Seqrite
Enterprise Mobility Management

SEQRITE

Release Notes

v3.7

29 November 2025

www.seqrite.com

Copyright Information

Phone: 1800-121-7377

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
1.5	August 25, 2023	Seqrite mSuite 3.0.1
1.6	September 23, 2023	Seqrite mSuite 3.1
1.7	January 13, 2024	Seqrite mSuite 3.2
1.8	March 2, 2024	Seqrite mSuite 3.2
1.9	April 6, 2024	Seqrite Enterprise Mobility Management 3.2
2.0	May 4, 2024	Seqrite Enterprise Mobility Management 3.2
2.1	Sep 14, 2024	Seqrite Enterprise Mobility Management 3.2.2
2.2	Nov 6, 2024	Seqrite Enterprise Mobility Management 3.2.2
2.3	Jan 11, 2025	Seqrite Enterprise Mobility Management 3.4
2.4	March 8, 2025	Seqrite Enterprise Mobility Management 3.5
2.5	June 1, 2025	Seqrite Enterprise Mobility Management 3.6
2.6	November 29, 2025	Seqrite Enterprise Mobility Management 3.7

Seqrite Enterprise Mobility Management

Seqrite Enterprise Mobility Management is the security solution to monitor, manage, and secure employee's mobile device within the enterprise. Seqrite Enterprise Mobility Management 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 Enterprise Mobility Management client is having built-in antivirus, which keeps the devices safe from any virus attack.

To manage the mobile device, Seqrite Enterprise Mobility Management 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 set up, configure, and deploy company owned devices.

Benefits of Seqrite Enterprise Mobility Management

- Secure and manage all Android devices.
- Secure data and resources, enhance user productivity, reduce costs, and maintain communications.
- Perform Seqrite Enterprise Mobility Management 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

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

Conditional Access Control for Seqrite BYOD:

- Account with Seqrite ZTNA.
- Policies and SaaS application integration setup in Seqrite ZTNA.

Mobile Device Specifications

- Android OS version 6.0.1 onwards
- iOS 14 onwards
- Android 7 and above for Android Enterprise Enrollment
- Android 11 and above for Work Profile for Corporate device Enrollment

- Android 7 and above for Work Profile for Personal device Enrollment

Browser Requirements

Administrator Web Panel

- Google Chrome (latest versions)
- Firefox (latest versions)
- Microsoft Edge (latest versions)

What's New

- **Custom Kiosk Mode**: Custom Kiosk Mode provides admin with advanced control over managed devices. In addition to restricting usage to specific apps, it includes additional layer of customization including UI and device feature restrictions.

- **Certificate Management:** Certificate management ensures that devices can securely connect to services like Wi-Fi and VPN by automatically distributing and maintaining digital certificates**.**

- Profile policy for users facing support messages,
    - **Long user-facing support message**: This policy allows admin to configure long support messages that are displayed to end users on Android tablets.
    - **Short user-facing support message:** This policy allows admin to configure short support messages that are displayed to end users on Android smartphones**.**

- Profile policy for **Block certificate changes:** This policy allows admins to block users from adding, modifying, or configuring their own credentials in the managed keystore.

- Profile policy for **Block system apps:** This policy allows admin to restrict or disable system applications on the device and ensures only approved apps are accessible on devices.

- Profile policy for **App auto update preference**: This policy gives admin control over when automatic app updates are applied on devices.

- **Android App Management Configuration Popup**: All Android app management configurations are now consolidated into a single popup window, making it easier for admin to view and configure app in one place.

- Additional android app management configurations to enhance flexibility and control.
    - Application ID
    - Application Tracking ID
    - App Upgrade Preference
    - Add Delegate Scope

- **Enhanced Wi-Fi Configuration Management**: Introduced two new **Security Options**, **802.1 x EAP** and **WPA/WPA2/WPA3- Enterprise** for Wi-Fi configuration management. Admin can configure Wi-Fi using four options, providing flexibility to align with the security policies the organization adheres to.

- Admin can manage eSIM configuration from the admin console allowing them to push eSIM to or remove eSIM from a device.

- **G Suite Authentication Using ZTNA for iOS Apps Management**: Secure access to G Suite emails via Seqrite ZTNA for iOS BYOD users, ensuring data protection and secure containerization.

Simplified User Experience

- Added **Group** option in column selection on the **Users** list page.
- **Device Profile visibility in device details (Edit>>Configuration):** Admin can now view the associated device profile directly within the **Device Details** page.
- **Additional fields in device details (Device Overview):** The Device Overview section now includes two new fields, Device Firmware No. and Embedded Identification.

Bug Fixes

- Geo fencing emails were incorrectly sent even when users remained inside the defined fence.
- Preventing custom app installation through EMM on Samsung KNOX devices running on Android 15.
- Custom applications were not working in KIOSK mode.
- Users were able to access restricted apps in AMA KIOSK mode.
- Users were able to access blocked websites.
- Some devices experienced freezing and screen blackout after upgrade.