SEQRITE

Enterprise Security Solutions by Quick Heal

Seqrite
Mobile Device Management

Available on

www.seqrite.com

Infinite Devices. One Unified Solution.

A simple yet powerful solution, Seqrite Mobile Device Management is a unified platform for managing and monitoring multiple mobile devices within your enterprise from an intuitive web-enabled user console.

Introducing Seqrite MDM

In today's hyper connected world, mobile devices and applications have become an integral part of every organization's success. IT departments are now tasked with looking into the lifecycle management of these devices. This task is made harder thanks to the popularity and growth of smartphone usage within enterprises to enhance employee productivity. However, when a new device is connected to the enterprise network the possibility of data loss, malware infections and other threats increases manifold.

Seqrite MDM allows you to implement a wide range of device controls without ever having to physically handle a user's device. Functioning completely over-the-air, MDM enables you to manage and regulate comprehensive device policies and configuration settings. Once Seqrite MDM has been enabled, enterprise users are a simple click away from completely secured access to their business assets.

Product Highlights

Seqrite MDM provides end-to-end deployment of anti-theft features, policy compliance, device status and safeguards corporate devices.

- Cloud-based mobile device management solution that offers true SaaS.
- Reliable and scalable solution that expands as your operations grow.
- Flexible deployment options available to suit your customized needs.
- Over-the-air enrollment makes setup easy, quick and economical.
- Proactive device security upholds compliance of enterprise devices.
- Flexible application control provides transparency and compliance of all installed apps.
- Anti-theft features and seamless configuration of profiles and policies.
- Custom reports about device non-compliance, data usage or infection status.

Features List

SEAMLESS CLOUD-BASED SOLUTION

Seqrite MDM is a completely cloud-based solution that works seamlessly and gives you all the advantages of a true SaaS (Software-as-a-Service). When it comes to deployment and management, you can enjoy the following benefits:

- Instant availability allows enterprises to get up and running within minutes
- Anytime and anywhere access gives enterprises tremendous flexibility
- Easy availability of any new features and enhancements
- Flexible deployment options for on-premise installation or cloud as per client needs

UNIFIED MANAGEMENT CONSOLE

Seqrite MDM allows you to manage all mobile devices within your enterprise with utmost ease. Through a simple graphical interface, IT administrators can gain a bird's eye view of all enrolled devices and enforce policies. The unified console provides:

- Comprehensive dashboard with global search in real-time
- Proactive notifications and alerts for actionable responses
- Holistic view of devices, infections and compliance status
- Individual device view for in-depth status and activities on a device
- Network and app usage stats showing trending apps and malware
- Simple navigation to details of all entities

EFFORTLESS DEVICE ENROLLMENT

Seqrite MDM minimizes resources spent towards setting up and configuring devices by carrying out seamless device enrollment over-the-air. Individual devices can enroll within minutes and enterprises can reach them irrespective of their location. Once the device is integrated into the MDM system, enterprises can also create custom user groups for flexible profile management.

- Flexible enrollment via email, SMS, or QR codes
- IMEI validation check against preset list during enrollment
- After authentication, real-time sync of configurations, policies, apps and restrictions
- Real-time notifications to users about pending actions
- Level-based user role privileges for IT administrators

PROACTIVE SECURITY MANAGEMENT

Enterprises can now dynamically monitor all enrolled devices for any security risks or insecure settings, and then take corrective action. Browsing protection, phishing protection and web protection is afforded to the devices and web categories/URLs can also be allowed or blocked.

- Policies to ensure security and compliance of all devices
- Enforce passcode policies with configurable parameters
- Remotely locate, lock and wipe data on lost or stolen devices
- Carry out a custom wipe of selected data
- Periodic tracking of device location

- SIM card changes can be flagged and communicated
- Block device USB access
- Schedule a Quick Scan/Full Scan at any time

CUSTOM REPORTING

IT admins can view customizable reports based on the requirements by selecting one or more entities and applying defined set of criteria. Real-time and interactive graphical summaries about infection status, app non-compliance, network data usage and more can be viewed. This allows admins to get a comprehensive view of the status of mobile devices within the enterprise.

- Custom reports can be defined by enabling the administrator to select data and define conditions
- Instant and detailed audits and real-time graphical summaries
- User activity logs for better visibility and transparency
- Warnings for non-compliance in case of app installation/uninstallation or pending device upgradation
- Real-time multiple device locations available on the map

APPLICATION CONTROL

Application control enables administrators to manage the app repository and install/uninstall apps and set restrictions on apps that are installed on devices. These settings can be managed on devices remotely from the server portal, thus enabling ease of use and access. Application control allows the administrator to perform the following functions on client devices:

- Manage app repository at the enterprise level
- Recommend apps to be installed on devices
- Block apps based on predetermined app categories
- Block/install apps and maintain a whitelist/blacklist of Android apps
- Block application installation on Android devices
- Upgrade custom apps or apps from Google Play

NETWORK DATA MONITORING

With the help of this feature, admins can monitor data usage details over mobile networks, Wi-Fi or roaming data to know how bandwidth is consumed. Admins can also get all details for calls/video calls/SMS/MMS sent and received on enterprise devices. Additionally, the following details can also be gained:

- Which apps or devices are using the most amount of data
- On what date and at what time was the most data consumed
- Complete data usage details of individual devices
- All incoming/outgoing calls and duration of calls on a particular device
- All incoming/outgoing SMS's on a particular device

SEQRITE LAUNCHER

This feature allows admins to customize how mobile devices function within the enterprise. Apps on the device and in-built features can be enabled or disabled as per company policies. Seqrite Launcher functions as a standalone app and ensures that mobile devices are locked down into kiosk mode for maximum productivity.

- Complete lockdown of apps with Seqrite Launcher
- Run apps in Kiosk Mode or Single App Mode
- Admins can customize the launcher's title and system settings and the notifications
- Configure Launcher to restrict or limit app usage on the user's devices
- App request from Seqrite Launcher

VIRTUAL FENCING

This feature works as a virtual boundary or fence to secure the corporate devices by immediately notifying admins when these devices enter or leave the designated location, time limits and Wi-Fi zone. By setting up triggers that allow or restrict device functionality on the basis of defined boundaries, enterprises can uphold compliance within the organization.

- Fencing to monitor and restrict the use of mobile devices beyond a fenced perimeter
- Allow an admin to set up triggers so when a device enters (or exits) the defined boundaries, an email alert is sent
- Geo-fencing to enable location-based configurations and policy management by defining virtual perimeter
- Time-fencing to manage configurations and policy based on predetermined time slots
- Wi-Fi-fencing to enable configurations and policy on devices when they connect to company's wireless networks

	Feature	Android	iOS*	Windows*
Features	**Enrollment**			
	Enrollment	✓	✓	✓
	Anti-Virus			
	Real-Time Protection	✓	×	×
	Scheduled Scan	✓	×	×
	Remote Scan	✓	×	×
	Auto Updates to Clients	✓	×	×
	Action on Device			
	Ring	✓	×	✓
	Lock	×	✓	✓
	Block	✓	×	×
	Unblock	✓	×	×
	Locate and Trace	✓	×	×
	Wipe	✓	✓	✓
	Call/SMS Monitoring	✓	×	×
	Reset Password	✓	×	×
	Network Data Usage Monitoring	✓	×	×
Configuration	**Anti-Theft Configuration**			
	Notification on SIM Change	✓	×	×
	Lock on SIM Change	✓	×	×
	Lock on Airplane Mode	✓	×	×
	Web Security Configuration			
	Browsing Protection	✓	×	×
	Phishing Protection	✓	×	×
	Web Protection	✓	×	×

	Feature	Android	iOS*	Windows*
	Blacklist/Whitelist URLs	✓	×	×
	Category Based Blocking	✓	×	×
	Wi-Fi Configuration			
	Support Different Security Options	✓	✓	✓
	Schedule Scan Configuration			
	Scheduling New Scan	✓	×	×
	Network Usage Configuration			
	Wi-Fi Data Usage Monitoring	✓	×	×
	Mobile Data Usage Monitoring	✓	×	×
	Roaming Data Usage Monitoring	✓	×	×
Policy	**Policy**			
	Password	✓	✓	✓
	Screen Lock Time	✓	✓	✓
	Password History			
	Block Camera	✓	✓	✓
	Block Factory Reset	✓	×	✓
	Block Access to Safe Mode	✓	×	×
	Block USB	✓	×	✓
	Block Bluetooth and Tethering	✓	×	✓
	Block Wi-Fi	✓	×	✓
	Block Hotspot	✓	×	✓
	Block NFC	✓	×	✓
	Call and Data Control While Roaming	✓	×	×
	Location Service to Locate the Device	✓	×	×
	Force to Set Google Account	✓	×	×

	Feature	Android	iOS*	Windows*
	Block Certificates	✗	✓	✓
	Block Screen Capture	✓	✓	✓
	Block App and Windows Store	✗	✓	✓
	Block iTunes	✗	✓	✗
	Restriction on Safari Browser	✗	✓	✗
	Block Face Time	✗	✓	✗
	Block Voice Recording	✗	✗	✓
	Block USB Connection	✗	✗	✓
	Block Text Copy-Paste	✓	✗	✓
	Block Primary Microphone	✓	✗	✗
	Block Voice Dialing on Lock Screen	✗	✓	✗
	Restrict Safe Mode Access	✓	✗	✗
	Block Siri	✗	✓	✗
	Device Time-Out	✓	✓	✓
	Force Auto Time Zone	✓	✗	✗
	Block Open Wi-Fi	✓	✗	✗
App Control	**App Management**			
	Restrict Access to Newly Installed Apps	✓	✗	✗
	Whitelist Apps	✓	✗	✓
	Recommend Apps to Install	✓	✓	✗
	Apps to Uninstall	✓	✓	✗
	Fully Block the Blacklisted Apps	✓	✗	✓
	App Repository	✓	✓	✗
	Individual Device Level App Control	✓	✓	✗
	App Blocking Based on Category	✓	✗	✗

	Feature	Android	iOS*	Windows*
Other	**Fencing**			
	Geo, Time, Wi-Fi Fencing	✓	✗	✗
	App Launcher			
	Advance Launcher	✓	✗	✗
	Exit Launcher	✓	✗	✗
	App Request	✓	✗	✗
	Broadcast Message			
	Broadcast Message	✓	✗	✗
	Upgrade Client Notification	✓	✗	✗

*MDM manages these devices using native OS level support. There is no need to install agent/client software on these devices.

Compatible with Android 4.2.X (Jelly Bean) and above, iOS 7 and above and Windows Phone 8.1.

Key Differentiators Seqrite MDM

- **True SaaS** – SaaS always turns CAPEX into OPEX. Seqrite MDM offers enterprises the advantage of an economical on-demand solution.
- **Easily Scalable** – With Seqrite MDM there is no limitation to the number of devices that can be supported. As your scale of operations and mobility expands, our MDM solution grows with you quickly and efficiently.
- **Multi-Tenant Architecture** – Seqrite MDM offers a multi-tenant architecture that allows instances of the software to support multiple enterprises (or tenants) without compromising the security of their data.
- **Flexible App Control** – Seqrite MDM grants complete control over the apps that are installed and run on any mobile device within an enterprise, thus allowing admins to align active applications with their business objectives.
- **Virtual Fencing** – Seqrite MDM allows admins to configure virtual boundaries based on Wi-Fi networks, geolocations or time so as to customize device functionality.
- **Comprehensive Reporting** – Seqrite MDM provides interactive and graphical summaries about a wide range of critical data such as infection status, network data usage and app non-compliance.

Corporate Office

Quick Heal Technologies Limited

Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune - 411014, Maharashtra, India

Email: info@seqrite.com | Website: www.seqrite.com