Seqrite mSuite

# Release Notes

23 September 2019

# Copyright Information

# Contents

# Seqrite mSuite

Seqrite mSuite is the security solution to monitor, manage, and secure employee's mobile device within the enterprise. Seqrite mSuite works on the Client-Server architecture where the console (Hosted on Cloud) manages all the mobile devices. The client agents can be installed on almost all the flavors of Android and iOS mobile. Seqrite mSuite client is having built-in antivirus, which keeps the devices safe from any virus attack.

To manage the mobile device, Seqrite mSuite applies certain policies and configurations such as, app configuration, web security configuration, anti-theft, network data usage, fence configuration, etc.

**Benefits of Seqrite mSuite**

- Secure and manage all the Android devices.
- Secure data and resources, enhance user productivity, reduce costs, and maintain communications.
- Perform Seqrite mSuite portal administration.
- Manage devices with policies and configurations.
- Monitor network data usage and Call/SMS.
- Manage apps on the device with app configuration.
- Restrict app usage and prevent misuse of the device with Seqrite Launcher or System Kiosk Mode.
- Monitor the device by applying fencing parameters such as time, location, and Wi-Fi.
- Generate the customized reports.

- Troubleshoot any critical issue with remote device control.

# Prerequisites

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

# Mobile device specifications

- Android OS version 5.0 to 9.0
- iOS 10 and later versions

# Browser requirements

- Administrator Web panel
- Google Chrome (latest versions)
- Firefox (latest versions)
- Microsoft Edge (latest versions)

# What's New

New features and enhancements of Seqrite mSuite 2.4:

- Implemented device naming preference for bulk enrollment using Group QR Code scan
    - For consistent nomenclature, you can use the device naming conventions using system generated names, IMEI Number, MAC Address, or the phone number.

- Introduced Data Transaction Usage for every tenant
    - Every tenant will be provided with data transaction usage limit. If the tenant exceeds the limit then the feature such as downloading custom APK, remote control, file upload and download in RDC session will be chargeable.
    - If the Data Transaction Usage is blocked then the Admin will not be able to apply configuration containing custom APK from Device and Group list page or add to console or add any custom APK in the app configuration. Also, the Admin will not be able to switch between app configurations containing custom APK and even between two different groups. Even the suggested custom APK will not appear for newly created app configuration.
    - In case the Data Transaction Usage limit exceeds, the RDC tab will not be accessible.

- Launched new enrollment process: Flash mRollment for Android
    - Android Flash mRollment is an enrollment method for streamlined and easy enrollment of devices in bulk.
    - In this enrolment, the Admin imports the devices' IMEI on mSuite console and the devices get enrolled and mSuite agent app is installed automatically on them. This process does not require to enter any OTP or Scan QR Code for the enrollment.

- Enhanced optimization
    - Dashboard screen is split in different tabs for fast loading of dashboard such as: Overview tab, Device Statistic, and Data Usage.
    - Reduced mSuite agent app size from 37 MB to 25 MB.
    - On App Store, we will show app icon for main app entry. For version-wise app entry, only version name and version code will be shown.
    - Network data usage for every app will be sent on a daily-usage basis rather than sending it on an hourly basis.

## Seqrite mSuite Agent App (Launcher)

- All whitelisted URL icons will be visible on the Launcher Home screen for easy browsing.
    - In web security configuration, if any URL is whitelisted then it is bookmarked on launcher Home screen.

# Known Issues

Known issues of Seqrite mSuite:

- Seqrite mSuite client and launcher can be forcibly uninstalled from some of the devices (Xiaomi, VIVO, etc.)
- If the Launcher is enabled on Samsung KNOX 8.0 devices, then the device Home button will not work.
- The iOS devices will receive commands only when they are active. If the device is locked/sleep mode, the commands will not reach to the iOS device.
- Known issues for Android 7 (Nougat) and Android 8 (Oreo) for Non-ADO devices:
  - Reset Password / Unblock device command may not work.
  - Set Password / Screen Capture policy may not work.
  - Safe Mode and USB Block policy may not work.
  - Hard keys may not block on Seqrite launcher.
- Blocking of websites based on Web categories may not work on default Internet browser of some of the devices (for example: Xiomi Redmi, Asus Zenfone, etc.)
- Seqrite mSuite do not have control over the third-party app(s) wipe action.
- mSuite client & launcher, both should have same version after upgrade. If both the mSuite client & launcher have mismatched versions, then issues may occur.
- Hard factory reset is not blocked in case of device owner.
- For Android 9 (Pie) devices, app notification for blocked applications will still be displayed.
- Device may misbehave if multiple device enrollment is done with device id.
- With normal enrollment, the hotspot policy does not work on devices with OS version 9. Device Actions for fence configurations does not work for "Fence Out" functionality.

6