



## **Administrator's Guide**

*Version 2.6*

## Copyright & License Information

---

© 2014–2021 Quick Heal Technologies Ltd. All Rights Reserved.

No part of this publication may be reproduced, duplicated, or modified in any form or incorporated into any information retrieval system, electronic or any other media or transmitted in any form without prior permission of Quick Heal Technologies Limited, Marvel Edge, Office No. 7010 C & D, 7th Floor, Viman Nagar, Pune 411014, India.

Marketing, distribution or use by anyone barring the people authorized by Quick Heal Technologies Ltd. is liable to legal prosecution.

This document is current as of the initial date of publication and may be changed by Quick Heal at any point of time.

### **Trademarks**

Seqrite is a registered trademark of Quick Heal Technologies Ltd.

### **License Terms**




Installation and usage of Seqrite mSuite is subject to user’s unconditional acceptance of the Quick Heal end-user license terms and conditions.

To read the license terms, visit <https://www.seqrite.com/eula/> and check the End-User License Agreement for your product.

## About This Document

---

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

Convention	Meaning
<b>Bold Font</b>	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.
You	Admin
User	Mobile, Tablet, or Phablet users
Entities	Users, departments, devices, groups, policy, configuration, and app configuration.
Company	The organization who have registered with Seqrite mSuite.
Enable	To turn on the button or to access the feature and its sub-sections.

# Contents

---

<b>1. Introducing Seqrite mSuite .....</b>	<b>1</b>
Seqrite mSuite.....	1
How does Seqrite mSuite work?.....	2
Seqrite mSuite variants.....	2
Features included in variants.....	2
Tenant and data retention policy on Cloud.....	3
Seqrite Workspace.....	3
Seqrite Workspace Advantages.....	4
<b>2. Getting started.....</b>	<b>5</b>
Prerequisites.....	5
System requirements.....	5
<b>3. Registration .....</b>	<b>6</b>
Registration.....	6
Registering with Seqrite mSuite.....	6
<b>4. Dashboard .....</b>	<b>8</b>
Notifications.....	9
User Profile.....	9
Menus.....	9
Dashboard.....	10
Informative Section.....	13
Common UI Terminologies.....	13
<b>5. Notifications .....</b>	<b>16</b>
Notifications Dialog box.....	17
Notifications List Page.....	17
Advanced Search for Notifications.....	18
<i>Searching notifications.....</i>	<i>18</i>
<i>With selected Options for Notifications.....</i>	<i>18</i>
<i>Using With selected option for notifications.....</i>	<i>18</i>
Enrollment Notifications.....	19
Enrollment Notifications.....	19
<i>Viewing enrollment notifications.....</i>	<i>19</i>
<i>Approving device enrollment request.....</i>	<i>19</i>

<i>Disapproving device enrollment request</i> .....	20
<i>Device Admin Notification</i> .....	20
Agent Vulnerable Notification .....	20
<i>Viewing agent vulnerable notifications</i> .....	20
Accessibility Permission Revoked .....	20
<i>Viewing devices on which accessibility services permission has been removed</i> .....	21
Alert Notification .....	21
Report Notification .....	21
Scan Report.....	21
<i>Viewing device scan summary</i> .....	22
Non-compliant Report .....	22
<i>Viewing the device non-compliance report</i> .....	22
Info Notification .....	23
Import Notifications.....	23
<i>Import a notification</i> .....	23
<i>Viewing import notifications</i> .....	23
Fence Notification.....	24
<i>Viewing fence notifications</i> .....	24
Battery Notification .....	24
<i>Viewing battery notifications</i> .....	24
Messages from Seqrite .....	25
mSuite App Log Notification .....	25
<i>Viewing mSuite App Log Notification</i> .....	25
App Request Notifications .....	25
Viewing app requests.....	25
Device app request report .....	26
Accepting or rejecting the app request .....	26
Device Accessibility Notification .....	26
Workspace Notifications.....	26
Viewing Workspace notifications .....	27
Delete all Notifications.....	27
Deleting all notifications .....	27
<b>6. User Profile .....</b>	<b>28</b>
User Management .....	28
Types of admin roles.....	28
<i>Super Admin</i> .....	29
<i>Assigning Super Admin role to an Admin</i> .....	29

<i>Admin</i> .....	29
<i>Advanced</i> .....	29
<i>Standard</i> .....	29
<i>Basic</i> .....	30
<i>Group-wise visibility for mSuite console</i> .....	33
Advanced Search for Admin roles .....	33
User Management List Page .....	33
With selected options for admin roles .....	34
Creating Admin role .....	34
Overviewing Admin Role .....	34
Editing admin role .....	35
Deleting admin role .....	35
Setup Services .....	36
Apple Certificate .....	36
Agent Upgrade .....	36
<i>mSuite Upgrade</i> .....	36
<i>Default Location for Seqrite mSuite</i> .....	37
<i>Custom URL for Seqrite mSuite</i> .....	37
<i>Upload Seqrite mSuite App</i> .....	38
<i>Launcher Upgrade</i> .....	38
<i>Default Location for Launcher</i> .....	38
<i>Custom URL for Launcher</i> .....	39
<i>Upload Launcher App</i> .....	39
<i>Workspace Upgrade</i> .....	40
<i>Default Location for Workspace app</i> .....	40
<i>Upload Workspace App</i> .....	41
mSuite Agent Preference .....	41
<i>Changing the mSuite Agent preference</i> .....	41
Company Branding .....	42
<i>Company Setting</i> .....	42
<i>Editing company name and logo</i> .....	42
<i>Device Wallpaper</i> .....	42
<i>Editing device wallpaper</i> .....	43
Notification Preference .....	43
<i>Creating Notification Preference</i> .....	43
SMS Settings .....	44
<i>SMS Gateway Integration</i> .....	44
<i>Configuring SMS Gateway</i> .....	44
<i>SMS Battery Notification</i> .....	44
<i>Configuring SMS for battery notification</i> .....	44
Custom Account Settings .....	45

<i>Email (IMAP/POP) Settings</i> .....	45
<i>Configuring Email (IMAP/POP) Settings</i> .....	45
<i>Contacts (LDAP/CARDDAV) Settings</i> .....	45
<i>Configuring Contacts (LDAP/CARDDAV) Settings</i> .....	45
<i>Calendar (CALDAV) Settings</i> .....	46
<i>Configuring Calendar (CALDAV) Settings</i> .....	46
Flash mEnrollment .....	46
<i>Enrolling device with Flash mEnrollment</i> .....	46
License Management.....	47
Buy Subscription .....	48
Renew .....	48
Adding devices to the mSuite license .....	49
Upgrade.....	49
Online Transaction from mSuite console to Seqrite Website .....	49
Change Password .....	49
Resetting the mSuite console password.....	50
Share Feedback.....	50
Contact Us.....	50
Email Support.....	50
Live Chat Support.....	50
Phone Support .....	51
Frequently Asked Questions .....	51
Administrator Guide .....	51
Release Notes .....	51
Log Out.....	51
<b>7. Users.....</b>	<b>52</b>
Users .....	52
Advanced Search for Users .....	52
Users List Page .....	53
With Selected Options for Users.....	53
Adding a user .....	53
Overview and edit user details .....	54
<i>Overviewing user details</i> .....	54
<i>Editing user details</i> .....	54
Importing users.....	56
Exporting users .....	56
Deleting users .....	56

<b>8. Departments.....</b>	<b>57</b>
Advanced Search for Departments.....	57
Departments List Page .....	57
With selected options for Departments .....	57
Overviewing Department Details .....	58
Adding a department.....	58
Editing department details .....	59
Adding users to the department .....	59
Deleting department.....	59
<b>9. Devices .....</b>	<b>60</b>
Device status.....	60
Advanced Search for devices .....	61
Devices List Page .....	61
With selected Options on Devices List Page.....	63
<i>Enrolling a new Android device.....</i>	<i>63</i>
<i>Enrollment via Email/SMS.....</i>	<i>64</i>
<i>Enrollment via QR Code.....</i>	<i>64</i>
<i>Enrollment using ADO .....</i>	<i>65</i>
Enrollment Time Matrix .....	67
Adding devices .....	67
Overviewing device details .....	68
<i>Select an Action (mSuite) .....</i>	<i>69</i>
<i>Select an Action (Workspace).....</i>	<i>72</i>
Actions on mSuite Agent from Device Overview page.....	72
<i>Turn on/off the fence configuration.....</i>	<i>72</i>
<i>Unblock the blocked device using secret code .....</i>	<i>73</i>
<i>Exit Launcher using passcode.....</i>	<i>73</i>
<i>Exiting launcher temporarily or permanently .....</i>	<i>73</i>
<i>Wiping the device data .....</i>	<i>75</i>
<i>Broadcast Files(s) / Message.....</i>	<i>75</i>
Actions on Workspace application from Device Overview page.....	77
Edit .....	77
<i>Edit details.....</i>	<i>77</i>
<i>Editing device details.....</i>	<i>77</i>
<i>Configuration .....</i>	<i>77</i>
<i>Editing device configuration.....</i>	<i>78</i>
Location.....	78
<i>Tracing device location.....</i>	<i>79</i>
<i>Locating device location.....</i>	<i>79</i>



<i>Locate Multiple Devices</i> .....	80
<i>Locating devices</i> .....	80
Apps .....	80
<i>Revoke App Settings</i> .....	80
<i>Install Launcher or Uninstall Launcher</i> .....	81
<i>App Status</i> .....	81
<i>Advanced Search for Apps</i> .....	81
<i>Viewing app inventory</i> .....	82
Data Usage .....	82
<i>Searching network data usage</i> .....	82
<i>Data Plan Details</i> .....	82
<i>Network Usage</i> .....	83
<i>Top 10 App Usage</i> .....	84
<i>Network Usage Graph</i> .....	84
<i>Usage Information</i> .....	84
<i>Viewing network usage details</i> .....	84
Call/SMS Logs .....	85
<i>Advanced search for call and SMS logs</i> .....	85
<i>Viewing call and SMS logs</i> .....	86
<i>Enable call and SMS monitoring</i> .....	86
<i>Exporting call and SMS logs</i> .....	87
<i>Clearing call and SMS logs</i> .....	87
Remote Control .....	87
<i>Remotely controlling the device</i> .....	89
<i>Important points to remember for seamless RDC connection:</i> .....	90
Activity .....	90
Admin .....	90
<i>Activity Status</i> .....	90
<i>Searching activity logs</i> .....	91
<i>Compliance Report</i> .....	91
<i>Scan Report</i> .....	91
Importing devices .....	92
Exporting devices .....	92
Deleting devices .....	92
<b>10. Groups</b> .....	<b>93</b>
Group QR Code .....	93
Advanced Search for Groups .....	93
Groups List Page .....	94
With selected Options for Groups .....	94
<i>Broadcasting files and messages to multiple devices in a group</i> .....	94

Adding a group.....	95
Viewing the group information.....	95
Editing group information and adding devices to the group.....	96
Bulk Enrollment with Group QR Code .....	96
<i>Generating group QR code</i> .....	96
Locating a group on map .....	97
Importing groups .....	97
Exporting groups.....	98
Deleting groups.....	98
<b>11. Profiles.....</b>	<b>99</b>
Policies .....	99
Advanced Search for Policies .....	99
Policies List Page .....	100
With selected options for policies .....	100
Adding a policy.....	100
Viewing a policy .....	100
Editing policy details and groups .....	101
Editing the policy.....	101
Policy Details.....	102
<i>History</i> .....	115
Importing a policy .....	115
Configurations.....	115
Advanced Search for Configurations .....	115
Configurations List Page.....	116
With selected Options for Configurations .....	116
Wi-Fi .....	116
<i>Adding Wi-Fi configuration</i> .....	116
<i>Overviewing Wi-Fi configuration</i> .....	117
<i>Editing Wi-Fi configuration</i> .....	117
Anti-Theft .....	118
<i>Adding Anti-Theft Configuration</i> .....	118
<i>Overviewing Anti-Theft configuration</i> .....	120
<i>Editing Anti-Theft configuration</i> .....	121
Web Security.....	121
<i>Adding Web Security Configurations</i> .....	122
<i>Overviewing Web Security Configuration</i> .....	123
<i>Editing Web Security Configuration</i> .....	123

<i>Edit details</i> .....	123
<i>Web Categories</i> .....	124
<i>Blacklist/Whitelist URLs</i> .....	125
<i>Devices</i> .....	125
Schedule Scan .....	125
<i>Adding schedule scan configuration</i> .....	126
<i>Overviewing Schedule Scan Configurations</i> .....	126
<i>Editing Schedule Scan Configuration</i> .....	127
Data Usage .....	127
<i>Adding Data Usage configuration</i> .....	128
<i>Overviewing Data Usage Configuration</i> .....	128
<i>Editing Data Usage Configuration</i> .....	129
Deleting Data Usage Configurations.....	130
<b>12. Workspace .....</b>	<b>131</b>
Advanced Search for Workspace Policies.....	131
Workspace Policies List Page .....	131
With selected options for Workspace policies .....	131
Adding a policy.....	132
Viewing a policy .....	132
Editing Workspace policy details and groups .....	133
Editing the policy.....	133
Workspace Policies .....	134
Profiles .....	139
Advanced Search for Workspace Profiles.....	139
Workspace Profiles List Page .....	140
With selected options for Workspace profiles .....	140
Add.....	140
<i>Creating Workspace profile</i> .....	140
<i>Editing Workspace profile</i> .....	141
<i>Exporting Workspace profile</i> .....	141
<b>13. Apps .....</b>	<b>142</b>
App Store .....	142
App Status.....	142
App Type .....	142
Source Type.....	143
Category .....	143
Advanced Search for Apps .....	143
App Store List Page .....	143

With selected options for App Store .....	143
Adding Apps Using App Store .....	144
<i>Adding apps using Google Play Store</i> .....	145
<i>Adding apps using iTunes Store</i> .....	145
<i>Adding apps using Custom App URL</i> .....	145
<i>Adding App using Upload Custom APK</i> .....	146
Configuration .....	147
Advanced Search for App Configurations .....	148
App Configurations List Page .....	148
With selected options for app configurations .....	148
Adding app configuration and activating the Launcher .....	148
<i>App Categories</i> .....	149
<i>Whitelisted Apps</i> .....	149
<i>Blacklisted Apps</i> .....	149
<i>Apps to Remove</i> .....	149
<i>Apps to Block</i> .....	149
<i>Published Apps</i> .....	149
<i>System Kiosk Mode</i> .....	150
<i>Launcher</i> .....	150
<i>Launcher Setting</i> .....	150
<i>Active Apps</i> .....	152
<i>Branding</i> .....	152
Adding new app configuration and activating the Launcher.....	152
Overviewing and editing app configuration and Launcher .....	156
Deleting App Configurations.....	157
<b>14. Fencing .....</b>	<b>158</b>
Fences .....	158
Advanced Search for Fences .....	158
Fences List Page .....	159
With selected options for Fences .....	159
Fences .....	159
<i>Wi-Fi Fence</i> .....	159
<i>Geo Fence</i> .....	159
<i>Time Fence</i> .....	160
Defining Fence .....	160
<i>Adding Wi-Fi Fence</i> .....	160
<i>Adding Geo fence</i> .....	160
<i>Importing Geo fence</i> .....	161
<i>Adding Time Fence</i> .....	161
<i>Overviewing and editing fence information</i> .....	162

Deleting Fences .....	162
Configurations .....	163
Advanced Search for Fence Configuration .....	163
Fence Configuration List Page.....	163
With selected Options for Fence Configuration .....	163
Add fence configuration .....	164
<i>Fence Group</i> .....	164
<i>Define Fence</i> .....	164
<i>Adding and defining fence configuration</i> .....	164
Overviewing and editing fence configurations.....	165
<b>15. Reports .....</b>	<b>167</b>
On Demand Reports.....	167
Generating a report .....	168
Custom Reports .....	168
Advanced Search for Custom Reports .....	169
Viewing reports.....	169
<i>Scheduling custom report</i> .....	170
Generating custom report .....	171
Editing custom reports.....	174
Scheduled Report.....	174
Activity Logs .....	175
Advanced Search for Activity Logs.....	175
Exporting Activity Logs.....	176
Action Logs .....	176
Action Logs List Page.....	176
Advanced Search for Action Logs .....	177
<i>Action Details</i> .....	177
Exporting Action Logs .....	178
<b>16. Index.....</b>	<b>179</b>

## Seqrite mSuite Features for Android and iOS

Feature list for Android and iOS devices:

	Feature	Android	iOS
<b>Features</b>	<b>Enrollment</b>		
	Enrollment	✓	✓
	<b>Antivirus</b>		
	Real-Time Protection, Scheduled Scan, Remote Scan, Seqrite mSuite App auto upgrade	✓	✗
	<b>Action on device</b>		
	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	✓	✗
<b>Configuration</b>	<b>Anti-Theft Configuration</b>		
	Notification on SIM change, Lock device on SIM Change, Lock device on Airplane Mode, Block device on SIM Change	✓	✗
	<b>Web Security Configuration</b>		
	Browsing Protection, Phishing Protection, Web Protection, Blacklist/Whitelist URLs, Category Based blocking*	✓	✓
	<b>Wi-Fi Configuration</b>		
	Support different security options	✓	✓
	<b>Schedule Scan Configuration</b>		
	Scheduling new Scan	✓	✗
<b>App Management</b>	<b>Network Usage Configuration</b>		
	Data usage monitoring for Wi-Fi, mobile data, and roaming	✓	✗
	<b>App Management</b>		
	Restrict access to newly installed apps	✓	✗
	Whitelist App	✓	✗
	Recommend app to install, Apps to Remove	✓	✓
	Fully block the blacklisted apps	✓	✗
App Repository	✓	✓	
<b>Other</b>	Individual Device Level App control	✓	✓
	App blocking based on Category	✓	✗
	<b>Fencing</b>		
	Geo, Time, Wi-Fi Fence	✓	✗
<b>App Launcher</b>			
	Advance Launcher, Exit Launcher, App Request	✓	✗

## Seqrite mSuite 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, Block NFC, Block Mobile Data while Roaming	✓	✗
Block Auto-Sync while Roaming	✓	✓
Block Outgoing Call in Roaming, Location Service (GPS), Sync Frequency	✓	✗
Block Certificate	✗	✓
Block Screen Capture	✓	✓
Block Text Copy and Paste	✓	✗
Block 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 mSuite supports Android OS version 5.0 to 9, and iOS 10 and later versions on mobile.

## Chapter

## 1

## Introducing Seqrite mSuite

---

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

This chapter includes:

[Benefits of Seqrite mSuite](#)

[How does Seqrite mSuite work?](#)

### Seqrite mSuite

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

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

#### Benefits of Seqrite mSuite

- Secure and manage all the Android and iOS devices.
- Secure data and resources, enhance user productivity, reduce cost, and maintain communications.
- Perform console administration functions.
- Monitor the device by using policy and configurations.
- Make device compliant with policies.



- Monitor network data usage and call/SMS.
- Manage device app with app configuration.
- Prevent misuse of the device by launching Seqrite Launcher.
- Monitor the device by applying fencing parameters such as time, location, and Wi-Fi.
- Generate the customized reports.
- Remotely access the enrolled mobile device.

## How does Seqrite mSuite work?

Seqrite mSuite works on the Agent-Server architecture where the console (Hosted on Cloud) manages all the mobile devices. The agents can be installed on almost all the flavors of mobile platforms (Android, iOS). For detailed description of console and Agent system requirements and compatibilities, see [System requirements](#). Seqrite mSuite Admin gets full control of the device to manage, monitor, or track the device.

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

## Seqrite mSuite variants

Seqrite mSuite comes in different variants: Standard and Advance.

- Standard: Standard Seqrite mSuite comes with limited set of features.
- Advance: Advance Seqrite mSuite includes all the advance features.

## Features included in variants

The table below gives complete information about the features included in the Standard and Advance Seqrite mSuite 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

- When you ask for trial, you will get the Advance Seqrite mSuite for 1 month and will be applicable for 5 devices.
- After you use your trial copy, you can either purchase the paid Standard or paid Advance variant.
- If you have opted for Standard variant, you can further [upgrade](#) your license to Advance at any point of time.
- If you have opted for Advance variant, you can [Top Up](#) and add more number of devices to your license.

## Tenant and data retention policy on Cloud

- The Trial and Standard license tenants will be completely deleted from mSuite server one month after the license expiry. In result of this, all the user data will be deleted and cannot be recovered.
- The Advance license tenant will be deleted three months after the license expiry. In such scenario, user data will be deleted and cannot be recovered.
- Every tenant Admin will get prior notification before deleting the tenant from mSuite database as follows:
  - 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 limited set of logs/reports on server (based on user license.)
- For Trial and Standard license tenants, only 1-month data will be kept on the server. Data which is 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 period.
- For Advance license tenants, 3 months data will be kept on the server. Data which is older than 3 months will be automatically deleted from the server (this action is irreversible.)

## Seqrite Workspace

Mobile container technology describes a set of software and services that deliver corporate apps, files, and services to a user on any device and over any network. Seqrite Workspace is a container-based application. With the BYOD concept, the mobile container applications become very useful. This helps the employees to maintain and access the personal and corporate data within the single device. Seqrite Workspace enhances employee experience,

security, and data breach protection. Workspace provides a perfect enterprise app catalog that can be mandatorily pushed or optionally downloaded.

### **Seqrite Workspace Advantages**

- With Workspace, you can excellently segregate your personal data with corporate data.
- Support for iOS and Android enables the use of preferred devices for work.
- Useful in managing and accessing your corporate emails and contacts.
- Sync with your corporate meetings with Calendar feature.
- Access or share the important documents that you receive in the vault repository.

## Getting started

---

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

[Prerequisites](#)

[System requirements](#)

### Prerequisites

Before installing Seqrite mSuite on your computer, follow these guidelines:

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

### System requirements

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

<b>Mobile device specifications</b>	<ul style="list-style-type: none"> <li>• Android 5.0 to 9 OS versions.</li> <li>• iOS 10 and later versions.</li> </ul>
<b>Browser requirements</b>	Administrator Web panel, Google Chrome (latest versions), Firefox (latest version), and EDGE (latest versions)
<b>Terminology</b>	<p><b>User:</b> An employee who enrolled the device with Seqrite mSuite.</p> <p><b>Administrator:</b> A user with access to the Seqrite mSuite console to manage the devices.</p>

To check for the latest system requirements, visit our website at [www.seqrite.com](http://www.seqrite.com).

## Registration

---

You must register your product soon after installing it.

This chapter includes the following sections.

[Registration](#)

### Registration

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

### Registering with Seqrite mSuite

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

1. Access the following URL: <https://cloud.mdm.seqrite.com/>
2. On the Sign In page, click **Try Now**.

The [Company](#) page appears.



Note:

---

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

---

3. On the Registration page, enter the **Contact Information**, **Company Information**, and **Verification Code** in the corresponding text boxes.
4. Select the **Terms of agreement** and **Privacy Policy** check box and click **Submit**.  
You will receive a confirmation email from Seqrite mSuite, which includes the product key and **Sign Up** link.
5. In the confirmation email, click the **Sign Up** link.  
Sign Up page is displayed.

6. On the Sign Up page, fill in the required information: First Name, Last Name, Mobile Number, Email ,Confirm Email, Product key, Password, and Confirm Password.
7. Click **Sign-up Account**.

On Successful Sign-up, user can log on to the mSuite console using email ID and password.

## Dashboard

---

Dashboard is the default screen that is displayed after you log on to the Seqrite mSuite console. Dashboard is unique and helps to navigate easily to all the components of the Seqrite mSuite console.

This chapter includes the following sections.

[Notifications](#)

[User Profile](#)

[Menus](#)

[Dashboard](#)

[Informative Section](#)

[Common UI Terminologies](#)

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

- **Notifications:** The upper-right section of the Seqrite mSuite console shows various types of notifications.
- **Global search:** Provides a common option to search all the Seqrite mSuite entities (user, department, device, group, policy, configuration, and app configuration) from any section of the Seqrite mSuite console. You can search by entering any keywords related to the entities. Global search option is available on all the pages of the Seqrite mSuite console.
- **User profile:** The user profile section shows information about the logged-in user. This section helps you to manage admin roles, setup services, and license. You can change password, share feedback about the application, contact support, or view the help and release notes.
- **Menus:** The left vertical section of the Seqrite mSuite console includes menus, which helps the user to navigate to the different sections of Seqrite mSuite application. The menus include Manage, Profiles, Workspace, Apps, Fencing, Reports, and Admin.
- **Dashboard:** The dashboard displays different statuses, which are showed in the form of tiles, graphs, and count. Dashboard shows device statistics, data usage, and information about Workspace.

- **Informative section:** The lower section of Seqrite mSuite console provides important links such as License Agreement and Privacy Policy.

## Notifications

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

Notification type	Description
App request notification	These are the requests to install an app on the device by using App Launcher.
Enrollment notification	These are device enrollment and device Admin notifications.
Device notifications	These notifications include device infection notifications and non-compliance notifications.
Import notification	These notifications are received when an import of any item is initiated or completed, battery notification, and notification for any message from Seqrite.

## User Profile

The User Profile section on the upper-right corner of dashboard shows the user name. When you click the logged on user name, multiple, useful options are displayed such as; [User Management](#), [Setup Services](#), [License Management](#), [Change Password](#), [Share Feedback](#), [Contact Us](#), [Administrator Guide](#), [Release Notes](#), and [Log out](#).

## Menus

Menus show different features of Seqrite mSuite console.

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




Fencing	This menu restricts the devices and app usage with the help of digital fence. The Administrator can configure and apply the fence on different groups.
Reports	Provides On-demand reports for infection status, network data usage, and app-compliance. The Administrator can also create a customized report as per requirement.

## Dashboard

The middle section of dashboard shows following sections:

Section	Description
<b>Overview</b>	
App Non-Compliance Devices (s)	This tile shows the devices which are app non-compliant. It lists those devices which are not compliant with applied app configuration. App is either in pending state for installation/un-installation or Launcher is in pending state for activation/deactivation.
Policy Non-compliance Device(s)	This tile shows the devices with policy non-compliance. It lists those devices which have violated the policy compliance and do not follow the applied policy restrictions.
Agent Vulnerable Device(s)	Displays the number of devices whose Device Administrator check for Seqrite mSuite app has been removed. These devices are vulnerable to Seqrite mSuite app uninstallation (that is - any user can uninstall the Seqrite mSuite Agent from these devices).
Agent Unauthorized Removal	This tile shows the number of devices from which the Seqrite mSuite Agent was removed forcefully without the notification of mSuite Administrator.
Anti-theft Locked Device(s)	Displays the count of the devices that are blocked by Seqrite mSuite Administrator. Click the title and see the details of blocked devices.
Rooted / Jailbroken Devices(s)	Displays the number of enrolled devices that are rooted or jailbroken. The operating system of such devices is tempered, and devices are compromised.
Total Devices	Shows the total number of devices added to Seqrite mSuite console.
Toggle Bar	Click the toggle bar and choose the OS of your device. <ul style="list-style-type: none"> <li>• Android Devices: Shows the total number of Android devices and their Agent versions in the Seqrite mSuite console.</li> <li>• iOS Devices: Shows the total number of iOS devices and their Agent versions in the Seqrite mSuite console.</li> </ul>

Section	Description
<b>Device Agent Enrollment Status</b>	
Unused	Shows the number of devices which are added in the console, but enrollment request is not sent to the devices.
Pending	Shows the number of devices which are pending for enrollment and the Administrator has sent enrollment request to the devices, however device user is yet to install the device.
Enrolled	Shows the number of devices on which the Seqrite mSuite Agent is successfully enrolled with mSuite console.
Uninstalled	Shows the number of devices from which the Seqrite mSuite app has been uninstalled.
Device Last Synced	Displays the total number of devices that synced with Seqrite mSuite 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 Transaction 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 tenant. The chart shows the percentage of data used for each type of transaction.
<b>Device Statistics</b>	
Available Storage	This pie chart shows the number of devices and the available storage on them.
Available Battery	This pie chart shows the number of devices and level of the battery.
Device Manufacturer	This pie chart shows the number of devices and the name of the manufacturer.

Section	Description
Malware Statistics	<p>Displays the graph statistics of virus infections detected on the devices, which are enrolled with the Seqrite mSuite console. Mouse hover over the graph shows the names of the viruses detected, the number of devices infected on a particular date and a link to view the details. This shows the status of infection for the devices that were added to the Seqrite mSuite network upto last 30 days.</p> <p>You can view the entire infection details on the Infection Status Details page. To view the infection details, hover over the graph tips and click the <b>View Details</b> link.</p> <p><b>Infection Status Details page:</b> 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.</p>
Top Malwares	<p>Displays the list of threats, which have affected the large number of devices and the count of the affected devices.</p>
<b>Data Usage</b>	
Data Usage Statistics	<p>The graph displays the status of the network usage for all the devices enrolled with the Seqrite mSuite console. 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.</p> <p>To view the network usage date-wise, you can use the following options: Today, Last 7 days, Last 30 days, Last 15 days, and current month.</p> <p> <b>Tip:</b></p> <hr/> <p>If <b>Today</b> 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.</p>
Max Data Usage Devices	<p>Displays the list of the devices that consume more network data. You can view the name of the device and the data used by the device.</p> <ul style="list-style-type: none"> <li>• To view the Reports page, click <b>View Details</b>. The report shows Internet usage of the devices with respect to Wi-Fi, mobile data, and in roaming status.</li> </ul>
Max Data Usage Apps	<p>Displays the list of the apps that are network-intensive and consume more network bandwidth. You can view the name of the app and the data used by that app.</p> <p>To view the Reports page, click <b>View Details</b>. The report shows the network usage of apps with respect to Wi-Fi, mobile data, and in roaming status.</p>

Section	Description
Most Popular Apps	<p>Displays the list of applications that are downloaded and installed by most of the users. You can view the name, category of the app, and the count of the devices on which the app is installed. On clicking the app count, you are directed to the Devices dialog box, which gives complete information about the devices that have the specific app installed.</p> <ul style="list-style-type: none"> <li>• To exclude the recommended standard apps, select the <b>Exclude recommended apps</b> check box on the right side of Top Installed Apps section.</li> <li>• To view the App Repository page and view all the installed apps within the Seqrite mSuite network, click <b>View Details</b>.</li> </ul>
<b>Workspace</b>	
Total Devices	Shows the total devices enrolled with Seqrite Workspace.
Toggle bar	<p><b>OS Version:</b> Shows the device OS version.</p> <p><b>Workspace Version:</b> Shows the mSuite Workspace version on the device.</p>
Workspace App Enrollment Status	<p><b>Pending:</b> Show the total number of devices on which the Workspace app activation is pending from device user's side.</p> <p><b>Enrolled:</b> Shows the total number of devices on which the user have activated the Workspace app.</p> <p><b>Uninstalled:</b> Shows the total number of devices from which, Workspace app has been uninstalled.</p>
Workspace Web Violation	Shows the number of devices which have violated the Workspace web policies in last 30 days.


## Informative Section

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

Section	Description
License Agreement	Shows the end-user license agreement.
Privacy Policy	Displays privacy policy of Seqrite mSuite.

## Common UI Terminologies

On all the pages of Seqrite mSuite console, few common fields and buttons are available. The table below gives information on common UI terminologies:

UI terminology	Description
Global search	Helps to search the entities from any part of Seqrite mSuite console.
Search	<p>Helps to search an entity by entering particular keywords as per your requirement.</p> <p>When you search anything from Users and Devices list page, make sure the respective column is available on the list page.</p> <p> <b>Tip:</b></p> <hr/> <p>To search the users or devices according to the mobile number, make sure that the mobile number column is visible on the respective list pages. If the column is not present, then the search for mobile number will not reveal the correct result. To get the relevant result, you should select the mobile number column from Filter columns list.</p>
View	<p>This list helps to select and view the number of records per page. Click inside the list and select the number of records to be viewed in single instance.</p>
Add	<p>The Add button is available on all the pages of different modules. With the Add button, you can add the required entity to the Seqrite mSuite console.</p> <p>This button is also available on the Details page of all the components of the Seqrite mSuite console.</p>
Import	<p>Use the Import option to import the entities to the Seqrite mSuite console. This option is helpful if you have a long list of entities or if you have exported the entities from the Seqrite mSuite console earlier. This button is available on all the list pages of the components of the Seqrite mSuite console.</p> <ul style="list-style-type: none"> <li>• You can import entities from Manage section, Policies, and Geo Fence.</li> <li>• To view the sample CSV file format, click <b>Download CSV sample Format</b>. Only CSV file format is supported.</li> </ul> <p>In case of importing the policy, only .xls file format is supported. Ensure to check dependencies before creating new policies.</p>
Export	<p>With the Export option, you can export the entities from the Seqrite mSuite console. This option is helpful if you have to export the long list of entities registered with the Seqrite mSuite console and want to retain them. You can import the other entities back to Seqrite mSuite easily whenever you require.</p> <p>This button is available on all the list pages of the components of the Seqrite mSuite console.</p>

UI terminology	Description
Filter columns	<p>The Filter columns tab is available on all the list pages of Seqrite mSuite console. Seqrite mSuite provides an option to filter the table columns and to choose the desired columns on the list page.</p> <ul style="list-style-type: none"> <li>• On Users list page, you can select up to 4 columns and on Devices list page, you can select up to 8 columns only.</li> <li>• The On Demand Reports and activity logs section do not show the Filter columns option.</li> </ul> <p>To filter the columns, follow these steps:</p> <ol style="list-style-type: none"> <li>1. To filter any columns from the list page, click <b>Filter column</b>. The list of available columns with check boxes is displayed.</li> <li>2. Select the desired column name check box, which is to be displayed in the table. Clear the check box if the column is not to be displayed on the list page table.</li> </ol>
Previous	<p>This button is available on the Overview pages of few modules. This button helps to go back to the previous entity and view the details of the previous entity.</p>
Next	<p>This button is available on many Overview pages of the modules. This button helps to proceed to the next entity and view the details. For example, if you are on the Overview page of User 1 and click the Next button, you are directed to the Overview page of User 2.</p>
Pagination	<p>Helps to navigate easily through the huge number of records.</p>
Sort	<p>Every table column on Seqrite mSuite console has the sorting icon. With this icon, you can organize the column data in ascending or descending order.</p>
With selected	<p>On selecting single or multiple entities on any list pages, the With selected option is displayed. The With selected list provides multiple options according to the entities.</p>

## Notifications

---

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

This chapter includes the following sections.

[Notifications Dialog box](#)

[Notifications List Page](#)

[Enrollment Notification](#)

[Enrollment Notification](#)

[Agent Vulnerable Notification](#)

[Accessibility Permission Revoked](#)

[Report Notification](#)

[Scan Report](#)

[Non-compliant Report](#)

[Info Notification](#)

[Import Notification](#)

[Fence Notification](#)

[Battery Notification](#)

[Messages from Seqrite](#)

[App Request Notification](#)

[Workspace Notifications](#)

## Notifications Dialog box

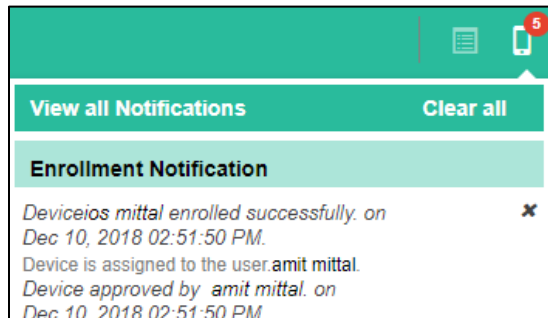


Figure 1

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

The notifications dialog box shows the following options:

Options	Description
View all Notifications	This option when clicked, navigates you to that specific notifications list page where all the notifications are displayed.
Clear all	With this option, all the notifications from the notification dialog box are cleared.
Mark as read (multiplication sign)	When the multiplication sign is clicked, that notification is marked as read and is removed from the notification dialog box. All the notifications Marked as read are added to the notifications list page.

## Notifications List Page

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

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



## Advanced Search for Notifications

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

### Searching notifications

To search the notifications, follow these steps:

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

Notifications can be searched using the following parameters:

- **Select limit from:** Select the limit to view the notifications for a particular period. The available options are Today, Since Yesterday, Last 7 days, Last 30 days, and Last 3 months.
- **Select Notification Type:** Search by selecting the type of notifications such as Enrollment Notification, Report Notification, Info Notification, App Request Notification, and Secure Workspace Notifications.
- **Select Report Type:** Depending on the selected notification type, select report type list is displayed. Select the required report type.



Note:

---

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

---

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

The search result is displayed.

### With selected Options for Notifications

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

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

### Using With selected option for notifications

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

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

Notifications list page is displayed.

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

The With selected option is displayed.

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

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

## Enrollment Notifications

The mobile icon on the upper-right side of the task bar indicates enrollment notifications. The enrollment notifications dialog box shows few newly received device enrollment notifications.

Enrollment Notification

Agent Vulnerable Notification

Accessibility Permission Revoked

## Enrollment Notifications

It lists all the notifications related to the device enrollment. These notifications include the status of the device enrollment such as; Approval, Approval Pending and time and date of the device enrollment. You can approve or disapprove the device enrollment directly using enrollment notifications.

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

## Viewing enrollment notifications

To view the enrollment alert, follow these steps:

1. Log on to the Seqrite mSuite console and click mobile icon.
2. Click **View all Notifications**. You are redirected to the notifications page.
3. On the Notifications page, click **Advanced Search**.
4. In Select Notification Type list, click **Enrollment Notification**.
5. In Select Report Type list, click **Enrollment Notification**.
6. Click the time duration to view the notifications and click **Search**.

All the enrollment notifications for the selected time period are displayed.

The list of enrollment requests is displayed.

## Approving device enrollment request

To approve device enrollment request, follow these steps:

1. Log on to the Seqrite mSuite console and click mobile icon.

On the enrollment notification dialog box, the requested enrollment notification will show Approve and Disapprove options.

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

### Disapproving device enrollment request

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

To disapprove the device enrollment request, follow these steps:

1. Log on to the Seqrite mSuite console and click mobile icon.  
On the enrollment notification dialog box, the requested enrollment notification will show Approve and Disapprove options.
2. Click the **Disapprove** option.
3. On the confirmation dialog box, click **Disapprove**.

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

### Device Admin Notification

This notification informs if any Device Admin is deactivated from the user device.

### Agent Vulnerable Notification

When the device ownership applied to Seqrite mSuite app is deactivated, then the mSuite Agent becomes vulnerable to many infections. Thus, when device administrator is deactivated, you receive Agent Vulnerable notification.

### Viewing agent vulnerable notifications

1. Log on to the Seqrite mSuite console and click mobile icon.
2. Click **View all Notifications**. You are redirected to the notifications page.
3. On the Notifications page, click **Advanced Search**.
4. In Select Notification Type list, click **Enrollment Notification**.
5. In Select Report Type list, click **Agent Vulnerable Notification**.
6. Click the time duration to view the notifications and click **Search**.

A list of notifications is displayed with device name from where Seqrite mSuite device ownership has been removed and mSuite Agent has become vulnerable.

### Accessibility Permission Revoked

You get this notification when the accessibility permission for Seqrite mSuite and Launcher app has been disabled or disconnected. If this notification is viewed, then the accessibility services

on the device would not be working as expected, that is, the web security and app control functionality would not be functioning.

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

### **Viewing devices on which accessibility services permission has been removed**

1. Log on to the Seqrite mSuite console and click mobile icon.
2. Click **View all Notifications**. You are redirected to the notifications page.
3. On the Notifications page, click **Advanced Search**.
4. In Select Notification Type list, click **Enrollment Notification**.
5. In Select Report Type list, click **Accessibility Permission Revoked**.
6. Click the time duration to view the notifications and click **Search**.

The notification list is displayed with the devices on which the Accessibility Service for mSuite and launcher app has been removed.

## **Alert Notification**

This notification sends alert messages that need immediate attention. The alert message may be on scan report, failed attempt for app upgrade, and if any device is non-complaint.

To view the alert notifications, follow these steps:

1. Log on to the Seqrite mSuite console.
2. Hover over the bell icon for alert notification.

All the alert messages are displayed in a list.

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

The details of the notification is displayed according to the incident such as failed attempt for app upgrade, non-complaint devices, and so on.

## **Report Notification**

This notification gives information in report format for scan and non-compliance.

## **Scan Report**

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

## Viewing device scan summary

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

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

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

## Non-compliant Report

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

## Viewing the device non-compliance report

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

1. Log on to the Seqrite mSuite console and click **Device Notifications** (bell icon).
2. Go to that device notification, of which you want to view the non-compliance report and click the **View Report** link available in front of it.
3. The Device Non-Compliance Report shows the non-compliant policies and configuration information as follows:
  - The policies table shows the name of the device and the recommended policy, and the following information:

- Policy: Shows the name and type of the policy.
- Reason: Shows the reason for device non-compliance with respect to the policy.
- Reported Date: Shows the date when the device was non-compliant with the policy.
- Resolved Date: Shows the date when the policy non-compliance was resolved.
- Status: Shows the status of the policy.
- The configuration table shows the following information:
  - Configuration Type: Shows the type of the configuration.
  - Name: Shows the name of the configuration.
  - Reason: Shows the reason of device non-compliance with respect to configurations.
  - Reported Date: Shows the date when the configuration non-compliance occurred.
  - Resolved Date: Shows the date when the configuration non-compliance was resolved.
  - Status: Shows the status of the configuration.

4. Click **Close**.

## Info Notification

This notification gives information about functionalities such as import, fence, battery, and message from Seqrite.

## Import Notifications

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

### Import a notification

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

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

### Viewing import notifications

To view the import notifications, follow these steps:

1. Log on to the Seqrite mSuite console and click the info notification icon.  
Few import notifications are displayed if they are available.
2. Click **View all Notifications**. You are redirected to the notifications page.

3. On the Notifications page, click **Advanced Search**.
4. In Select Notification Type list, click **Info Notifications**.
5. In Select Report Type list, click **Import Notification**.
6. Click the time duration to view the notifications and click **Search**.

All the import notifications for the selected time period are displayed.

## Fence Notification

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

### Viewing fence notifications

To view the import notifications, follow these steps:

1. Log on to the Seqrite mSuite console and click the info notification icon.  
Few fence notifications are displayed if they are available.
2. Click **View all Notifications**. You are redirected to the notifications page.
3. On the Notifications page, click **Advanced Search**.
4. In Select Notification Type list, click **Info Notifications**.
5. In Select Report Type list, click **Fence Notification**.
6. Click the time duration to view the notifications and click **Search**.

All the fence notifications for the selected time period 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 notifications

To view the import notifications, follow these steps:

1. Log on to the Seqrite mSuite console and click the info notification icon.  
Import notifications dialog box displays few newly received notifications.
2. Click **View all Notifications**. You are redirected to the notifications page.
3. On the import notifications dialog box, click the **View all Notifications** link.
4. On the Notifications page, click **Advanced Search**.
5. In Select Notification Type list, click **Info Notifications**.

6. In Select Report Type list, click **Battery Notification**.
7. Click the time duration to view the notifications and click **Search**.

All the battery notifications for the selected time period are displayed.

## Messages from Seqrite

The mSuite Administrator receives notifications from Seqrite about different Seqrite announcements, upgrades, license information etc. These notifications are displayed as push notifications and once read, they get listed in Messages from Seqrite notification list.

### mSuite App Log Notification

In case the mSuite App is locked, a notification is sent to the administrator.

### Viewing mSuite App Log Notification

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

1. Log on to the Seqrite mSuite console and click the info notification icon.
2. All the notifications are displayed, if they are available.
3. To see the details of a notification, click on the link under the notification. You are redirected to the relevant screen.

## App Request Notifications

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

### Viewing app requests

To view the app request notifications, follow these steps:

1. Log on to the Seqrite mSuite console and click Note icon.
2. In App Request Notification dialog box, click **View All App Requests**.

The Notifications page is displayed with a list of App Request Notifications.

3. To view the details of the selected app request notification, click **View Details** on the App request notification.

The Device App Request notification is displayed.



## Device app request report

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

## Accepting or rejecting the app request

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

1. Log on to the Seqrite mSuite console and click **Alerts**.
2. In the Alert dialog box, click **App Request**.

The details of app request are displayed with 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**.

## Device Accessibility Notification

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

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

## Workspace Notifications

In this section, all the Workspace related notifications are received. You receive notifications about the enrollment and uninstallation of the Workspace app, locking of Workspace app and complete deletion of data from the Workspace app.

- **Workspace Enrollment:** This notification gives information about the device enrollment with the Workspace app.
- **Workspace Uninstallation:** This notification gives information about the devices from which the Workspace app has been removed.
- **Workspace Time-bomb Trigger:** This notification gives information about the devices from which the Workspace data has been removed completely.

- **Workspace Locked:** This notification gives information about the devices which were locked for the specified time due to invalid login attempts.

## Viewing Workspace notifications

To view Workspace notifications, follow these steps:

1. Log on to the Seqrite mSuite console.
2. Hover over the Workspace notification icon. Few Workspace-related notifications are displayed.
3. To view all the Workspace notifications, click the **View All Workspace Notifications**.
4. On the Notifications page, click **Advanced Search**.
5. In Select Notification Type list, click **Workspace Notifications**.
6. In Select Report Type list, select the required notification type.
7. Click the time duration to view the notifications and click **Search**.

All the Workspace related notifications for the selected time period are displayed.

## Delete all Notifications

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

### Deleting all notifications

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

1. Log on to the Seqrite mSuite console and click any of the notifications icon.
2. In notifications dialog box, click the link to view all the notifications.  
Notifications list page is displayed.
3. To delete the notifications from the Notifications list page, you can use either of the options:
  - In the upper-right corner, click the **Delete all Notifications** button. On the confirmation screen click **OK**.  
All the notifications of a specific notification type are deleted.  
OR
  - On notifications list page, select the notifications check boxes which are to be deleted. The With selected option is displayed. From With selected list, select **Delete** > click **Submit** > click **OK**.

## User Profile

---

This chapter includes following sections:

[User Management](#)

[Setup Services](#)

[License Management](#)

[Change Password](#)

[Share Feedback](#)

[Administrator Guide](#)

[Contact Us](#)

[Release Notes](#)

[Log Out](#)

## User Management

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

The Super Administrator is the main administrator of the Seqrite mSuite console. The Super Administrator can create the admin by assigning the admin roles and privileges to any existing user.

### Types of admin roles

The admin roles are based on privileges with restricted access to the mSuite console.

## Super Admin

The Super Admin role is created when your Seqrite mSuite company is created. For the entire Seqrite mSuite console, a single Super Admin is assigned. The Super Admin can create multiple Admins with administrator role. The Super Admin has all the privileges such as read, create, update, delete, assign/unassign, approve/disapprove, and perform basic, advance, and critical actions, for all the modules of Seqrite mSuite. The Super Admin also has the privilege to set up services such as APNS, Agent upgrade, Agent preference etc. and also can customize the reports as per requirement.

### Assigning Super Admin role to an Admin

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

## Admin

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

## Advanced

The Advanced Admin role type has all the privileges except the delete privilege for the assigned department only. The Advanced Admin role doesn't have any privilege to create, update, assign/unassign, and delete admin role. Also, cannot upgrade or renew the license.

## Standard

The Standard Admin role type has all the privilege such as update, assign, and unassign. The Standard Admin role is restricted only to the assigned department.

The Standard Admin role cannot:

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

## Basic

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

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

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

Privileges	Entity / Admin Roles				
	Basic	Standard	Advanced	Admin	Super
<b>User</b>					
Read	✓	✓	✓	✓	✓
Create	✗	✗	✓	✓	✓
Update	✗	✓	✓	✓	✓
Delete	✗	✗	✗	✓	✓
Send enrollment request	✗	✗	✓	✓	✓
<b>Department</b>					
Read	✓	✓	✓	✓	✓
Create	✗	✗	✓	✓	✓
Update	✗	✓	✓	✓	✓
Delete	✗	✗	✗	✓	✓
Assign/Unassign	✗	✓	✓	✓	✓
<b>Admin Role</b>					
Read	✓	✓	✓	✓	✓
Create	✗	✗	✗	✓	✓
Update	✗	✗	✗	✓	✓
Delete	✗	✗	✗	✓	✓
Assign/Unassign	✗	✗	✗	✓	✓
<b>Device</b>					
Read	✓	✓	✓	✓	✓
Create	✗	✗	✓	✓	✓
Update	✗	✓	✓	✓	✓
Delete	✗	✗	✗	✓	✓

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

Privileges	Entity / Admin Roles				
	Basic	Standard	Advanced	Admin	Super
Read	✓	✓	✓	✓	✓
Renew	✗	✗	✗	✓	✓
Upgrade	✗	✗	✗	✓	✓
<b>Report</b>					
Read	✓	✓	✓	✓	✓
Create	✗	✗	✓	✓	✓
Delete	✗	✗	✗	✓	✓
Update	✗	✓	✓	✓	✓
<b>App Control</b>					
Read	✓	✓	✓	✓	✓
Create	✗	✗	✓	✓	✓
Update	✗	✓	✓	✓	✓
Delete	✗	✗	✗	✓	✓
App Repository	✗	✗	✓	✓	✓
Assign/Unassign	✗	✓	✓	✓	✓
<b>Notification</b>					
Read	✓	✓	✓	✓	✓
Delete	✗	✗	✗	✓	✓
<b>Workspace Device Actions</b>					
Basic actions (*): Remote Buzz/Locate/Trace/Scan/Sync/Broadcast	✗	✓	✓	✓	✓
Advance actions (**): Lock/Unlock/Push(Policy/Configurations)/Add-Remove App/Call-SMS log	✗	✗	✓	✓	✓
Critical actions (***): Wipe/Disconnect/Uninstall	✗	✗	✓	✓	✓
<b>Workspace Policy</b>					
Create	✗	✗	✓	✓	✓
Update	✗	✓	✓	✓	✓

Privileges	Entity / Admin Roles				
	Basic	Standard	Advanced	Admin	Super
Delete	x	x	x	✓	✓
Apply/Revoke	x	✓	✓	✓	✓
<b>Workspace Profile</b>					
Create	x	x	✓	✓	✓
Update	x	✓	✓	✓	✓
Delete	x	x	x	✓	✓
Apply/Revoke	x	✓	✓	✓	✓

\* You can change the privileges as per your requirement or you can assign the default privileges.

### Group-wise visibility for mSuite console

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

When such restricted user with 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 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 advanced search option, follow these steps:

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **User Management** > **Advanced Search**.
2. From the Select Created By list, select the desired creator name and click **Search**.

The result gets displayed.

### User Management List Page

The User Management list page displays all the available admin roles in Seqrite mSuite console. The table shows the information about all the admin roles.



## With selected options for admin roles

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

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



Note:

---

- You cannot delete the default admin roles.
  - You cannot delete a user assigned to an admin role.
- 
- Select the required options and click **Submit**.

## Creating Admin role

To create a new admin role, follow these steps:

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **User Management > Add**.

The Create Admin Role page is displayed.

2. Enter the Admin Role Name.
3. In the Inherit from list, select the admin role type.

After you select the admin role type, the default privileges assigned to the admin role type appears.

4. Modify the privileges and click **Save**.

The new admin role is created.

## Overviewing Admin Role

After you create a new admin role, you can view the information of the admin role and add the users to any particular role type. You can edit the newly created admin roles, change the privileges, and assign the newly created admin roles to the users. You cannot edit the default admin role types.



Note:

---

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

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

---

To view the Admin Role Details page, follow these steps:

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **User Management**.
2. On the User Management page, select the admin role and click the **Edit** icon.

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

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

## Editing admin role

This section allows you to 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 the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **User Management**.
2. On the User Management page, select the Admin role and click the **Edit** icon > **Edit** tab > **Edit details**.
  - You can edit the admin role name, admin role type, and turn on/off the privileges.



Note:

---

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

---

3. Click **Admins** section.

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



Tip:

---

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

---

## Deleting admin role

1. To delete the Admin role, log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **User Management**.

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

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

The default admin roles cannot be deleted and so Delete icon is not available in the table for such default admin roles.

- On User Management list page, select single or multiple admin roles. The With selected option is displayed. From With selected list, select **Delete** and then click **Submit**.

## Setup Services

The Setup Services section lets you register cloud services for the Android and iOS devices. These setup services allow the communication between Agent and server. It is a one-time activity to be done on the Seqrite mSuite console. The service helps you to send messages from the server to the enrolled devices. This acts as an interface between the Agent and server. The Setup Services include Apple Certificate, Seqrite mSuite and Launcher Upgrade Setting, Agent Preferences, Company Branding, Notification Preferences, and SMS Settings.



Note:

---

The Setup Services section is visible to Super Admin and to the Admin with the Super Admin privilege.

---

## Apple Certificate

Apple Push Notification Service helps you to configure cloud services for the iOS devices. Customers must have an Apple ID for configuring APNS mSuite certificate and use their Apple mSuite Certificate to send the push notification to the device. This is the one-time activity and follow the further instructions given on the Seqrite mSuite console.

Two options are displayed:

- **Renew Now:** Use this option to renew the Apple mSuite Push Certificate prior to its expiration.
- **Remove Certificate:** Use this option, if you do not wish to manage the iOS devices.

## Agent Upgrade

The Upgrade Setting section gives you information about sharing the updated versions of Seqrite mSuite Agent app and Seqrite Launcher Agent app using different app source types.

## mSuite Upgrade

The Seqrite mSuite Upgrade setting helps you to send the updated version of the Seqrite mSuite Agent from the server to the user's device. Keeping the Seqrite mSuite Agent app updated gives you access to the latest features and improves the device security. This setting provides different sources to download and install the updated version of the Seqrite mSuite Agent.

Before you send the update of the Agent app to the users, you must enable the Upgrade Seqrite mSuite Notification option. In addition, you must set the frequency to send the upgrade

Seqrite mSuite alert. This alert helps to send the prompt to the users to update the Seqrite mSuite app to the latest version at the selected frequency.

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

### **Default Location for Seqrite mSuite**

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

### **Updating Seqrite mSuite app via Default Location**

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

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Setup Services > Agent Upgrade > mSuite Upgrade**.
2. Turn ON the **mSuite Upgrade Notification** and select the **Alert To Upgrade mSuite** duration in hours.
3. Select the App Source Type as **Default Location**.  
The Package ID option will be pre-filled.
4. Click **Save**.

### **Custom URL for Seqrite mSuite**

With the Custom URL option, you can download the Seqrite mSuite Agent app from the custom URL on your own company's Cloud. After you upload the Seqrite mSuite Agent app on Cloud, the user receives a prompt about the availability of the update of the Seqrite mSuite Agent app. Thus, the user can download and install the updated Seqrite mSuite Agent and in-built wakeup app from the company's Cloud URL.

### **Uploading custom URL on Cloud**

To upload custom URL on Cloud, follow these steps:

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Setup Services > Agent Upgrade > mSuite Upgrade**.
2. Turn ON the **mSuite Upgrade Notification** and select the duration from the **Alert To Upgrade mSuite** list.
3. Select the App Source Type as **Custom URL**.  
The Custom URL section is displayed.
4. Select **App MD5 hash**.
5. Enter Version Name, Version Code, Package Id, and URL of apk. file in the respective text boxes.
6. Click **Save**.

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

### Upload Seqrite mSuite App

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

### Uploading APK on Seqrite mSuite Cloud

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

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Setup Services > Agent Upgrade > mSuite Upgrade**.
2. Turn ON the **mSuite Upgrade Notification** and select the duration from the **Alert To Upgrade mSuite** list.
3. Select the App Source Type as **Upload mSuite App**.  
The Package ID option will be pre-filled.
4. Select **App MD5 hash**.
5. Select the APK file and click **Save**.

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

6. On the device, tap the **Install** button to install the latest Seqrite mSuite 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 updated Launcher Agent gives you the access to the latest features and improves the device security. The new launcher version can be downloaded and installed from Default Location, custom URL, or APK.

To send the update of the Launcher Agent to the users, you must enable the Launcher Upgrade Notification option. In addition, you must set the frequency to send the user the alert to upgrade the Launcher application.

### Default Location for Launcher

With this option, you can send the updated version of the Launcher app via Default Location. All the Seqrite Launcher users can download the app from the default location of Launcher app and install it on the device.

## Updating Launcher Agent via Default Location

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

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Setup Services > Agent Upgrade > Launcher Upgrade**.
2. Turn ON the **Launcher Upgrade Notification** option and select the frequency, in hours to send the alert to the user to upgrade the Launcher.
3. From the App Source Type option, select **Default Location**.

Package ID is pre-filled.

4. Click **Save**.

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

## Custom URL for Launcher

The custom URL option is helpful to you to download the Launcher Agent from the custom URL on your own company's Cloud. After you upload the Launcher Agent on Cloud, the user receives a prompt about the availability of the update. The user can download and install the updated Launcher Agent from the company's Cloud URL.

## Downloading Launcher Agent from custom URL

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

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Setup Services > Agent Upgrade > Launcher Upgrade**.
2. Turn ON the **Launcher Upgrade Notification** option and select the frequency, in hours. This will help you to send an alert to the user to upgrade the Launcher Agent.
3. From the App Source Type option, select **Custom URL**.
4. Select **App MD5 hash**.
5. Enter Version Name, Version Code, Package Id, and URL of apk. file.
6. Click **Save**.

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

## Upload Launcher App

With this option you can upload the Launcher APK on Seqrite mSuite Cloud. After the APK is uploaded on the Seqrite mSuite Server, the Seqrite Launcher app will be downloaded to the device and the user must install it.

## Uploading Launcher APK on Seqrite mSuite Cloud

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

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Setup Services > Agent Upgrade > Launcher Upgrade**.
2. Turn ON the **Launcher Upgrade Notification** option and select the frequency, in hours. This will help you to send an alert to upgrade the Launcher Agent.
3. From the App Source Type option, select **Upload Launcher App**.  
The Package ID option will be pre-filled.
4. Select **App MD5 hash**.
5. Select the file from your computer to upload the APK and click **Save**.  
If the old version of Launcher is installed on the device, then as soon as the device syncs with the server, the APK will be downloaded automatically on the device. The user will be prompted to install the new version of the Seqrite mSuite Agent.
6. On device, tap the **Install** button to install the latest Seqrite Launcher Agent.

## Workspace Upgrade

With Workspace Upgrade option you can send the updated version of the Workspace app from the server to the users' device. The updated Workspace app gives you access to the latest version of Workspace. The upgrade can be downloaded and installed from the default location or Workspace app APK.

To send the update of the Workspace app to the users, you must enable the upgrade notification option. In addition, you must set the frequency to send alert to the users to upgrade the Workspace application.

### Default Location for Workspace app

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

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

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Setup Services > Agent Upgrade > Workspace App Upgrade**.
2. Turn ON the **Workspace App Upgrade Notification** option and select the frequency, in hours, to send the alert to the users to upgrade the Workspace app.
3. From the App Source Type option, select **Default Location**.  
The Package ID is pre-filled.

4. Select **App MD5 hash**.
5. 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 Seqrite mSuite Cloud. After the APK is uploaded on the Seqrite mSuite Server, the Workspace app will be downloaded on the devices and the users must install it.

### Uploading Workspace APK on Seqrite mSuite Cloud

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

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Setup Services > Agent Upgrade > Workspace App Upgrade**.
2. Turn ON the **Workspace App Upgrade Notification** option and select the frequency, in hours. This will help you to send an alert to Agent.
3. From the App Source Type option, select **Upload Workspace App**.

The Package ID option will be pre-filled.

4. Select the file from your computer to upload the APK and click **Save**.

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

- To install the latest Workspace app on the device, tap **Install**.

### mSuite Agent Preference

Seqrite mSuite Agent Preference option gives you the privilege to choose the default or custom build of mSuite Agent on your organization's Android devices for enrollment. Selecting the Agent preference is one-time activity. Make sure all your devices have same Agent app preference. If you wish to change the Agent app preference, uninstall all the devices from the console and again enroll them with the required Agent preference.

Default App: Choose this option if you wish to use the default mSuite app from Seqrite.

Custom App: Choose this option if you have customized the app as per requirement.

### Changing the mSuite Agent preference

To change the Agent app preference, follow these steps:

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Setup Services > mSuite Agent Preference**.
2. In App Preference section, select either Default or Custom app, as per your requirement.
3. Click **Save**.



## Company Branding

With the Custom Settings, you can edit the company name, logo, Launcher wallpaper, QR code validity of the logged in tenant, and email setting for non-compliance reports.

### Company Setting

In this section, as soon as you update the company name, it gets reflected on the Seqrite mSuite console, About screen of Seqrite mSuite Agent app, and on the Launcher app. The Company Logo option is to edit the company logo on the Launcher. Whenever, the device syncs with the server, the updated logo reflects on the Launcher.

#### Editing company name and logo

To edit the company name and logo, follow these steps:

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Setup Services** > **Company Branding** > **Company Setting**.
2. In Company Setting section, click the company logo.  
Camera icon is displayed.
3. Click the arrow next to the camera.
  - To add a new company logo, click **Upload**.
  - To remove company logo, click **Delete**.



Note:

---

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

---

### Device Wallpaper

To have a good user experience, the device wallpaper can be edited. You can upload the wallpaper from the server console and this wallpaper reflects on the devices that are ADO and KNOX supported with OS 6 or later versions. The updated wallpaper reflects on the device when the device syncs with the server or the Admin sends a sync command.



Note:

---

- The device wallpaper image resolution must be 1080 x 1920.
- The device wallpaper reflects on the device when the device syncs with the server or the Admin sends a sync command.

- There is a provision to change the launcher wallpaper from [Launcher Settings](#) section of app configuration. The Launcher Settings (app configuration) override the Launcher Wallpaper Setting (Custom Setting).
- 

## Editing device wallpaper

To edit the Launcher wallpaper, follow these steps:

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Setup Services > Company Branding > Company Settings > Device Wallpaper**.
2. Hover over the device wallpaper space. The Camera icon is displayed.
3. Click the arrow next to the camera.
  - To add a new device wallpaper, click **Upload**.
  - To remove the device wallpaper, click **Delete**.

## Notification Preference

With Notification Preference, the Admin can set the channel to receive notification on the mSuite console. Few default notifications are selected, but you can select your own preference of notifications to be received.

- **Console Notification:** You can select the required notification type check box to receive the notifications on the console. By default, Message from Seqrite notification is already set and cannot be changed. Other few notifications are also selected by default, but you can change the preference as per your requirement.
- **Email Notification:** With this option, you can select the check boxes to receive email notification for selected incidents. You will not receive any email notification for Fence Trigger as it is configured in fence configuration settings. You can add maximum three email IDs to send email notifications to the respective users.

## Creating Notification Preference

To create notification preference, follow these steps:

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Setup Services > Notification Preference**.
  - From Console Notification list, select the required check boxes to receive the notifications on mSuite console for the specific notification type.
  - From Email Notification list, select the required check boxes to receive notifications from email. Then enter the comma-separated email IDs in the text field to send email notification. Thus, only the added users will receive the email notification for each incident.

For example, to receive notifications for device enrollment on console and through email, select the Console Notification and Email Notification (to receive email, add in the email IDs in the text field) check boxes available in front of Device Enrollment option.

Notification Type	Console Notification ⓘ	Email Notification ⓘ
Device Enrollment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Malware detection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Non-compliance	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Low Battery	<input checked="" type="checkbox"/>	<input type="checkbox"/>

2. Click **Save**.

Notification preference to receive notifications on the console and through email is set.

## SMS Settings

Configure the third-party SMS gateway to receive SMS notification when the battery level goes below 15%.

### SMS Gateway Integration

If you want to receive the battery notification when any device battery level goes below 15%, then you must configure your own SMS gateway. The third-party SMS gateway is required to send SMS to the device users.

#### Configuring SMS Gateway

To configure the SMS gateway, follow these steps:

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Setup Services > SMS Settings**.
2. In the first field, enter the SMS server URL.
3. Then enter the Sender Id, mobile number key, and message key.
4. Click **Save**.

### SMS Battery Notification

When the SMS Battery Notification is configured, then you receive a SMS notification for those devices, whose battery level goes below 15%. To receive this SMS notification, you must configure your SMS Gateway with mSuite console.

#### Configuring SMS for battery notification

To configure SMS Battery Notification, following these steps:

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Setup Services > SMS Settings > SMS Battery Notification**.
2. Select the **Send SMS for battery below 15%** check box.
3. Add in the admin mobile number. You can add up to three, comma-separated mobile numbers.

4. Click **Save**.

## Custom Account Settings

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

### Email (IMAP/POP) Settings

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

#### Configuring Email (IMAP/POP) Settings

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

1. Log on to the Seqrite mSuite console. On the right upper corner, hover over the setting icon and then click **Setup Services**.
2. On the Setup Services screen, click **Custom Account Settings**.
3. In Email (IMAP/POP) Settings, select the **Account Type**. You can select IMAP or POP service for email communication.
4. Configure **Incoming mail server, Port and Encryption Type, Outgoing mail server (SMTP), and Port and Encryption Type**. Ensure 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 the Seqrite mSuite console. On the right upper corner, hover over the setting icon and then click **Setup Services**.
2. On the Setup Services screen, 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 the Seqrite mSuite console. On the right upper corner, hover over the setting icon and then click **Setup Services**.
2. On the Setup Services screen, click **Custom Account Settings**.
3. In Calendar (CALDAV) Settings, configure **Server URL** and **Port**.
4. To save your settings, click **Save**.

## Flash mEnrollment

The Flash mEnrollment allows bulk enrollment without manual interference for individual device. The Admin imports device IMEI on mSuite console and the device gets enrolled automatically with the mSuite by installing the mSuite agent on the device. This enrollment is done without the need for OTP or Scan QR code for the enrollment. Enterprise device users can have a hassle-free use of the device without thinking about the registration, OTP, or configurations.

If you prefer Flash mEnrollment, you must import device IMEI, group name and device owner 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.



Note:

---

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

---

## Enrolling device with Flash mEnrollment

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

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Setup Services** > **Flash mEnrollment**.
2. 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.
3. 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.

4. 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.
5. Click **Save**.

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

## License Management


The License section lets you view the license details of the product. You can view the details of the owner of the licensed copy with the following information:

- **Overview:** With Overview, you can view the Company Name, Company Code, Product Name, Product Type, License Type, Product Key, License Valid, Number of Devices, Workspace Devices, Contact Name, Contact Email, and Contact Number. In addition, you can edit the Contact Name, Contact Email, and Contact Number.

In the license section, you can perform different actions such as:

- **Update License Information:** Helps to refresh or sync the details of the license.
- **Renew:** Helps to renew the product license. This option is visible to the users' whose license is about to expire or has expired.
- **Add Devices to License:** Helps to include additional devices to your product license. This option is visible to the active paid users.
- **Upgrade:** This option helps to upgrade the mSuite software to avail of the advanced features. If the user has Standard license then they can upgrade to Advanced variant.
- **History:** The History tab lets you view the details of the product license. The history of the license stores all the changes that have been done to the product license such as Registration, Update, Addition, and Renew.
  - The License History table shows the following information:

Columns	Description
Action	Displays the action that is performed on the product license. The actions can be registration of the license, updating the license, renewing, and the addition of the devices to the Seqrite mSuite account. The actions include Registration, Update, Addition, and Renew.
Action Date	Displays the date on which the action was performed on the product license.

License Type	Displays the type of the license.
Product Key	Displays the product key of the license.
Total Devices	Shows the total number of the devices enrolled for a product license.
Duration	Shows the duration of the license.
Expiry Date	Displays the liable expiry date of the license.
Contact Email	Displays the email id of the Super Admin.
Contact Name	Displays the contact name of the Super Admin.
Contact No.	<p>Displays the contact number of the Super Admin.</p> <p> Note:</p> <hr/> <p>Whenever the Admin is changed, you can edit the Contact Name, Contact Email, and Contact Number.</p> <hr/>

## Buy Subscription

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

To purchase Seqrite mSuite, follow these steps:

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **License Management** > **Buy Subscription**.  
OR click **Buy Subscription** on the console header.
2. On the Seqrite web page, add in the endpoints > Add to cart > Checkout > fill in billing information.
3. Then click **Continue**. Receive order review > click **Place Order**.
4. Make your payment. The process is complete.
5. Re-login to the mSuite console to see the changes in the license information.

## Renew

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

To renew Seqrite mSuite software, follow these steps:

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **License Management** > **Renew**.
2. On the re-login notification, click **OK**.

3. You are redirected to the renewal page. Add the required information and complete the renewal transaction.
4. Re-login to the mSuite console and check the updated renewal information.

## Adding devices to the mSuite license

Use this option to include additional number of devices to your Seqrite mSuite license. If the license is about to expire in one month then this option will not be visible.

To use the Add devices to License, follow these steps:

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **License Management**.
2. On License Details page, click **Add Devices to License**.
3. On the re-login notification, click **OK**.

You are redirected to a page where you add in your device information and complete the transaction.

4. Re-login to the mSuite console and check the updated Number of Devices added to your license.

## Upgrade

After using the Standard license of Seqrite mSuite, you may like to use the advance feature of Seqrite mSuite, thus you can upgrade to Advance variant.

To upgrade to advance variant of Seqrite mSuite, follow these steps:

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > **License Management**.
2. In License Details page, click **Upgrade**.
3. You are redirected to the Upgrade page. Select the current version of Seqrite mSuite and further follow the instructions.

## Online Transaction from mSuite console to Seqrite Website

Multiple transactions such as subscription, renewal, upgrade, device addition to license etc. can be easily done with online transaction from mSuite console. For any online transaction, the user is redirected to the [Seqrite website](#).

## Change Password

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



## Resetting the mSuite console password

To reset the mSuite portal upgrade to advance variant of Seqrite mSuite, follow these steps:

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > **Change Password**.
2. In the Change Password dialog box add in 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 the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Share Feedback**.

On Send us feedback dialog box, you can mention your web portal experience, report a bug or give your valuable suggestions.

2. Select the question and enter your feedback in the text field.
3. For any technical queries, write to us at [mdm.support@seqrite.com](mailto:mdm.support@seqrite.com)
4. Click **Submit**.

## Contact Us

With this option you can contact Seqrite Support in multiple ways. It includes the following support facilities such as Email Support, Live Chat Support, and Phone Support.

### Email Support

If you have a query and want to submit a ticket to us, you can visit our Email Support system. Here, you can submit a ticket with the issues. Our experts will contact you with the appropriate inputs.

- To submit a ticket, click **Submit Ticket**.
- To share your feedback about Seqrite mSuite, click **Share Feedback**.

### Live Chat Support

To get a live technical support or answers to the issues, you can chat with our technical experts.

- To avail of live chat, click **Chat Now**.

## Phone Support

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).

## Frequently Asked Questions

This option helps you to know the answers to the frequently asked questions (FAQ) related to the Seqrite mSuite console.

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Contact Us** > **FAQ**.

## Administrator Guide

To know more about the mSuite console, you can use the Administrator guide.

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Administrator Guide**.

## Release Notes

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

1. Log on to the Seqrite mSuite console and in the right upper corner, click the logged on user name > click **Release Notes**.

## Log Out

This options helps you to exit the Seqrite mSuite console.

## Users

---

### Users

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

### Advanced Search for Users

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

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

1. Log on to the Seqrite mSuite console and in the left pane, click **User > Advanced Search**.

Advanced search parameters are displayed.



Note:

---

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

---

2. Select the required search parameters.

The search parameters are as follows:

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

3. Click **Search**.

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

## Users List Page

The Users list page displays all the users available in the Seqrite mSuite console. On Users list page, you have a privilege to choose the table columns of your choice. You can select maximum of four columns only.

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



Note:

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

## With Selected Options for Users

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

- **Send Enrollment Request:** Sends an enrollment request to single or multiple selected users' devices. You can enroll a device with Seqrite mSuite via Email/SMS, QR Code, and Enrollment with ADO Enablement.  
To know more about the enrollment, see [Enrolling a new device](#).
- **Delete:** Deletes single or multiple selected users.
- **Export CSV:** Exports a list of single or multiple selected user details in the CSV format.
- **Export PDF:** Exports a list of single or multiple selected user details in the .pdf format.
  - To use the With selected options for the users, log on to the Seqrite mSuite console and click **Manage > Users >** select a single or multiple users > select the required With selected option and click **Submit**.

## Adding a user

The user with the admin privilege can add the users to the Seqrite mSuite console.

To add a new user, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane click **Users > Add**.  
The Add User page is displayed.
2. Enter the First Name, Last Name, Email, Phone No., Mobile No., and select a Department.  
You can also upload a photo of the user.
3. Click **Save**.  
The user is added successfully.



Tip:

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

## Overview and edit user details

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

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

### Overviewing user details

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

1. Log on to the Seqrite mSuite console and in the left pane click **Users**.
2. In the Users table, select the user name and then click the **Edit** icon.

The User Details page is displayed with the following options:

- **Overview:** Shows the personal information of the user enrolled with the Seqrite mSuite console. The personal information includes First Name, Last Name, Email, Department, Photo, Phone No., Mobile No., Last Login, Enrolled Devices, and Admin Role(Type). You can also view the date and time when the user was created. In addition, you can enroll a device through the available options; Enrollment via email/SMS, QR code, and Enrollment with ADO Enablement.
- **Edit:** Allows to edit the personal information of the user. The Edit tab includes the Edit details, Privileges, and Visibility Restriction sections.

### Editing user details

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

To edit the user details, follow these steps:

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

The user information is successfully edited.

4. Click **Privileges**.

5. To assign admin privileges to the selected user, select the **Allow admin access** check box and enable the privileges section.

If the Allow admin access check box is not selected, then other sections on the page will not get enabled.

6. Change the Admin role and click **Save**.

To know more about Admin roles, see [Admin Roles](#).

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



Note:

---

After you assign the admin privileges to the user, the user gets an email to set the password to access the Seqrite mSuite console. To know more about privileges, see [Privileges](#).

If you want the user to have a restricted visibility of available entities such as users, devices, groups, policies, configurations, fence, reports and etc., then visit the [Visibility Restriction](#) section.

7. On the confirmation dialog box, click **OK**.
8. In Visibility Restriction section,
  - i. If you want a user to manage all the mSuite groups then turn on the **Assign visibility for all groups** option. On the confirmation dialog box, click **OK**.
  - ii. If you want a user to manage restricted groups then click **Assign Group Visibility**. Select the groups and click **Assign Group**. The user gets restricted visibility only to those assigned groups.
9. Click the **Enrolled Devices** tab.

If the devices are enrolled with the user, you will see a list of enrolled devices. From the devices list, you can either edit or delete a single device.

10. To enroll new devices for the selected user, click the **Enroll new device** button.

The Add Device dialog box appears.

11. Enter Device Name, select Ownership and Group. You can send an enrollment request to the device by selecting the **Send Enrollment Request** check box. Then the enrollment request is sent to the device. To know more about the enrollment, see [Enrolling a new device](#).



Tip:

---

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

---

12. Click **Create**.

The new device is successfully enrolled.

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

## Importing users

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

To import users, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Users > Import**.
2. In Import Users page, click **Select File** and browse the file that is to be uploaded.  
To get more information about the file format, click **Download CSV file format**.
3. Click **Import**.

The users get imported successfully.

## Exporting users

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

To export the users, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Users > Export**.  
CSV and PDF options are displayed.
2. Select the desired format.

Users are exported in the selected file format.

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

## Deleting users

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

To delete the users, follow these steps:

Users can be deleted using any of the either options:

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

## Departments

---

The Departments option lets you add a new department to the Seqrite mSuite 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. You can also assign departments up to N-level hierarchy.

### Advanced Search for Departments

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

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Departments > Advanced Search**.

Advanced search parameters are displayed.

- **Select Parent Department:** Search departments by selecting parent department.
- **Select Created By:** Select this option to search the department by the creator name.

2. Click **Search**.

- To reset the selected criteria, click **Reset**.
- To customize the categories of the Advanced Search, click **Modify**.

### Departments List Page

The Departments list page displays all the departments which are part of the Seqrite mSuite console. The table displays the information about all the departments.

### With selected options for Departments

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

- **Delete:** Helps you to delete the multiple selected departments.
- **Export CSV:** With this option, you can export a list of single or multiple selected departments’ information in the CSV format.



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

## Overviewing Department Details

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

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Departments**.
2. On Departments page, select the department and then click **Edit**.

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

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

## Adding a department

To add a new department, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Departments > Add**.
2. On Add Department page, enter the **Department Name**, **Parent Department**, and **Description**.

**Department hierarchy:** In Seqrite mSuite, there is an N-level hierarchy. One level will be a parent department and the remaining levels will be the child departments.

3. To create a new group of the department, you can select the **Create Group** check box.  
New group is created with the same department name.
4. Click **Save**.

New department is created as well as the group.

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

## Editing department details

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

To edit the department details, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Departments**.
2. On Departments page, select the department and click the **Edit** icon > **Edit** tab > **Edit details**.

Edit the information such as Department Name, Parent Department, and Description.

3. Click **Save**.

You have successfully edited the department information.

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

## Adding users to the department

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

To add users to a department, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Departments**.
2. On Departments page, select the department and click the **Edit** icon > **Edit** tab > **Users** > **Add user to department**.

The Add user to department dialog box is displayed.

3. Select the users that you want to add to the selected department.
4. Click **Add Users**.

Users are added successfully to the selected department.

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

## Deleting department

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

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

## Devices

---

The Devices option is the most significant module of the Seqrite mSuite 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

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

Different device statuses include:

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

## Advanced Search for devices

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

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

1. Log on to Seqrite mSuite console and in the left pane, click **Devices > Advanced Search**.  
Advanced Search parameters are displayed.
2. Select the parameters. The search parameters include the following options:
  - **Select Policy:** Helps you to search the devices with the help of a policy.
  - **Select Device Status:** Helps you to search the devices by selecting the device status.
  - **Select Compliant Status:** Helps you to search the devices with device compliant status.
  - **Select Created By:** Helps you to search the devices by the creator name who added the device.
  - **Select Device Ownership:** Helps you to search the devices with device ownership.
  - **Select Device Type:** Helps you to search the devices using device types such as tablet, mobile, or phablet.
  - **Select Group:** Helps you to search the devices from a particular group.
  - **Select Device Block Status:** Helps you to view a list of the devices having a blocked status. To search, you can select Yes or No.
  - **Select Device Root Status:** Helps you to search the rooted devices on Seqrite mSuite console. To search the rooted devices, you can use Yes option.

 Note:

---

Out of all the advanced search categories, only three options are displayed by default.

---

3. To view the result, click **Search**.
  - To change already set search categories, click **Modify**.
  - To change the search categories, click **Reset**.

## Devices List Page

The Devices list page shows all the available devices on Seqrite mSuite console. On the Devices list page, you can select maximum of 10 columns only. The system does not allow you to select more than 10 columns.

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

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



Note:

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

Columns	Description
Id	Displays the Id of the device.
OS	Shows the operating system of the device.
Status	Shows device status.
Workspace Status	Shows the status of the Workspace application.
Workspace Version	Shows the version of Workspace application running on the device.
Device Name	Displays the name of the device.
Owner	Shows the name of the device owner.
Group	Shows the group name assigned to the device.
Policy	Shows the policy name assigned to the device.
Mobile No.	Shows the mobile number of the device.
Enroll Date	Shows the device enrollment date and time.
Ownership	Shows whether the device is a corporate or personal device.
Device type	Shows the type of the device such as mobile, tablet, or phablet.
Last Synced	Shows the date and time when the device last synced with Seqrite mSuite console.
Agent Vulnerable	<ul style="list-style-type: none"> <li>• If the status is Yes, then the user can uninstall/remove the Seqrite mSuite App from the device.</li> <li>• If the status is No, then the user cannot uninstall/remove the Seqrite mSuite App from the device.</li> </ul>
Agent Version	Shows the version of the mSuite Agent.
Launcher	Shows the current Launcher status on Seqrite mSuite Agent. The Launcher status can be activated or deactivated.
Manufacturer	Shows the name of the device manufacturer.
Model	Shows the name of the device model.
Launcher Version	Shows the version of launcher that is available on Agent device.

Columns	Description
IMEI	Shows the IMEI number of the devices and is beneficial to search the device with IMEI number.
Enroll Type	Shows the type of device enrollment such as Knox, Normal, Supervised or ADO.
OS versions	Shows the OS version of the device.
Action	The action items include: Edit: Helps you to edit the device information. Delete: Helps you to delete a single selected device.

## With selected Options on Devices List Page

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

- **mSuite Enrollment Request:** Allows you to send enrollment request using email or an SMS.
- **Uninstall mSuite:** Allows you to send notification for uninstalling mSuite.
- **Delete:** Allows you to delete multiple selected devices from the Seqrite mSuite server.
- **Export:** Allows you to export the details of multiple selected 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.
- **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, Push Workspace, Revoke Workspace, Uninstall Workspace, and Push File into Workspace.
- **Device actions:** Allows you to perform device actions on multiple selected devices. The device actions include Approve, Sync, Locate, Trace On, Trace Off, Scan, Broadcast Files(s) / Message, Call/SMS Monitoring ON, Call/SMS Monitoring OFF, and Uninstall. To know more about device actions, see the [Device Actions](#) table below.

1. Select the required With selected option and its sub-options (if any) and click **Submit**.

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

## Enrolling a new Android device

Device Enrollment is the process of enrolling the mobile device with the Seqrite mSuite console. After enrollment, the mobile device users become members of the Seqrite mSuite 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, or Enrollment with ADO Enablement.

### Enrollment via Email/SMS

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

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices**.
2. On Devices list page, select single or multiple selected devices.  
The With selected option is displayed.
3. From the With selected list, select **Send Enrollment Request > Enrollment via Email/SMS >** and then click **Submit**.

The enrollment details dialog box is displayed.



Note:

---

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

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

---

After sending the enrollment request, the device user will receive the enrollment details (Company Code and OTP) using email and SMS. The user must tap the enrollment link on the device, which navigates the user to the enrollment page. The user must follow the instructions given on the enrollment page. Now, the user must download and install the Seqrite mSuite Agent along with inbuilt wakeup app and enter the Company Code and OTP in the given text box on the enrollment wizard.

4. Tap the **Enroll** button. The Activate Device Administrator screen is displayed.
5. To activate the Device Administrator, tap **Activate**. The company code and OTP details will be validated. The device gets enrolled with the help of email/SMS.

After completing the enrollment process, the enrollment request gets auto approved and all the mapped policy and configurations are applied on the device.

### Enrollment via QR Code

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

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices**.
2. On Devices list page, select devices.

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

The enrollment details dialog box is displayed with the company code, OTP, Enrollment URL, Owner Email, and Device ID information.



Note:

---

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

---

- On the Enrollment Details screen of the device, tap the arrow available on the header of the enrollment wizard. The Scan QR Code option is displayed.
- Tap the arrow next to the Scan QR Code option to scan the QR code on the device. The camera app opens.
- Bring the device in front of the QR code available on the desktop and scan it.  
After the QR code is detected, the Activate Device Administrator screen is displayed.
- To activate the Device Administrator, tap **Activate**. The QR code details will be validated.

The device gets enrolled with the help of QR code.



Note:

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

## Enrollment using ADO

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

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

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

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





Note:

---

Make sure there are no accounts configured on your device.

---

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

### Using ADB assign device ownership to Seqrite mSuite

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices**.
2. On Devices list page, click **ADO Enroll** button.

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

### Enrolling device with ADO enablement

To assign Seqrite mSuite Agent your device ownership, you must follow these three steps:

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

The ADO enrollment process using QR code is completed.

3. Enroll Seqrite mSuite Agent.

- i. After assigning Seqrite mSuite Agent the device ownership, you must follow the Seqrite mSuite enrollment process by tapping the Seqrite mSuite icon on the device. Further follow the instructions on the screen.

## Enrollment Time Matrix

Network Type	Network Speed	Approx. time taken to download the Agent App	Approx. time taken to complete enrollment
3G	512 Kbps	1 min	4 minutes
4G	1.2 Mbps	55 secs	4 minutes
Wi-Fi	1.2 Mbps	15 secs	1 minute
2G	25 Kbps	33 mins	4 minutes



Note:

---

\*The time mentioned in the table is approximate timing and is subject to vary depending on multiple factors.

---

## Adding devices

To add a new device, follow these steps:

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

The Add Device page is displayed.

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

The default policy is assigned by default when a new device is added to the Seqrite mSuite console.

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

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

4. Select the group.

The policy is applied by default.

5. Click **Save**.

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

6. Enroll the device using the details.

The device is added successfully.

To know more about enrollment, see [Enrolling a new device](#).

## Overviewing device details

After the device is enrolled with the Seqrite mSuite console, the Device Details page is displayed.

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices**.
2. On Devices page, select a device that is to be viewed and click the **Edit** icon.

On the Device Details page, following tabs are displayed.

- Overview: Helps you to view mSuite Agent and Workspace application information.
- Edit: Helps you to edit device details.
- Location: Helps you to trace or locate the device.
- App Inventory: Helps you to view the app inventory of the device.
- Network Usage: Helps you to view network usage of the device.
- Remote Control: Helps you to take the control of user's device remotely.
- Call/SMS Logs: Helps you to view call and SMS logs.
- Activity: Helps you to view the device activities.

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

Options	Description
<b>Device Details</b>	
Enroll Date	Shows the device enrollment date and time.
Enroll Type	Shows the type of enrollment with which the device was enrolled with mSuite; ADO, supervised, normal, Knox.
Enrollment Status	Shows the device enrollment status.
Device Status	Shows <a href="#">device status</a> . See <a href="#">secret code</a> .
Mobile Number	Shows mobile number.
Owner	Shows the device owner name.
Ownership	Shows the ownership of the device whether personal or corporate.
Group	Shows the group assigned to the device.
Policy	Shows the policy assigned to the device.
Fence Config	Shows the fence configuration applied on the device. The applied fence configuration can be <a href="#">turned on/off</a> .

Options	Description
Agent Version	Shows the version of Seqrite mSuite device agent app.
Launcher	Shows the status of the Launcher.
Agent Vulnerable	If Yes, then the Seqrite mSuite app is not secure from uninstallation. The User can uninstall/remove the Seqrite mSuite App from the device. If No, then Seqrite mSuite app is secured from uninstallation. User cannot uninstall/remove the Seqrite mSuite app from the device.
Last Sync	Shows the date and time when the device was last synced with the mSuite console.
<b>Hardware and Storage</b>	
Model	Shows model of the device.
Manufacturer	Shows the manufacturer of the device.
OS Type	Shows operating system of the device.
IMEI	Shows the IMEI number of the device.
SIM ID (s)	Shows the SIM ID of the device.
SIM Carrier(s)	Shows the service provider name.
MAC Address	Shows the MAC ID of the device.
Bluetooth	Shows the Bluetooth MAC ID.
Network	Shows the network used by the device.
Device Storage	Shows available storage on the device.
Battery Level	Shows the battery level of the device.
CPU Usage	Shows the CPU usage of the device.
Mobile Signal	Shows mobile signal strength if it is; Excellent, Good, Fair, Poor, or No Signal.

### Select an Action (mSuite)

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

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

- If the device status is in Approved state, then the Select an Action list shows the following options;

Device actions	Description
Sync	Helps you to sync the selected device with the Seqrite mSuite server. After sending this command the device will send the latest app details, scan, and compliance report to the server.
Locate Device	This command fetches the current location of the Android device and shows it on the server.
Scan	This command initiates virus scanning on the Android device and forwards the scan report to the server.
Remote Buzz	This command plays the ringtone on the selected Android device.
Anti-Theft Block	This command blocks the Android device completely and the user cannot access the device. This command should be used in critical situations only.
Anti-theft Unblock	This command unblocks the blocked Android device.
Exit Launcher	This command allows the user to exit the launcher temporarily or permanently.
Fetch Logs	This command is to fetch the activity logs, which are performed on the device. Click <b>Download Device Logs</b> on the upper-right side of the Device Details page to download the logs. You can download the logs in formats such as .txt, .log, crash files, etc.
Wipe	This command will wipe off the device data. The Wipe option includes different types of wipes such as Full Wipe, SD Card, Factory Reset, and Custom Wipe.
Reset Password	This command is to reset the password of the selected device through Seqrite mSuite.
Broadcast Files(s) / Messages	This command is to broadcast a message or file URLs to the Android and iOS devices. To know more about Broadcast Message, see <a href="#">Broadcasting File and Message</a> .
Push Web Security Configuration	This command is to reapply the latest version of the Web Security configuration on the selected device. You can use this command when previously applied Web Security configuration fails to execute on the device.
Push Policy	This command is to reapply the latest version of mapped policy on the selected device. You can use this command only when the previously applied policy fails to execute on the device.

Device actions	Description
Push App Configuration	This command reapplies the latest mapped App Configuration on the selected device. You can use this command only when the previously applied app configuration fails to execute on the device.
Push Data Usage Configuration	This command is to reapply the latest version of the Network Usage configuration on the selected device. You can use this command only when the previously applied Network Usage configuration fails to execute on the device.
Push Fence Configuration	This command is to apply a fence configuration on the selected device.
Disconnect	This command will disconnect the device from the Seqrite mSuite server. After the command is executed on the device, the device cannot be managed by the Seqrite mSuite console.
Uninstall	This command is to remotely uninstall the Seqrite mSuite Agent from the selected ADO/Knox devices.



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.

## Workspace

On the Device Details page, the Workspace section shows the following information about the Workspace container.

Options	Description
Enroll Date	Shows the date when the Workspace was enrolled by the device user.
Enrollment Status	Shows the status of Workspace enrollment: <b>Pending:</b> When Workspace application is pushed on the device, but the user is yet to installed the application, it shows as Pending. <b>Activated:</b> When the user installed the Workspace application on the device, the status changes to activated.
Workspace Status	Activated: Inactive: Shows that the Workspace application is inactive for some time. Uninstalled: Shows that the Workspace application has been removed from the device.

Policy	Shows the applied policy on the Workspace.
Profile	Shows the profile applied on the Workspace.
Workspace Email	Shows the configured email by the user on Workspace.
Email Type	Shows the type of email configured by the user.
Workspace version	Shows the version of Workspace application.

### Select an Action (Workspace)

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	This command is to reset the password of Seqrite Workspace.
Wipe Workspace Data	This command is to delete the Workspace data.
Block Workspace	With this command, you can block device Workspace application.
Unblock Workspace	With this command, you can unblock the blocked Workspace application.
Uninstall Workspace	With this command, you can uninstall the Workspace application from the device.
Push Workspace Policy	With this command, you can push any Workspace policy on Workspace application.
Push Workspace Profile	With this command, you can push any Workspace profile on Workspace application.

### Actions on mSuite Agent from Device Overview page

As an admin, you can send different commands to the mSuite Agent device from the device overview page. These commands can be for mSuite application or for Workspace application.

#### Turn on/off the fence configuration

If fence configuration is applied on the device, then the applied fence configuration name is displayed on the Overview page. It also shows an option to turn on/off the fence configuration

for the device. If you turn off the fence configuration, then all the fence restrictions are removed from the device until you turn on the fence configuration again. When the fence configuration is turned off, the default restrictions (policy, web security configuration, and app configuration) are applied on the device.

### Unblock the blocked device using secret code

In case the device status is blocked, you can send the secret code to the user device mentioned against the Device Status option to unblock the device.

- To view the secret code, click **Secret Code**.

### Exit Launcher using passcode

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



Note:

---

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

---

### Exiting launcher temporarily or permanently

You can exit launcher temporarily or permanently as follows:

#### Exit launcher permanently

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

#### Exit launcher temporarily

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





Note:

---

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

### Exiting the launcher

The user can exit the launcher using the following steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices** > select the device > click **Edit** icon.

The Device Details page is displayed.

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

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

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

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

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

### Activating the launcher

The admin can activate the launcher using the following steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices** > select the device > click **Edit** icon.

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

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

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

## Wiping the device data

To wipe the device data, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices** > select the device > click **Edit** icon.

The Device Details page is displayed.

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

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

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



Note:

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

## Broadcast Files(s) / Message

The Broadcast Files(s) / Message action helps to send the broadcast messages and files to the Android and iOS devices.

With this action, the Administrator can have bulk file distribution mechanism. You can send the broadcast message to an individual device or bulk devices. In this way, you can reach out to larger audience and convey the message. For more information, see [Broadcasting files and messages to multiple devices in a group](#).

## Download file/message silently

This option helps you to send file(s)/message to the device silently and these files get stored on the default location (\\Download\\mSuite).

- If you have defined any specific location, then the sent files will be downloaded at that location on the Android devices.

- If download file location does not exist, then the mSuite Agent will create the same download path on the Android device and download the broadcast files silently.



Note:

---

- Both the above scenarios are not applicable for iOS devices.
- 

### Prompt user to download file/message

With this option, you can send file(s)/message to the device to download the files manually. If you have set this option, the device user will receive a prompt with the message/file(s) URLs.

- To download the files, the device user must click the URLs. The files get downloaded on the device default download location.

### Broadcast message and multiple files

To broadcast files and message, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices** > select the device > click **Edit** icon.

The Device Details page is displayed.

2. From Select an Action list, select **Broadcast Files(s) / Message** and then click **Submit**.

The Broadcast Files(s) / Message dialog box is displayed.

3. Enter the message or file URL to the broadcast message. For bulk file distribution, you can enter comma-separated URLs of the file

4. Select the required message type:

- Download file/message silently: Select this option if you want the file and the message to be downloaded silently on the device. Make sure the file path is correctly defined, or the file will not be downloaded.
- Prompt user to download file/message: Select this option if you want to send a prompt to the user to download the file or message manually.

5. Enter the download path. Make sure to give correct download path or the file will not be downloaded.

6. Click **Broadcast**.

The broadcast message is sent successfully.



Note:

---

- To broadcast files/messages to all the devices, you need to go to Group List page, select all the group and Send Broadcast Files(s) / Message.
- You need to make sure that valid file URL (ending with file name, no short URLs) is been given.

- Allowed file Extensions to broadcast to devices:
  - Text - doc, docx, pdf, txt, ppt, pptx, html, htm, xls, xlr, xlsx, csv<
  - Video - mp4, mov, mpg, mpeg
  - Image - bmp, jpeg, jpg, png
  - Executable - apk, xml, jar, ipa
  - Audio - mp3, wav, wma

## Actions on Workspace application from Device Overview page

As a mSuite Administrator, you can select the commands mentioned in the Select an Action list and click Submit. The action is carried out on the Workspace-installed device.

### Edit

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

#### Edit details

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

#### Editing device details

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

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

The device information is edited successfully.

#### Configuration

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



Note:

---

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

---

## Editing device configuration

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

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


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

4. Click **Save & Apply**.

You have successfully configured the device.

## Location

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

Options	Description
Locate	<p>This command is to fetch and locate the current location of the selected device.</p> <p> Note:</p> <hr/> <p>Location will be fetched only if the Location Services is enabled on the device.</p> <hr/>
Trace On	<p>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.</p>
Location view list	<p>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).</p>
Clear	<p>With the Clear option, you can delete the tracked locations.</p> <ul style="list-style-type: none"> <li>• To delete all the traced locations, click <b>Clear</b>.</li> <li>• To delete the particular location, select the check box of the traced location and click <b>Clear</b>.</li> </ul>

Options	Description
Export	<p>With Export, you can get the detailed information about the traced locations. You can export the details in CSV or PDF file format.</p> <ul style="list-style-type: none"> <li>• To get information about all the traced locations, just select the export option.</li> <li>• To get information about a specific traced location &gt; select the location &gt; click <b>Export</b> &gt; select the export option.</li> </ul>

## Tracing device location

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

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

To trace the device location, follow these steps:

1. Log on to the Seqrite mSuite 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 > **Location** tab.
3. Turn on the **Trace** option.
4. On the Configure Trace Frequency dialog box, select the **Trace Frequency** in minutes and click **Configure**.
  - The Trace On command is submitted successfully.



Note:

---

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

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

This command is applicable only to the Android device.

---

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

## Locating device location

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

To locate the device location, follow these steps:

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

The 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 the Seqrite mSuite console.
2. Select any device. You may select multiple number of devices.

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

### Revoke App Settings

If you have applied any app settings such as whitelist, block, added new app to the device or uninstall the app from device app inventory, then you can reverse previously applied settings by using Revoke App Settings option.

For example, previously if you have blocked an app (WhatsApp, Facebook) from device app inventory, then you can use the Revoke App Setting option to reverse the settings.

## Install Launcher or Uninstall Launcher

Uninstall/Install button is provided to uninstall or install the App Launcher on the selected devices. If the Launcher is active on the mobile device, the button will show as Uninstall Launcher, and if the Launcher is not active on the mobile device, the button will show as Install Launcher. To know more about App Launcher, see [Activating Launcher](#).



Note:

---

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

---

## App Status

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

- **Installed:** This status is showed when the app is already installed on the device.
- **Published:** The app that is recommended by the Admin to install on the device will have the status as Published.
- **Recommended:** If the user installs the app which has Published status, then the app will have the status as Recommended.
- **Whitelisted:** If any installed app is whitelisted by 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

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

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices**.
2. On Devices page, select the device and click **Edit** icon > **App Inventory** > **Advanced Search**.
3. Select the app type, app status, and app category.

You can select all the options or only one.

4. Click **Search**.

The Search result is displayed.

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



## Viewing app inventory

To view app inventory, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices**.
2. On the Devices page, select the device and click **Edit** icon > **App Inventory** tab.

The App Inventory list is displayed.



Note:

- 
- The iOS app inventory page will list only the downloaded apps and not the system apps.
- 

## Data Usage

The Data Usage option lets you monitor Internet data usage of 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 mSuite 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 number of days or by selecting a date range. The available options to search network data usage are Today, Last 7 days, Last 15 days, Last 30 days, Current Month, and Select a Range.

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices**.
2. On the Devices page, select the device and click **Edit** icon > **Data Usage**.
3. Select the number of days or the date range from the list.



Tip:

---

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

---

4. Click **Search**.

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

### Data Plan Details

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

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



Note:

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

Parameters	Description
Network Usage Configuration	Shows the name of the network configuration of the device. Clicking the network configuration name will navigate you to the Network Usage Configuration Details page. To know more about network configurations, see <a href="#">Network Usage Configurations</a> .
Billing Cycle Start Date	Shows the date on which the billing cycle begins.
Number of Days	Shows the number of days in one billing cycle.
Mobile Data Plan Limit	Shows the limit of the mobile data plan.
Wi-Fi-Daily Usage Limit	Shows the daily limit of the Wi-Fi usage.
Mobile Data Usage %	Shows the percentage of the mobile data usage in a specified mobile data billing cycle.
Setting icon	<p>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.</p> <p> Note:</p> <hr/> <p>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.</p>

## Network Usage

This section shows the graphical representation of network usage in a selected date range. The chart shows the usage of network data through Wi-Fi, Mobile Data, and Roaming. The data usage information is provided in MB's. 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 consumed the maximum Internet data in the selected date range. The mouse hover over the pie chart shows the details of Internet data usage by the apps. This option also shows the apps, which consumed maximum Internet data in the selected date range. It gives the details of the Internet data usage by the user and help you to configure the app configuration.

## Network Usage Graph

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

## Usage Information

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

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



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

## Call/SMS Logs

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



Note:

---

The Call/SMS Logs option is supported only when the calling feature is enabled on your device. These logs are visible only for the Android devices.

---

## Advanced search for call and SMS logs

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

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

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices**.
2. On the Devices page, click **Edit** icon > **Call/SMS Logs** > **Advanced Search**.
3. Select either or all the search categories such as log type, call/SMS type, and date range.

- Click **Search**. The search result is displayed.


### Viewing call and SMS logs

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

To view Call/SMS logs, follow these steps:

- Log on to the Seqrite mSuite console and in the left pane, click **Devices**.
- On the Devices page, select the device and click the **Edit** icon > **Call/SMS Logs**.

The following options are available:

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

### Enable call and SMS monitoring

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

 Note:

---

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

---

To enable call/SMS monitoring, follow these steps:

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

The Sync Logs option is displayed.

4. Click **Sync Logs**.

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

### Exporting call and SMS logs

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

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices**.
2. On the Devices page, select the device and click **Edit** icon > **Call/SMS Logs** > **Export**.
3. Select either CSV or PDF format.

Log is exported.

### Clearing call and SMS logs

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices**.
2. On the Devices page, select the device and click **Edit** icon > **Call/SMS Logs** > **Clear all logs**.
3. On the confirmation screen, click **OK**.



Note:

---

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

---

## Remote Control

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



Note:

---

By default, every mSuite 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, then 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.



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.
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.



Note:

---

- The Remote Control (RDC) feature is applicable to Android OS 7, 8, and later versions.
  - The Remote Control feature is supported on Seqrite mSuite 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 is 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's device, follow these steps:

1. Log on to the Seqrite mSuite 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. In 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 Activity log, you can see the status of RDC session.

5. The device user has to accept and provide the consent.
  - For Seqrite mSuite 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 mSuite console and the remote session starts.



Note:

---

- For normal device 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.
- 
- 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.  
We may observe some delay (based on network speed) in screen appearance during RDC if network connection is slow.
- When the Admin requests for remote access, device user has to accept the RDC request, then RDC connection will be established.
- Device should have consistent 400 kbps network speed for smooth remote connection.
- Device should have minimum 150 kbps network speed for establishing remote connection.

### Activity

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

### Admin

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

### Activity Status

Following are the various statuses of the activities:

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



Note:

---

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

---

- **Notified:** This status appears when the command/policy/configuration has reached the device, but its status has not yet been received by the server.

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

### Searching activity logs

To search the activity logs, follow these steps:

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

Activity logs are displayed.

### Compliance Report

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

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

### Scan Report

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

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

The device scan report shows:

- **Scan summary:** Shows the report type (what type of reports are generated) and the number of threats detected.

- **Threat details:** Shows the threat icon, name, type, location, threat installed date, action on the detected threat, and the date on which the action was taken on the threat.



Note:

---

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

---

## Importing devices

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

To import the devices, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices > Import**.
2. Select the CSV file, which is to be imported and click **Select File**.

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

3. Click **Import**.

Devices are imported successfully.

## Exporting devices

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

To export devices and its details, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Devices > Export**.
2. Select the file format in which the devices are to be imported; CSV or PDF.

Devices are exported successfully.

## Deleting devices

Devices can be deleted using any of the either options:

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

## Groups

---

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

### Group QR Code

The Group QR Code option provides the facility to enroll multiple Android or iOS devices of any group in a single instance. The devices enrolled using Group QR Code option will be added to Seqrite mSuite console as per the group name with incremental numbering. For example; if the group name is QR Group, then the devices added to the Seqrite mSuite 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 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 mSuite 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 devices in the groups. The categories to search groups include the following options:

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Groups > Advanced Search**.

2. Select the search categories:
  - **Select Policy:** Helps you to search groups of a particular policy.
  - **Select Created By:** Helps you to search groups by the creator name.
3. Click **Search**.

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

## Groups List Page

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

## With selected Options for Groups

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

- **Delete:** Helps you to delete the single or multiple selected groups.
- **Export CSV:** Helps you to export a list of single or multiple selected groups in .csv format.
- **Device actions:** Helps you to apply anti-theft actions on the devices of the single or multiple selected groups. You can perform actions such as applying default anti-theft setting, apply web security settings, apply Wi-Fi, apply schedule scan, apply app configuration, apply data usage, apply policy, apply fence configurations, broadcasting files and messages, and push file on device.
- **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 syncing Workspace, apply Workspace policy, apply Workspace profile, Workspace enrollment request, revoke enrollment request, uninstall Workspace, and push file into workspace.

1. Select the required With selected option and sub-option (if any) and the click **Submit**.

## Broadcasting files and messages to multiple devices in a group

When you want to broadcast the messages or files to the 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 the Seqrite mSuite console and in the left pane, click **Groups**.
2. Select all groups check box.
3. In With selected list, click **Device actions**.
4. In Apply Anti-Theft list, click **Broadcast Files/Messages** and then click **Submit**.

**Broadcast Files(s) / Messages** command will be executed only on the supported devices.

5. In Message field, enter the message or file URL. You can enter comma-separated multiple URLs.
6. In Broadcast Type list, select the required option.
7. In 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

Groups can be added by the Admin.

To add a new group, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Groups > Add**.  
The Add Group page is displayed.
2. Enter the mandatory fields; Group Name and Assigned Policy. Select the required Fence Config, App Configuration, Workspace policy, Workspace profile, and description.  
To know more about policies, see [Policies](#).
3. Select the **Default** check box to make this group as the default group. All the newly added devices will be added to the default group.
4. Click **Save**.

The group is created successfully.

## Viewing the group information

After the new group is created with the Seqrite mSuite console, the Group Details page is displayed.

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Groups**.
2. On Groups page, select the group and click the **Edit** icon.

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

- **Overview:** This option helps you to view the entire information of the group. You can view the Group Name, Assigned Policy, Fence Configuration, App Configuration, Workspace Policy, Workspace Profile, Total Devices, Description, default group. It also displays recently added devices to the group. To view all the devices added to the selected group, click **Show all**.

- **Edit:** Allows you to edit the group information. The Edit tab includes Edit details, Devices, and [Group QR Code](#) sections.
- **Bulk Enrollment:** Allows you to generate a group QR code for selected groups. This functionality is applicable only to the Android devices.

## Editing group information and adding devices to the group

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

To edit the group information, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Groups**.
2. On Groups page select a group and click **Edit** icon > **Edit** tab > **Edit details**.
3. Edit the following information such as the Group Name, Assigned Policy, Fence Configuration, App Configuration, Workspace Policy, Workspace Profile, and Description, and click **Save**.

To export the group details, click **Export**.

4. Click the **Devices** section and then click **Add device to group**.

The Add device to Group dialog box is displayed.

5. Select the devices that you want to add to the group.
6. Click **Add Devices**.

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 the Seqrite mSuite console and in the left pane, click **Groups** > select the group > click **Edit** icon > click **Edit** > click **Bulk Enrollment**.
2. 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 the Android devices.

3. Assign owner to the group by clicking **Assign Owner** button and select the owner.

4. To select the consistent naming convention for the devices, select the required option from **Select Device Name** list from below-mentioned options.
  - 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.
5. Select the validity of the QR code by selecting the number of days from the list.
6. Click **Generate QR Code**.  
An email will be sent to the group owner with the respective QR code details.
  - The QR code is generated. To generate new QR code, click the **Try new QR code** link.
  - The group QR Code is generated with the details such as; Company Code, OTP, Enrollment URL, Expiry date, Group owner, Group name, Auto Approval.
7. Other than the group owner, you can send the QR code to other users by entering multiple comma-separated email IDs. Add the email address in the **Send Email** text box and click **Send**.
  - To update the QR code details, click **Update QR Code**.
  - To cease the QR code at any instance, click **Terminate QR Code**.



Note:

---

If device user have 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 the Seqrite mSuite 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, maximum of 1000 device groups can be imported.

To import the groups, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Groups > Import**.
2. In Import Groups dialog box, select the file that is to be imported.



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

3. Click **Import**.

The groups are imported successfully.

## Exporting groups

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

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

## Deleting groups

Groups can be deleted using any of the either options:

- A single group can be deleted by clicking the **Delete** icon on Groups list page.
- On Groups list page, select single or multiple groups. The **With selected** option is displayed. From the list, select **Delete** and then click **Submit**.

## Profiles

---

The Profiles option allows you to create and apply policies and configurations on the mobile devices enrolled with your Seqrite mSuite 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 the crucial information. You can assign or unassign the policies, edit, and remove the policies.



Note:

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

### Advanced Search for Policies

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Policies > Advanced Search**.
2. From the Select Created By list, select the desired creator name and click **Search**.

The search result gets displayed.

## Policies List Page

The Policies list page displays all the available policies in Seqrite mSuite.

### With selected options for policies

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

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



Note:

---

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

---

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

### Adding a policy

To add a new policy, follow these steps:

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

The Add Policy page is displayed.

The Edit Policies tab includes different policies divided in sections such as; All, Password Policies, Device, Device Applications, and App Security. To know more about policies, see [Policy Details](#).

5. To get complete information of the policy from already created policies, select the policy from the **Inherit From** list.
6. To turn on (enable) the policy, click in the red circle. This policy gets active and applies restriction on the device.
7. Click **Save and Publish**.

New policy is created successfully.

### Viewing a policy

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

To view the policy information, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Policies**.

2. On Policies list page, select the policy and click the **Edit** icon.

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

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

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

## Editing policy details and groups

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



Note:

---

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

---

To edit the policy information, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Policies > Edit icon > Edit > Edit details**.
2. You can edit the information such as; Policy Name and Description.
3. To make this policy a default policy, select the **Default** check box.



Note:

---

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

---

4. Click **Save**.
5. Click the **Groups** section and then click **Add policy to groups**.  
The Apply Policy to Group dialog box is displayed. You can search the groups or select the groups from the list.
6. Select the group that you want to add to the policy and click **Add Group**.  
The groups are added to the devices.

## Editing the policy




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

To edit a policy, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Policies > Edit icon > Edit Policies**.

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

Sign indicators on policy page are as follows:

Applied		: The parameter is part of that policy.
Not Applied		: The parameter is not part of the policy. To apply that parameter, click in the circle.
Not available		: The parameter does not apply to that specific operating system.

To know more about policies, see Policy Details.

2. Click **Save and Publish**.

All the edited policies are displayed.

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



Note:

---

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

---

## Policy Details

To know the types and details of the policies, navigate to the Edit Policies tab, which includes all policies. The policies are also differentiated into different sections for better understanding such as: Password, Policy for Device Application, Policy for App Stores, Policy for Downloaded Apps, Policy for ADO enabled devices, and Policy for KNOX supported devices.

Sections	Description
All	<p>This section shows all the policies available in Seqrite mSuite.</p> <p>Shows all the policy options available in the Seqrite mSuite console. Options include Password, Device, Device Applications, and App Security. You can choose any of the policies listed here.</p> <p>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.</p> <ul style="list-style-type: none"> <li>Click the <b>Select All</b> option on the right side of the Edit Details tab if you want to select all the policies.</li> </ul> <p>It includes all the policies related to Password, Devices, Device Applications, and App Security. To know more about these policies, see <a href="#">Password Policy</a>, <a href="#">Device policy</a>, <a href="#">Device Application policy</a>, <a href="#">App Security policy</a>, <a href="#">ADO Security</a>, and <a href="#">KNOX Security</a>.</p> <ul style="list-style-type: none"> <li><b>Inherit From:</b> Allows to inherit the password policy from already created policies. While creating a new policy, you can select the <b>Inherit From</b> list to inherit the policies from already created policies.</li> </ul>
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.
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	<p>The ADO policy is applicable to those devices where Seqrite mSuite Agent is the device owner.</p> <ul style="list-style-type: none"> <li>All the ADO policies are superscripted with “D” for easy identification.</li> <li>This policy is applicable to the devices where the Seqrite mSuite Agent is the device owner. Also, check on the Seqrite mSuite console the specific OS versions of the devices to which this policy can be applied.</li> </ul>
Policy for KNOX supported devices	<p>The KNOX policies are applicable to the Samsung KNOX-supported devices.</p> <ul style="list-style-type: none"> <li>All the KNOX policies are superscripted with “K” for easy identification.</li> </ul>

Seqrite mSuite 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 has not applied this policy, the device will be shown as the Non-compliant device.

The following are the three values of the password:

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

### **Password Minimum Length**

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

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



Note:

---

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

---

### **Password Age**

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

### **Device Autolock**

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

### Password History

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

### Block 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 the 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, then the device will be locked and the device password will get reset.

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



Note:

---

- This policy is dependent on the Require Password policy.
  - This policy may or may not be applicable to some of the devices.
  - For ADO devices, this policy is applicable only when the device OS version is 6 or later.
  - This policy is applicable to the non-ADO devices with OS 6 and earlier versions.
  - 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 the Safe Mode. The access to Safe Mode will be permanently blocked. If you do not want to block the Safe Mode access for a specified user, then revoke the policy for that user.

If this policy is applied to the KNOX devices, then those device users will not be able to access the Safe Mode.





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

### Block Camera

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



- 
- 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 Block Camera policy.

### Block Factory Reset from Device Setting

This policy disables the Factory Reset option on the device. Thus, the device user cannot factory reset the device. The Restrict Factory Reset policy is applicable only to the devices where Seqrite mSuite Agent is the Device Owner or to the Samsung KNOX supported devices or to the Supervised iOS devices.



---

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

---

### Block Bluetooth

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

### **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 the ADO devices where Seqrite mSuite Agent is the device owner.

### **Block Wi-Fi**

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

### **Block Open Wi-Fi**

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

### **Block Mobile Hotspot**

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



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.

---

### **Block Mobile Data while Roaming**

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



Note:

---

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

---

### Block Auto-Sync while Roaming

After applying this policy on the device, the user cannot auto-sync the mobile data in roaming. The auto-sync option will be disabled for the user if this policy is applied. You can apply this policy to the Android as well as Supervised iOS devices.

### Block Outgoing Call in Roaming

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



Note:

---

This policy is applicable only to the Android devices.

---

### Location Service (GPS)

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

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



Note:

---

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

### Sync Frequency

To set the frequency of the reports from the server, turn on the Sync Frequency policy. After applying this policy on the device, the device will send 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.



Note:

---

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

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

---

### **Block Text Copy and Paste**

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



Note:

---

This policy is applicable only to the Android devices. 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.



Note:

---

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

This policy is not supported by Lenovo devices.

---

### Block Siri

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

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

### Device Time-out

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

### Set Auto Time Zone

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

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

### Block Profile Switch

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



Note:

---

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

---

### **Device Accessibility Service & App Usage**

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 the services within the set number of days, hours, minutes, or seconds.

### **Block Accounts Modification**

To restrict user 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 mSuite Agent is the device owner 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 mSuite Agent is the device owner.

---

### **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 mSuite agent is the device owner.

---

### **Block Adding New User Profile**

To restrict the user from creating 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.



Note:

---

This policy is applicable to both, the KNOX Samsung devices and ADO supported devices where the Seqrite mSuite Agent is the device owner.

---

### **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 mSuite Agent is the device owner.

### **Block Outgoing Calls**

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



Note:

---

This policy is applicable to both, Samsung KNOX and the ADO supported devices where the Seqrite mSuite Agent is the device owner.

---

### **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.



---

This policy is applicable to both, Samsung KNOX and the ADO supported devices where the Seqrite mSuite Agent is the device owner.

---

### **Block Notification Area**

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



---

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

---

### **Block Cellular Data**

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



---

This policy is applicable to the Samsung KNOX supported devices.

---

### **Block Mock Location**

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



---

This policy is applicable to the Samsung KNOX supported devices.

---

### **Block Outgoing MMS and SMS**

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

### **Block Airplane Mode**

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





Note:

---

This policy is applicable to the Samsung KNOX supported devices.

---

### **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 the Supervised iOS devices.

### **Block Safari**

To hide the Safari app on the user device, mSuite Admin can turn on the Block Safari policy.

### **Block App Uninstallation**

To restrict the Seqrite mSuite Agent uninstallation by any unauthorized user, turn on this policy. This policy is applicable only to the iOS Supervised 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 restriction on iCloud functionality. You can apply this policy only to the Supervised iOS devices.



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.

---

## History

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

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

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

The policy history list is displayed with the information about the version, created on, created by and action on the policy. The available action item is View (eye-shaped icon).

This action helps you to view the entire details of the policy.

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

## Importing a policy

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

To import a policy, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Policies > Import**.
2. In Import policy dialog box, select the file to be imported and click **Import**.

Policy file is imported successfully.

## Configurations

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

## Advanced Search for Configurations

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

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Configurations > Advanced Search**.
2. Select the search categories:

- **Select Configuration type:** Select this option to search configurations according to the configuration type.
- **Select Created By:** Select this option to search the configurations by creator name.

### 3. Click **Search**.

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

## Configurations List Page

The Configurations list page displays the default and created configurations. The table displays the information about all the configurations added to Seqrite mSuite console.

### With selected Options for Configurations

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

- **Delete:** You can delete single or multiple selected configurations with this option.
- **Apply to Groups:** Helps to apply the selected configuration to the selected groups.
- **Apply to Device:** Helps to apply the selected configuration to the selected devices.



Note:

---

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

---

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

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

## Wi-Fi

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

### Adding Wi-Fi configuration

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Configurations > Add > Wi-Fi**.

The Add Wi-Fi Configuration page is displayed.

2. Enter Network SSID and select the Security option for the company. The security options include WEP, WPA/WPA2 PSK, and None.

- If you select WEP, the Password Type appears. There are password types such as ASCII, and Hexadecimal.
  - In case of WPA/WPA2 PSK, the Password text box is displayed.
3. Select the security option and enter the password, and then click **Save**.

The Wi-Fi configuration is applied successfully.



Note:

---

WEP type is supported only on the Android devices.

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

---

## Overviewing Wi-Fi configuration

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

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Configurations >** select a configuration > click the **Edit** icon.

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



Note:

---

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

---

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

## Editing Wi-Fi configuration

The Edit tab includes Edit details and Devices sections.

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



Note:

---

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

---

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

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

The Apply configuration to devices dialog box is displayed.

4. Select the devices that you want to add to the configuration and click **Apply.**

Configurations are applied to the device.

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

## Anti-Theft

The anti-theft configuration helps you to block the device and trace the device in case of loss or theft. The default anti-theft configurations are created when you add a new device at the time of approval. With the help of this option, you can create the Anti-Theft configuration and can apply them to the Android devices or iOS supervised devices.

### Adding Anti-Theft Configuration

To apply Anti-theft configurations, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Configurations > Add.**
2. In the Add list, select the **Anti-Theft** option.

The Create Anti-Theft Configuration page is displayed.

3. Enter the Configuration Name and the mobile number of the Admin and click **Add.**

The mobile number gets displayed in Admin Mobile Numbers list.



Note:

---

In this section, you have to add contact numbers of the other Seqrite mSuite Admins. You can add up to nine mobile numbers and these numbers will be displayed on the blocked screen of the device for the user to contact the Admin.

---

4. Enter the message in the **Block Screen Message** text box that should be displayed when the device gets blocked.



Note:

---

The blocked screen message is displayed whenever the user device gets blocked. A default blocked screen message is already displayed in its text box. However, you can edit this message if required.

---

5. Select the **Lock device on Airplane Mode** check box. This is optional.

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



Note:

---

If the Lock device on Airplane Mode is applied, the lock screen appears.

---

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

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

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



Note:

---

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

This action is not applicable for the iOS devices.

---

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



Note:

---

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

This action is not applicable for the iOS devices.

---

- **Block device on SIM Change:** When you select this option on the Seqrite mSuite 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.

---

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

The Anti-Theft configuration is created successfully.

## Overviewing Anti-Theft configuration

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

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

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

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

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

## Editing Anti-Theft configuration

The Edit tab includes the Edit details and Devices sections.

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



Note:

---

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

---

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Configurations**.
2. Select the anti-theft configuration to be edited and click the **Edit** icon > **Edit** tab > **Edit details**.

The Anti-Theft Configuration Details page is displayed.

3. You can edit the configuration details such as the Setting Name, Administrator Mobile Numbers, Block Screen Messages, and notification options such as Lock device on SIM Change, Notify admin on SIM Change, Block device on SIM Change, and Lock device on Airplane Mode.
4. Select **Default** check box to make the Anti-Theft configuration as the default configuration, and click **Save**.
5. Click **Devices** section and then click **Apply configuration to device**.

The Apply configuration to device dialog box is displayed.

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

The configuration is edited and applied to the selected devices.

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

## Web Security

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





Note:

---

For iOS devices, you can only whitelist or blacklist the websites or use auto filter.

---

## Adding Web Security Configurations

To create new Web Security configurations, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Configurations > Add**.
2. In the Add list, select **Web Security**.  
The Create Web Security Configuration page is displayed.
3. Enter Configuration Name, select the Security Settings options by selecting the Browsing Protection, Phishing Protection, and Web Protection check boxes.
4. To make the web security configuration default, select the **Default** check box.



Note:

---

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

---

5. Click **Next**.

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

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



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.

---

7. Click **Next**.

The Blacklist/Whitelist URLs section is displayed.

8. Enter a URL in the **Enter Keyword or URL to filter web access** text box and click **Add**.
9. The keyword or URL gets added to the Blacklist. To move the blacklisted URL into the whitelist or vice-versa, double-click the keyword or URL. You can add any keyword or URL to the blacklist or whitelist. You can also block keywords, URLs, or domains by adding specific keywords. Also, add the keywords from URL or domain name to blacklist or whitelist.
  - To move all the blacklisted Keywords or URLs to Whitelist, click **Whitelist All**.

- To move all the whitelisted Keywords or URLs to Blacklist, click **Blacklist All**.
- 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.

#### 10. Click **Save**.

Web Security configuration is created successfully.



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.

---

## Overviewing Web Security Configuration

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

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Configurations >** select a configuration > click **Edit** icon.

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



Note:

---

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

---

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

## Editing Web Security Configuration

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

### Edit details

With this option, you can edit the Web Security configuration added to the Seqrite mSuite console.

## Editing web security configuration details

To edit the configurations, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Configurations**.
2. Select the Web security configuration, which is to be edited and click the **Edit** icon > **Edit** tab > **Edit details**.
3. You can edit the configuration name and security settings such as Web categories and Blacklist/Whitelist URLs.
4. You can create the icons of the white listed URLs for easy access of the links on your launcher.
5. You can edit the configuration name and security settings such as Browsing Protection, Phishing Protection, and Web Protection.
6. Select the **Default** check box to make the configuration as the default Web Security configuration.



Note:

---

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

---

7. Click **Save**.

The Web Security configuration details are edited successfully.

## Web Categories

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

### Blocking Web Categories

To block the Web categories, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Configurations**.
2. Select the configuration to be edited and click **Edit** icon > **Edit** tab > **Web Categories**.

The Web Security configuration details page is displayed.

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

The Web categories are blocked successfully.

### Blacklist/Whitelist URLs

Websites on mobile devices will be allowed/blocked based on the added keywords/URL(s) in blacklist/whitelist. In this section, you can edit the black listed or white listed keyword or URL. You can easily create the icons for the white listed URLs on the Launcher by selecting the “Creating icon on the Launcher for Whitelisted Url” check box.

### Blacklisting or whitelisting the URLs

For details to black list or white list any URLs or keywords follow the steps mentioned in [Adding Web Security Configurations](#) section, the [8<sup>th</sup> step](#).

### Devices

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

### Applying Web Security configuration to the devices

To apply configurations on the device, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Configurations**.
2. Select the Web Security configuration and click **Edit** icon > **Edit** tab > **Devices > Apply configuration to device**.

The Apply configuration to devices dialog box is displayed.

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

The Web security configuration is applied successfully.



Note:

---

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

---

### Schedule Scan

With the Schedule Scan option, you can scan all the enrolled devices of Seqrite mSuite 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 mSuite 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 mSuite 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 the Seqrite mSuite console and in the left pane, click **Profiles > Configurations > Add**.
2. From the configurations list, select **Schedule Scan**.  
The Schedule Scan Configuration page is displayed.
3. Enter Schedule Scan Configuration Name and select the schedule scan type such as Quick or Full.
  - **Quick scan:** Lets you scan all the apps installed on the devices.
  - **Full scan:** Lets you scan the entire device such as external SD card, internal memory, and apps, etc.
4. Select a scan cycle to perform a scan at fixed intervals such as daily, weekly, fortnightly, or monthly.
5. Select the **Update virus definition database on mSuite Agent app when connected to Wi-Fi** check box to update the virus definition database using the available Wi-Fi.



Note:

---

If the Update Virus definition database on Agent app via Wi-Fi only check box is not selected on the Seqrite mSuite 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.

## Overviewing Schedule Scan Configurations

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

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Configurations**.
2. On the Configurations page, select the Scheduled Scan configuration which is to be viewed and click the **Edit** icon.

The Schedule Scan Configuration Details page is displayed. The following options are available.

- **Overview:** This option helps you to view the Schedule Scan configuration details. You can view the Setting Name, Schedule Scan Type, Schedule Scan Cycle, and Total Devices. You can also view recently added devices. To display all the devices added to the selected configuration, click **Show all**.
- **Edit:** Allows you to edit the Schedule Scan configuration details and assign the default configurations.

## Editing Schedule Scan Configuration

The Edit tab includes Edit details and Devices.



Note:

---

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

---

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

To edit the schedule scan configuration, follow these steps:

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

You can edit the configuration details such as the Schedule Scan Configuration Name, Schedule Scan Type, and Schedule Scan Cycle. You can also select the option to update the virus definition database on Agent app using Wi-Fi.

3. Click **Save**.
4. Click **Devices** section and then click **Apply configuration to device**.
5. Select the devices to which you want to apply the configuration and click **Apply**.

The scheduled scan configuration is edited and applied to the device successfully.

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

## Data Usage

With the Network Usage configurations, you can monitor the Internet data usage with respect to Wi-Fi, Mobile Data, and in Roaming status. You can create the new network configurations and apply the configurations to any particular device or any group. This configuration helps you to monitor the usage of Internet across all the devices enrolled with Seqrite mSuite. You can monitor mobile data usage and Wi-Fi usage (Seqrite mSuite 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 mSuite network.

## Adding Data Usage configuration

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Configurations > Add**.
2. From the configurations list, select **Network Usage**.  
The Create Network Usage Configuration page is displayed.
3. Enter Configuration Name and configure Mobile Internet Plan by adding the following details:
  - Billing Cycle Start Date: Helps you to select the billing cycle start date.
  - Number Of Days: Helps you to add the billing period; such as 28 days or 30 days or 31 days.
  - Mobile Data Plan Limit (in MB): Helps you to set the mobile data plan limit.
  - Alert Notification At: Helps you to set the percentage of mobile data usage limit and to send the alert notification to the user when the set percentage is reached.
4. Configure Wi-Fi Settings by adding the following details:
  - Wi-Fi Daily Usage Limit (in MB): With this option, you can set the daily Wi-Fi usage limit and send the user an alert when the set daily Wi-Fi usage is exceeded.
  - Monitor wifi usage: This options helps to monitor Wi-Fi network.
    - Monitor all Wi-Fi: This option monitors Wi-Fi data usage of Android devices across all SSIDs.
5. Click **Save**.

The network usage setting is configured successfully.



Note:

---

After you apply the Network Usage configuration, the Seqrite mSuite 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.

---

## Overviewing Data Usage Configuration

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

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Configurations**.
2. On the Configurations page, select the network usage configuration to be viewed and click the **Edit** icon.

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

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

## Editing Data Usage Configuration

The Edit tab includes Edit details and Devices.

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

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Profiles > Configurations**.
2. On the Configurations page, select the network usage configuration to be edited and click the **Edit** icon > **Edit tab > Edit details**.

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

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

The Apply configuration to device page is displayed, which consists of the list of the devices added on the Seqrite mSuite console.

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

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

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



## Deleting Data Usage Configurations

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

To delete any customized configurations, follow these steps:

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

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

Chapter  
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 the Seqrite mSuite console and in the left pane, click **Workspace > Policies > Advanced Search**.
2. From the Select Created By list, select the desired creator name and click **Search**.

The search result gets displayed.

### Workspace Policies List Page

The Policies list page displays all the available Workspace policies in Seqrite mSuite.

### With selected options for Workspace policies

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

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



Note:

---

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

---

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

## Adding a policy

To create a new Workspace policy, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Workspace > Policies > Add**.
2. Enter Policy Name and Description.

Select the **Default** check box to make this policy as the default policy. This default policy will be applied to all the newly added devices.

3. Click **Next** to apply the policies.

The Add Policy page is displayed.

4. The Edit Policies tab includes different policies divided in sections. Visit each section, and select the required policy components. To turn on (enable) the policy, click in the red circle. This policy gets active and applies restriction on the device.

To get complete information of the policy from already created policies, select the policy from the **Inherit From** list.

5. Click **Save and Publish**.

New policy is created successfully.

## Viewing a policy

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

To view the policy information, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Workspace > Policies**.
2. On Workspace Policies list page, select the policy and click the **Edit** icon.

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

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

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

## Editing Workspace policy details and groups

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



Note:

---

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

---

To edit the Workspace policy information, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Workspace > Policies > Edit icon > Edit > Edit details**.
2. You can edit the information such as; Policy Name and Description.
3. To make this policy a default policy, select the **Default** check box.



Note:

---

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

---

4. Click **Save**.
5. Click the **Groups** section and then click **Add policy to groups**.  
The Apply Policy to Group dialog box is displayed. You can search the groups or select the groups from the list.
6. Select the group that you want to add to the policy and click **Add Group**.  
The groups are added to the devices.




## Editing the policy

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

To edit a policy, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Workspace > Policies > Edit icon > Edit Policies**.
2. A policy is divided into different sections. Visit each section, and turn on the required policy and choose the required options.

Sign indicators on policy page are as follows:

Applied		It indicates that the parameter is part of that policy.
Not Applied		It indicates that the parameter is not part of the policy. To apply that parameter, click in the circle.
Not available		It indicates that the parameter does not apply to that specific operating system.

To know more about policies, see Policy Details.

### 3. Click **Save and Publish**.

All the edited policies are displayed.

### 4. Enter the comments about the changes 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 device. 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 File Manager App	Helps you to provide access to the authorized file sharing application 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 also 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.

## 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 the file extensions that you can allow the user to upload or download it 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 Screenshot(s) on Browser App	Helps to enable or disable the functionality to take screen shot 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 the 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, then the device user has to configure the same email account to access through Workspace.
2	Allow Email Attachment	<p>Helps you to enable or disable the functionality to share email attachments through Workspace.</p> <p>If this option is enabled, then the device user can share the email attachments and if it is not enabled then the device user cannot share any email attachments.</p>
3	Allowed File Formats for Email Attachments	<p>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 then only you can access this policy.</p> <p>If this option is not set, then the user can share any type of file as an attachment.</p>
4	Allow Attachment from outside the Workspace	<p>Helps you to enable or disable the functionality to share the attachment from different options other than Workspace.</p> <p>If this option is not enabled then the device user can share the attachments only through WorkSpace.</p>
5	Allowed domains for outgoing mails	<p>Helps you to enable or disable the functionality to set the corporate domains to which the device user can send the emails through Workspace.</p> <p>If this option is disabled, then the device user can send emails to any domain.</p>
6	Maximum size limit of attachment (MB)	<p>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.</p> <p>If this option is disabled, then the device user can download email attachment of unlimited file size.</p>
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 then only the BCC option is visible while composing email through Workspace. If this option is disabled, BCC option will not be visible.



8	Allow Screenshot(s) on Emails App	Helps you to enable or disable the functionality to take screenshot of the emails received in the Workspace.
---	-----------------------------------	--

### Password Policy

To access Workspace, you require 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	<p>This options, helps you to set the password strength for device user. If you set PIN, moderate, or strong, accordingly the device user will be able to set the password for Workspace.</p> <p>PIN: The user can set Pattern, PIN or password. The user can set the password of 4-digit numeric PIN. This is less secure option.</p> <p>Moderate: The user can set the password of 6 or more alphanumeric (UPPER case) characters. This is secure option.</p> <p>Strong: The user can set the password of 8 or more characters including UPPER or lower case, number, and symbols.</p>
2	Password Minimum Length	This policy depends on 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 use 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 Screenshot(s) 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 Screenshot(s) 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 Screenshot(s) 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 black listing URLs, black listing certain URLs of a website irrespective of the domain, blacklisting or whitelisting keywords. If any keyword or URL is blacklisted, then it will not be accessible through the Workspace browser. But if any keyword or URL is whitelisted, then 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 the Seqrite mSuite console and in the left pane, click **Workspace > Profiles > Advanced Search**.

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

The search result gets displayed.

## Workspace Profiles List Page

The profiles list page displays all the available Workspace profiles in Seqrite mSuite. The list gives information about the profiles, version of the profile, number of groups which are assigned with this Workspace profiles, creator name and so on.

### With selected options for Workspace profiles

The With selected list appears on the profiles list page when you select single or multiple profiles. The With selected list shows the following option:

- Delete:** Helps you to delete single or multiple selected Workspace profiles.



Note:

---

You cannot delete a Workspace profile which has a group assigned to it.

---

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

## Add

This option helps you to create new Workspace profile.

### Creating Workspace profile

This section helps you to create the Workspace profile and block the Websites with the help of URLs and keywords.

To create Workspace profile, follow these steps:

- Log on to the Seqrite mSuite console and in the left pane, click **Workspace > Profile > Add**.
- Add name in **Profile Name** text field.
- Add description in the text field and click **Next**.
- In Website filtering section enter the keyword or URL to filter the Web access, and click **Add**.

The keyword or the URL entered is added under the Blacklisted URLs/Keywords section.

- To remove the black listed URL or keyword from the list, click the multiplication sign.
- To whitelist all the black listed URL or keywords, click **Whitelist All**.
- To block access to all URLs except the ones you allowed in whitelist, select the check box.

- Click **Save**.

## Editing Workspace profile

1. Log on to the Seqrite mSuite console and in the left pane, click **Workspace > Profile**.
2. From the profiles list page, click the Edit icon of the profile that is to be edited.
3. Click **Edit** tab, make the necessary changes.
4. Click Website filtering, make changes to the keyword or URL.
5. In blacklisted list, you can either white list all the keyword or URL, or remove a the keyword or URL added to the list. From white list, you can black list all the keywords or URLs.
  - To block access to all URLs except the ones you allowed in whitelist, select the check box.
6. Click **Save**.

## Exporting Workspace profile

You can export the profile in .csv format.

To export Workspace profile, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Workspace > Profile**.
2. From the profiles list page, click the edit icon of the profile.
3. On the profile details page, click **Export**.

All the information related to that profile and the black listed or white listed information is exported in the .csv file.

## 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 the multiple versions of the application to the store. You can upload the 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, following information is collected from the newly added app.

### App Status

In Seqrite mSuite following app statuses are found:

- **Recommended apps:** These apps are suggested to install on user device.
- **Apps to Uninstall:** These apps are restricted to install on the user device.

### App Type

Seqrite mSuite categorizes the apps as follows:

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

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

## Source Type

The Source Type shows the options from where the applications were downloaded and installed.

- Google Play
- Custom App URL
- Upload Custom APK

## Category

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

## Advanced Search for Apps

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Apps > App Store > Advanced Search**.
2. Following search categories are displayed:
  - **Select App Type:** Select this option to search apps according to the app type.
  - **Select OS:** Select this option to search the apps according to the operating system.
  - **Select Category:** Select this option to search the apps according to the app category.
3. Select the required search options and click **Search**.

The result gets displayed.

## App Store List Page

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

## With selected options for App Store

The With selected list is beneficial to delete multiple selected apps. The following With selected options 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.



Note:

---

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

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



Note:

---

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

---

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Apps > Repository** > select a single or multiple apps.

The With selected option is displayed.

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

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

## Adding Apps Using App Store

The Add option on the upper-right side of the App Store page 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 mSuite 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.



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 the Android device users.

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Apps > App Store > Add > From Google Play Store**.

The Add app from Google play store dialog box is displayed.

2. Enter Google Play Store URL of the app in the given text box. You can refer to the example of the URL given in the dialog box.
3. 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 the iOS device users.

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Apps > App Store > Add > From iTunes Store**.

The Add app from iTunes store dialog box is displayed.

2. 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.
3. 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 the Android device users. You can also add the other versions of the app via Custom App URL.

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Apps > App Store > Add > Custom App URL**.

The Add Custom App URL dialog box is displayed.



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



Note:

---

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

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

A new app is added to the app repository.

### Adding App using Upload Custom APK

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

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 then the user cannot perform 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 mSuite 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 group if that group has custom APK app configuration. For example, Admin cannot move 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 the Seqrite mSuite console and in the left pane, click **Apps > App Store > Add > Upload Custom APK**.

The Upload Custom APK dialog box is displayed.

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



---

Maximum file size of APK can be up to 150 MB and only the files with APK extension are allowed.

---

### 3. Click **Upload**.

The new app is uploaded to the App Repository.



---

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.

---

## Configuration

The app Configuration option lets you control and apply app restrictions (black list) 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 device. For non-ADO and non-Knox devices, restriction 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 version, 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 mSuite. You can apply restrictions to block apps for the full time. You can also recommend apps for installation on the user devices. You can add a particular version or multiple versions of the apps as suggested, restricted, fully blocked, or whitelisted.

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



---

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

---

## Advanced Search for App Configurations

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

To search app configurations, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Apps > Configuration > Advanced Search**.
2. Following search category is displayed:
  - **Select Created By:** Select this option to search configurations as per creator name.
3. Select the creator name and click **Search**.

The search result gets displayed.

## App Configurations List Page

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

### With selected options for app configurations

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

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



Note:

---

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

---

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

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

## Adding app configuration and activating the Launcher

The Add button on the upper-right side of the App Configuration page lets you create a new app configuration. With the help of this app configuration, you can block access to newly

installed apps, block apps based on their categories, recommend an app or restrict an app from uninstalling. You can also block an app fully as per your requirement. Also, you can configure Launcher to restrict and limit the usage of the apps on the user's device.

App configuration provides many useful features to manage the apps as follows:

## **App Categories**

Seqrite mSuite provides App Categories section to help block different categories to which the applications belong. The app category blocking is applicable only to the Android devices. You can select either a single or multiple or all the app categories.

## **Whitelisted Apps**

With this option, you can white list the apps. The white listed apps are accessible, even if their category is blocked. You can also add particular versions of the app to the white list. Only the selected, white listed versions of the application will be accessible to the user and other versions would be blocked. You can remove single or multiple versions of the app from the whitelist.

## **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, then select the entire package to uninstall all the versions. You can also add the particular version of the app to the uninstall apps list. The selected single or multiple app versions will be blocked and the other app versions will be accessible. This functionality is only applicable to the Android devices.

### **Apps to Block**

The Apps to Block option helps you to add the particular version of the app to the block list. The selected single or multiple app versions will be blocked and the other app versions will be accessible. If you want the user to block all the versions of the app, then select the entire application. You can fully block the apps of Android mobile devices.

- The Apps to 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 to the recommended list. The selected app version will be recommended and the other app versions will be blocked. If you want the user to access all the versions of the app, then select the entire app and add to the recommended list. If the Restrict new app installation on ADO & Knox Enabled Devices check box is selected in the app configuration settings, then you will receive a prompt to clear the check box and then recommend the apps.



Note:

---

The device user will not be able to uninstall, force stop, and clear cache for the Published Apps on the KNOX devices.

The mSuite Admin can remotely install the apps on any Supervised iOS devices.

The mSuite Admin can remotely uninstall only those apps, which were installed from mSuite 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 mSuite Agent is the device owner and also to the Samsung KNOX supported devices. At times if both Kiosk Modes (System Kiosk Mode and Launcher [Kiosk Mode](#)) are enabled, then System Kiosk Mode will have the priority. Thus, System Kiosk Mode setting will be applied on the device. But for Non-ADO devices, Launcher [Kiosk Mode](#) will be applied.

In System Kiosk Mode, you can add only one app to the ADO-supported devices 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

Seqrite Launcher gives the experience of customized style and function of your mobile device. The Launcher tab helps you to activate the Seqrite Launcher.

### Launcher Setting

In this section, you can configure Seqrite Launcher, 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, then the Launcher may not work properly on the device. After activating Launcher, only the active apps will be visible on Seqrite Launcher and other apps will not be accessible.

If any app configuration with the Launcher is activated on the device, then the Launcher configurations will have the highest preference and all the other app configurations will be

overridden. In case, you have deactivated the Launcher, then the App Configurations will be activated on the device by overriding the Launcher configurations.

At times, if the Restrict new app installation on ADO & Knox Enabled Devices check box is selected, you will receive a prompt to clear the check box and then recommend an app for Launcher setting.

Also, you can configure the exit launcher duration from the Launcher section.

### 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.
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 aspect 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. In case, the added apps are not installed on the device then the apps will be added to the recommended list on the user's device and the user must install the 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.



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 the Seqrite mSuite console and in the left pane, click **Apps > Configuration > Add**. The Create [App Configuration](#) page is displayed.
2. In Edit Details section, enter the configuration name in **App Configuration Name** text box.
3. To restrict the user from using the newly installed apps on ADO and KNOX supported devices, select the **Restrict new app installation on ADO & Knox enabled devices** check box.
  - If you do not want to block the new app installation on ADO and KNOX devices, clear the check box.



Note:

---

If you are recommending the apps, adding app to the Launcher, or adding app to System Kiosk Mode, then you will receive a prompt to clear the **Restrict new app installation on ADO & Knox Enabled Devices** check box. Then either use the check box or the App Configuration settings.

The Launcher Setting and Branding options are visible only for the Android device.

---

4. To make this app configuration a default configuration, 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 which are to be blocked.
  - ii. To select all the available app categories, you can select the **Select All** check box.
  - iii. To exclude any app from the blocked category, you can add that particular app to the Whitelisted apps list by clicking **Add Apps**.

In Add apps to whitelist dialog box, you can perform an advance search to view the downloaded, system, suggested, and restricted apps. Also, white list 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.



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 mSuite 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 new window, select the apps. Add Apps button gets visible. Click **Add Apps**. Make sure the **Restrict new app installation on ADO & Knox Enabled Devices** check box is not selected in app configuration.



Note:

- 
- User will not be able to uninstall, force stop, and clear cache for 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 [Launcher Setting](#) section, you can turn on the device Launcher. After enabling the Launcher, on the confirmation screen, click **Activate**.

The Restrict new app installation on ADO & Knox Enabled Devices check box must be cleared before recommending an app for Launcher.



Note:

- 
- The Launcher configuration will always have the highest preference as compared to app configurations. If Launcher is activated, only the Launcher configuration will work on the device and app configurations will not be applicable. When the Launcher is deactivated, all the app configurations will be applied again on the device.
  - If the Seqrite Launcher option is turned OFF, the Launcher will get deactivated from the device. The device user will not receive any prompt to uninstall the Launcher.
-

When the Launcher activates, you can configure the following things:

- **Launcher reminder:** Use this option to set the time and send a prompt to the user to activate the Launcher on the device. The available options are 1 minute, 2 minutes, 3 minutes, 5 minutes, 10 minutes, and 30 minutes.
- **Launcher Exit Duration:** You can configure the time to exit the Launcher. Enter the time in the Launcher Exit Duration field to allow the user to exit the Launcher for a limited period. The user of the device must enter the passcode to exit the launcher. The default time to exit the launcher is 30 minutes.
- **Primary Settings:** Configure the primary settings to access the selected settings on the device Launcher screen. To know more about primary settings, see [Primary Settings](#).
- **Device Settings:** Configure the device settings options to access the selected device settings on the Launcher screen.

17. Click **Next**.

The [Active Apps](#) section is displayed.

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 is displayed. Select the apps that you want to view on the Launcher and click **Add Apps**.



Note:

- 
- In Kiosk Mode, you can add only one app to the Active Apps list. This Launcher Kiosk Mode is applicable to the non-ADO devices.
  - If the System Kiosk Mode settings are active with Launcher Kiosk Mode, then System Kiosk Mode settings will be applied on the ADO supported devices.
  - Only the selected app versions are visible on the Launcher.
  - Make sure that the apps added to the Active Apps list are installed on the user's device.
- 

19. Click **Next**.

You are directed to the [Branding](#) section, where all the fields would be dimmed/disabled. You can make following changes to the Launcher setting.

20. On the Branding page, select the **Enable Launcher Branding** check box.

All the other fields on the page get enabled, where you can change the **Company Name**, **Company Logo**, and **Launcher Wallpaper**.

- i. Change the Company logo and Launcher Wallpaper by clicking the **down arrow** > **Upload** > selecting the image. For best logo and wallpaper image experience, you must use the following image resolutions:

- Company logo: Between 300 X 300 pixels to 1000 X 1000 pixels.
- Wallpaper: 1080 x 1920

#### 21. Click **Save**.

The changes are reflected on the Launcher.

The app configuration is created successfully.

You can export the details of the configuration in PDF format.



Note:

---

The changes done to company name, logo, and launcher wallpaper, from this section (Launcher Setting) will override all the company and launcher settings of [Custom Settings](#).

---

## Overviewing and editing app configuration and Launcher

After the app configuration is added to the Seqrite mSuite console, the App Configuration page is displayed. You can edit configuration details.

To overview and edit the app configurations, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Apps > Configuration > Edit** icon.

Overview of the app configuration is displayed.

The Overview page informs about the configuration created date, setting name, number of devices to which the configuration is applied, version of the configuration, if the configuration access is blocked for newly installed apps or if the configuration is marked as default. Also, it lists the devices to which the configuration was applied.

2. Click the **Edit** tab.

Edit details and Device options are displayed.

3. In Edit details section, you can edit the configuration details; such as configuration name, mark it as default or block the configuration access to the newly installed apps.

4. Click the **Devices** tab.

List of devices to which the configuration is applied is displayed.

5. To apply the configuration to any device, click **Apply configuration to device**. In the new screen, select the devices and click **Apply**.

6. Click the **Edit Configuration** tab. In this section,

- In App Categories section, you can block the category or remove category blocking by selecting or clearing the check boxes. Also, white list the apps or app versions.
- In Blacklisted Apps section, you can edit the uninstall list or fully blocked list.
- In 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](#).

7. Click the **Launcher** tab.

In this section, you can change the Launcher settings and edit the Active Apps list as follows:

- Turn on or off the Launcher, or change the alert time, or change the Launcher exit duration.
- You can change primary settings or device settings.
- You can edit the active apps list.
- With respect to branding, you can add or change the company logo and wallpaper that will be displayed on the Launcher.

8. To save the edited configuration, click **Save**.

## Deleting App Configurations

The app configurations can be deleted using any of the either options:

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

## Fencing

---

With the rise in the number of mobile devices, securing the confidential data has become crucial. Seqrite mSuite upholds a very strong feature of fencing for securing the confidential data. The Fencing feature acts as a virtual boundary.

Fencing allows you to setup rules to allow or to restrict the user by applying the profiles or app configurations to the user device.

Seqrite mSuite defines the safe areas for the devices. The fence triggers and sends alerts when the device leaves the assigned boundaries. The virtual barrier allows you to know the user device entry or exit of defined boundaries. You can set up the triggers when the device meets the defined boundaries. The fencing technique uses geographical locations, Wi-Fi SSIDs, and time as boundaries.

After the fence is created, apply the restrictions on the device. The configurations must be applied on the device to limit the usage of the features on the device.

This chapter includes the following sections:

[Fences](#)

[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 mSuite provides the following fences: Wi-Fi Fence, Geo Fence, and Time Fence.

### Advanced Search for Fences

The Advanced Search option allows you to perform an advanced search for different fences created in Seqrite mSuite.

To search fences, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Fencing > Fences > Advanced Search**.

Following search category is displayed:

- **Select Configuration type:** Select this option to search fences of a particular configuration types including Wi-Fi, Geo, and Time.

2. Select the required configuration type and click **Search**.

The result gets displayed.



Note:

---

Fencing is applicable only to the Android devices.

---

## Fences List Page

The Fences list page displays all the configured fences. You can change the look of Fences list page either as a map or in the table format.

- **Table:** If Table is clicked, all the fence configuration details are displayed in table format.

## With selected options for Fences

When you select single or multiple fences, the With selected option appears on the Fences list page.

- Select **Delete** and then click **Submit**. The selected action is carried out on the selected fences.

## Fences

Seqrite mSuite helps you to create virtual boundaries for your devices with the help of fences.

Seqrite mSuite supports the following fence types.

### Wi-Fi Fence

The Wi-Fi fencing is a technique that uses Wi-Fi SSID to define the fence. Whenever the user device gets connected to the defined SSID, the Wi-Fi fence triggers and then the selected restrictions in that Wi-Fi fence are applied on the device. While creating a Wi-Fi fence, you can provide any Wi-Fi SSID, and in addition you can select only the existing SSID from Wi-Fi configuration list.



Note:

---

The new SSID which is added while creating a Wi-Fi fence, will not be the part of Wi-Fi Configuration. The Wi-Fi fence will be triggered only after the authentication process.

---

### Geo Fence

The Geo fencing helps to create the fence with restrictions in a geographical area. This option lets you allow or restrict the usage of the features within a specific area by tracking the device

via GPS (global positioning system). Whenever the device enters the defined location, then the Geo fence triggers on the device and all the restrictions are applied on the user's device. This fencing allows to create a virtual barrier around a location on a map. This option helps to detect entry or exit of the device from the defined perimeter. You can draw a circle on the map to define the boundaries. You can add a new geo fence by defining radius or length on a geographical location of a map.

When multiple Geo fences are added in an organization, then the details of each Geo fence is important and should be handy. So, Seqrite mSuite facilitates to import the Geo fence details. On Fences list page, the **Import Geo Fence** button is available to import the Geo fence details. In single instance, maximum of 1000 Geo fences details can be imported.

## Time Fence

The Time fencing helps you to setup the time-based rules to be applied on the user devices. This option helps to limit the users of Seqrite mSuite by defining the time as the boundary. You can define a particular time and particular dates to define the fencing. Whenever the defined time is executed on the device, then the fence triggers on the device and the restrictions are applied on the device. If you want to execute time fencing on particular days within the defined time range, you can select the days that you want to execute fencing. You can also exclude executing the fencing on a particular date from the defined fencing period.

## Defining Fence

The Add option on the upper-right side of the Fencing page helps you to add a new fence. This helps you to add different types of fences that complies the requirement.

## Adding Wi-Fi Fence

To add a Wi-Fi fence, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Fencing > Fences > Add > Wi-Fi Fence**.

The Add Wi-Fi page is displayed.

2. Enter the name of the Wi-Fi and then select **Wi-Fi SSID**. If the Wi-Fi SSID is a new one, then enter SSID. If you want to use existing SSID from Wi-Fi configuration, then select **Existing Wi-Fi SSID**. After selecting existing Wi-Fi SSID, all the configured Wi-Fi SSIDs of Wi-Fi configuration are displayed.

3. Click **Add**.

A new Wi-Fi fence is added.

## Adding Geo fence

To add Geo fence, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Fencing > Fences > Add > Geo Fence**.

The Add Geo Fence page is displayed.

2. Enter the place name to select the location and define the boundaries. The place name you entered will show the exact location on the map or will help to locate the place.
3. Click **Add Geo Fence**.

The Save Geo Fence dialog box is displayed.

4. Enter the Fence Name, radius in meters, and then click **Save**.

The Geo Fence is created successfully and a red circle with defined boundary length is displayed on the map. You can create multiple Geo fences from the same map by selecting locations. If you want to see all the created Geo fences, click **Show All Geo Fences**.



Note:

- 
- The radius of the location must be at least 100 meters.
  - Please be noted that the Geo fence triggers only when you select High Accuracy mode location service.
- 

## Importing Geo fence

The feature to import geo fence is beneficial to import multiple fences in a single instance and get all the geo fence details. This feature shows valuable data of geo fence, which helps the Admin to make appropriate changes to the geo fences. The imported geo fence details provide information about fence name, location, latitude, longitude, and radius of the fence. In one instance, you can import maximum of 1000 fence details.

To import geo fence, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Fencing > Fences > Import Geo Fences**.
2. Select the CSV file in which fence details are added and click **Import**.

To get more information about the CSV file format, click **Download CSV sample format**.

## Adding Time Fence

To add a new time fence, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Fencing > Fences > Add > Time Fence**.

The Add Time Fence page is displayed.

2. Enter the name of the time fence, select **Set Time Fence on** option. The Set Time Fence on option includes two types: Date Range and Recursive on Days.
  - **Date Range:** Select the Date Range option to define a particular date range. The fencing is executed on the selective date range.



- **Recursive on Days:** Select this type to execute fencing on the selected days.
3. Set the **From Time** and **To** time to define the time period.
  4. In case you want to exclude the fence on certain dates, select the dates and then click **Save**.  
The time fence is added successfully.

## Overviewing and editing fence information

After you add a new fencing to the Seqrite mSuite console, you can view and modify the fencing details as required. This option helps you to edit fencing details of the fencing, which you have entered at the time of creating a new fence. You can also view the information of a selected fencing.

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Fencing > Fences**.
2. Select the fence which is to be viewed or edited and then click the **Edit** icon from Actions column.



Tip:

---

To edit the time fence, click the Edit icon in front of the Time Fence only. Similarly, to edit the Geo or Wi-Fi fence, click the Edit icon in front of Geo or Wi-Fi fence only.

---

3. The Fence overview page is displayed with fence details.  
The fence details change according to the type of fence selected.
4. Click **Edit** tab.
  - For Wi-Fi and Time fence, in Edit details section, you can edit the fence information.
  - For Geo fence, in Edit tab a map is displayed with the fence balloon. To edit the geo details, click the balloon. In Save Geo Fence dialog box, make the required changes.
5. To save the edited fence configurations, click **Save**.

To get the complete detail of the fence configuration, click the **Export** button.

## Deleting Fences

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

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

## Configurations

The fencing configurations allow you to map with the defined fences and implement the applied restrictions on the devices. With the help of fencing configurations, you can configure the profiles and app configurations on the device.

The Fencing Configuration option lets you control and apply restrictions on the device. The restrictions include policies, configurations, and app configurations. You can create new fencing configurations and apply the configurations on the devices. You can block access to the device if GPS, Wi-Fi, and Automatic Date and Time are disabled on the device to ensure the fence triggers as per the defined fence conditions.

You can add new configurations, add fence group, and define a new fence if required.

### Advanced Search for Fence Configuration

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

To search fence configurations, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Fencing > Configurations > Advanced Search**.
2. Following search category is displayed:
  - **Select Created By:** Select this option to search the fence configuration according to the creator name.
3. Select the creator name and click **Search**.

The search result is displayed.

### Fence Configuration List Page

The Configurations list page displays and provides information of all the fence configurations available in Seqrite mSuite.

### With selected Options for Fence Configuration

The With selected option appears on the Fence Configurations page when you select single or multiple fence configurations. The available options in the With selected list are:

- **Delete:** Deletes the selected fence configurations. You can delete a single or multiple selected apps.
- **Apply to Groups:** Helps you to apply the selected fence configuration to the groups. You can apply the single fence configuration to multiple selected groups.

1. Select the required option and follow either steps:
  - Select **Delete** and click **Submit**. Or

- Select **Apply to Groups** > click **Select Groups** > select the groups to apply the configuration > click **Apply**.

## Add fence configuration

The Add option on the upper-right side of the Fence Configuration page helps you to add a new fence configuration. This helps you to add the fence configuration according to the requirement.

When creating fence configuration, you need to understand:

### Fence Group

Fence group includes the list of fences, actions, policies, and restrictions that have to be applied on the device when the device meets the defined fence condition. You can select the actions and restrictions to be applied on the device. You can create maximum 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.

### Define Fence

The define fence option helps to create new fence for Geo, time, and Wi-Fi.

## Adding and defining fence configuration

1. Log on to the Seqrite mSuite console and in the left pane, click **Fence > Configurations > Add**.

The Add Fence Configuration page is displayed.

2. Enter the name of the configuration and description.
3. Select the following required check boxes:
  - **Compel 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.
4. Select either options:
  - **Add Fence Group:** Select this option to apply restrictions on the already defined fences.
  - **Define Fence:** Select this option to define a new fence.
5. To create a new fence, follow these steps:
  - i. Click **Define Fence**. The Define Fence page is displayed.

- ii. Select the fence type such as Geo, Wi-Fi, and Time fence and create the new fence as required. To know how to create different types of fences, see [Add Fences](#).
  - iii. After the new fence is created, click **Add Fence Group** to apply restrictions on the defined fences. The Fence Group section is displayed.
6. Select the Geo Fence, Time Fence, and Wi-Fi Fence that you want to apply on the device.
  7. Set the Fence Relation option to AND or OR as required.
    - If you select AND, the fence triggers only when all the defined fence conditions are met.
    - If you select OR, the fence triggers when any of the defined fence conditions meet.
  8. Select any **Set Trigger on** option:
    - **Fence In:** If you select the fence In, the restrictions will be applied on the device when the device goes into the defined fences (Geo, Time, Wi-Fi) fence.
    - **Fence Out:** If you select Fence Out, the restrictions will be applied on the device when the device goes out of the defined fences (Geo, Time, Wi-Fi).
  9. Select Action/Alert/Restriction to be performed when the fence configuration is applied on the device.
    - **Define Actions:** When the device comes in the defined fence, the defined actions will be carried out on the device such as Block, Trace, and Notification. The Seqrite mSuite Admin will get the notifications.
    - **Alerts:** If this option is selected, the user will receive email notification when the fence is triggered.
    - **Apply Restriction:** Helps to apply restriction on the device when the fence configuration is applied on the device. The restrictions include Policies, Web Security, and App configurations.
  10. Click **Save**.

The new fence configuration is created.

Click **Save & Push** if you want to create and also apply the policy on the devices.



Note:

- 
- You can reorder the fence groups to change their priority.
  - If GPS is blocked in any policy then it will not map with Geo Fence. If Wi-Fi is blocked in any policy then it will not map with Wi-Fi Fence.
- 

## Overviewing and editing fence configurations

After the fence configuration is created, the fence Configuration Details page is displayed.

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Fencing > Configurations**.

2. On Fence Configurations page, select the configuration and click **Edit** icon.

The Fence Configuration Details page displays the following:

- **Overview:** This page shows the fence configuration details. You can view the Name, Version, Description, and number of groups assigned to the configuration. You can also view recently added groups. To display all the groups added to the selected configuration, click **Show all**.

3. To edit the fence configuration details, click **Edit** tab.

The Edit tab includes Edit details and Groups sections.

4. In Edit details section, you can edit the configuration and fence group details.
5. Click **Save**.
6. Click **Groups**. In this section you can add the groups or remove the groups from the fence configuration.



Note:

---

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

---

7. Click **Add Groups to Fence Configuration**.

The Apply Fence Configuration to device group dialog 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**.

## Reports

---

Seqrite mSuite 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](#)

### On Demand Reports

On Demand Report helps you to get the detailed reports on various factors including whether the devices comply with the policy of the organization or if there has 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.
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.
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 the Seqrite mSuite console.
2. In the left pane, click **Reports** and then select **On Demand Reports**. The Reports page is displayed.
3. Under the Reports screen, 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 <b>Confirm</b> . 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 mSuite 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 data, the report cannot be viewed and it gives a warning message. In such scenario, if any date fields are available in the report, you can use them to filter the columns and generate the custom report.

## Advanced Search for Custom Reports

The Advanced Search option allows you to perform an advanced search of the custom reports.

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Reports > Custom Reports > Advanced Search**.

The advanced search parameter is displayed.

- **Select Created By:** Select this option to search custom reports according to the creator name.

2. Click **Search**.

The search result is displayed.

## Viewing reports

You can view the custom reports created as per your requirement. The custom reports can be viewed in the following formats.

- **Data table:** Displays the set of rows and columns in the tabular format. The table gives a clear understanding and observation of each and every column and row.
- **Pivot table:** Summarizes, analyzes, explores, and displays the data as per your requirement. You can simplify the complexity of any table and organize your table by using the Pivot table. This table helps you to generate a table that has column and row headers, which is devoid of blank rows. You can click any cell in the range of cells or table. A pivot table can automatically sort, count, total or display the average of the data stored in one table or spreadsheet and displays the results in a second table showing the summarized data. Pivot table helps to create unweighted cross tabulations. You can customize the table by dragging and dropping the fields graphically.
- **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 the Seqrite mSuite console and in the left pane, click **Reports > Custom Reports > 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.



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 can schedule the report generation process by clicking **Schedule Report**.



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 the Seqrite mSuite console and in the left pane, click **Reports > Custom Reports**.
1. On Custom Reports list 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.
    - Report sending period cannot exceed 90 days for daily and weekly cycle.
    - 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.



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 custom report

You can generate the custom report by selecting the multiple entities.

To generate custom report, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Reports > Custom Reports**.

The reports page is displayed. If reports are not available, then the Reports page will be empty.

2. Click **Add**.

The Create Report page is displayed.

3. Enter Report Name, and then select the Root entity as per your requirement.

The root entities include User, Department, Device, Device Group, Admin Role, Policy, App Repository, Configurations, and Fence Configurations.



Note:

Only one entity should be selected from the Root entity list.

After you select the Root entity, all the entities related to the selected root entity are displayed.

5. Click the sub-entities as per your requirement.

6. After the entities are selected, they are displayed under the **Selected Entities** section. Click the entity from the list; the relevant columns of the selected entity are displayed.


7. Select all or few columns of the selected entity that you want to include in the report. The selected columns are displayed in the lower-half section of the Report Details page.



Note:

When creating the custom reports, maximum of 15 columns can be included. The report should not exceed the set limit of 15 columns.

The Report Details page includes the following columns:

Options	Description
Entity	Displays the selected entity. The entities include User, Department, Device, Device Group, 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.
Search Criteria	<p>The Select Criteria column includes two sections such as Select Where Operator and Filter parameter.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p>You can use the following operators with the respective data type:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• Boolean data: Supported operators for Boolean data are Yes, and No. For example: Is Compliant, Is Seqrite Launcher activated, etc.</li> </ul> <p>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.</p> <p> • Please be noted that you must enter inputs as zero or one, true or false and yes or no to search Boolean data.</p> <ul style="list-style-type: none"> <li>• You must enter the date in DD-MM-YYYY format to search time stamp data.</li> <li>• You cannot use Like operator for string type data with predefined values.</li> </ul> <p>For example: Device status.</p>

Options	Description
Search Criteria	<ul style="list-style-type: none"> <li>• <b>Filter parameter:</b> 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.</li> </ul>
Group By	Group By functionality is used to group rows that have similar values. It gives the summary of the database.
Aggregate functions	<p>Aggregate function allows you to perform calculation on multiple rows of a single column of a table and give a single value.</p> <p>The aggregate functions include:</p> <ul style="list-style-type: none"> <li>• <b>COUNT:</b> The COUNT aggregate function gives the total number of values in a field.</li> <li>• <b>AVG:</b> The AVG aggregate function gives the average of the values in a specified column. It is applicable only for numeric data.</li> <li>• <b>SUM:</b> The SUM aggregate function gives the sum of the values in a specified column and is applicable only for the numeric data.</li> <li>• <b>MAX:</b> The MAX aggregate function gives the largest value from the specified table field.</li> <li>• <b>MIN:</b> The MIN aggregate function gives the smallest value from the specified table field.</li> </ul>
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	<p>The action items include few icons:</p> <ul style="list-style-type: none"> <li>• <b>View:</b> Helps you to view the selected report.</li> <li>• <b>Download:</b> Helps you to download the selected custom report.</li> <li>• <b>Edit:</b> Helps you to modify the selected custom report.</li> <li>• <b>Delete:</b> Helps you to delete the selected report.</li> </ul>

Columns	Description
With selected	<p>The With selected option appears on the Custom Reports page when you select single or multiple reports. The available action in With selected list is:</p> <ul style="list-style-type: none"> <li>• <b>Delete:</b> Helps you to delete the single or multiple selected reports. To delete the report, select the reports. The With selected option is displayed. Select <b>Delete</b> and then click <b>Submit</b>.</li> </ul>

## Editing custom reports

This option helps to make changes to the generated custom reports.

To edit the custom report, follow these steps:

1. Log on to the Seqrite mSuite 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 Report

Scheduled reports page shows all the available On Demand and Custom reports that are scheduled for given specific time and frequency in the mSuite 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 a track of the actions performed by all the Admins. The activity logs are created when any of the Admin perform any action on the Seqrite mSuite 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.
Date	Displays the date and time of the activity performed.

## Advanced Search for Activity Logs

The Advanced Search option on the upper-right side of the Activity Logs page allows you to perform an advanced search of the users' activity logs.

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

1. Log on to the Seqrite mSuite 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 the Seqrite mSuite 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 a track of the device actions executed on the devices by the Seqrite mSuite 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 mSuite 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.
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; <ul style="list-style-type: none"> <li>• <b>View:</b> Helps you to view the status of the action performed on the device. On clicking the View icon, you will be navigated to the <a href="#">Action Details</a> page.</li> </ul>

## Advanced Search for Action Logs

The Advanced Search option on the upper-right side of the Action Logs page allows you to perform an advanced search of the device actions.

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

1. Log on to the Seqrite mSuite console and in the left pane, click **Reports > Action Logs > Advanced Search**.

Advanced search parameters are displayed.

The search parameters are as follows:

- **Select Action Type:** Select this option to view the action logs of a particular action performed on the device.
- **Select Date:** Select this option to view the action logs for a particular date.

2. Click **Search**.

- To reset the selected criteria, click **Reset**.
- To get the complete details of the search result in CSV format, click **Export**.

## Action Details

The Action Details section helps you to know the detailed status of the execution of the action performed on the device. You can view the type of the task performed, action Id, and percentage of the task completed.

The Action Logs page includes the following:

Column	Description
Device Id	Displays the Id of the device on which the action is performed. To know more details of the device, click the <b>Device Id</b> . You will be redirected to the Device Details page.
Device Name	Displays the name of the device.
Status	Displays the <a href="#">activity status</a> of the action performed.
Description	Shows the description of the action performed.



Last updated	Shows the last updated date and time of the action performed.
Refresh	Helps to refresh the Action Details page.

## Exporting Action Logs

To export the action logs, you can use the advanced search criteria. The action logs are exported in CSV file.

To export action logs, follow these steps:

1. Log on to the Seqrite mSuite console and in the left pane, click **Reports > Action Logs > Advanced Search**.

Search criteria are displayed.

2. Select the action type and then select the action days or date range, and click **Export**.



Tip:

---

Exported data will be based on the selected search criteria, so choose the search criteria properly.

---

3. On confirmation screen, click **OK**.

The action logs are exported.

## Index

---

### A

- Action Logs
  - Export action logs .....176
  - Track device actions .....176
- Actions from device overview page
  - How to broadcast the message ..... 70, 72
  - How to exit the launcher permanently and temporarily ..... 70, 72
  - How to wipe the device data ..... 70, 72
  - What is message broadcasting ..... 70, 72
  - When and how to activate the launcher ..... 70, 72
- Activity
  - How to check actions performed on device .....90
- Activity Logs
  - Export activity logs .....175
  - Keep track of admin actions .....175
- Activity status
  - Pending, notified, expired, success, cancelled, failed, and in progress .....90
- Adding Apps Via
  - App repository .....144
  - Custom APK .....146
  - Custom App URL .....145
  - Google Play Store .....145
- Admin roles privileges
  - Read, update, assign, unassign, create, delete .....30
- Admin roles type
  - Create super admin, admin, advanced, standard, basic .....28
- Admin Upgrade Settings
  - To upgrade mSuite and Launcher Agent .....36
- Agent App Compromised
  - How to check if mSuite Agent uninstallation is secure or not .....62
- App categories
  - 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. .... 143
- App configurations
  - Wi-Fi, web security, anti-theft, schedule scan, network data usage, app configuration ..... 77
- App Configurations
  - Helps to block newly installed apps, block apps by categories, recommend app, restrict app from uninstalling, fully block app, and configure launcher ..... 148
- App inventory
  - How to uninstall or install the App Launcher ..... 80
  - How to whitelist or block or uninstall an app ..... 80
  - Install new apps via Google Play, Custom App URL, Upload Custom APK, and App Repository ..... 80
- App Repository
  - Add multiple versions of the apps ..... 142
  - How to suggest or restrict apps ..... 143
  - Place for all the installed apps on enrolled devices .. 142
  - What is app repository ..... 143
- App request notifications
  - Device app request report
  - Rejecting the app request ..... 25
- App source type
  - Custom app URL ..... 143
  - Google Play ..... 143
  - Upload custom APK ..... 143
- App status
  - Apps to remove ..... 142
  - Installed, published, recommended, whitelisted, blocked ..... 81
  - Recommended ..... 142
- App type
  - Downloaded ..... 142
  - Restricted ..... 142
  - Suggested ..... 142
  - System ..... 142
- Apps

- Activate launcher on device .....142
- Block apps partially or fully.....142
- Manage all installed apps on device.....142
  
- B**
- Broadcast files and message
  - What is informative or action required message .....73
  
- C**
- Call/SMS logs
  - Exporting and clearing calls and SMS logs .....87
  - How to track call logs, video calls, SMS and MMS.....85
- Call/SMS monitoring
  - How to enable call/SMS monitoring, synchronizing with the server .....86
- Common UI Terminologies
  - Global search, Search, View, Add, Import, Export, Filter column, Previous, Next, Pagination, Filter icon.....13
- Custom Report
  - Using Aggregate functions.....173
  - Using Where Operator and filter parameter .....172
- Custom Reports
  - View in data or pivot table .....168
- Custom Settings
  - How to edit Launcher wallpaper .....43
  
- D**
- Dashboard
  - Notifications, Profiles, Global search, Menus, Informative section .....8
- Dashboard center
  - How to get license status, how to check added devices and enrolled devices that are rooted, how to check if uninstallation is unsecure, how to check blocked devices, how to check device enrollment status, how to check devices connected from particular period, how to check the devices which have violated the restrictions, how to check device status infection, how to check the threat affected large number of devices, how to find network usage status, how to check the network usage devices, how to check the apps that utilized the network, how to check the app that was installed by many users .....10
- Department
  - How to create and edit departments
    - How to create groups of selected departments.....57
- Device overview page
  - How to exit Launcher using passcode .....68
  - How to select device actions .....68
  - How to turn on/off fence configuration .....68
  - How to Unblock the blocked device using secret code68
- Device status
  - Approval pending, inactive, disapproved, approved, blocked, uninstalled devices, disconnected, app violation, non-compliance, mSuite upgrade ..... 60
  - How to check device statuses ..... 60
  - Device status with device actions
    - Device status approval pending - Approve, disapprove, disconnect.....69
    - Device status approved - sync, locate, scan, ring, block, unblock, exit launcher, fetch logs, wipe, Broadcast Files(s) / Message, reset password, push fence config, disconnect, uninstall ..... 69
    - Device status uninstalled or pending - Enrollment via Email/SM, QR Code..... 69
- Devices
  - From where to get compliance and scan report ..... 91
  - How to add device fence configuration ..... 60
  - How to add new mobile device, assign ownership, assign device owner, assign group, assign configuration ..... 60
  - How to check the app inventory ..... 60
  - How to check the device network usage ..... 60
  - How to check various actions performed on the device ..... 60
  - How to enroll device ..... 60
  - How to import, export, and delete devices ..... 60, 92
  - How to install/uninstall launcher ..... 60
  - How to locate device..... 60
  - How to monitor call/SMS logs..... 60
  - How to use different device actions ..... 60
  
- E**
- Enrolling new device
  - How to enroll device via email/SMS ..... 63
  - How to enroll device via QR Code..... 63
- Enrollment Notifications
  - How to view or disapprove device enrollment request ..... 19
- Entities
  - Users, departments, devices, groups, policy, configuration, and app configuration ..... 3
- Exit launcher
  - Exit launcher permanently ..... 73
  - Exit launcher temporarily ..... 73
  
- F**
- Fencing
  - Done with geographica location, Wi-Fi SSID, and time boundaries ..... 158
  - How to define safe areas for devices ..... 158
  - Import Geo fence ..... 159
  - Virtual boundaries for devices ..... 158
- Fencing - Fence configuration
  - Applied to fence groups and defined fence ..... 164
  - Triggers when Fence In or Fence Out..... 165

**G**

Groups  
 Helps to add and view groups, add device to group, assign policy to group, apply configurations, apply fence configurations, and importing, exporting, deleting groups .....93

**L**

Launcher Upgrade Via  
 Custom URL .....39  
 Default location .....38  
 Launcher APK.....39

License  
 View Company Name, Company Code, Product Name, Product Type, Product Key, License Valid till, Number of Devices, Contact Name, Contact Email, and Contact Number .....47

**M**

mSuite Upgrade Via  
 Custom URL .....37  
 Default location .....36  
 mSuite APK .....38

**N**

Network usage  
 How to monitor internet data usage with Wi-Fi, mobile data, roaming status .....82

Notifications  
 App request notifications, Enrollment notifications, Device notifications, Import notifications .....16

Notifications components  
 How to find notification, Advanced search, with selected options, notifications dialog, notifications main page.....18

**P**

Profiles  
 Helps to create and apply policies and configurations on device .....99

Profiles configuration  
 What are anti-theft, web security, Wi-Fi, schedule scan, and network usage configuration .....115

Profiles configuration - anti-theft  
 Block and trace device .....116  
 Lock On Airplane Mode .....116  
 Lock On SIM Change .....116  
 Notify On SIM Change .....116

Profiles configuration - network usage  
 Monitor Internet data usage for Wi-Fi, mobile data, and roaming .....127

Profiles configuration - schedule scan  
 Scan all enrolled devices of mSuite .....125

Virus definition database update for mSuite Agent via Wi-Fi..... 125

Profiles configuration - web security  
 Block website, black list URL, blacklist or whitelist keywords, ..... 121  
 Protect from phishing and malicious websites ..... 121

Profiles configuration - Wi-Fi  
 Enable Wi-Fi on device without sharing the credentials ..... 116

Profiles policies  
 Adding, viewing, editing details and groups ..... 100, 132  
 Categorized as all, password policies, device policies, device applications policies, app security policies ..... 102, 134

You can assign policies to the group and manage devices in the group ..... 99

Profiles policies details  
 Editing policies ..... 102, 134

**R**

Reports  
 Custom Reports ..... 167  
 On Demand Reports..... 167  
 What type of reports..... 167

**S**

Search devices  
 How to search devices with policy, device status, compliant status, created by, ownership, device type, group, device block status, device root status ..... 61

Seqrite Launcher  
 How to customize the mobile functionality ..... 150  
 If app config is active with Launcher, then the Launcher config will have highest preference ..... 150  
 If System Kiosk mode is active with Launcher Kiosk settings, then System Kiosk Mode will have highest priority for ADO supported devices ..... 150  
 Mention Launcher reminder and Launcher exit duration ..... 155  
 Restrict the app access..... 150  
 Single app usage in Kiosk mode for non-ADO devices ..... 150

System Kiosk Mode  
 Applicable to ADO supported device, mSuite Agent is device owner and also to KNOX supported devices ..... 150

**U**

User Profile  
 User Management, Setup Services, License Management, Change Password, Share Feedback, Administrator Guide, Contact Us, Release Notes, Log Out ..... 28

Users

Search users with department, device ownership,  
Admin role, created by  
How to overview, add, edit, import, export, and  
delete users.....52

**W**

With selected  
How to perform a action on multiple selected entities  
..... 15