SEQRITE

Seqrite **mSuite** V3.0

Release Notes

www.seqrite.com

Copyright Information

Phone: +91 20 66813232

Email: info@quickheal.com

Official Website: www.seqrite.com

Trademark

Contents

Revision History

The information in this document is provided for the sole use of Quick Heal Research and Development and Support Team. It is strictly forbidden to publish or distribute any part of this document to any other party.

Doc Version	Date	Comment
1.0	January 10, 2022	Seqrite mSuite 2.7
1.1	April 28, 2022	Seqrite mSuite 2.7.1
1.2	August 27, 2022	Seqrite mSuite 2.8
1.3	January 20, 2023	Seqrite mSuite 2.9
1.4	May 18, 2023	Seqrite mSuite 3.0

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.

Android Enterprise Enrollment using Android Management APIs empowers the admin with an extended range of device settings and extra policy controls to setup, configure, and deploy company owned devices.

Benefits of Seqrite mSuite

- Secure and manage all 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 customized reports.
- Troubleshoot any critical issue with remote device control.
- Android Enterprise Enrollment to have better control over corporate devices.

Prerequisites

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

Mobile device specifications

- Android OS version 5.1 to 13.0
- iOS 12.1 to iOS 16.3
- Android 7 and above for Android Enterprise Enrollment

Browser requirements

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

What's New

New features and enhancements in Seqrite mSuite 3.0.

Android Enterprise Users

- **Zero Touch Enrolment for Company-Owned Devices**

  Deploy corporate-owned devices in bulk without manually setting each. Devices can be used immediately, as all necessary management, applications, and configurations are pre-set.

- **Seamless Integration with Google's Android Enterprise**

  mSuite integrates seamlessly with Google's Android Enterprise (Fully Managed), providing a streamlined mechanism to enroll, operate, and secure your company-owned devices.

  With mSuite,

  - Search and publish applications from Google Play Store on your managed devices.
  - Enforce Enterprise policies on your devices.
  - Publish a website as a Web App on managed devices and configure per-app restrictions/permissions.

- **Multi-App Kiosk Mode on Android**

  This unique feature allows you to lock down your devices into a specific set of apps instead of a single one, as seen in single-app kiosk mode.

- **Availability on Google Play Store**

  SEQRITE mSuite for Android Enterprise users is now Google Compliant and available on Google Play Store.

- **Android Enterprise Certified**

  Fulfils Google's stringent enterprise security requirements, ensuring seamless device management and on-time security patches & updates; hence, listed on Enterprise Solutions Directory.

Known Issues of Seqrite mSuite

- Some of the devices (Xiaomi, Vivo, etc.) force stop/kill running applications in the background (mSuite). On such devices, mSuite may not work properly.
- The enrollment process, Flash mEnrollment, will not work on the devices with Android OS version 10.
- Seqrite mSuite client and launcher can be forcibly uninstalled from some of the devices (Xiaomi, VIVO, etc.).
- The iOS devices will receive commands only when they are active. If the device is locked/sleep mode, the commands will not reach the iOS device.
- Blocking of the websites based on Web categories works only on Chrome browsers.
- We cannot prevent the device Hard factory reset for non-Knox devices, not even in the case of the device owner.
- Device Actions defined in fence configurations do not work for the “Fence Out” trigger.
- Device IMEI will be viewed only for ADO Enabled Android devices.
- Remote Desktop connection for iOS will work on iOS 13 and above.
- Fence restrictions will not work for Android Enterprise enrolled devices.

Known Issues for Workspace App

- Android Work Profile cannot be created on ADO Enabled Devices.
- Work profile implementation is supported from Android version 6 and later.
- Every time Workspace App sync up with server, Android System display a prompt "You are using this app within work profile" to the user.
- Apps within Workspace can be forcibly uninstalled from some of the devices (Xiaomi, VIVO, etc).
- Workspace App Email Application
    - Email notification may not display on some of the devices (i.e., Mi, etc.) as these devices force stop/kill running applications (Workspace) in the background.
    - Email notification on Android devices will not be real time.
    - Email notifications will not be displayed on iOS devices and sometimes emails on server may not synchronize with the emails on the app.
    - Email folder structure on the App may mismatch with the folder structure on the email server.
- In the iOS browser App, the Session is not saved if the user comes out of the app and URLs get reloaded upon coming back to the browser app.
- On Web View, if you select a text and search, it may redirect to the system browser on some of the devices.
- Workspace Vault App supports limited office file formats on Android.
    - User can view/edit only these file types: doc, docx, xls, xlsx, ppt, pptx however PDF and text file types are read-only.
    - Other file formats are not supported for viewing and editing.
- Sometimes replicas of the inline attached images may be created in draft email and inline images may be loaded in draft email.
- When the text is copied to the clipboard, the copied text may show in Google/Swift/Custom Keyboard recommendation and the user may use it to paste to another app even though the block clipboard policy is applied.