MaaS360 for Mobile Devices - FAQs

As MaaS360 launches its Mobile Device solution into this very lively market, we anticipate a large number of questions from businesses as they try to figure out the who, what, when, why and how of managing their smartphone devices, the MDM service providers, and what solutions are right for them. This guide is meant to help answer some of the initial frequently asked questions we expect prospects to ask as we position the MaaS360 for Mobile Devices solution.

This FAQ document covers two phases of the MaaS360 for Mobile Devices solution:

- **MaaS360 for Exchange/ActiveSync Devices** provides a single portal for managing your Microsoft Exchange/ActiveSync connected devices. Using ActiveSync, MaaS360 provide very broad support for all major smartphone and tablet platforms—including iOS (iPhone, iPad and iPod Touch), Android, Windows Mobile, Windows Phone, Symbian, and Palm WebOS.

- **MaaS360 for iOS Devices** provides deeper management capability around visibility, policy and security for iOS devices based on the Apple MDM API, including System Setup, Over-the-Air (OTA) Configuration Management, Device Enrollment, key Help Desk Operations, and extensive reporting.

The document covers what we think will be the top questions posed by prospects. For additional questions you would like to include in the FAQs, please send them to MDManswers@fiberlink.com. We will have them added within 24 hours.

**MAAS360**

Fiberlink’s MaaS360 platform is an open, extensible, multi-tenant, change-ready platform that is offered to IT administrators as a Software as a Service application for securely managing mobility. The MaaS360 platform is designed to quickly adapt to the rapidly changing Smartphone environment with no impact to existing customer deployments.

**MOBILE DEVICE MANAGEMENT**

This solution secures, monitors, manages and supports mobile devices deployed across an enterprise. Enterprise-grade MDM functionality typically includes over-the-air distribution of data and configuration settings for all types of mobile devices, including mobile phones and Smartphones.

**FAQS – MAAS360 FOR EXCHANGE/ACTIVESYNC DEVICES**

1. **What are the System Requirements for using the MaaS360 for Exchange/ActiveSync solution?**

   **Answer:**
   - Exchange 2007 or 2010 Environment, or Office 365
   - An instance of Visibility Service, version 2.5 or higher, with the Exchange/ActiveSync Cloud Extender installed on a device of the customer’s choosing
   - Network access to the Active Directory Server and the Exchange Server(s)
   - Access to the Internet over port 443
   - An Active Directory account and credentials with sufficient rights to perform Exchange Admin functions
   - The Exchange Management Tools from Microsoft installed on the same device as the Cloud Extender
   - Windows PowerShell
2. **Does this replace my Exchange Server?**

   **Answer:**
   No, your existing Exchange Server will not be replaced; the MaaS360 MDM service will securely communicate with the exchange server for a two-way sync of policy changes between the Exchange server and MaaS360.

3. **How is communication secured between the customer network and the Fiberlink Cloud Extender?**

   **Answer:**

4. **How long does it take to sync policies between MaaS360 and the Exchange server?**

   **Answer:**
   All new policies made within MaaS360 are delivered real time to the device; policy information will be checked and synced with the Exchange server every 60 minutes.

5. **Do the different device platforms support all Exchange/ActiveSync policies?**

   **Answer:**

6. **What device details are available in MaaS360 reporting?**

   **Answer:**
   Available hardware attributes:
   - Installed Date
   - Manufacturer
   - Operating System
   - ActiveSync Agent
   - ActiveSync GUID
   - Mailbox Server
   - Email Address
   - Model
   - Default Language
   - ActiveSync Device ID
   - ActiveSync Identity
Available security and compliance attributes:

- Mailbox Approval State
- Remote Wipe Support
- Last Wipe Applied Date (GMT)
- Last Policy Updated Date (GMT)
- Rule Set Configured
- Approval Comments
- Device Wiped
- Exchange ActiveSync Policy
- Device Passcode Status
- Rules Compliance State

7. Do the different device platforms support all Exchange/ActiveSync policies?

Answer:
There are two types of wipe, typically referred to as “Remote Wipe” and “Selective Wipe.” In this case, using ActiveSync, MaaS360 performs a full wipe of the remote device. That is based on how ActiveSync works. This wipe returns the device back to factory settings. MaaS360 does provide “Selective Wipe” functionality in our Advanced Management and Security for iOS and Android Devices module.

Note: The ActiveSync wipe is based on the device’s implementation of said functionality. Some earlier Android devices do not wipe completely.

8. How do users enroll their devices into Exchange/ActiveSync for email/calendars/etc.?

Answer:
The end user will use native software on the device to gain access to the corporate Exchange server. They will need AD credentials, and their corporate mail server and domain to get access.

9. What policy changes are supported?

Answer:
Currently all supported policies within ActiveSync can be managed through the MaaS360 portal, though not all devices support all policy sets available (Windows phone supports all, iOS most, Android some). For a detailed listing of features supported by platform, use this link: [http://refraction.co.uk/blog/wp-content/uploads/2010/11/Exchange-ActiveSync-Policies.pdf](http://refraction.co.uk/blog/wp-content/uploads/2010/11/Exchange-ActiveSync-Policies.pdf)

10. What actions are supported with MaaS360?

Answer:
- Refresh Device Information
- Block Device
- Wipe Device
- Change Exchange ActiveSync Policy
- Remove Device from Exchange Server
- Change Rule Set
• Hide Device Record

11. What happens when a new user or user with a new phone tries to connect to the Exchange server?

Answer:
MaaS360 for ActiveSync provides a Quarantine function that will put all new users trying to connect to the Exchange email server in a quarantined state, keeping them from connecting to the server and gaining email access, until the device is approved by the administrator. This feature is off by default, but the administrator can enable it.

12. Can I get email alerts when new users try to connect to the Exchange server?

Answer:
Yes, alerts can be set up to email the administrator(s) when a new device tries to access the Exchange server.

13. What devices are supported?

Answer:
The MaaS360 for Mobile Devices solution supports all devices that are compatible with Exchange ActiveSync, including:
• **Apple**: iPhone, iPod Touch, and iPad all support Exchange ActiveSync.
• **Nokia**: Nokia offers Mail for Exchange on their Eseries mobile phones. E-mail, calendar, and contact data can be synchronized over a cellular network or a wireless LAN.
• **Sony Ericsson**: Sony Ericsson offers Exchange ActiveSync support on several of their newer smartphones. They also support Direct Push through a third-party program.
• **Palm**: Palm offers some models of mobile phones that have the Windows Mobile operating system. These devices support Direct Push.
• **Motorola**: Motorola has its own synchronization framework that enables over-the-air synchronization through Exchange ActiveSync on many of its devices.
• **Symbian**: Symbian Limited licenses Exchange ActiveSync for use in the Symbian operating system. This operating system is an open standard operating system for mobile phones.
• **Android**: Many mobile phones with the Android operating system support Exchange ActiveSync. However, these mobile phones may not support all available Exchange ActiveSync mailbox policies.

14. What additional functionality does the MaaS360 solution provide on top of Exchange ActiveSync?

Answer:
• Pulls devices into an easy-to-use GUI for approval, policy management, policy assignment, and remote wipe.
  • Smart search and grouping features for simplifying mass policy actions.
• Provides a simple approval workflow engine for new devices.
  • Plus, add auto-quarantine capability to Exchange 2007 (which doesn’t offer that feature natively).
• Tracks all actions in a simple, clear audit log.
• Builds Dashboards that quickly summarize your ActiveSync and device operational and security posture.
• Provides clickable, detailed reports that are exportable in multiple formats.
15. Can we mark if the device is employee owned or corporate owned?

**Answer:**
Yes, when you receive a new user request for access to the Exchange Server, during that approval process the option is given to select whether the device is user or corporate owned. This attribute is then carried over to the device reports. In addition, for existing users there is the ability within Device Management Views to edit the **Owned By** field at any time.

16. What about my BlackBerry devices?

**Answer:**
BlackBerry devices currently are not supported in Exchange ActiveSync, but Fiberlink does offer a separate MaaS360 Cloud Extender to pull device inventory and policy information for BlackBerry devices for reporting in the MaaS360 portal.

**FAQS - MAAS360 FOR IOS DEVICES**

1. What OS versions are supported?

**Answer:**
iOS 4.0 and above.

2. What is APNs?

**Answer:**
The Apple Push Notification Service (APNS) is a mobile service created by Apple that “pushes” notifications and alerts from applications on servers to iPhones, iPads and iPods.

3. Are we required to get the APNS certificate from Apple to use the MDM API functionality?

**Answer:**
Yes, each business must have the certificate to manage their iPhones (and perform other private actions, such as installing enterprise applications on their devices). It is free, and is available from Apple. Search the Internet for **Apple enterprise developer program** to learn more.

4. What policy settings are available?

**Answer:**
Supports all policies allowed via the Apple MDM API, including:

- Wi-Fi Profiles
- Email Profiles
- VPN Profiles
- Passcode Requirements
- Restrictions (Camera, App Store, and more)
- Allow Siri/Allow Siri While Locked
- Allow diagnostic data to be sent to Apple
- Allow Cloud Backup
• Allow Document Sync
• Allow Photo Stream Sync
• Prevent Moving Mail to other Accounts
• Prevent Third Party Apps from Sending Mail

Note: This is just a partial list.

5. For iOS, can this integrate with Active Directory to pull information?

Answer:
Yes, MaaS360 for iOS has a cloud extender that can be used to enroll users via their Active Directory information. This can help simplify the enrollment process for the end user by only requiring them to enter username and email information to enroll.

6. What other actions are supported?

Answer:
iOS Control Support Actions:
• Refresh Device Information
• Last Known Location
• Send Message
• Lock Device
• Reset Device Passcode
• Selective Wipe (Restrict Device)
• Wipe Device (includes email, VPN, Wi-Fi)
• Change iOS Policy
• Change Plan
• Distribute App
• Remove iOS Control
• Hide Device Record
• Change Rule Set
• ActiveSync Actions (Block Device, Change ActiveSync Policy, Remove Device from Exchange Server)

7. How is the iOS profile installed on the device?

Answer:
The administrator has the ability to send out an enrollment request to the end user, based on how service is initially configured. Options are:
• Via MaaS360 send out an enrollment request to the user which includes a one-time password.
• Via MaaS360 send an enrollment request that will authenticate the user against the corporate Active Directory server. This requires installation of the Cloud Extender.

Once the user receives the enrollment request, they simply need to click on the link and follow easy instructions.
8. **Does the user have the ability to remove the profile?**

**Answer:**
Yes, as Apple has implemented their MDM API the user does have the ability to remove the management profile. However, doing so is the same as a selective wipe and will remove corporate pushed information on the device.

9. **What is the difference between a remote wipe and a selective wipe?**

**Answer:**
A remote wipe removes all data/apps and returns the device to factory settings. With iOS support admins can perform a Selective Wipe, which will only remove corporate data that was sent to the device (email, VPN profiles, etc.), but retains all of the user’s personal data and apps on the device.

10. **What additional infrastructure does this service require?**

**Answer:**
None. MaaS360 for Mobile Devices cloud-based service for iOS does not require any new servers to be installed; it relies on communication to the device through Apple MDM API. If you would like to pull user information from Active Directory, then a MaaS360 Cloud Extender application is required.

11. **What is a MaaS360 Cloud Extender?**

**Answer:**
The MaaS360 Cloud Extender is a term used to describe Fiberlink’s light touch reach into the customer enterprise to get visibility to systems like the Exchange Server, Active Directory and BES.

12. **What are some of the device details that MaaS360 for iOS can provide?**

**Answer:**
MaaS360 for iOS Visibility Details (API-based):

- Hardware Inventory
  - Manufacturer
  - Model
  - Model ID
  - Email Address
  - Apple Serial Number
  - UDID
  - Operating System
  - Operating System Version
  - Modem Firmware Version
  - Activation Date
  - Total Internal Storage
  - Free Internal Storage
  - Battery Level
• Last Reported Date

• Network
  • Phone Number
  • ICCID
  • Last Roaming Status
  • Network Type
  • Data Roaming
  • Voice Roaming
  • Home Carrier
  • Current Carrier
  • Home Country
  • Current Country
  • Wi-Fi Mac Address
  • Bluetooth Mac Address
  • IP Address
  • Subnet Mask

• Security and Compliance
  • Device Jailbroken
  • Jailbreak Detection Date
  • Device Passcode Status
  • Hardware Encryption
  • MDM Policy
  • Last MDM Policy Update Date
  • Last MDM Policy Update Source
  • Policy Compliance State
  • Rules Compliance State
  • Out-of-Compliance Reasons
  • Device Wiped
  • Mailbox Approval State

• App Distributions
  • App Catalog Enabled
  • App Name
  • Status
  • Distribution Target
13. Do you support the ability to add custom attributes?

Answer:
Yes, custom attributes are available to be added via Device Management Views. This is available for both ActiveSync and iOS services. In addition there are several pre-populated fields already created for you to add information about the device, including:

- Custom Asset Number
- Device Owner
- Owned By
- Vendor
- Purchase Order Number
- Purchase Type
- Purchase Date
- Purchase Price
- Warranty Number
- Warranty Type
- Warranty Expiration Date
- Office/Location
- Department/Business Unit

One of the custom attributes is Important Device (Skip Enforcement Action). Any device with this designation is exempt from the enforcement actions set up in the Compliance Engine.