Knet MaaS MDM for Android Devices Powered by Fiberlink's MaaS360®

Mobile Device Management (MDM) Challenges

The mobile device landscape is constantly changing. Android users insist the platform is secure and demand access to corporate systems. Many times they get back door access to Exchange servers simply by enabling ActiveSync. You need instant visibility into devices that are entering the Enterprise, both personally and corporately owned, and to get them configured for secure enterprise access. At a minimum, you must be able to enforce device passwords and encryption policies, and be able to wipe corporate data if devices are lost or employees leave the organization.

KNet MaaS for Android Devices

KNet MaaS provides a lightweight agent that interfaces with the Android Mobile Device Management API framework to provide inventory details, enforcement of policies and profiles, and the ability to push actions.

Complete Android Device Management

Set up and start managing corporate and employee Android devices in minutes. Over-the-air provisioning, enrollment, security, policy management and support workflows help IT support your devices.

Flexible Enterprise Application Management

Provide users with a secure, easy-to-use system to advertise, distribute and update public and private Android applications.

Advanced Security Management

Protect devices with automated security rules, continuous device monitoring, problem detection and policy enforcement.

Cost Controls

Get real-time monitoring, tracking and notification of data usage.

Compliance Dashboard And Watch List Alerts

Gain insight with graphical dashboards, actionable reports and alerts that highlight real-time compliance metrics, as well as asset and network details.

Device Information

KNet MaaS provides detailed information, including:

- Model
- Operating system
- Applications (includes version data and size)
- Device ID (phone number, IMEI and email address)
- Device restrictions
- Installed policies
- Security policies (including the identification of rooted devices)

IT Management Capabilities

KNet MaaS allows your IT department to:

- Report on all mobile devices connected to your infrastructure
- Block devices that may represent a security risk
- Enforce policies for passwords and encryption
- Perform password reset and remote wipe
- Blacklist restricted applications
- Geo-locate devices
- Manage Wi-Fi profiles
- Track changes for audits
- Enable corporate app stores

Knet MaaS MDM for Android Devices

KNet MaaS App Management

KNet MaaS App Management provides organizations with a private, easy-to-use system to advertise, distribute and update in-house developed, enterprise-specific applications, as well as Android Market applications recommended or approved by the enterprise. In addition, the intuitive Android user interface provides a complete application catalog with simple application installation and upgrade actions for the end user.

KNet MaaS Advanced Security And Compliance Engine

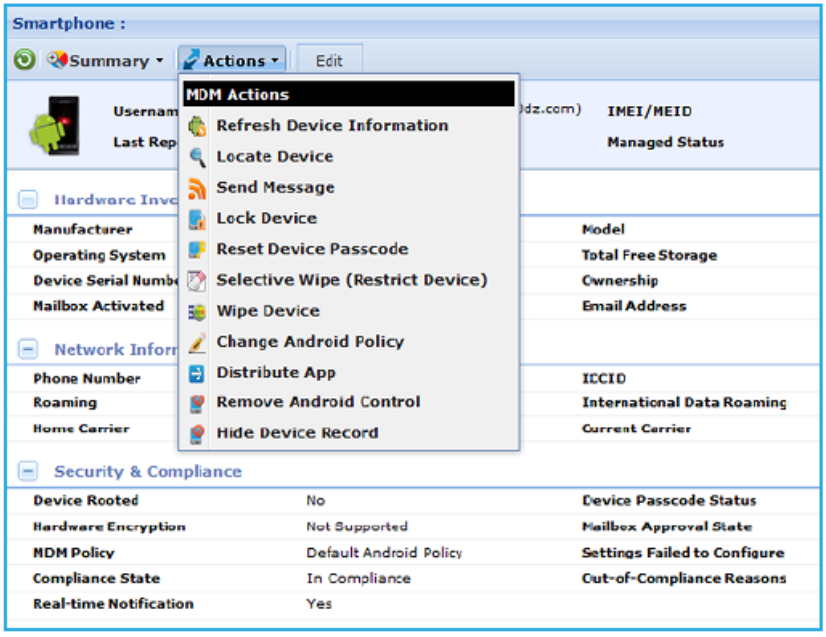
KNet MaaS goes beyond baseline securities policies to provide more advanced management capabilities. KNet MaaS's Compliance Engine lets IT administrators easily define and implement powerful compliance rules for smartphones and tablets to deal with specific events and contextual changes. Managed devices are continuously monitored against defined rules or events. If a security policy violation occurs, KNet MaaS can be configured to immediately and automatically take actions such as warning the user with onscreen messaging, blocking corporate email access or even wiping the device's memory to factory default settings.

KNet MaaS Cost Management And Control

KNet MaaS enables the real-time monitoring for data, voice and SMS. Alerts and notifications can be sent to both the end-user as well as the administrator when usage thresholds are met or exceeded. This includes notifications on device detected for international data roaming.

Mobility Intelligence

KNet MaaS delivers integrated dashboards, analytics, and reporting that provide actionable intelligence to IT about their mobile device environment. IT administrators see the distribution of mobile devices across operating system platform, approval status, device capabilities, ownership, and more.



KNet MaaS And TouchDown™ For Secure Email

KNet MaaS has integrated with NitroDesk's TouchDown email application which encrypts sensitive data on the device such as email, calendar and contacts. In addition to being able to remotely configure and remove the exchange accounts on TouchDown, KNet MaaS allows the IT administrator to configure many key security policies for the application including:

- Passcode policy (local to the application)
- Encrypt email and attachments
- Allow attachments
- Allow backup
- Disable copy functions

For More Information

To learn more about our technology and services visit www.knet.com.au.
104 Byng St, Orange NSW 2800
Phone +61 2 6363 8999 | **Fax** +61 6363 1500 | sales@knet.com.au