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

Provision, Manage and Secure iOS Devices, Apps and Documents

Instant Apple iOS Management

Smartphones and tablets have revolutionized businesses. Employees are now using their favorite devices to get work done anytime, anywhere. The KNet MaaS platform offers something no other vendor does; true software-as-a-service (SaaS) that delivers instant enterprise mobile device (MDM), application(MAM), document and expense management—all from a single screen. It is the fastest way to secure these devices and the corporate data they contain. You can enroll them over the air OTA), and use security policies and compliance rules to can enforce passcodes and encryption, detect and restrict jailbroken devices, whitelist or blacklist apps, control file backups and more. Organizations can rapidly give people secure access to corporate data from their personal devices. And with the industry's broadest device support, intuitive workflows, set-and-forget deployment options, and advanced management and security features, KNet MaaS makes Bring Your Own Device (BYOD) simple.

A Whole New Level of Security and Control

KNet MaaS for iOS devices provides the visibility and control your IT staff needs to support iPhones and iPads in the Enterprise, supporting iOS versions 4.3 and higher, including the iPhone 5s, iPhone 5c, iPhone 5, iPhone 4s, iPhone 4, iPhone 3GS, new iPad, iPad 2, iPad mini, iPod Touch 5th generation and 4th generations. It supports iOS 7 today, and provides tools you can use to gain insight, perform actions, set and distribute policies, manage apps and documents, and much more. KNet MaaS makes it easy for you to finally say "Yes!" to the latest BYOD- and corporate-owned iOS devices.

Launch Day Support

KNet MaaS's 100% cloud-based platform delivers immediate support for all new mobile OS releases and upgrades.

New Features for iOS 7 Devices

- Manage Open In
  - Restrict Opening Files from Corporate to Personal Apps
  - Restrict Opening Files from Personal to Corporate Apps
- Per App VPN
- Volume Purchase Program (VPP) Enhancements for Apps and Books
- Streamlined MDM enrollment
- Enterprise Single Sign On (SSO)
- Third Party App Data Protection
- Third Party App Configuration

New Configuration Options for iOS 7 Devices

- Touch ID Control
- Silent App Install
- Report on Activation Lock
- Personal Hot Spot Control
- New Lock Message
- Lock Screen Control
- Set Wallpaper
- Block User's Email & Calendar Accounts
- Check for iTunes Account
- VPN On Demand
- And so much more including
  - Restrict AirDrop
  - Configure AirPrint printers
  - Whitelist AirPlay destinations
  - Configure accessibility options

KNet MaaS MDM for iOS Devices

Gain Insight

- Model
- Serial number
- Operating system
- Home network/current network
  - Roaming status
  - Mac address
- Amount of free storage
- Applications, versions & size
- Device ID (phone number, IMEI, email address)
  - Encryption level
  - Jailbreak detection
  - Passcode status
  - Device restrictions
  - Installed profiles
  - Security policies

Perform Actions

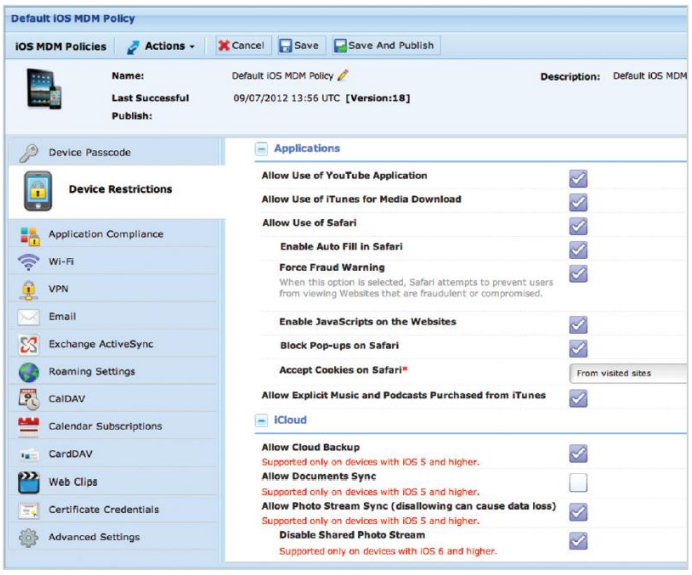
- Refresh device details in real-time
- Perform Help Desk operations like locking a device or resetting a forgotten passcode
- Perform a full wipe of a lost device
- Selectively wipe corporate data while maintaining personal data from an employee-owned device
- Change iOS policy
- Voice & Data Roaming Controls
  - Enable or disable roaming in real-time. Note: Users can override this setting locally on the device

Application Catalog

- Enterprise App Manageability: Mobile apps distributed by KNet MaaS to iOS devices become fully controlled, allowing you to simplify app deployments while increasing manageability
  - Suggest iTunes apps for employees
  - Distribute "home grown" apps
  - Publish updates to apps
  - Remotely push an app to a device
  - Delete an app & its data, on-demand or as part of a selective wipe action
  - Automatically remove corporate apps if the user deletes the MDM profile on the device
  - Allow/prevent app backups to iTunes or iCloud
  - Securely distribute documents to devices
  -
- Apple Volume Purchase Program Management
  - Distribute & install pre-paid apps without visiting Apple's App Store

Set & Distribute Policies

- Enforce passcode requirements
- Configure device restrictions
  - ✓ Enforce encrypted backups
  - ✓ Restrict the use of the camera, FaceTime & screen capture
  - ✓ Restrict application installation
  - ✓ Restrict the use of YouTube, Safari & voice dialing
  - ✓ Distribute Wi-Fi, VPN & email profiles, such as Exchange ActiveSync settings
  - ✓ And much more…
- Manage iCloud Controls
  - ✓ Manage Document, Application Data, Device Backup & Photo synching with iCloud by allowing you to put restrictions in place for specific users, groups, or your entire population
- Increase Email Security
  - ✓ Restrict users from moving emails between accounts, eliminating the risk of corporate data leakage
  - ✓ 3rd party applications can be restricted from sending emails
- Advanced Wi-Fi Configuration
  - ✓ Manage & push proxy settings & SSID auto-join
- iTunes Password Enforcement
  - ✓ Require users to enter their iTunes password in order to access the content, apps & data stored in iTunes
- Non-Trusted Certificates
  - ✓ IT can decide if end users can accept certificates from non-trusted sources



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