SEQRITE

Seqrite mSuite

Release Notes

7 January 2019

Copyright Information

© 2014–2019 Quick Heal Technologies Ltd. All Rights Reserved.

No part of this publication may be reproduced, duplicated or modified in any form or incorporated into any information retrieval system, electronic or any other or transmitted in any form without prior permission of Quick Heal Technologies Limited, Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune 411014, Maharashtra, India.

Phone: +91 20 66813232

Email: info@quickheal.com

Official Website: www.seqrite.com

Trademark

Seqrite is the registered trademark of Quick Heal Technologies Ltd. while other brands and product titles are trademarks of their respective holders.

Contents

© 2014–2019 Quick Heal Technologies Ltd.

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 8.1
- 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 2.0:

Seqrite mSuite Console

- **Seqrite mSuite with multiple variants**

  Seqrite mSuite comes in different variants: Standard and Advance.

  - Standard: Standard Seqrite mSuite comes with limited set of features.
  - Advance: Advance Seqrite mSuite includes all the advance features.

  The table below gives complete information about the features included in the Standard and Advance Seqrite mSuite variants.

Features	Variants	
	Standard	Advance
Device Management	✓	✓
Application Management	✓	✓
Security Management	✓	✓
Real Time Malware Protection	✓	✓
Network Data Monitoring	✓	✓
Launcher Mode	✗	✓
Call & SMS Monitoring	✗	✓
Device Lockdown	✗	✓
Virtual Fencing (Geo, Wi-Fi, Time based)	✗	✓
Remote Device Control	✗	✓
Reporting	Basic	Custom
Logs and Reports	1 month	3 months
Tenant data deletion after license expiry	• Standard paid: 1 month	• Advance trial: 1 month • Advance paid: 3 months
Prior notification to tenant before deleting the tenant from mSuite database	• Standard paid: 7, 15, and 25 days.	• Advance trial: 7, 15, and 25 days. • Advance paid: 15, 30, 45, 60, and 75 days
After license expiry, tenant’s data maintained on mSuite server	• Standard paid: 1 month	• Advance trial: 1 month • Advance paid: 3 months

  - When you ask for trial, you will get the Advance Seqrite mSuite for 1 month and will be applicable for 5 devices.
  - After you use your trial copy, you can either opt for paid Standard or Paid Advance variant.
  - If you have opted for paid Standard, you can further upgrade it to paid Advance.
  - If you have opted for paid Advance, you can Top Up and add more number of devices to your license.

© 2014–2019 Quick Heal Technologies Ltd.

- **Enhanced product registration**
  - Auto approval registration for trial Company registration (Default license of 30 days for 5 devices).
  - One Step Sign-up process (Sign-up with set password)
  - Sign-up using Trial (Advance), Standard paid and Advance paid product key
- **Seqrite mSuite support for iOS device; enrollment, configurations, and policies**
  - Seqrite mSuite now supports iOS device 10 and later versions.
  - Supervised mode enrollment for iOS devices.
  - Configurations supported by iOS devices:
    - Anti-theft: Lost and Locate
    - Web Security: Whitelist or Blacklist Websites and Auto filter
    - App Configuration: System Kiosk Mode, remote app installation, and remote app un-installation for Managed Apps.
    - Wi-Fi Configuration
    - Commands: Sync, Lock, Clear passcode, Un-install, Disconnect, Broadcast message from Server to iOS device, Locate, Ring/Fetch Logs.
  - **New policies for iOS devices:**
    - Password Policy: Password policy (requires password, min length, password age, device autolock) for iOS devices
    - Block Camera: Restricts the user from using the device camera.
    - Device Time-out: This policy ensures that the device remains connected to the server even when the device is not communicating with server for specified number of days.
    - Set Auto Time Zone: Helps to set automatic date, time and time zone on user device.
    - Block App Uninstallation: Restricts unauthorized uninstallation of Seqrite mSuite client application.
    - Block Voice Dialing from Lock Screen: Restricts user from voice dialing from locked device screen.
    - Block the user to Modify accounts: Restricts user from modifying any user accounts.
    - Block Notification on lock screen: On applying this policy, the user will not be able to view the notifications on locked device screen.
    - Block Control center on lock screen: with this policy, the Control Center on locked screen is not visible.
    - Block Auto-Sync while Roaming: Restricts the user from auto sync of the device while in roaming.
    - Block Factory Reset from Device Setting: Restricts the user from factory reset of the device.

    - Block Safari: With this policy Safari app will not be visible on the device and also the Safari app pop-ups will be blocked.
    - Block iMessage: Helps to block iMessages app on supervised iOS device.
    - Block Apple Books: Blocks Apple books on the devices.
    - Block In-app purchase: Restricts the user from making any in-app purchase on the device.
    - Block backup to iCloud: Restricts the user from placing the device backup on iCloud.
    - Block Siri: Restricts Siri on user device.
    - Block iTune App: Blocks the iTune app on the user device.
    - Block App Store: Blocks App store on the user device.
    - Block Certificate: Blocks untrusted TLS certificate on user device.
    - Block Screen Capture: Blocks screen capture on the user device.

- **Online transactions available from mSuite portal to Seqrite Website**

  Following online transactions can be made:
  - Trial users can subscribe for Advance version.
  - Standard license users can renew, upgrade, or add additional devices to the license.
  - Advance license user can renew or add additional devices to the license.
- **Notifications to all the tenants from SU tool (from Seqrite) to mSuite console**
  - Option to send broadcast notifications to all types of Tenants i.e. All/Trial/Paid/Standard/Advance.
  - When the mSuite Admin logs in, the notification popup will be displayed.
  - After the Admin views the notification, it gets listed in the Notification section.
- **Implemented SU Admin tool**
  - The tool gives option to extend validity and device count for trial users
  - Use different domains, show enrolled device count on Company page, and re-use the trial email ID to sign-up for paid account.
- **Enhanced Remote Control feature**
  - Easily create, rename, delete, or transfer file from mSuite portal to Android devices and vice versa.
- **Multiple enhancements for mSuite console**
  - Migrated from GCM to Firebase Cloud Messaging (FCM) for better communication with the devices.
  - Sign-Up process is now GRDP compliant.
  - Auto-approval for device enrollment using Email/SMS.
  - Device Overview page displays the latest date and time when the device synced with mSuite.
  - Fence group in fence configuration is now limited to two groups.
  - Apps added to Fully Block list will be hidden in ADO/KNOX devices.

  - Apps will be remotely uninstalled/disabled from the ADO/KNOX devices if the action is initiated from the With selected or app configuration options.
  - Removed “Register IMEI” option from Admin settings.
  - Color and theme changes done to Seqrite mSuite software.
  - After the installation of recommended apps, the device will automatically sync with mSuite.

Seqrite mSuite Client

- iOS device support (iOS 10 and later versions)
  - Supervised mode enrollment for iOS devices
- iOS Agent Enrollment via OTP/Company Code & QR Code Scan
- Supported configurations, commands and policies for iOS supervised devices:
  - Anti-theft : Lost and Locate
  - Web Security : Whitelist or Blacklist Websites and Auto filter
  - App Configuration : System Kiosk Mode, App un-installation (only for Managed Apps) remotely, App Installation remotely
  - Wi-Fi configuration
  - Commands: Sync, Lock , Clear passcode, Un-install, Disconnect, Broadcast message from Server to iOS device, Locate, and Ring/Fetch Logs.
  - Multiple new policies for iOS devices: Password Policy, Block Camera, Device Time-out, Set Auto Time Zone, Block App Uninstallation, Block Factory Reset from Device Setting, Block the user to Modify accounts, Block Notification on lock screen, Block Control center on lock screen, Block Auto-Sync while Roaming, Block Voice Dialing from Lock Screen, Block Safari , Block iMessage, Block Apple Books , Block In-app purchase ,Block backup to iCloud ,Block Siri , Block iTunes App ,Block App Store, Block Certificate, Block Screen Capture.
- For iOS devices, the device details page shows information about disk, free memory, and Jailbreak.
- The App Inventory tab for iOS devices on mSuite portal will be read-only. The App Inventory tab will list only the downloaded apps and not the system apps.
- When upgrading the mSuite client, the user may receive a Google prompt (Google Play Protect permission to allow app installation), for which, the user must grant permission once.

Known Issues

Known issues of Seqrite mSuite:

- 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.
- Know 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.