.

10. You can also send the QR code to other users. Enter the email addresses separated by a comma in the **Send Email** text box and click **Send**.

- To update the QR code details, click **Update QR Code**.

[i] Note:

If a device user has not set the mobile number in the SIM, the device name will not be set as a phone number.

Locating a group on map

With this option, you can locate all the devices of a group on a single map.

To locate the group, follow these steps:

1. Log on to Seqrite EMM console.

2. Select a group and then click the map icon available under the Action column.

   The devices of the group are displayed on the map.

Importing groups

In one instance, you can import a maximum of 1000 device groups.

To import the groups, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, select **Groups** > **Add Group** > **Import**.

2. In the Import Groups dialog box, select the file containing the information about the groups 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 group details

When you use the export groups option, you get information about all the available groups of Seqrite EMM. You can export the group information in PDF 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 group details, follow these steps:

1. Log on to Seqrite EMM console and in the left pane click **Groups**.

2. On the Groups page, select the desired group and click the Edit icon.

3. On the Group Details page, click **Export Users, Export and Move Users as required**.

    The User group details are exported in a PDF file that is downloaded to your device or moved as selected.

Deleting groups

You can delete groups using any of the either option:

- You can delete a single group by clicking the **Delete** icon on the Groups list page.
- On the Groups list page, select single or multiple groups. The **Take Action** list appears. From the list, select **Delete** and then click **Submit**.

Adding User through Groups for Enrollment

You can add user through the Groups page as follows:

1. Logon to Seqrite EMM console using your credentials.

2. Navigate to the **Groups** page, select group in which you want to add devices.

3. Click the Edit Icon (pencil) for the selected group.

4. On the Group Details page, click **Move Users**.

5. On the Import Devices dialog, download the sample CSV file.

6. In the downloaded CSV file, enter the User email addresses of the users for which you want to add the devices and later enroll.

7. Click **Select File** and browse and select the CSV file and click **Import.** The devices are imported to the selected group and associated policies applied.

11.Profiles

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

This chapter includes the following sections.

Policies

Configurations

Policies

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

![Note icon] Note:

- KNOX-supported policies are applicable to all the KNOX-supported devices.

- Some Samsung devices may not indicate that they are KNOX-supported, however 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 Seqrite EMM console and in the left pane, select **Profiles** > **Policies**.

2. On the Policies list, click **Advanced Search**.

3. From the Select Created By list, select the desired creator name and click **Search**.

    The search result gets displayed.

Taking an action on policies

The Take Action list appears on the Policies list page when you select single or multiple policies. The Take Action list is as follows:

- **Create EMM Policy Copy**: Lets you create a copy of existing policy.
- **Delete**: Lets you delete single or multiple selected policies.

  [i] Note:

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

  o   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 Seqrite EMM console and in the left pane, select **Profiles** > **Policies**.

2. On the Policies page, click **Add Policy**.

    If you have a long list of policies, you can import the policies.

3. Enter the Policy Name and Description.

    If you want to make this policy a default policy, select the **Default** check box. This default policy will be applied to all the newly added devices.

4. To save your settings, click **Next**.

    A list of policies appears.

    On the policy page, you can see the default policies.

    All the policies that are enabled appear with a tick mark, the disabled policies appear with a cross mark, and the polices that are not available appear in grey color.

    Also, some polices may not be available for Android or iOS.

    You can modify the polices as per your requirement.

    Under All, you can see all the policies, while under Password, Policy for Device Applications, Policy for App Stores, Policy for Downloaded Apps, Policy for ADO enabled devices, and Policy for KNOX supported, you can see the respective polices.

    To know more about policies, see [Policy Details](#).

5. To enable a policy, click on the cross mark. This policy is enabled and applies restriction on the device. To disable a policy, click on the tick mark. This policy is disabled and applies restriction on the device.

6. Click **Save**.

    New policy is created successfully.

ℹ️ Note:

> You can save a normal EMM policy without configuring the Edit Enterprise Policy.
>
> However, to save an AMA policy, you must create and save a normal EMM policy first.

7. To add AMA related policies, click **Edit Enterprise Policy**.

8. Configure as required. For details regarding AMA Policies, see [Android Management API policy.](#)

9. Click Save and Publish.

    The policy is updated successfully.

Editing the 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 apply the selected policy to more groups. You can also add the selected policy to the new groups and devices.

ℹ️ Note:

> If your device is enrolled using Android Management API, you can further edit the corresponding AMA policies through the Edit Enterprise Policy tab.

To edit the policy information, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, select **Profiles** > **Policies**.

2. On the Policies page, select a policy and then click the **Edit** icon. Select **Edit** > **Edit details**.

3. Edit the Policy Name and Description.

4. If you want to make this policy a default policy, select the **Default** check box. This default policy will be applied to all the newly added devices.

5. Click **Save**.

6. To apply the modified policy to a group, click the **Groups** tab and then click **Apply policy to**

groups.

7. The Apply Policy to Group list appears.

8. Select the groups to which you want to apply the policy and click **Add Group**.

9. The policies are applied to the groups.

10. You can further edit the policies through the **Edit Policy** and **Edit Enterprise Policy** tabs.

11. Click **Save and Publish** save the changes.
    Whenever you modify a policy, an updated version of the policy is created.

Policy Details

Normal policies are differentiated into different sections for better understanding such as Password, Policy for Device Applications, Policy for App Stores, Policy for Downloaded Apps, Policy for ADO enabled devices, and Policy for KNOX supported devices. The Android Management API (AMA) policies are differentiated into sections for All, Password Policy, Device Functionality, Device Location, Device Network, Keyguard Management and Device Sync & Storage.

EMM Policies

Sections	Description
All	This section shows all the policies available in Seqrite EMM. • 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. • **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.
Policy for Device Applications	▪ Lists the policies related to the device. You can turn on the policies as per your requirement.
Policy for App Stores	This policy lists the policies related to the device applications. You can turn on the policies as per your requirement.

Sections	Description
Policy for Downloaded Apps	This policy defines more about security of the downloaded apps. You can turn on the following policy as per your requirement.
Policy for ADO enabled devices	The ADO policy is applicable to those devices where Seqrite EMM Agent is the device user. • All the ADO policies are superscripted with "D" for easy identification. • This policy is applicable to the devices where the Seqrite EMM Agent is the device user. Also, check on the Seqrite EMM console the specific OS versions of the devices to which this policy can be applied.
Policy for KNOX supported devices	The KNOX policies are applicable to the Samsung KNOX-supported devices. • All the KNOX policies are superscripted with "K" for easy identification.

Seqrite EMM supports following policies:

Requires Password

This policy applies a screen lock and sets the password on the device. Different password types 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 does not apply this policy, the device will be shown as a 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-compliant device.

Password Age

To set the expiry age for the password, turn on the Age policy and then select the expiry age for the password such as 15 Days, 30 Days, 45 Days, and 90 Days.

This policy is dependent on the Requires Password policy. After the specified time expires, the user must reset a new 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, 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 Voice Dialing from Lock Screen

To block voice dialing, turn on the Block Voice Dialing on Lock Screen policy. After applying this policy on the device, the user will not be able to use voice dialing when the device is locked with a password.

This policy is dependent on the Require Password policy. This policy is applicable only to Supervised 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, 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.

i Note:

- o This policy is dependent on the Require Password policy.
- o This policy may or may not be applicable to some of the devices.
- o For ADO devices, this policy is applicable only to device OS versions 6 and later.
- o This policy is applicable to the non-ADO devices with OS 6 and earlier versions.
- o For Android 10 and above, the password policy will be applied only if ADO is enabled. Ensure that ADO is enabled before you apply the password policy.

Block Safe Mode

To restrict the access of 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 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, revoke the policy for that user.

If this policy is applied to the KNOX devices, those device users will not be able to access Safe Mode.

i Note:

- o To apply this policy, it is mandatory that the *Requires Password* type must be set to Medium or High.
- o For ADO devices, this policy is applicable only when the device OS version is 6 or later.
- o For non-ADO devices, this policy is applicable only when the device OS version is 6 or earlier versions.
- o 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.

i Note:

- o For Android 10 and above, the camera can be blocked only if ADO is enabled. Ensure that ADO is enabled before you apply the Block Camera policy.

Block Face Time

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

Block Factory Reset from Device Setting

This policy, if applied, disables the user from performing a Factory Reset on the device. The Restrict Factory Reset policy is applicable only to the devices where Seqrite EMM Agent is the Device user or to the Samsung KNOX supported devices or to the Supervised iOS devices.

> [i] Note:
>
> This policy is applicable to non-ADO Android devices with OS 6 or earlier versions.

Block Bluetooth

To block the usage of Bluetooth, turn on the Block Bluetooth policy. After applying this policy on the device, Bluetooth mode is disabled on the device.

The Block Bluetooth policy is applicable to KNOX devices and to Android ADO devices where Seqrite EMM Agent is the device user.

Block Configuring Bluetooth

The Block Configuring 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 ADO devices where Seqrite EMM Agent is the device user.

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 on the device.

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 use of mobile as a Hotspot, turn on the Block Mobile Hotspot policy. After applying this policy on the device, the user cannot switch on the mobile Hotspot.

> **ⓘ Note:**
>
> This policy is applicable only to the Samsung devices that support KNOX.

Block NFC

To block the usage of 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.

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:**
  >
  > o   This policy is applicable to Android devices.
  > o   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 the 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.

Block Screen Capture

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

[i] 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.

[i] Note:

This policy is applicable only to Android devices. However, this policy would not work on Android 10 and above.

Block iTunes App

To hide the iTunes app on the Supervised iOS devices, turn on the Block iTunes App policy. After applying this policy on the device, the user will not be able to view/access the iTunes app on the device.

Block App Store

To hide the app store on the Supervised iOS devices, turn on the Block App Store policy. The app store will be blocked, and the user will not be able to view/access anything 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.

> **i** Note:

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

Inactive 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 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, the device will go into 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 Seqrite EMM Agent is the device user, the device user would be able to turn it off, but within 30 seconds the auto time zone is turned on automatically by Seqrite EMM Agents.

Block Profile Switch

At times, the user may have multiple user profiles 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

With this policy, the user is forced (Strict) or notified (Notify) to apply the accessibility and app usage services within the defined time. The user can be forced or notified to apply for the services within the set number of days, hours, minutes, or seconds.

Block Accounts Modification

To restrict users from modifying any user profile, turn on the Block 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 to those devices where Seqrite EMM Agent is the device user or Supervised iOS devices or Knox supported devices.

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 Seqrite EMM Agent is the device user.

Block App Control

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

ⓘ Note:

This policy is applicable to the ADO supported devices where the Seqrite EMM agent is the device user.

Block Adding New User Profile

To restrict the user from creating a new user profile, turn on the Block Adding New User Profile policy. This policy is applicable to all ADO enabled devices.

Block deletion of user profile

To restrict the user from deleting any user profile, turn on the Block deletion of 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.

> ℹ️ Note:
>
> This policy is applicable to both, the KNOX Samsung devices and ADO supported devices where the Seqrite EMM Agent is the device user.

Block Configuring Mobile Data Setting

To restrict the user from configuring the mobile data on the device, turn on the Block Configuring Mobile Data Setting policy. This policy is applicable to the ADO enabled devices where Seqrite EMM Agent is the device user.

Block Outgoing Calls

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

Note:

This policy is applicable to both, Samsung KNOX and the ADO supported devices where the Seqrite EMM Agent is the device user.

Block Mounting Physical Media

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

Note:

This policy is applicable to the Samsung KNOX supported devices.

Wi-Fi On in Sleep Mode

To keep the Wi-Fi on even in sleep mode, turn on the Wi-Fi On in 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 the 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 Seqrite EMM Agent is the device user.

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.

![i] Note:

This policy is applicable to both, ADO and KNOX supported devices. For ADO devices, it is applicable where the Seqrite EMM Agent is the device user and OS of the device is Marshmallow (6.0) or later.

Block Cellular Data

To restrict the apps and services on user devices, 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 the Internet using Cellular Data.

![i] 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 users from creating the mock location of their device, turn on the Block Mock Location policy.

![i] 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 calls 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.

![i] Note:

This policy is applicable to the Samsung KNOX supported devices.

Block Notification on Lock Screen

When this policy is applied, the user will not be able to view the earlier notifications or today's events when device screen is locked. This policy is applicable only to the Supervised iOS devices.

Block Control Center on Lock Screen

To block the control center on the locked screen, turn on this policy. When this policy is applied, the device user will not be able to view the control center if the device screen is locked. You can apply this policy only to Supervised iOS devices.

Block Safari

To hide the Safari app on the user device, Seqrite EMM Admin can turn on the Block Safari policy.

Block App Uninstallation

To restrict the Seqrite EMM Agent uninstallation by any unauthorized user, turn on this policy. This policy is applicable only to the Supervised iOS devices.

Block iMessage

With this policy you can block the iMessages on Supervised iOS devices. The user will not be able to view any iMessages.

Block Apple Books

To block the Apple books on the supervised iOS devices, turn on the Block Apple Books policy. The user will not be able to access any Apple books on the device.

Block In-app Purchase

To restrict the user from making any in-app purchase from the device, turn on the Block in-app Purchase policy. The device user will not be able to perform any in-app purchase from the device. This policy is applicable only to the Supervised iOS devices.

Block Backup to iCloud

To restrict the user from automatically placing the device backup on iCloud, turn on the Block Backup to iCloud policy. This policy will put restrictions on iCloud functionality. You can apply this policy only to Supervised iOS devices.

i Note:

Policies superscripted with "**D**" and "**K**" alphabets are applicable only to the ADO enabled and KNOX-supported devices. Such policies are not applicable to non-ADO and non-KNOX devices.

Block Factory Reset from Device Setting

Allows you to block Factory reset from device setting. If this option is enabled from the Seqrite EMM console, the device user cannot do Factory reset.

i Note:

Policies superscripted with "**D**", "**K**", and "**S**" alphabets are applicable only to KNOX-supported Samsung devices, iOS Supervised devices, and Device Owner enabled devices.

Block USB Debug Mode

Allows you to restrict the device users from accessing the debug mode when the USB is connected to the system.

i Note:

Policies superscripted with "**D**" and "**K**" alphabets are applicable only to KNOX-supported Samsung devices and Device Owner enabled devices.

Factory Reset Protection

Factory Reset Protection (FRP) policy prevents anyone from using the device if it is factory reset by an unauthorized user. During the device setup (after factory reset) it requires the login credentials such as email address and passwords that were configured on the device. This means that if a device is lost or stolen, no one else will be able to reset or use it.

Moreover, if enterprise-managed devices are allotted to the employees for business usage, the devices are configured with email addresses of the employees. If the FRP has been enabled on the devices, it will prevent misuse of the device after factory reset.

In an organization, devices are allotted to different users based on requirement. For example, when an employee leaves the organization, the device is handed over to another employee for which the factory resetting would be required.

With FRP, the admin can select a Google account that can be used to activate the devices. This account can be associated with devices by enabling and publishing FRP policy.

After configuring FRP, you can provision the devices with personal Google accounts. However, when a factory reset is done even by hard reset, the devices can be activated only using the

Google account selected by the admin. This ensures the devices are always managed by the Seqrite EMM admin.

This policy is applicable for devices with 6.0 OS or later versions and provisioned as Device Owner.

To know how to map the corporate email address with Google Id, see our knowledge based article https://docs.seqrite.com/docs/seqrite-emm/self-help/managing-frp/.

Maximum Failed Password Attempt for Wipe

This option will erase the device if the maximum number of password attempts, as specified in the policy, is exceeded during the password reset process.

Delay Automatic OS updates

You can use this option to delay the updates of Android operating system by 30 days. If there is an update in the Android operating system and the users find the update not required immediately, they can delay the update by 30 days. However, the update cannot be delayed further.

For more information, see:

https://developer.android.com/work/dpc/system-updates

Android Management API (AMA) policy

i Note:

You need to configure normal policies before configuring AMA policies.

AMA Policies

Sections	Description
All	Lists all the AMA policies available in Seqrite EMM.
Password Policy	Lists the policies related to the password criteria. You can turn on the policies as per your requirement.
Device Functionality	Lists the device policies that can be controlled using AMA API for functions such as camera, audio, call, SMS and other settings.
Device Location	Lists the policies related to the device location.

Sections	Description
Device Network	Lists the policies related to device connectivity.
Keyguard Management	Lists the policies related to keyguard.
Device Sync & Storage	Lists the policies related to storage, debugging and file transfer.

Password type

This policy applies a screen lock and sets the password on the device. Different password types are specified. After applying this policy on the device, the user has to set the password as per the type of the applied password policy. If the device user does not apply the policy applied by the admin, the device will be shown as a non-compliant device.

The following are the available password policy options that you can set for the device user:

- **PIN/Password**: Set password with numbers for PIN or a combination of numbers, letters, and symbols.
- **Alphabetic**: Set password with at least one letter and a combination of numbers, letters, and symbols.
- **Alphanumeric**: Set password with at least one number and a combination of numbers, letters, and symbols.
- **Custom**: Set password as configured in the policy.

[i] Note:

Each time the admin changes the password type from lower to higher security level, the device user gets a notification and the apps are disabled until the user sets a new password that meets the conditions of the applied policy. Device users can access only Google, Phone and Play store apps. Refer the images.

Password Minimum Length

To set the length of the password, turn on the **Password Minimum Length** policy. This policy is dependent on the **Password type** 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 **PIN/Password**, then the password length must be between 4 to 16.
- If the password type is **Alphabetic**, then the password length must be in between 8 to 16.
- If the password type is **Alphanumeric**, then the password length must be in between 8 to 16.
- If the password type is **Custom**, then the password length must be between 8 to 16.

> **i** Note:
>
> The user must apply settings as per the applied policy. Otherwise, the device will be shown as Non-compliant device.

Minimum Letters

This policy is enforced only for Custom type password and specifies the minimum number of letters in the password.

Minimum Lower Case Letters

This policy is enforced only for Custom type password and specifies the minimum number of lower-case letters in the password.

Minimum Upper Case Letters

This policy is enforced only for Custom type password and specifies the minimum number of upper-case letters in the password.

Minimum Non-Letter Characters

This policy is enforced only for Custom type password and specifies the minimum number of non-letter characters (numbers or symbols) in the password.

Minimum Symbols

This policy is enforced only for Custom type password and specifies the minimum number of symbols in the password.

Minimum Numeric Characters

This policy is enforced only for Custom type password and specifies the minimum number of numerical digits in the password.

Password Age

To set the expiry age for the password, turn on **the Password Age** policy and then select the expiry age for the password such as 15 Days, 30 Days, 45 Days, and 90 Days.

This policy is dependent on the **Password type** policy. After the specified time expires, the user must reset a new password. Otherwise, the device will be shown as a non-compliant device.

Minimum Time To Lock

To lock the device automatically after a preset idle time, turn on the **Minimum Time To Lock** policy.

This policy is dependent on the **Password type** policy. After applying this policy on the device, if the device screen remains idle for the selected time, the device will be automatically locked. The time can be set to 1 min, 2 mins, 5 mins, 10 mins, and 15 mins.

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. You can save up to ten old passwords. The user will not be able to set a password that is already saved in the history. A value of 0 indicates that there is no restriction.

Camera Access

To allow or restrict camera usage, turn on the **Camera Access** policy and select the appropriate option as required.

- If the camera access is set to **User Choice**, then the user can access the camera.
- If the camera access is set to **Disabled**, then the camera access is blocked for the user.
- If the camera access is set to **Enforced**, then the user can access the camera.

Block Volume Button

To disable the volume adjustment done by the user, turn on the **Block Volume Button** policy.

Microphone Access

To allow or restrict microphone usage, turn on the **Microphone Access** policy and select the appropriate option as required.

- If the option is set to **User Choice**, then the user can mute or unmute the microphone.

- If the option is set to **Disabled**, then the user cannot unmute the microphone.
- If the option is set to **Enforced**, then user can unmute the microphone.

Block User Profile Icon

To restrict the user from changing the profile icon, turn on the **Block User Profile Icon** policy.

Block Wallpaper

To restrict the user from changing the wallpaper, turn on the **Block Wallpaper** policy.

Block Feature Access on Lock

To restrict the user from applying the keyguard features, turn on the **Block Feature Access on Lock** policy and select the appropriate options as required from the list.

Keep Screen On while Charging

To keep the device display on, during charging, turn on the **Keep Screen On while Charging** policy and select any one or all options from the list. The device display remains on during charging by the selected modes.

- If the option is set to **AC**, then the device display is on during charging by AC adapter.
- If the option is set to **USB**, then the device display is on during charging by USB port.
- If the option is set to **Wireless**, then the device display is on during by charging in wireless mode.

Block Creating Window

To block creation of windows other than app windows, turn on the **Block Creating Window** policy.

Block Factory Reset

To restrict the user from resetting the device to factory settings, turn on the **Block Factory Reset** policy.

Factory Reset Protection Admin Mail

To restrict the user from using any email account other than the admin, after factory reset, turn on the **Factory Reset Protection Admin mail** policy.

i Note:

Factory Reset Protection Admin Mail policy will not apply if the admin runs Wipe or Uninstall Device Management options from the Device Details page. The device then becomes a normal device without Android Enterprise Enrollment.

Block Outgoing call

To restrict the user from making outgoing calls, turn on the **Block Outgoing call** policy.

Block Outgoing SMS

To restrict the user from sending SMS, turn on the **Block Outgoing SMS** policy.

Block Mount physical media

To restrict the user from using physical media, turn on the **Block Mount physical media** policy.

Unknown sources installation

To control the installation from unknown sources, turn on the **Unknown sources installation** policy and select the required option.

- If the option is set to **Disallow untrusted app installation**, then installation from unknown sources is restricted.
- If the option is set to **Allow untrusted app installation**, then installation from unknown sources is allowed on the device.

Block Developer Options

To restrict the user access to the developer settings, turn on the **Block Developer Options** policy.

Block Location Sharing

To restrict sharing of the device location, turn on the **Block Location Sharing** policy.

Location Service (GPS)

To control the tracking of the device, turn on the **Location Service (GPS)** policy and select the required option.

- If the option is set to **User Choice**, then the location sharing depends on the user's selection.
- If the option is set to **Enforced,** then the device location sharing is always enabled.
- If the option is set to **Disabled**, then the device location cannot be shared.

Block Bluetooth

To restrict the use of Bluetooth on the device, turn on the **Block Bluetooth** policy.

Block Network Reset

To restrict the user from resetting the network, turn on the **Block Network Reset** policy.

Block Screen Capture

To restrict the user from taking screenshot on the device, turn on the **Block Screen Capture** policy.

Block Mobile Network Config

To restrict the user from changing network configuration settings, turn on the **Block Mobile Network Config** policy.

Block Config of Cell Broadcast

To disable wireless emergency alerts, turn on the **Block Config of Cell Broadcast** policy.

Block Wi-Fi Settings

To restrict the user from changing Wi-Fi configuration settings, turn on the **Block Wi-Fi Settings** policy.

Play Protect App Verification

To control the app verification process, turn on the **Play Protect App Verification** policy and select from the following required option.

- If the option is set to **Allows the user to choose whether to enable app verification,** then user can opt for app verification.
- If the option is set to **Force-enables app verification,** then the app verification is mandatory.

Block Auto Date & Time

To control the user from changing the date and time of the device, turn on the **Block Auto Date & Time** policy and select the required option.

- If the option is set to **Auto date, time and time zone** are left to the user's choice, then the user can change the date and time on the device.
- If the option is set to **Enforce auto date, time and time zone on the device**, then network timings are set on the device and user cannot change the date and time.

Block Tethering config

To control the use of the device as a Wi-Fi hotspot, turn on the **Block Tethering config** policy.

Block USB File Transfer

To restrict the file transfer from the device, turn on the **Block USB File Transfer** policy.

System Update Type

To control update install behaviour, turn on the **System Update Type** policy. The following options are available:

- **Automatic**: Set this option to automatically install updates as soon as they are available.
- **Windowed**: Set this option to install updates in the maintenance window.
- **Postpone**: Select this option to postpone automatic installation of updates by 30 days.

System Update Window Start Minutes

If the System Update Type is selected as Windowed, turn on the **System Update Window Start Minutes** policy and then set the start timings for the maintenance window between 0 and 1439 minutes after midnight.

System Update Window End Minutes

If the System Update Type is selected as Windowed, turn on the **System Update Window End Minutes policy** and then set the end timings for the maintenance window between 0 and 1439 minutes after midnight. If the specified time for the window is smaller than 30 minutes, then the time is automatically extended to 30 minutes beyond the start time.

Block Usage of Non-Compliance Devices After (days)

To block the devices automatically that do not comply with the policies after the specified days, turn on **Block Usage of Non-Compliance Devices After (days)** policy.

Wipe Non-Compliance Devices After (days)

To wipe the data on the non-compliant devices after the specified days, turn on the **Wipe Non-Compliance Devices After (days)** policy.

Block Accounts Modification

To restrict Google account additions to the device, turn on **Block Accounts Modification**. If enabled, the user cannot add another Google account to Play Store.

Configurations

Seqrite EMM provides the following configurations: Wi-Fi, Anti-Theft, Web Security, Schedule Scan, and Data Usage.

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 EMM console and in the left pane, select **Profiles** > **Configurations**.

2. On the Configurations page, click **Advanced Search**.

3. 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.

4. Click **Search**.

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

Taking an action for Configurations

The Take Action list appears when you select single or multiple configurations. The Take Action list for configurations is 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).

    o   Select **Delete** and then click **Submit**.

    o   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

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 Seqrite EMM console and in the left pane, click **Profiles** > **Configurations**.

2. On the Configurations page, select **Add Configuration > Wi-Fi**.

   The Add Wi-Fi Configuration page appears.

3. 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.

4. Select the security option and enter the password, and then click **Save**.

   The Wi-Fi configuration is applied successfully.

   [i] Note:

   WEP type is supported only on Android devices.

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

Editing Wi-Fi configuration

You can edit a Wi-Fi configuration and apply it to the devices.

Whenever you modify a configuration, a new version of the configuration is created.

To edit a policy, see Adding Wi-Fi Configuration.

   [i] Note:

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

Anti-Theft

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 apply it to the Android devices or iOS supervised devices.

Adding Anti-Theft Configuration

To apply Anti-theft configurations, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, select **Profiles > Configurations.**

2. On the Configurations page, select **Add Configuration > Anti-Theft**.

    The Create Anti-Theft Configuration page appears.

3. Enter the Configuration Name and the mobile number of the Admin and click **Add**.

    The mobile number is displayed in Admin Mobile Numbers list.

    i Note:

    In this section, you have to add contact numbers of the other Seqrite EMM 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.

    i 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.

    i Note:

    If the Lock device on Airplane Mode is applied, the lock screen appears.

6. If the SIM is changed, you can take appropriate action on the device. 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 appears. If required, you can select this option.

       The Lock device on SIM Change option is based on three categories:
       o   If the password is not set on the device, the device is blocked on SIM change.

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

> **Note:**
>
> To avoid blocking the device, ensure to apply the password on the device as per the policy.
>
> This action is not applicable for the iOS devices.

- **Notify admin on SIM Change**: If you enable this option, and the user of the device changes the SIM, a notification is sent to the alternate numbers (mentioned in anti-theft alternative contact number list) of the Admin. If the user of the device unlocks or unblocks the device within five minutes, 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.
>
> This action is not applicable for the iOS devices.

- **Block device on SIM Change**: When you select this option on the Seqrite EMM console 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.
>
> This action is not applicable for the iOS devices.

If you want to make this configuration a default one, select the **Default** check box. The default configuration will be applied to the newly added device automatically.

7. Click **Save**.

The Anti-Theft configuration is created successfully.

Editing Anti-Theft configuration

You can edit a configuration and apply the edited configuration to the devices.

Whenever you modify a configuration, a new version of the configuration is created.

To edit a policy, see [Adding Anti-Theft Configuration](#).

[i] Note:

To remove an Anti-Theft Configuration from any device, go to the Devices section and select the check box available in front of the device name and click Remove.

Web Security

The Web Security configuration helps you to restrict the Web access of the user's device by blocking website-based categories, blacklisting URLs, blacklisting 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 Android devices. You can easily create a few icons for your launcher by whitelisting the URLs for easy browsing.

[i] Note:

For iOS devices, you can only whitelist or blacklist the websites or use auto filter.

Adding Web Security Configuration

To create new Web Security configurations, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Profiles** > **Configurations**.

2. On the Configurations page, select **Add Configuration > Web Security**.

   The Create Web Security Configuration page appears.

3. Enter Configuration Name, select the Web security settings by selecting the Browsing Protection, Phishing Protection, and Web Protection check boxes.

   If you want to make this configuration a default one, select the **Default** check box. The default configuration will be applied to the newly added device automatically.

4. Click **Next**.

   The Web Security Configuration page appears.

   The Web Security Configuration page includes a list of security settings. Certain security settings are selected by default. However, you can modify the settings as per your requirement.

   [i] Note:

> To block all the URLs with the bad language and sexually explicit language on iOS devices, select the AutoFilter (applicable for iOS devices only) check box.

5. Click **Next**.

   The Blacklist/Whitelist URLs page appears.

6. Enter a URL in the Enter Keyword or URL to filter web access field and click Add.

   By default, the keyword or URL gets added to the Blacklist. However, you can move the blacklisted URL into the whitelist or vice-versa by double-clicking 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**.

   - To whitelist URLs and display them in the form of icons on the launcher, select the **Create Icon on the Launcher for Whitelisted URL** check box. This helps easy browsing of the links without adding them to the browser.

7. Click **Save**.

   Web Security Configuration is created successfully.

   i Note:

   > On the Android device, the Web Security configuration will work only on the Google Chrome browser.

   > The Web Security configuration will work only on the supervised iOS devices.

Editing Web Security Configuration

You can edit a Web Security configuration and apply it to the devices.

Whenever you modify a configuration, a new version of the configuration is created.

To edit a policy, see [Adding Web Security Configuration](#).

Applying Web Security configuration to the devices

To apply configurations on the device, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, select **Profiles** > **Configurations**.

2. On the Configurations page, select the Web Security configuration and click the **Edit** icon.

Click the **Edit** tab and then navigate to the **Devices** tab.

3. Click Apply configuration to device.

The Add device to group list appears.

4. Select the devices to which you want to apply the configuration and click the **Add Devices** button.

The Web security configuration is applied successfully.

🔲Note:

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

Schedule Scan

With the Schedule Scan option, you can scan all the enrolled devices of Seqrite EMM 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 EMM Agent only when the device is connected to the Wi-Fi.

If the "Update Virus definition database on Agent 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 EMM 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 Agent 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 Seqrite EMM console and in the left pane, click **Profiles** > **Configurations**.

2. On the Configurations page, select **Add Configuration > Schedule Scan**.

3. On the Create Schedule Scan Configuration page, 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 EMM Agent app when connected to Wi-Fi check box to update the virus definition database using the available Wi-Fi.

> **i** Note:
>
> ---
>
> If the Update Virus definition database on Agent app via Wi-Fi only check box is not selected on the Seqrite EMM console, then the virus definition database on the Agent app will be automatically updated when the device gets connected to the Internet.
>
> The Schedule Scan configuration is not applicable for the iOS devices.
>
> ---

6. Click **Save**.

   The schedule scan is configured successfully.

Editing Schedule Scan Configuration

You can edit a scan schedule and apply it to the devices.

Whenever you modify a configuration, a new version of the configuration is created.

To edit a policy, see [Adding Schedule Scan configuration](#).

> **i** Note:
>
> ---
>
> To remove a scan scheduled from any device, go to the Devices section and select the check box available in front of the device name and click Remove.
>
> ---

Data Usage

With the Network Usage configurations, you can monitor the Internet data usage with respect to Wi-Fi, Mobile Data, and 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 the Internet across all the devices enrolled with Seqrite EMM. You can monitor mobile data usage and Wi-Fi usage (Seqrite EMM 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 across Seqrite EMM network.

Adding Data Usage configuration

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

1. Log on to Seqrite EMM console and in the left pane, click **Profiles** > **Configurations**.

2. On the Configurations page, select **Add Configuration > Data Usage**.

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 data usage 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.

5. Click **Save**. The network usage setting is configured successfully.

Note:

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

The Network Usage configuration is not applicable for the iOS devices.

Editing Data Usage Configuration

You can edit the data usage configuration and apply it to the devices.

Whenever you modify a configuration, a new version of the configuration is created.

To edit a policy, see [Adding Data Usage configuration](#).

Note:

To remove the data usage setting from any device, go to the Devices section and select the check box available in front of the device name and click **Remove**.

Apply Data Usage to Group or Device

To apply the data usage policy, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Profiles** > **Configurations**.

2. On the Configurations page, select the configurations that you want to apply to a group or

device. The Take Action list appears.

3. From the Take Action list, select **Apply to Groups** or **Apply to Device** as per requirement.

   ▪ If you select Apply to Groups, a list of all groups appears. Select the groups and then click **Apply**.

   ▪ If you select Apply to Device, a list of all devices appears. Select the devices and then click **Apply**.

4. On confirmation dialog box, click **OK**.

12.Workspace

Workspace policies and profiles are applicable only to the Seqrite Workspace installed on users' devices. The policies are basically about the Workspace-provided corporate apps such as email, browser, contacts, file manager, camera, note, text editor and calendar.

The Workspace policies and profiles can be assigned to the group and manage the devices in that group. These policies and profiles can be assigned to multiple groups also to secure the devices from losing the crucial information.

The secure Workspace, with policies, allows the Seqrite Administrator to share documents, audio-video files etc. to their employees without the risk of data breach.

Advanced Search for Workspace Policies

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

1. Log on to Seqrite EMM console and in the left pane, select **Workspace** > **Policies**.

2. On the Workspace Policies page, click **Advanced Search**.

3. From the Select Created By list, select the desired creator name and click **Search**.

    The search result gets displayed.

Taking an action for Workspace Policies

The Take Action list appears on the Workspace Policies list page when you select a policy. The Take Action list includes the following options:

*   **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 a copy of multiple policies.

*   **Delete**: Helps you to delete single or multiple selected policies.

    i Note:

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

*   To take an action, select the required option from the list and click **Submit**.

Adding a Workspace Policy

To create a new Workspace policy, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, select **Workspace** > **Policies**.

2. On the Workspace Policies page, click **Add Workspace Policy**.

3. Enter Policy Name and Description.

   If you want to make this policy a default one, select the **Default** check box. The default policy is applied to the newly added device automatically.

4. Click **Next** to apply the policies.

   The policy setting page appears.

5. The Edit Policy tab includes different policies divided into sections. Navigate to the required section and select the required policy components. To enable a policy, click on the red circle. This policy gets active and applies restrictions on the device.

   To get complete information of the policy from already created policies, select the policy from the **Inherit From** list.

6. Click Save and Publish.

   New policy is created successfully.

Editing the Workspace Policy

You can edit a Workspace policy as per requirement and apply the policy to a group.

To edit a policy, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, select **Workspace** > **Policies**.

2. On the Workspace Policies page, click the **Edit** icon.

3. To edit the policy name, description, and apply the policy to a group, click the **Edit** tab.

4. To modify the policy settings, click the **Edit Policy** tab.

   A policy is divided into different sections. Visit each section and turn on the required policy and choose the required options.

5. Click Save and Publish.

   The policy name appears.

6. Enter the comments as required in the description text field and click **Confirm**.

   Note:

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

Workspace Policies

Workspace policies include all the policies that can be applied to Workspace to access and manage the Workspace components. The policies are categorized into different sections of the container such as application access, policies related to container, browser, email, password, calendar, contacts, and vault.

Application Access

This policy is created to provide access and manage all the applications added to Seqrite Workspace. As an Administrator, you can enable or disable the use of such applications according to the organization strategy. This policy can be applied to both, Android and iOS devices. You can apply policies on applications such as email, browser, file manager, camera, contacts, and so on. The components of application access policy are as follows:

Sr. No.	Policy	Description
1	Enable Email App	Helps you to provide access to the email application on the Workspace.
2	Enable Browser App	Helps you to provide access to the assigned browser inside the Workspace.
3	Enable Vault App	Helps you to provide access to the secure folder inside the Workspace.
4	Enable Camera App	Helps you to provide access to the camera application.
5	Enable Notes App	Helps you to provide access and use the note application when working in Workspace environment.
6	Enable Text Editor App	Helps you to provide access to the authorized text editor to be used inside Workspace.
7	Enable Contacts App	Helps you to provide access to the user's corporate email contacts list.
8	Enable Calendar App	Helps you to provide access to the Outlook calendar events so that the user remains up to date with the day-to-day calendar events.

Container policy

This policy is applicable to both Android and iOS devices with Seqrite Workspace container. With this policy, you can access or apply restrictions on the container itself.

Sr No.	Policy	Description
1	Access Workspace Offline	Helps you to give access to the user to access the Workspace even in offline mode.
2	Workspace Lockout Time	Helps you to enable or disable this functionality and set the lock time of Workspace if the app remains inactive for that set period.
3	Lock Workspace App in the Background	Helps you to lock the Workspace in the background.
5	Time-Bomb Period (days) to Wipe Workspace	Helps you to enable or disable the auto wipe functionality of Workspace to delete all its data in set number of days. You can add the number of days in between 1 to 999.
6	Allow Clipboard	Helps you to enable or disable the use of clipboard functionality (cut-copy-paste) inside the Workspace.
7	Allow Screen Recording	Note: This policy is applicable only for iOS devices. Helps you to capture your device's screen activity including any apps, games, or videos you may be playing.

Browser Policy

This policy is applicable to the default browser of the Workspace that can be applied to the Android and iOS devices. Different components of browser policy are as follows:

Sr. No.	Policy	Description
1	Set Default Home Page	Helps you to enable or disable the functionality to change or add the default browser to be used inside the Workspace. If this policy is enabled, then the device user can access only the defined browser.
2	Allow Unsecure (http) URLs	Helps you to enable or disable the functionality to access the unsecure (http) URLs through Workspace browser.
3	Allow File Upload	Helps you to enable or disable the functionality to upload the file through Workspace browser.
4	Allow File Download	Helps you to enable or disable the functionality to download the file through Workspace browser.
5	Allowed File Formats for Download/Upload	Helps you to add file extensions that you can allow the user to upload or download from Workspace browser. If this option is not enabled, then the device user can access any type of files through Workspace browser.
6	Enable Privacy and Security Settings	Helps you to enable or disable the privacy and security settings of Workspace. If this option is enabled, then the device user can make changes to the browser settings.
7	Allow Screenshots on Browser App	Helps to enable or disable the functionality to take a screenshot of Workspace browser.

Email Policy

With this policy, you can apply different strategies and control the organizational emails. You can manage different email components such as account type, attachments and its file type or the size and so on with this email policy.

Sr. No.	Policy	Description
1	Email Account Type	Helps you to enable or disable the functionality to select the email account type for Workspace. By default, Seqrite provides Outlook, GSuite, IMAP/POP email accounts.
		Thus, you can select your respective corporate Outlook or GSuite account. If you set this account and enable it, the device user must configure the same email account to access through Workspace.
2	Allow Email Attachments	Helps you to enable or disable the functionality to share email attachments through Workspace.
		If this option is enabled, the device user can share the email attachments and if it is not enabled, the device user cannot share any email attachments.
3	Enlist File Formats for Outgoing Email Attachment	Helps you to enable or disable the functionality to define the attachment file types that can be shared through Workspace email account. This component is dependent on the Allow Email Attachment component, if it is enabled, only then you can access this policy.
		If this option is not set, the user can share any type of file as an attachment.
4	Allow Attachment from outside Workspace	Helps you to enable or disable the functionality to share the attachment from different options other than Workspace.
		If this option is not enabled, the device user can share the attachments only through Workspace.
5	Enlist Domains for Outgoing Emails	Helps you to enable or disable the functionality to set the corporate domains to which the device user can send the emails through Workspace.
		If this option is disabled, the device user can send emails to any domain.
6	Allow Maximum Size Limit for Download (MB)	Helps you to enable or disable the functionality to set the maximum downloadable size of the attachment in MB. Any attachment exceeding the maximum downloadable value will not be downloaded.
		If this option is disabled, the device user can download email attachment of unlimited file size.
7	Shows BCC Field in Emails	Helps you to enable or disable the functionality to show the BCC option in the email. If this option is enabled, only then the BCC option is visible while composing email through Workspace. If this option is disabled, BCC option will not be visible.
8	Allow Screenshots on Emails App	Helps you to enable or disable the functionality to take screenshot of the emails received in Workspace.

Password Policy

To access Workspace, you require a password. Thus, password policy helps you to manage the Workspace password. You can set minimum password length or expiry days and so on. Depending on the defined password policy, the device user can view the password fields and will be restricted to use the defined password type.

Sr No.	Policy	Description
1	Password Strength	This option helps you to set the password strength for device users. If you set PIN, moderate, or strong, accordingly the device user will be able to set the password for Workspace.
		PIN: The user can set Pattern, PIN or password. The user can set the password of 4-digit numeric PIN. This is a less secure option.
		Moderate: The user can set the password of 6 or more alphanumeric (UPPER case) characters. This is a secure option.
		Strong: The user can set the password of 8 or more characters including UPPER or lower case, number, and symbols.
2	Minimum Length for Password	This policy depends on the Password Strength policy. If you have defined PIN, moderate, or strong, then accordingly 4, 6, 8 text fields will be displayed on the device.
3	Password Expiry (days)	Helps you to set the password expiry days for Workspace and enable or disable this functionality.
4	Enable Touch ID	Helps you to enable or disable the Touch ID functionality. It forces the user to user the same fingerprint to login to the mobile device and Workspace.
5	Account Lockout Threshold for Invalid Logon	Helps you to enable or disable the functionality to set the value for invalid logon attempts to Workspace. If the user exceeds this invalid logon attempts, then the Workspace gets locked for the defined time of 30 minutes.

Calendar Policy

With this policy, you can apply this policy to the Workspace calendar app.

Sr. No.	Policy	Description
1	Allow Screenshots on Calendar App	Helps you to enable or disable the functionality to take screenshot of the Workspace calendar app.

Contact Policy

With this policy, you can apply policy on the Workspace contacts.

Sr. No.	Policy	Description
1	Allow Screenshots on Contact App	Helps you to enable or disable the functionality to take the screenshot of the contacts available in the Workspace.

Vault Policy

With this policy, you can apply policy on the Workspace vault.

Sr. No.	Policy	Description
1	Allow Screenshots on Vault App	Helps you to enable or disable the functionality to take the screenshot of the Workspace vault.

Profiles

The Profiles section of Workspace helps you to restrict the Web access of the user's device by blacklisting URLs, blacklisting certain URLs of a website irrespective of the domain, blacklisting or whitelisting keywords. If any keyword or URL is blacklisted, it will not be accessible through the Workspace browser. But if any keyword or URL is whitelisted, it will be accessible through the custom browser.

Note:

For iOS devices, you can only whitelist or blacklist the websites or use auto filter.

Advanced Search for Workspace Profiles

This search option allows you to perform an advanced search for different Workspace profiles. To search profiles, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, select **Workspace** > **Profiles**.

2. On the Workspace Profile page, click **Advanced Search**.

3. From the Select Created By list, select the desired creator name and click **Search**.

    The search result gets displayed.

Take an action for Workspace Profiles

The Take Action list appears on the profiles list page when you select single or multiple profiles. The Take Action list shows the following option:

- **Delete**: Helps you to delete single or multiple selected Workspace profiles.

    ![i] Note:

    You cannot delete a Workspace profile which has a group assigned to it.

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

Adding a Workspace Profile

This section helps you to create a new Workspace profile on the devices where you can configure the Web/App access policy. You can enable the device users' access certain URLs on the Workspace app browser or block them as required. You can apply Workspace Profile Restrictions and have Application Management in Work Profile.

To create Workspace profile, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, select **Workspace** > **Profiles**.

2. On the Create Workspace Profile page, click **Add Workspace Profile**.

3. Write the **Profile Name** and add a description in the text field and click **Next**.

4. In the Website filtering section, enter the keyword or URL to filter the Web access, and click **Add**. Click **Next**.

    The keyword or the URL entered is added under the Blacklisted URLs/Keywords section.

    - To remove the blacklisted URL or keyword from the list, click the multiplication sign.

    - To whitelist all the blacklisted URL or keywords, click **Whitelist All**.

    - To block access to all URLs except the ones you allowed in whitelist, select the check box.

5. In the Workspace Profile Restrictions section, enable or disable the restriction policy and then apply the following restrictions. Click **Next**.

    - Allow Screen Capture in Work Profile

- Allow Copy/Paste from other profiles

- Allow Camera in Work Profile

- Allow App installation from unknown sources

- Allow App Installation in Work Profile

- Allow App Un-installation in Work Profile

- Enable App Control in Work Profile

- Enable Password Protection in Work Profile

6. In the Workspace App Management section, set the delivery method on how the apps will be shared such as On Demand or Auto.

   You can push corporate-approved apps in Work Profile by selecting Apps from App store. If you need to push an app in Work Profile that is not available in the App Store, you can add a new app in the App Store.

7. Click **Save**.

Workspace Profile Restrictions

Workspace Profile Restrictions include all the restrictions that can be applied to Workspace.

Sr. No.	Policy	Description
1	Allow Screen Capture in Work Profile	Allows you to capture screenshots in Work Profile.
2	Allow Copy/Paste from other profiles	Allows you to copy/paste from other profiles to Work Profile.
3	Allow Camera in Work Profile	Allows camera usage in Work Profile.
4	Allow App installation from unknown sources	Allows you to install apps from unknown sources.
5	Allow App Installation in Work Profile	Allows you to install apps in Work Profile.
6	Allow App Un-installation in Work Profile	Allows you to uninstall apps from Work Profile.
7	Enable App Control in Work Profile	Allows controlling of apps in Work Profile.
8	Enable Password Protection in Work Profile	Implements password protection to Work Profile. If password protection is implemented, you can password-protect Work Profile.
9	Block Printing	Restricts to print from a particular device. Need to update the policy and push it to that device.

Workspace App Management

In this section, you can ship the apps to the device either on demand or automatically. You can add the apps from App Store and push the apps to the devices or even suggest other apps to the device users.

Work Profile App Management

In this section, you can install or uninstall the apps to the device either on demand or automatically. You can also add the apps from App Store, push the apps to the devices or even recommend apps to the device users.

Adding Apps to Work Profile

1. Login to Seqrite EMM console using your credentials.
2. Navigate to **Workspace > Profiles > Edit**.
3. On the Workspace Profiles Details page, click **Work Profile App Management**.
4. Click **Add Apps**. The Android Management Apps dialog is displayed. You can also add custom .apk through the Private Apps option.
5. Select the app and click Select. for e.g. Outlook. The App permission dialog is displayed.
6. On the App Permissions dialog, select **Install Silently** if you do not want any user intervention and app to be installed automatically on device. If the **Install Silently** option is not selected, the app is just downloaded on the enrolled device and user has to install it manually.
7. Click **Ok**.
8. Click **Save**. The app is downloaded and installed on the enrolled device.

Uninstalling/Removing apps

1. Logon to Seqrite EMM console using your credentials.
2. Navigate to **Workspace > Profiles > Edit**.
3. On the Workspace Profiles Details page, click **Work Profile App Management**.
4. In the **Install Apps** section, select the app that you want to remove. The Remove button is displayed.
5. Click **Remove**.
6. Click **Ok** on the confirmation box. The App is removed from the device.
7. You can also go to the **Uninstall Apps**, click Add App. Select and add the app to the Uninstall List.
8. Save the configuration. The app will be removed from the Work Profile.

Note: If admin adds any app in uninstall list, then this app will not be visible in PlayStore even if PlayStore mode policy is on.

iOS Work Profile App Management

In this section, you can add apps to the work profile. You can also add the apps from App Store, push the apps to the devices or even recommend apps to the device users.

Adding Apps to Work Profile

1. Login to Seqrite EMM console using your credentials.
2. Navigate to **Workspace > Profiles > Edit**.
3. On the Workspace Profiles Details page, click **iOS Work Profile App Management**.
4. Click **Add Apps**. Add iOS Apps to Container dialog is displayed. You can also add custom. ipa through the Private Apps option.
5. Select the app and click **Add Apps.**
6. Click **Save**. The app is downloaded and installed on the enrolled device.

Adding New Application to App Store

You can add a new iOS app to the app store. This helps you whenever you want to recommend the app in case the app is not present in the app store.
Seqrite Enterprise Mobility Management provides the following options to add apps to the App store:
- iTune Store
- Enterprise App for iOS

Adding Apps Using iTunes Store

1. Login to Seqrite EMM console using your credentials.
2. Navigate to **Workspace > Profiles > Edit**.
3. On the Workspace Profiles Details page, click **iOS Work Profile App Management**.
4. Click **Click here**.
5. Click **iTune Store**.
6. Enter iTunes Store URL of the app in the given text box. The URL format must be as per the given example in the dialog box.
7. Click **Add**.

Adding Enterprise App for iOS

1. Login to Seqrite EMM console using your credentials.
2. Navigate to **Workspace > Profiles > Edit**.
3. On the Workspace Profiles Details page, click **iOS Work Profile App Management**.
4. Click **Click here**.
5. Click **Enterprise App for iOS**.
6. Enter App Name, Package Id, Version Name, Version Code, and custom IPA
7. Select the .ipa file that you want to add to the app store.
8. Click **Upload**.

Restrictions on iOS Managed Apps

There are few restrictions that can be applied to iOS managed apps.

Sr. No.	Restriction	Description
1	Allow data to export from Managed to unmanaged	Allows you to restrict a user's personal sources and accounts from opening documents in your organization's managed destinations.
2	Allow data to import from unmanaged to Managed	Allows you to prevent an organisation's managed sources and accounts from opening documents in a user's personal destinations.
3	Allow unmanaged apps to read managed contacts	Allows unmanaged app apps to read the contact of the managed app
4	Block Sharing Managed Document using AirDrop	Allows you to restrict user from sharing managed document with other nearby iOS device using AirDrop
5	Allow Remove of managed apps on MDM Removal	Allows you to restrict user from removing any app from the managed apps.
6	Restrict Apps uninstallation	Allows you to restrict the user from uninstalling any app
7	Restrict Data Backup to iTunes	Allows you to restrict user from backing up data to the iTunes
8	Allow Managed apps cloud sync	Allows user to sync device data with iCloud.

Personal Space App Management

In this section, you can ship the apps to the device either on demand or automatically. You can add the apps from the App Store and push the apps to the devices or even suggest other apps to the device users.

Note: Apps can be silently installed in the workspace but not in the personal space of the device.

Adding Apps to Personal Space

1. Login to Seqrite EMM console using your credentials.
2. Navigate to **Workspace > Profiles > Edit**.
3. On the Workspace Profiles Details page, click **Personal Space App Management**.
4. Click **Add Apps**.The **Android Management Apps** dialog is displayed. You can also add custom .apk through the Private Apps option.
5. Select the app and click **Select**. for e.g. Outlook. The App permission dialog is displayed.
6. Click **Save**. The app is downloaded and installed on the enrolled device.

Uninstalling/Removing apps

Device user can not install app added in uninstall app list in the personal space. If the app is already present/installed before, it will be removed from personal space.
To uninstall the app from personal space, follow these steps:

1. Logon to Seqrite EMM console using your credentials.
2. Navigate to Workspace > Profiles > Edit.
3. On the Workspace Profiles Details page, click Personal Space App Management.
4. In the Install Apps section, select the app that you want to remove. The Remove button is displayed.
5. Click Remove.
6. Click Ok on the confirmation box. The App is removed from the device.
7. You can also go to the Uninstall Apps, click Add App. Select and add the app to the Uninstall List.
8. Save the configuration. The app will be removed from the personal space.

Note: If admin adds any app in uninstall list, then this app will not be visible in PlayStore even if PlayStore mode policy is on.

Edit Work Profile Restrictions

Managing Policies

1. Logon to Seqrite EMM console using your credentials.
2. Navigate to Workspace > Profiles > Edit Work Profile Restrictions.
3. Configure the policies under the sections as required.
4. Click Save and Publish. The policies are pushed to the enrolled devices

Android Management API (AMA) policy options

Note: You need to configure normal policies before configuring AMA policies**.**

Work Profile Policies

Section	Description
All	Lists all the AMA policies available in Seqrite EMM.
Password Policy	Lists the policies related to the password criteria. You can turn on the policies as per your requirement.
Work Profile Functionality	Lists the policies for Work Profile Functionality
Policy Compliance Enforcement	Lists the policies for company compliance

All the policy restrictions are applied at the Work Profile level only.

Password Policy

This policy applies a screen lock and sets the password on the device. Different password types are specified. After applying this policy on the device, the user has to set the password as per the type of the applied password policy. If the device user does not apply the policy applied by the admin, the device will be shown as a non-compliant device.

Password Type

This policy applies a screen lock and sets the password on the device. Different password types are specified. After applying this policy on the device, the user has to set the password as per the type of the applied password policy. If the device user does not apply the policy applied by the admin, the device will be shown as a non-compliant device.

The following are the available password policy options that you can set for the device user:

- **PIN/Password**: Set password with numbers for PIN or a combination of numbers, letters, and symbols.

- **Alphabetic**: Set password with at least one letter and a combination of numbers, letters, and symbols.

- **Alphanumeric**: Set password with at least one number and a combination of numbers, letters, and symbols.

- **Custom**: Set password as configured in the policy.

Note: If admin selects a higher password criterion and then device user cannot set a lower password as device has higher password criteria.
If the user has set a password to device, then even if Admin unchecks the password policy, password will not be removed until work profile is uninstalled.

Password Minimum Length

To set the length of the password, turn on the **Password Minimum Length** policy. This policy is dependent on the **Password type** 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 **PIN/Password**, then the password length must be between 4 to 16.

- If the password type is **Alphabetic**, then the password length must be in between 8 to 16.

- If the password type is **Alphanumeric**, then the password length must be in between 8 to 16.

- If the password type is **Custom**, then the password length must be between 8 to 16.

Note: The user must apply settings as per the applied policy. Otherwise, the device will be shown as Non-compliant device.

Password Age

To set the expiry age for the password, turn on **the Password Age** policy and then select the expiry age for the password such as 15 Days, 30 Days, 45 Days, and 90 Days.

This policy is dependent on the **Password type** policy. After the specified time expires, the user must reset a new password. Otherwise, the device will be shown as a non-compliant device.

Maximum Time To Lock

To lock the device automatically after a preset idle time, turn on the **Maximum Time To Lock** policy.

This policy is dependent on the **Password type** policy. After applying this policy on the device, if the device screen remains idle for the selected time, the device will be automatically locked. The time can be set to 1 min, 2 mins, 5 mins, 10 mins, and 15 mins.

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. You can save up to ten old passwords. The user will not be able to set a password that is already saved in the history. A value of 0 indicates that there is no restriction.

USB Data Access

To restrict the files/data transferred via USB turn on this policy and select the required option.

- If the User Data Access set to **Unspecified** then nothing is specified yet.

- If the User Data Access set to **Allow USB Data Transfer** then user can transfer the data through USB.

- If the User Data Access set to **Disallow USB Data Transfer** then user can not transfer the data through USB.

- If the User Data Access set to **Disallow USB file Transfer** then user can not transfer the file through USB.

Configure Wifi

To allow or restrict the user to configure the wifi turn on this policy and select the required option.

- If the Config Wifi set to **Allow Config Wifi** then user can not configure the wifi.

- If the Config Wifi set to **Disallow Add Config Wifi** then user can not edit the wifi configuration.

- If the Config Wifi set to **Disallow Config Wifi** then the user can not configure the wifi.

Work Profile Functionality

Camera Access

To allow or restrict camera usage, turn on the Camera Access policy and select the appropriate option as required.

- If the camera access is set to **User Choice**, then the user can access the camera.

- If the camera access is set to **Disabled**, then the camera access is blocked for the user.

- If the camera access is set to **Enforced**, then the user can access the camera.

Unknown sources installation

To control the installation from unknown sources, turn on the **Unknown sources installation** policy and select the required option.

- If the option is set to **Allow untrusted app installation in personal profile**, then installation from unknown sources is allowed on the personal profile.

Note: Unknown source installation in work profile is not allowed.

Block Screen Capture

To restrict the user from taking screenshot on the device, turn on the **Block Screen Capture** policy.

Play Protect App Verification

To control the app verification process, turn on the **Play Protect App Verification** policy and select from the following required option.

- If the option is set to **Allows the user to choose whether to enable app verification,** then user can opt for app verification.

- If the option is set to **Force-enables app verification,** then the app verification is mandatory.

Block Accounts Modification

To restrict Google account additions to the device, turn on **Block Accounts Modification**. If enabled, the user cannot add another Google account to PlayStore.

Cross Profile Data Sharing

- If **Cross Profile Data Sharing disallowed** is turned on, data cannot be shared from personal to work profile and from work profile to personal.

- If **Data Sharing Work to Personal disallowed is turned on,** data sharing from work profile to personal is not allowed and personal to work profile data sharing is allowed.

- If **Cross Profile Data Sharing allowed** is turned on, data can be shared from personal to work profile and from work profile to personal.

Cross Profile Copy Paste

- If **Allowed** option is turned on, you can copy/paste from work profile to personal and personal to work profile.

- If **Disallowed** option is turned on, you cannot copy/paste from work profile to personal or personal to work profile.

Show Contact in Personal Profile

- If **Disallowed** option is turned on, work profile contacts are not visible

- If **Allowed** option is turned on, work profile contacts are visible.

Play Store Mode

- If Play Store Mode option is turned On, Play Store apps are displayed.

- If Play Store Mode option is turned Off, only pushed apps are displayed.

Block Printing

To restrict the data printing from work profile, turn on this policy.

Camera disabled

To disable the camera of the device, turn on this policy.

Max Days With Work Off

To set the number of days to pause the user's work, profile turn on this policy.

Note: Minimum number of days are 3 days.

Installed App Disabled

To disable the app installation in work profile, turn on this policy.

Mount Physical Media Disabled

To disable the mounting of external physical media, turn on this policy.

Uninstall Apps Disable

To disable the app uninstallation from work, profile turn on this policy.

Outgoing Calls Disabled

To disable the outgoing call from work profile, turn on this policy.

Policy Compliance Enforcement

Block Usage of Non-Compliance Devices After (days)

To block the devices automatically that do not comply with the policies after the specified days, turn on **Block Usage of Non-Compliance Devices After (days)** policy.

Wipe Non-Compliance Devices After (days)

This is a dependent policy. The Work profile will be wiped out automatically from the non compliance devices.

Editing Workspace Profile

You can edit a Workspace profile and apply it to the devices.

Whenever you modify a profile, a new version of the configuration is created.

To edit a profile, see Adding a Workspace Profile.

Workspace Agent

Workspace is a containerized application on the user's mobile device that gives them access to the corporate applications, email, access files and services they need to do their job. A Workspace separates work apps and data from personal apps and data. Your organization manages your work apps and data while your personal apps, data, and usage remain private.

To make Seqrite Workspace available on your users' mobile devices, you (admin) need to setup the Workspace agent on the users mobile devices.

The user cannot copy the data from work profile to personal profile and from personal profile to work profile as per the policy set in Workspace Profile Restrictions. See Workspace Profile Restrictions.

Prerequisite: You need to activate the Workspace feature on the EMM console by navigating to Workspace before you can start using Workspace.

The agent can be installed on the user mobile devices in two ways:

- You can push the Workspace agent to the mobile device through EMM console (Enrollment)

- If the app is not downloaded automatically, the mobile user can download the Workspace app from Seqrite app store.

Workspace Enrollment through EMM console

There are various ways devices can be enrolled for using Workspace with Seqrite EMM.

- **Workspace without Device Management**

    You can avail of Seqrite Workspace directly without opting for device management.

    To enroll devices, follow one of the steps as required,

    o User > Select User > Take Action > Enrollment Request > Select Workspace without Device Management > Select Enrollment using Email/SMS or using QR Code.

    o Devices > Select Device > Take Action -Enrollment Request >Workspace without Device Management > Select Enrollment using Email/SMS or using QR Code > Submit.

    o Groups > Select a Group > Bulk Enrollment > Enrollment Preference > Workspace without Device management

- **EMM for Device Management**

    A user device enrolled by EMM for Device Management can avail Workspace, through any of the following steps:

- o Devices > Select Device > Edit > Workspace > Select an action > Workspace Enrollment Request > Submit.

- o Devices > Select Device > Take Action - Workspace Action > Workspace Enrollment Request > Submit.

- o Groups > Select Group > Take Action – Workspace Action > Workspace Enrollment request > Submit.

Activating Workspace app on enrolled device

After enrolling the device through the EMM console, Workspace app is downloaded on user device.

To activate Workspace, follow these steps:

1. Tap **Workspace** app on your device.
   Work Profile is created on your device.

2. A partition with two different spaces is created on the device. For example, Personal Profile and Work Profile.

3. Navigate to **Work Profile** and tap **Work Profile**.

4. Tap **Workspace** app that is created inside the Work Profile.

   A prompt appears asking you to uninstall the Workspace app in the Personal Profile.

5. Set the password for **Workspace app** and **Work Profile** app.

   Note: Admin needs to apply necessary password policies before the user can set the password. For more details, see Password Policy.

Workspace Applications

After the Workspace is activated through the EMM console, admin can setup the applications that will be available on Workspace app on device.

The following applications are available in Workspace:

1. **Email**

   Admin can setup one of the email clients from the following:

   - o Outlook
   - o GSuite
   - o IMAP
   - o POP

Admin can set the Email policy for the users' device. For more details, see [Email Policy.](#)
User can access the inbox, search, delete, edit and send emails.

Email search option is now available for iOS clients (Outlook & Gmail).

2. **Browser**

Admin can set the Browser policy to users' device and set the default home page. Users can use the browsers as per the policies passed by the admin. For more details, see [Browser Policy.](#) The following actions are available:

- o Download and upload files
- o Access websites
- o Filter by Websites

3. **Vault**

Vault is like a protective folder for user's data. However, the admin can wipe data in the users vault through a policy. For more details, see [Vault Policy.](#)

Users can store the following file types in the vault:

- o Documents
- o Applications
- o Images
- o Audio
- o Video
- o Broadcast (Bulk message Files)
- o Others (All other file formats)

4. **Camera**

Admin can enable or disable the device camera through a policy. Camera data is securely stored in the vault.

5. **Notes**

The Notes app helps you keep track of jottings, points and ideas.

6. **Text Editor**

Create, edit, and store text files as required.

7. **Contacts**

Device users can access official emails in-sync with well-integrated calendar and contacts. User contacts saved in Outlook or Gmail are saved here.

Note: Calls may not be allowed to the saved contacts as per the policy set by Admin. For more details, see Contacts Policy.

8. **Calendar**

The user can use the calendar to view and attend meetings in Outlook or Gmail. Admin can set the calendar policies as required. For more details, see Calendar Policy.

9. **Settings**

The user can view the app version and code. User can setup the password, profile settings, and give feedback and avail the help options.

10. **Work Profile App**

Apps setup by admin are seen under Recommended Apps. The Work Profile is subject to settings by admin for app management and browser use and other restrictions as applied. For more details, see Profiles.

13.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 Store and App Configuration.

This chapter includes following sections:

[App Store](#)

[Configuration](#)

App Store

The App Store 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 Store. You can tag a label to the published apps and the apps that are to be uninstalled.

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

When the app is added to the App Store, the following information is collected from the newly added app.

App Status

In Seqrite EMM following app statuses are found:

- **Recommended apps**: These apps are suggested to be installed on user device.
- **Apps to Uninstall**: These apps are restricted to installing on the user device.

App Type

Seqrite EMM 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 as seen under **Add Apps** shows the options from where the applications were downloaded and installed.

- Google Play

- iTunes Store
- Custom App URL
- Upload Custom APK

Category

All the apps on the Seqrite EMM console are categorized 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 Seqrite EMM console and in the left pane, select **Apps** > **App Store**.

2. On the App Sore page, click **Advanced Search**.

3. 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.

4. Select the required search options and click **Search**.

   The result gets displayed.

Taking an action for App Store

The Take Action list is beneficial to delete multiple selected apps. The following actions are available for App Repository.

- **Tag 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.

- **Tag 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 Tag**: 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.

i 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.

i Note:

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

To use the Take Action list for App Repository, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, select **Apps** > **App Store**.

2. Select an app.

   You can select multiple apps. The Take Action list appears.

3. Select the required option from the Take Action list and click **Submit**.

   The selected action is carried out on the selected apps.

Adding Apps Using App Store

The **Add Apps** option helps you to add a new app to the store. This helps you whenever you want to recommend the app in case the app is not present in the app store. Seqrite EMM provides the following options to add apps to the repository: From Google Play Store, iTunes Store, Custom App URL, and Upload Custom APK.

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

i 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 using Google Play Store

With this option, you can add a new app to App Repository from Google Play Store. This is applicable only to Android device users.

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

1. Log on to Seqrite EMM console and in the left pane, select **Apps** > **App Store**.

2. On the App Store page, select **Add Apps** > **Google Play Store**.

    The Add app from Google play store dialog box appears.

3. 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 box.

4. Click **Add**.

    A new app is added to the app repository.

Adding apps using iTunes Store

With this option you can add a new app to App Repository from iTunes store. This is applicable only to iOS device users.

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

1. Log on to Seqrite EMM console and in the left pane, select **Apps** > **App Store**.

2. On the App Store page, select **Add Apps** > **iTunes Store**.

    The Add app from iTunes store dialog box appears.

3. Enter iTunes Store URL of the app in the given text box. The URL format must be as per the given example in the dialog box.

4. Click **Add**.

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 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 Seqrite EMM console and in the left pane, select **Apps** > **App Store**.

2. On the App Store page, select **Add Apps** > **Custom App URL**.

    The Add Custom App URL dialog box appears.

3. Enter the App Name, Package Id, Version Name, Version Code, and APK URL in the

respective text boxes.

![i] 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.

4. 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 Android device users. You can also upload the other versions of the app to the app repository via Upload Custom URL.

Every tenant is allocated with some data transaction usage limit in GB and upload of custom APK is part of data transaction usage limit. Thus, whenever the transaction usage limit exceeds then the customer has to buy/purchase additional data transaction usage limit.

If user exceeds the data transaction usage limit, the user cannot perform the following functions:

- Admin will not be able to apply app configuration containing custom APK from device and group list page.

- Admin will not be able to upload custom APK to the Seqrite EMM console.

- Admin will not be able to add any custom APK in the app configuration.

- Admin will not be able to switch app configuration from one app configuration to another if that configuration has the APK. For example: Admin cannot switch from app configuration A1 to A2, if app configuration A2 contains any custom APK.

- Admin will not be able to switch groups if that group has custom APK app configuration. For example, Admin cannot move a group from G1 to G2, if G2 has A2 app configuration with custom APK.

- Suggested custom APK will not appear for newly created app configuration.

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

1. Log on to Seqrite EMM console and in the left pane, select **Apps** > **App Store**.

2. On the App Store page, select **Add Apps** > **Upload Custom APK**.

   The Upload Custom APK dialog box appears.

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

> [i] Note:
> _____
>
> Maximum file size of APK can be up to 150 MB and only the files with APK extension are allowed.
> _____

4. Click **Upload**.

    The new app is uploaded to the App Repository.

> [i] Note:
> _____
>
> If the data transaction usage limit has exceeded, then every transaction of downloading custom APK will be charged. Thus, the users should download the custom APK cautiously.
> _____

Adding Enterprise Apps for iOS

You can add a new iOS app to the app store. This helps you whenever you want to recommend the app in case the app is not present in the app store.

To add a new enterprise app for iOS, follow these steps:

1. Log on to Seqrite EMM console using your credentials.
2. Navigate to **Apps > App Store > Add Apps > Enterprise Apps for iOS**.
   The **Enterprise Apps for iOS** dialog box is displayed.
3. Enter App Name, Package Id, Version Name, Version Code, and custom IPA.
4. Select the .ipa file that you want to add to the app store.
5. Click **Upload**.

Note: File with only .ipa extension is allowed to upload.

Configuration

The app Configuration option lets you control and apply app restrictions (blacklist) on the device. You can create new app configurations and apply the configurations on the devices.

When you create the app configuration, you can restrict any new app installation (even published apps) on ADO and Knox supported devices. For non-ADO and non-Knox devices, restrictions will not be applied on new app installation, but the app which you are about to install will be blocked.

You can also recommend apps with specific versions, but if the user has the higher or earlier versions of the app, then also the recommended app will not be blocked by using the "Do not block apps which are pending for upgrade/downgrade" option. You may configure this setting where your recommended app will not be blocked.

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 EMM. 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 Launcher option, the user will be able to see and access only the selected active apps. After 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.

You can configure apps for the devices that are enrolled using Android Management API Enrollment through the Android App Management tab. This App Management will not be applicable to any other enrolled devices.

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 Seqrite EMM console and in the left pane, select **Apps** > **Configuration**.

2. On the App Configurations page, click **Advanced Search**.

3. Following search category is displayed:

    ▪ **Select Created By**: Select this option to search configurations as per creator name.

4. Select the creator name and click **Search**.

    The search result gets displayed.

Taking an action for App configurations

The Take Action list appears on the App Configurations page when you select a single or multiple Admin role. The available options in the Take Action 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.

    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 Take Action list and then select one of the following actions:

   - Select **Delete** and click **Submit**.

   - Select **Apply to Groups** to select the groups or devices to apply the configuration > click **Apply**.

     The selected action is carried out on the selected apps.

Adding app configuration and activating 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. Next, you can configure the management of apps through the Android Management API (AMA). For more information on AMA app configuration, see [Android App Management](#).

App configuration provides many useful features to manage the apps as follows:

App Categories

Seqrite EMM provides App Categories section to help block different categories to which the applications belong. The app category blocking is applicable only to Android devices. You can select either a single or multiple or all the app categories.

Whitelisted Apps

With this option, you can whitelist the apps. The whitelisted apps are accessible, even if their category is blocked. You can also add particular versions of the app to the whitelist. Only the selected, whitelisted versions of the application will be accessible to the user and other versions will be blocked. You can remove single or multiple versions of the app from the whitelist.

Blacklisted Apps

The Blacklisted Apps feature applies restriction on apps in the following ways:

Apps to Remove

If you want the user to uninstall all the versions of the app, select the entire package to uninstall all the versions. You can also add a 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 Android devices.

Apps to Block

The Apps to Block option helps you to add a 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 remove and Apps to block lists are not visible to the ADO and KNOX supported devices.

Published Apps

Published Apps functionality helps the user to add the apps to the Published Apps list and view the list. You can select the entire app or a specific version of the app and add it 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 it 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 Published Apps on the KNOX devices.

The Seqrite EMM Admin can remotely install the apps on any Supervised iOS devices.

The Seqrite EMM Admin can remotely uninstall only those apps, which were installed from EMM console on any Supervised iOS devices.

System Kiosk Mode

System Kiosk Mode is applicable to the ADO enabled Android devices or Supervised iOS devices, where Seqrite EMM Agent is the device user and 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 or Supervised iOS 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 add an app to System Kiosk Mode.

To enable System Kiosk mode on iOS device, make sure the added app is already installed on the iOS device. If the app is not installed on the device, the device will be blocked.

Launcher

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 the Launcher, Whitelisted Apps & Settings, and Custom Device Settings on Launcher.

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, 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, the Launcher configurations will have the highest preference and all the other app configurations will be overridden. In case, you have deactivated the Launcher, 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.

Whitelisted Apps & 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.

Settings	Description
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.
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.
Allow Camera App	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.

Custom Device Settings on Launcher

The Device Settings help to manage and control the following aspects of the device such as brightness, volume, Wi-Fi, data network, auto rotate, Bluetooth, Airplane 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. If 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 published 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.

- **Custom 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.

  ℹ️ 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.

  The Launcher functionality is applicable only to the Android devices.

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 Seqrite EMM console and in the left pane, click **Apps** > **Configuration.**

2. On the App Configurations page, click **Add App Configuration**.

    The Create App Configuration page appears.

3. In the Edit Details section, enter the **App Configuration Name**.

4. 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.

    [i] Note:

    If you are recommending 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.

    The Launcher Setting and Branding options are visible only for the Android device.

    If you want to make this app configuration a default one, select the **Default** check box.

5. To allow any recommended app irrespective of its upgrade or downgrade, select the **Do not block the apps which are pending for upgrade/downgrade** check box.

6. Click **Next**.

    The Edit Configurations tab displays App Categories, Blacklisted Apps, Published Apps, and System Kiosk Mode sections.

7. In App Categories section, you can take the following steps:

    i.   Select the app categories check boxes that you want to block.

    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 box, you can perform an advance search to view the downloaded, system, suggested, and restricted apps. Also, whitelist particular version of an app.

8. Click **Next**.

9. In Blacklisted Apps section, you can restrict the apps by adding the apps to the **Apps to remove** list and **Apps to block** list.

> **i** Note:
> _____
>
> Apps added to the **Apps to block** list are not visible/disabled on the ADO and KNOX supported devices.
>
> Apps added to Apps to remove list can be remotely uninstalled or disabled from ADO and KNOX devices.
>
> For iOS devices only those apps can be uninstalled which are added by Seqrite EMM console.
> _____

   i. To add the apps to the list, click **Apps to remove**. 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 **Apps to block**. Click the **Add Apps** button. In new window, select the apps. Add Apps button gets visible. Click **Add Apps**.

     When adding apps to Apps to remove or Fully Blocked list, you can also perform an advanced search to view the separate list of downloaded, system, suggested, and restricted apps.

10. Click **Next**.

11. In Published Apps section, to recommend any Android app or app version, click **Add Apps**. In the new window, select the apps. Add Apps button is displayed. Click **Add Apps**. Make sure the **Restrict new app installation on ADO & Knox Enabled Devices** check box is not selected in app configuration.

> ⓘ Note:

- Users will not be able to uninstall, force stop, and clear cache for published apps on Samsung KNOX devices.

- Custom Apps in recommended list will be silently installed on the ADO and Samsung KNOX devices.

12. Click **Next**.

13. In System Kiosk Mode section, you can recommend a single app in Kiosk mode for ADO and KNOX 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.

14. Click **Next**.

    A confirmation to enable the ADO Kiosk mode is displayed.

15. Click **OK**.

    You are directed to the Launcher settings section.

16. In the Launcher 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.

- **Whitelisted Apps and Settings**: Configure the Whitelisted Apps and other settings to access the selected settings on the device Launcher screen.

- **Custom Device Settings on Launcher**: Configure the device settings to access the selected device settings on the Launcher screen.

17. Click **Next**.

The Active Apps section appears.

18. 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 box appears. Select the apps that you want to view on the Launcher and click **Add Apps**.

i Note:

- o 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.
- o 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.
- o Only the selected app versions are visible on the Launcher.
- o Apps added to the Active Apps list must be installed on the user's device.

19. Click **Next**.

You are directed to the Branding section, where all the fields would be dimmed/disabled. You can make the following changes to the Launcher setting.

20. On the Branding page, select the **Branding on Launcher** check box.

All the other fields on the page are 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** > Select the image. For good results, use the following image resolutions:

- Company logo: Between 300 X 300 pixels to 1000 X 1000 pixels.
- Wallpaper: 1080 x 1920

The changes are reflected on the Launcher.

21. Click **Save**.

Editing the app configuration and Launcher

You can edit the app configuration details at any point of time.

To edit the app configurations, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Apps** > **Configuration**.

2. On the App Configurations page, select one of the app configurations, and then click the **Edit** icon.

3. To edit the configuration name, device and group details, click the **Edit** tab.

   In the Devices section, you can add the devices to which the configuration needs to be applied.

   In the Groups section, you can add the groups to which the configuration needs to be applied.

4. To edit the app configuration, click the **Edit Configuration** tab.

   ▪ In the 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 the Blacklisted Apps section, you can edit the uninstall list or fully blocked list.

   ▪ In the Published 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](#).

5. 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, change the alert time, or change the Launcher exit duration.

   ▪ You can change the Whitelisted Apps and other 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.

6. To save the edited configuration, click **Save**.

Android App Management

Android App Management configuration is applicable only to the Android Management API (AMA) enrolled devices. This feature lets you manage app permissions, installation, uninstallation, and app verification. You can add and uninstall apps silently on the device.

> **ⓘ Note:**
>
> If the apps are not installed due to network issues, then go to **Play store > Manage apps & device > Manage > Select Android Device Policy > Open > Sync.** The device is synced with the Seqrite EMM server and remaining apps if any are installed.

App Management Policy

The App Management Policy section, lets you control the following aspects of the apps:

Policy Name	Description
Default Application Permission	Allows you to set prompt, grant, or deny permissions to apps. PROMPT: Prompts the user to grant permission to the apps. GRANT: Automatically grants permission to the apps. DENY: Automatically denies the permission to the apps.
Disable Apps Installation	Enable this option to restrict the installation of existing and new apps. Note: This policy will work only after you remove the apps from the Install App section under Application Management.
Disable Apps Uninstallation	Enable this option to restrict the uninstallation of apps. Note: This policy will work only after you remove the apps from the Uninstall Apps section under Uninstall Apps.
Play Store Mode	Enable this option to allow the installation of apps from Play Store.

Application Management

The Application Management section lets you install apps through the Android Normal Mode or the Android Kiosk Mode**.**

Android Normal Mode

You can install apps on the user device through the **Android Normal Mode** in the following ways:

1. Make apps available for installation through the **Manage apps and device** option of Play Store on the user device. Users can install these apps as required.

2. Make apps available through the **Application Management** section of the EMM console. The application management section lets you add apps to the device Play Store, silently

install standard apps, install private apps, and web apps using URL on the device.

The following installation options are available:

- Select apps to be available on the Play Store on the user device.

- Select **Install Silently** option to install the apps silently through Play Store on the user device.

- Select **Private apps** > Click **Plus (+)** > Enter **Title** > Click **Upload APK** and upload .apk file for installation on the user device.
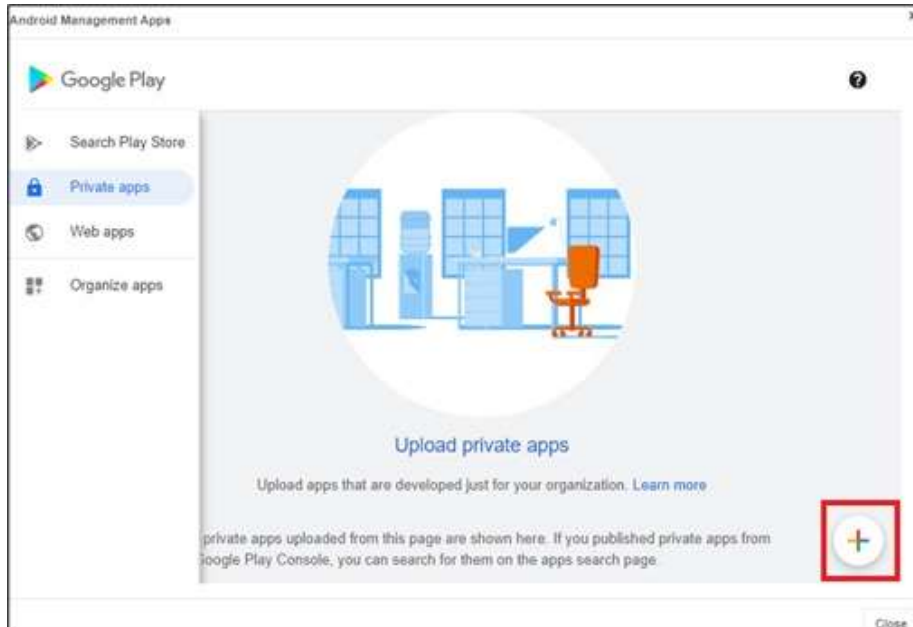
- Select **Web apps** > Click **Plus (+)** > Enter **Title** and **URL >** Select **Display** size > Click **Upload** icon > Click **Create** for installation of web-based apps on the user device.
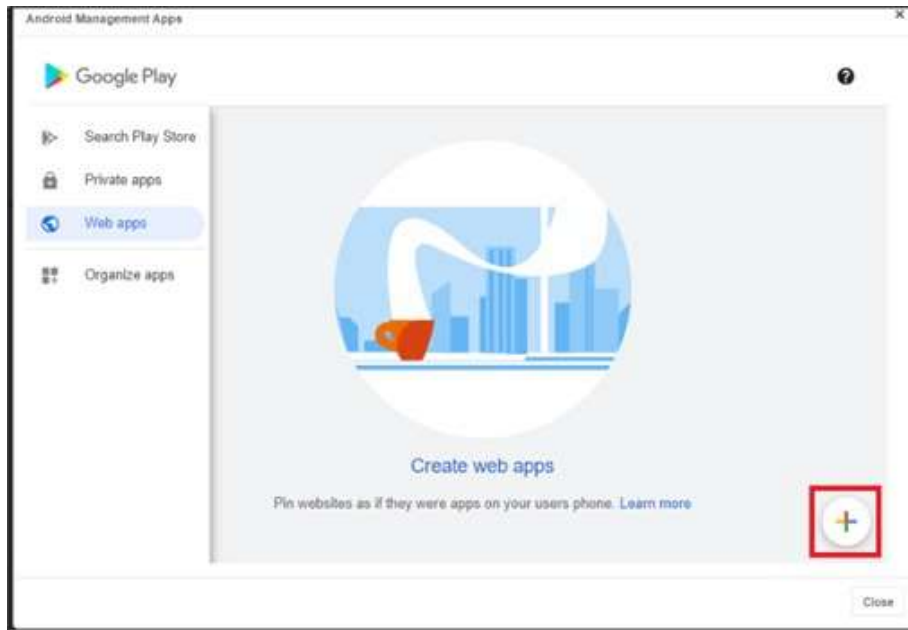
Android Kiosk Mode

In this mode, all the above options of **Android Normal Mode** are available. However, the Install Silently option is enabled by default and enforces silent installation of selected apps on the user device. In this mode all apps are disabled except for the whitelisted apps in the kiosk mode.

You can also configure the following **Advanced Settings** options.

- **Power Button Actions**: Restricts or allows the action when the user presses and holds the power button of the device.
- **System Error Warnings**: Blocks the system apps forcefully without user's intervention or allows the user to close the unresponsive system apps.
- **Navigation**: Blocks or allows the user to use the navigation buttons of the device. **Users** can use **only** the Home button when the Home Button Only option is set for the device.
- **Status Bar**: Blocks or allows the display of the system information and the notifications on the status bar of the device.
- **Device Settings**: Blocks or allows the user to access the device settings app.
- **Single App Kiosk Mode**: Lets admin configure only single app or required apps on the device.

[i] Note:

You can set the Default Application Permission as PROMPT, GRANT or DENY as per the requirements before installing the apps on the device.

Uninstall Apps

The Uninstall Apps section lets you add the apps to the Uninstall Apps list. Apps in this list are automatically uninstalled from the device. If you want to reinstall the same app again on the device, then you need to remove the app from the Uninstall Apps list and add that app to the Install list.

Configuring Android App Management

To add new app configuration for AMA, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Apps** > **Configuration.**

2. On the App Configurations page, click **Add App Configuration**.

   The Create App Configuration page appears.

3. In Edit details section, enter the **App Configuration Name**.

   $\boxed{i}$ Note:

   Settings for Restrict new app installation on ADO & Knox enabled devices and Do not block the apps which are pending for upgrade/downgrade are not required for Android Enterprise enrolled devices and can be skipped.

   ---

4. Click **Next**. Skip the settings for **Edit Configuration** and **Launcher** tabs. You are navigated to **Android App Management** tab.

5. In the **App Management Policy** section, configure the app policies as required. A tick mark signifies that the policy is enabled. A cross mark signifies that the policy is disabled.

   You can modify the following policies as per your requirement.

   - **Default Application Permission**: Select at least one option from the list as required.
   - **Disable Apps Installation**
   - **Disable Apps Uninstallation**
   - **Play Store Mode**: Enable to allow the installation of the apps on the device.

6. Click **Next**.

7. In the **Application Management** section, select either the **Android Normal Mode** or **Android Kiosk Mode**. For more information about the Android Normal Mode or Android Kiosk Mode, see **Application Management**.

You can add apps to the Application Management list, in Android Normal Mode or Android Kiosk Mode.

   o If **Android Normal Mode** option is selected, you can add apps silently or

normally to the device.

- In the **Install Apps** section select the **Install Silently** check box to add apps silently on the device.

- If **the Install Silently** option is not selected, apps are added to the play store list of the device. If required, the user can install the apps from the Play Store.

  i. To add apps, click **Add Apps.**
     The **Android Management Apps** dialog box appears. Select the app and approve, complete the approval preferences/permissions as required.

  ii. Click **OK**. The app is added to the list.

  iii. Click **Next**.

- o If the **Android Kiosk Mode** option is selected, then the apps are added either silently to the device or made available for installation through the Manage apps and device option on the Play Store of user device. Next, you can configure the advanced settings if required.

  - In the **Kiosk Apps** section, click **Add Apps**.

  i. The **Android Management Apps** dialog box appears. Select the app and approve, complete the approval preferences/permissions as required.

  ii. Click **OK**. The app is added in the list

  iii. Click **Next.**

  - In the **Advanced Settings** section, configure the Power Button Actions, System Error Warnings, System Navigation, Status Bar, Device Settings, and Single App Kiosk Mode settings as required and then click Next.

8. In the **Uninstall Apps** section, click **Add Apps** to add the apps to the uninstall list. These apps are later uninstalled from the device on next sync.

9. Click **Save**.

Editing the Android App Management

You can edit the app configuration details at any point of time.

To edit the app configurations, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Apps** > **Configuration**.

2. On the App Configurations page, select one of the app configurations, and then click the **Edit** icon.

3. To edit the configuration name, device, and group details, click the **Edit** tab.

   Next, click **Android App Management** tab, configure the settings as required.

   ![i]Note:

   Applicable only for Android Enterprise Enrollment devices.

4. To save the edited configuration, click **Save**.

14.Fencing

With the rise of use of mobile devices, securing confidential data has become crucial. Seqrite EMM upholds a very strong feature of fencing for securing confidential data. The Fencing feature acts as a virtual boundary.

Fencing allows you to create policies to allow or to restrict the user by applying the profiles or app configurations to the user device.

Seqrite EMM 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 a secure 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

Configurations

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 EMM includes the following fences: Wi-Fi Fence, Geo Fence, and Time Fence.

> **Note:**
>
> Fence restrictions will not work for Android Enterprise Enrollment devices.

Advanced Search for Fences

The Advanced Search option allows you to perform an advanced search for different fences created in Seqrite EMM.

To search fences, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Fencing** > **Fences**.

2. On the Fencing page, click **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.

3. Select the required configuration type and click **Search**.

The result gets displayed.

i Note:

Fencing is applicable only to the Android devices.

Taking an action for Fences

Take Action is an option that helps you take appropriate action for the fences.

To take an action for fences, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, select **Fencing** > **Fences**.

2. On the Fencing page, select a fence.

3. The Take Action list appears.

4. Select **Delete** and then click **Submit**.

The selected action is carried out on the selected fences.

Fences

Seqrite EMM helps you to create virtual boundaries for your devices with the help of fences.

Seqrite EMM supports the following fence types.

Wi-Fi Fence

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.

ℹ️Note:

The new SSID which is added while creating a Wi-Fi fence, will not be 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 you 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 are important and should be handy. So, Seqrite EMM facilitates importing the Geo fence details. On the Fences list page, the **Import Geo Fence** button is available to import the Geo fence details. In a single instance, a maximum of 1000 Geo fences details can be imported.

Time Fence

The Time fencing helps you to set up the time-based rules to be applied on the user devices. This option helps to limit the users of Seqrite EMM 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.

Adding fences

Fence is like restriction that you want to apply to the devices. You can create fences for Wi-Fi, Geo, and Time restrictions.

Adding Wi-Fi Fence

To add a Wi-Fi fence, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Fencing** > **Fences**.

2. On the Fencing pages, select **Add Fence > Wi-Fi Fence**.

    The Add Wi-Fi page appears.

3. Enter the name of Wi-Fi and then select **Wi-Fi SSID**.

    If the Wi-Fi SSID is a new one, enter SSID. If you want to use an existing SSID from Wi-Fi configuration, select **Existing Wi-Fi SSID**. After selecting the existing Wi-Fi SSID, all the configured Wi-Fi SSIDs of Wi-Fi configuration appear.

4. Click **Save**.

    A new Wi-Fi fence is added.

Adding Geo Fence

To add Geo fence, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Fencing** > **Fences**.

2. On the Fencing pages, select **Add Fence > Geo Fence**.

    The Add Geo Fence page appears.

3. 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.

4. On the map, click **Add Geo Fence**.

    The Save Geo Fence list appears.

5. Enter the Fence Name, radius in meters, and then click **Save**.

    Latitude and Longitude are displayed automatically.

    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 entering locations. If you want to see all the created Geo fences, click **Show All Geo Fences**.

    Note:

    o The radius of the location must be at least 100 meters.

    o 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 fences that 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 a maximum of 1000 fence details.

To import geo fence, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, select **Fencing** > **Fences**.

2. On the Fencing page, click **Import Geo Fences**.

3. 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 Seqrite EMM console and in the left pane, click **Fencing** > **Fences**.

2. On the Fencing page, select **Add Fence > Time Fence**.

    The Add Time Fence page appears.

3. Enter the name of the time fence and select **Set Time Fence on** option. The Set Time Fence on option includes two types: Date Range and Recursive on Days.

    ▪ **Date Range**: Select a date range when the fencing should be executed.

    ▪ **Recursive on Days**: Select this type to execute fencing on the selected days.

4. Set the **From Time** and **To Time** to define the time range.

5. In case you want to exclude the fence on certain dates, select the dates and then click **Save**.

    The time fence is added successfully.

Editing the fence information

You can change the fencing information as per your requirement.

To edit the fencing information, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, select **Fencing** > **Fences**.

2. Select the fence type that you want to edit and then click the **Edit** icon from Actions column.

    The Fence overview page is displayed with fence details.

3. Click the **Edit** tab.

    ▪ For Wi-Fi and Time fence, in the Edit details section, you can edit the fence information.

    ▪ For Geo fence, in the Edit tab a map is displayed with the fence balloon. To edit the geo details, click the balloon. In Save Geo Fence dialog box, make the required changes.

4. To save the edited fence configurations, click **Save**.

    To get the complete detail of the fence configuration, click the **Export** button.

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 Seqrite EMM console and in the left pane, select **Fencing** > **Configurations**.

2. On the Configurations page, click **Advanced Search**.

3. Following search category is displayed:

    ▪ **Select Created By**: Select this option to search the fence configuration according to the creator name.

4. Select the creator name and click **Search**.

    The search result is displayed.

Taking an action for Fence Configurations

Take Action is an option that helps you take an appropriate action for the Fence Configurations.

To take an action for the Fence Configurations, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, select **Fencing** > **Configurations**.

2. On the Configurations page, select a fence configuration.

3. Select one of the following actions:

   ▪ Select **Delete** and click **Submit**.

   Delete: Helps you to delete the selected fence configurations. You can delete multiple apps at one go.

   ▪ Select **Apply to Groups** > click **Select Groups**. Click the groups to apply the configuration and then click **Apply**. On the confirmation page, click **OK**.

   Apply to Groups: Helps you to apply the selected fence configuration to a group. You can apply the single fence configuration to multiple groups.

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 a maximum of two fence groups in one fence configuration. The 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.

Adding Fence Configuration

1. Log on to Seqrite EMM console and in the left pane, click **Fence** > **Configurations**.

2. On the Configurations page, click **Add Fence Configuration**.

   The Add Fence Configuration page appears.

3. Enter the name of the configuration and description.

4. Select the following required check boxes:

   ▪ **Compel user to keep GPS ON**: 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 user to keep Wi-Fi ON**: 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.

5. Select either of the options:

   ▪ **Add Fence Group**: Select this option to apply restrictions on the already defined fences. On the Fence Group, add a fence and select the restrictions that you want to apply.

   ▪ **Define Fence**: Select this option to define a new fence.

6. To create a new fence, follow these steps:

    i.   Click **Define Fence**. The Define Fence page appears.

1. 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 [Adding Fences](#).

2. After the new fence is created, click **Add Fence Group** to apply restrictions on the defined fences. The Fence Group section is displayed.

7. Select the Geo Fence, Time Fence, and Wi-Fi Fence that you want to apply on the device.

8. Set the Fence Relation option to AND 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.

9. 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).

10. 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 Seqrite EMM Admin will get the notifications.

    - **Alerts**: If this option is selected, the user will receive email notification when the fence is triggered. The user can provide a minimum of 5 email addresses separated by comma in the given text box.

    - **Apply Restriction**: Helps to apply restriction on the device when the fence configuration is applied on the device. The restrictions include Policies, Web Security, and App configurations.

11. Click **Save**.

    A new fence configuration is created.

    Click **Save & Push** if you want to create and also apply the policy on the devices.

    Note:

    o   You can reorder the fence groups to change their priority.

    o   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.

Editing the fence configurations

You can change the fencing configuration as per your requirement. To edit the fence configuration, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Fencing** > **Configurations.**

2. On the Configurations page, select a configuration and click **Edit** icon.

3. To edit the fence configuration details, click the **Edit** tab.

4. In the Edit details section, edit the configuration and fence group details.

5. Click **Save**.

6. Click the **Groups** tab. In this section you can add the groups or remove the groups from the fence configuration.

    ![i] 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 box 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**.

15.Reports

Seqrite EMM 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:

On Demand Reports

Custom Reports

Scheduled Reports

Activity Logs

Action Logs

On Demand Reports

On Demand Report helps you to get detailed reports on various factors including whether the devices comply with the policy of the organization or if there have been any malware attacks.

You can generate reports for the following factors.

Report Type	Description
Device Compliance Report	Shows whether the devices comply with the policy of the organization.
Device Health Report	Shows the status of the devices.
Device Asset Tracking Report	Shows if the assets of the devices in the network.
Device Sync Report	Shows which devices connected to the Seqrite EMM console and whether data from the devices synced with the server.
Malware Detection Report	Shows where there has been any malware attack on the devices.
Internet Data Usage Report	Displays the Internet usages of the devices.
Call/SMS logs Tracking Report	Displays call and SMS logs done on the devices.

Report Type	Description
App Non-Compliance Report	Shows the devices that violate any compliance policy.
Web Volition in Workspace	Shows if there has been any web violation.

Generating a report

To generate a report, follow these steps.

1. Log on to Seqrite EMM console.

2. In the left pane, click **Reports** and then click **On Demand Reports**.

    The Reports page appears.

3. On the Reports page, select a report type and then click **Search**. The relevant report is generated.

The following buttons allow you to carry out certain actions.

Button	Description
Search	Allows you to filter the report.
Reset	Allows you to reset the report type.
Schedule Report	Allows you to schedule generating reports automatically.
	To schedule a report, click the Schedule Report option and then write the report name, set the frequency (Daily, Weekly, Monthly) when the report should be generated, set the report period for which the report is required, and then set the email addresses to which the report should be sent. After setting all the options, click **Confirm**.
	The report would be generated and sent on the schedule.
Export	Allows you to export the generated report.

You can further view the details of a user or the device. To see the details, click the User Name or the device name.

For example, if you have generated a report on Device Compliance, you can see and edit the details, see the location and app installed on the device, data usage and call/SMS logs, and so on. Different factors may be available for different reports.

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 EMM console.

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 amount of data, the report cannot be viewed and it gives a warning message. In such a 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 Seqrite EMM console and in the left pane, select **Reports** > **Custom Reports**.

2. On the Custom Reports page, click **Advanced Search**.

    The advanced search parameter is displayed.

    ▪ **Select Created By:** Select this option to search custom reports according to the creator name.

3. Click **Search**.

    The search result appears.

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 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 columns 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.

- **Schedule Report**: After generating the report, you can schedule the report to be generated as per requirement.

To view the custom report, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, 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). You can choose Pivot Table if

required to change the report preview.

[i] 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**.

   - To get the report with same parameter, you scan schedule the report generation process by clicking **Schedule Report**.

   [i] 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.

- While scheduling the custom report if more than one date range columns are available, then you can choose the required date range option.

Scheduling custom report

To schedule report generation, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Reports** > **Custom Reports**.

1. On the Custom Reports page, click the view (eyes) icon available in front of the reports.

2. On the report page, select the criteria and again generate the report or directly click **Schedule Report**.

3. In the Schedule Report dialog box make the following changes:

   - Enter report name.

- In Report Sending Frequency section, select Daily, Weekly or Monthly. As per your selection, you can select the days of the week or day of the month.

  o Report sending period cannot exceed 90 days for daily and weekly cycle.

  o Report sending period cannot exceed 180 days for monthly cycle.

- From the calendar, select the appropriate Report Sending Period.

- In Email Recipient text field add the comma-separated email IDs of the admin to receive the generated report in the form of attachment.

4. Click **Confirm**.

   The custom report is scheduled for the given time and frequency.

   [i] Note:

   - While scheduling the custom report if more than one date range columns are available, then you can choose the required date range option.

Generating a custom report

You can generate the custom report by selecting multiple entities.

To generate custom report, follow these steps:

1. Log on to Seqrite EMM console and in the left pane, click **Reports** > **Custom Reports**.

   The reports page appears. If reports are not available, the Reports page will be empty.

2. Click **Add**.

   The Create Report page appears.

3. Enter Report Name and then select the Root entity as per your requirement.

   The root entities include User, Department, Device, Device Group, Admin Role, Policy, App Repository, Configurations, and Fence Configurations.

   [i] 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.

i Note:

When creating custom reports, you can include a maximum of 15. 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, Admin 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.

Options	Description

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 note 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.

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.

Options	Description
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
Take Action	The Take Action list 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 Take Action list appears. 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 Seqrite EMM console and in the left pane, 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.

Scheduled Reports

Scheduled reports page shows all the available On Demand and Custom reports that are scheduled for given specific time and frequency in the Seqrite EMM portal. Only the Super admin can schedule the reports and other sub-admins can view the reports.

Scheduled report gives complete information about the reports such as.

- Id: Shows the Id of the report.
- Report Name: Shows the name of the report.
- Report Status: Shows different report status such as.
- ▪ Completed: Shows that the scheduled report has been generated.
- ▪ In Progress: Shows that the scheduled report has not completed the set frequency of the report.
- ▪ Pending: Shows that the scheduled report is yet to start with report generation.
- Report Frequency: Shows the scheduled report frequency.
- Report Type: Shows the report type.
- Created by: Shows the name of report creator.

- Created On: Shows the date and time when the report was scheduled.

Activity Logs

The Activity Logs section helps you to keep track of the actions performed by all the Admins. The activity logs are created when any of the Admins perform any action on the Seqrite EMM console. 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.

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 Seqrite EMM console and in the left pane, click **Reports** > **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 Seqrite EMM console and in the left pane, click **Reports** > **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 track of the device actions executed on the devices by the Seqrite EMM console. 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 EMM console. 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.

Options	Description
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 Seqrite EMM console and in the left pane, click **Reports** > **Action Logs** > **Advanced Search**.

    The 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.

Column	Description
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 Seqrite EMM console and in the left pane, click **Reports** > **Action Logs** > **Advanced Search**.

   The search criteria are displayed.

2. Select the action type and then select the action days or date range and click **Export**.

   Tip:

   The exported data will be based on the selected search criteria, so choose the search criteria properly.

3. On the confirmation screen, click **OK**.

   The action logs are exported.