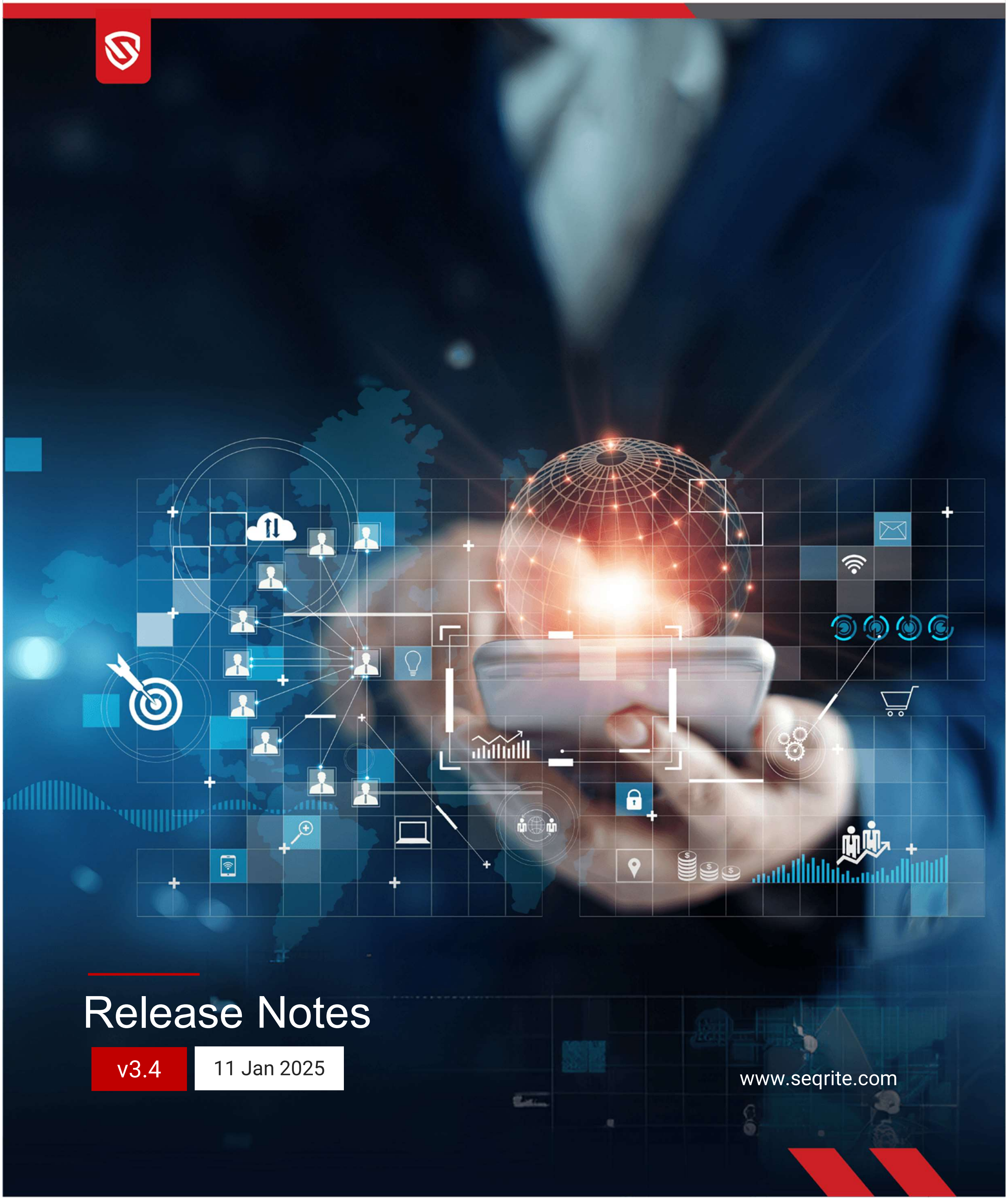
Seqrite
Enterprise Mobility Management



Release Notes

v3.4

11 Jan 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

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 setup, 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

- Device must be connected to the Internet via any network (Mobile data/Wi-Fi).
- Account with Seqrite ZTNA.
- Policies and SaaS application integration setup in Seqrite ZTNA.

Mobile device specifications

- Android OS version 6.0.1 to 15
- iOS 14 to iOS 18.1
- Android 7 and above for Android Enterprise Enrollment

  Android 11 and above for Work Profile for Corporate device Enrollment

Browser requirements

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

What’s New

- In this release, the new enrollment type that is **COPE Enrollment** (Company Owned Personal Enabled) has been introduced for the company owned Android devices for work as well as personal Android devices. With this enrollment, user can use the same device securely and privately for work and personal purposes.
  Admin can control following settings and features for the entire device:

  - Setting requirements for the device password
  - Controlling Bluetooth and data roaming
  - Configuring factory reset protection

- Containerization for iOS devices. A logical container is created that isolates work and personal data. It allows users to use their own devices for work and personal use.
  It ensures that users don't accidentally send sensitive information to the wrong people.

- The admin can distribute the custom app to iOS devices.

- With this release, we are also now compliant with the four management sets provided by Google.

  1. Work Profile Management
     Enables platform-level separation of work apps and data. Enterprises have control over all data and security policies within the work profile. Outside the work profile, the device remains suitable for personal use—ideal for BYOD deployments.

  2. Full device management
     Provides full MDM and app management for granular control over company-owned devices. Choose from 80+ settings to enforce and benefit from Android’s full suite of app management features. This option is designed for devices intended primarily for corporate use.

  3. Dedicated device management
     Transform company-owned devices into purpose-built devices. Lock them down to a single app or suite of apps to serve specific employee or customer-facing scenarios. Enforce an extended range of security policies to prevent users from escaping apps and accessing the lock screen.

  4. Mobile app management (MAM)
     Benefit from Android's full suite of enterprise app management features combined with basic device security. Distribute public and private apps, curate the Play Store on user’s devices, and restrict access to work apps if a device doesn't meet minimum password policies.

- Introduced an all-new product theme providing a refined look.

Bug Fixes

The issue where the last five digits of SIM IDs were showing as zero in the device asset tracking report during export has been resolved.

Known Issues of Seqrite Enterprise Mobility Management

- Some of the devices (Xiaomi, Vivo, etc.) force stop/kill running applications in the background (Seqrite EMM). On such devices, Seqrite EMM may not work properly.
- The enrollment process, Flash Enrollment, will not work on the devices with Android OS version 10.
- Seqrite Enterprise Mobility Management 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.
- Android Enterprise enrolled devices fail to lock when airplane mode is activated.

Known Issues for Workspace App

- After Workspace App upgrades to version 03.01.20, user will need to sign-in again into the Workspace email account (if email account is configured in Seqrite Email App under Workspace App). This is a one-time activity for the device user.
- 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.
- Email Authentication for Work Profile will work on mobile device having android OS 8 version and above.
- ZOHO Email Authentication will work only on ZOHO email App in the Work Profile.

  Email authentication through Seqrite ZTNA for iOS is not supported on Google Workspace account.
- Google apps are not being removed when you switch the device group. However, you can uninstall them from the uninstall apps section.
- The Wipe command will not work for Android 14 devices.