MaaS360®
by Fiberlink

MaaS360® for iOS Devices

Provision, Manage and Secure iOS Devices, Apps and Documents

Manage the Devices Your Colleagues Want

The MaaS360 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.

MaaS360 for iOS devices gives you a cloud-based console to enroll iOS devices over-the-air, configure corporate policies, support devices, users, apps and documents, and monitor and report on your entire mobile IT environment.

Built on a secure, multi-tenant cloud architecture, MaaS360 enables instant enterprise mobility management in just minutes with effortless scalability, whether you have 10 or 100,000 users, and seamless integration into existing enterprise systems. And because there are no servers to install, upgrades to the latest technology are automatic. Affordability is unmatched with no upfront costs and no expensive change management.

Get the Visibility and Control You Need

MaaS360 for iOS devices provides the visibility and control your IT staff needs to support iPhones and iPads in the Enterprise, supporting iOS versions 4.0 and higher, including the iPhone 5, iPhone 4S, iPhone 4, iPhone 3GS, new iPad, iPad 2, iPod Touch 5th generation and iPod Touch 4th generation.

MaaS360 supports iOS 6 today, and provides tools you can use to gain insight, perform actions, set and distribute policies, manage apps and documents, and much more.

MaaS360 makes it easy for you to finally say “Yes!” to the latest BYOD- and corporate-owned iOS devices.

iOS 6

Launch Day Support

MaaS360 is ready now to help you manage iOS 6 devices, apps and data, due to our 100% cloud-based platform delivering immediate support for all new mobile OS releases and upgrades.

New Features for iOS 6 Devices

- Disable Shared Photo Stream
- Block recent contact synchronization
- Disable Passbook while device is locked
- Disable diagnostic info submission to Apple

New Features for iOS 6 Supervised Devices

These features apply when managing Supervised devices using MaaS360’s integration with Apple Configurator:

- Guided Access — limit device to one app by disabling the Home button
- Set wallpaper for lock screen, home screen or both
- Disable iMessage
- Disable iBookstore
- Disable Game Center
- Force all internet traffic through a global HTTP proxy
- Restrict manual configuration profile installation

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

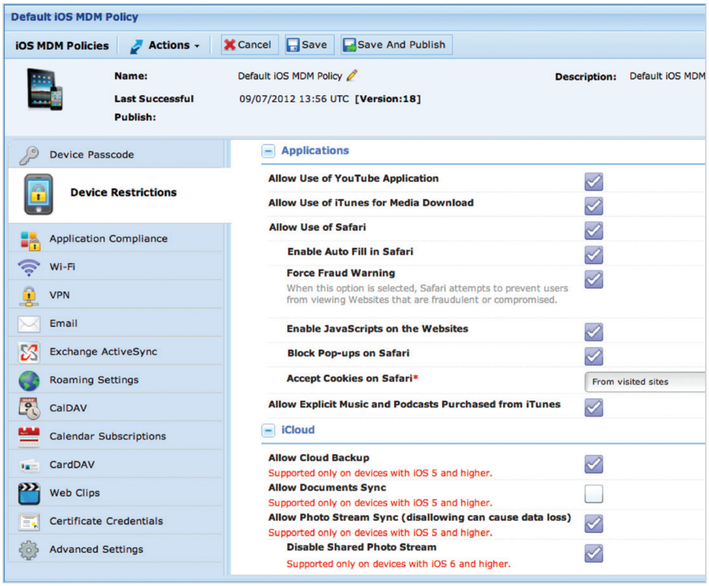
- Refresh device details in real-time
- Perform Help Desk operations like locking a device or resetting a forgotten passcode
- Perform a full wipe of a lost device
- Selectively wipe corporate data while maintaining personal data from an employee-owned device
- Change iOS policy
- Voice & Data Roaming 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 MaaS360 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



Name: Default iOS MDM Policy

Last Successful Publish: 09/07/2012 13:56 UTC **[Version:18]**

Description: Default iOS MDM

Applications

Allow Use of YouTube Application	☑
Allow Use of iTunes for Media Download	☑
Allow Use of Safari	☑
Enable Auto Fill in Safari	☑
Force Fraud Warning When this option is selected, Safari attempts to prevent users from viewing Websites that are fraudulent or compromised.	☑
Enable JavaScripts on the Websites	☑
Block Pop-ups on Safari	☑
Accept Cookies on Safari*	From visited sites
Allow Explicit Music and Podcasts Purchased from iTunes	☑

iCloud

Allow Cloud Backup Supported only on devices with iOS 5 and higher.	☑
Allow Documents Sync Supported only on devices with iOS 5 and higher.	□
Allow Photo Stream Sync (disallowing can cause data loss) Supported only on devices with iOS 5 and higher.	☑
Disable Shared Photo Stream Supported only on devices with iOS 6 and higher.	☑

All brands and their products, featured or referred to within this document, are trademarks or registered trademarks of their respective holders and should be noted as such.

For More Information

To learn more about our technology and services visit www.maaS360.com.
1787 Sentry Parkway West, Building 18, Suite 200 | Blue Bell, PA 19422
Phone 215.664.1600 | **Fax** 215.664.1601 | sales@fiberlink.com