SEQRITE

Release Notes 2.2 - Beta

15 January 2019

Copyright Information

Phone: +91 20 66813232

Email: info@quickheal.com

Official Website: www.seqrite.com

Trademark

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 2.2:

- **Seqrite mSuite now supports Android OS version 9.**
- **Seqrite mSuite console visibility restriction**
  - This allows to restrict the mSuite Console visibility for the admin only to the assigned group and all the associated entities with it. The Admin can view only the devices, policies, configuration, and user which are mapped to the respective group only.
- **Broadcast File(s) and Messages**
  - File broadcasting (silent file download) for iOS devices.
  - Bulk iOS device enrollment using Group QR Code enrollment.
- **Remote Control**
  - In case of network fluctuation, RDC connection will not terminate as it will re-establish the connection automatically (automatically).
  - The mSuite Administrator is allowed to take maximum of two RDC sessions at a time.
- **Revoke App Settings**
  - If the settings such as whitelist, block, added new app to the device or uninstall the app from device App Inventory are used, then such previously applied settings can be reversed by using Revoke App Settings option.
- **Increased the custom APK file size**
  - The supported custom APK file size has been increased to 150 MB.

Seqrite mSuite Client (Android)

- **Optimized Geo fencing**
  - Enhanced geo fencing mechanism so that it can apply restriction more accurately.

Seqrite mSuite Client (iOS)

- **Download broadcast file(s)**
  - Silently download the broadcast files.
- **Enrollment with Group QR Code**
  - Bulk enrollment with Group QR Code is now available for iOS devices.

Known Issues

Known issues of Seqrite mSuite:

- Seqrite mSuite client and launcher can be forcibly uninstalled from some of the devices (Xiaomi, VIVO, etc.)
- Some of the devices may force stop the Seqrite mSuite app to optimize the device battery, thus in such condition some functionality might not work.
- Broadcast file: Manual file download for the broadcast file URLs; the links display as a text on Android 6 and earlier versions.
- RDC File Management: File transfer to the attached USB device/OTG on the device, may or may not work (depends on file accessibility).
- Device details (CPU usage, Battery) on device Overview page will not be displayed for Android OS 8+ and later versions.
- User may receive multiple prompts (when device tries to connect to Wi-Fi) if Block Open Wi-Fi policy is applied on the device.
- If the Launcher is enabled on Samsung KNOX 8.0 devices, then the device Home button will not work.
- Known issues for iOS devices:
  - Device will receive commands only when they are active. If the device is locked/sleep mode, the commands will not reach to the iOS device.
  - Device details (CPU Usage, Battery level, Network, Signal Strength) on the device Overview page will not be displayed.
  - Only the recent command will reach to iOS device in case multiple commands are in queue.
  - Activity tab: The "i" icon on the Activity tab may show duplicate entries of the configurations applied on 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
- Known issues for Android 8 (Oreo) for Non-ADO devices:
  - On Console, go to Device > Overview page: some device information may not display.
  - Mobile Hotspot / Block Notification policy may not work.
  - Notification may be accessible on device block screen.
- Device user cannot exit the launcher using passcode if the launcher has been reactivated after permanent exit.
- The Location service on the device must be enabled in High Accuracy Mode to get the best results of Geo fencing (on Non-ADO devices).

- The mSuite client application may send multiple notifications for the defined fences.
- The communication between the mSuite server and the device will be stopped if the Secure Zone option of the Lenovo device is activated.
- The Exclude dates option in Time fence will not function when the Fence Trigger option is set to OUT in fence configuration.
- Call/SMS logs Monitoring:
  - Phone number and name are not available for all outgoing MMS.
  - Video call logs are displayed as call logs for all the other devices except for the Samsung devices.
- When the fence policy on mSuite client is updated multiple times, the updation may not reflect for some time.
- 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.).
- Blocking of websites may not work sometimes when user access the links/video of the whitelisted Web page.
- Seqrite Launcher may not work on some of the devices (for example: Xiomi Redmi, etc.).
- The Block Primary Microphone policy may not work for third party apps such as Hangouts, Skype, etc., for LENOVO devices.
- When devices are in fence and if the Location Services policy on Samsung KNOX devices is updated multiple times, the updation may take some time.
- Auto Sync configuration will not work for the configurations defined under the fence.
- Seqrite mSuite do not have control over the third-party wipe action. In case, if the third-party app wipes the data from the device, the MSUITE app will be uninstalled and the user's data will also be deleted.
- mSuite client & launcher both should have a same version after upgrade. If both the mSuite client & launcher have mismatched version, then issues may occur.
- Hard factory reset is not blocked in case of device owner.
- On Seqrite Launcher, Recent Apps and Mini Apps may be accessible from the task bar of some of the Tablets.
- We may observe prompt/popups of any app which is not whitelisted.
- App control block screen is not coming on those apps for which, by default, the pop up is opening.
- User may be able to share the files with unpaired device even if the Block the user to Configure Bluetooth policy is applied.