SEQRITE

Release Notes - Internal

28 April 2022

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	10 January 2022	Seqrite EMM 2.7
1.1	28th April 2022	Seqrite EMM 2.7.1

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 5.1 to 12.0
- iOS 12.1 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 in Seqrite mSuite 2.7.1.

Seqrite mSuite

- Factory Reset Protection (FRP)
    - Factory Reset Protection (FRP) policy prevents anyone from using the device if it is factory reset by unauthorized user. During the device setup (after factory reset) it requires the login credentials such as email address and passwords that were configured on the device. This means that if a device is lost or stolen, no one else will be able to reset or use it.

- Egg. Optimization:
    - Software stack upgrade for AWS EMM Platform.
    - On-Cloud Scanning support for mSuite Android agent
    - mSuite Launcher App Android SDK upgraded to version 32
    - Introduction of AWS Secrets Manager to manage credentials.

Known issues of mSuite App

- 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 mRollment, 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.).
- If the Launcher is enabled on Samsung KNOX 8.0 devices, 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.
- Blocking of the websites based on Web categories may not work on default Internet browser of some of the devices (For example: Xioami Redmi, Asus Zenfone, etc.).
- We cannot prevent the device Hard factory reset, not even in case of device owner.
- Device Actions defined in fence configurations does not work for “Fence Out” trigger.

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.
- To upgrade Workspace App from version 2.6 to 2.7, first we need to un-install the Workspace App 2.6 from device, then enroll the version 2.7 freshly on the device.
- 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).
- 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 app.
- Email folder structure on App may mismatch with the folder structure on email server.
- In the iOS browser App, 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.
- Sometime replica 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 user may use it to paste to another app even though the block clipboard policy is applied