Understanding the Role of Exchange ActiveSync in Mobile Device Management
Understanding ActiveSync’s Role in Mobile Device Management

You can’t understand enterprise mobility without understanding the role of Exchange ActiveSync (EAS). As EAS has evolved and spread it has become an integral piece of mobility infrastructure, yet many people don’t understand its evolution, its strengths and weaknesses, or what is needed to complement EAS in order to meet today’s enterprise mobility requirements. This white paper will help you understand the appropriate role of Exchange ActiveSync in mobile device management at your company.

Microsoft Exchange is a messaging and collaboration server technology developed by Microsoft that provides email, calendar, contact, and task management. ActiveSync is a data synchronization technology and protocol originally released by Microsoft in 1996.

Microsoft integrated ActiveSync into Exchange with the release of Exchange 2003. Called Exchange ActiveSync (EAS), the integration of these technologies provided push synchronization of email, calendar, contacts and tasks between an Exchange server and ActiveSync-enabled clients.

In October 2005, Microsoft released Exchange 2003 SP2. This release introduced device security policies to ActiveSync. These capabilities allowed basic security policies to be defined on the Exchange server, pushed to the mobile device, and enforced by the ActiveSync agent embedded on the mobile device. The figure below depicts the high-level ActiveSync architecture.
Initially, only devices running the Microsoft Windows Mobile operating system included an ActiveSync agent, but today, Microsoft licenses ActiveSync to almost every major smartphone operating system vendor, including Apple iOS, Google Android, HP webOS, and Nokia Symbian. These vendors ship ActiveSync-capable devices that can synchronize email, calendar, and contacts with an Exchange server, and also perform basic mobile device management. There are even ActiveSync clients available from third-party vendors for some BlackBerry devices.

Microsoft also licenses ActiveSync to most major vendors of messaging infrastructure, including IBM's Notes Domino and Novell's GroupWise. These vendors provide their own client software for the major smartphone platforms that enables email synchronization and mobile device management via ActiveSync with their messaging servers.

While you can expect that most ActiveSync-capable servers and devices will provide full support for the synchronization of email, contacts, calendar and tasks, you cannot make the same assumption in regard to the device security features of ActiveSync.

Understanding ActiveSync Security Policies

Microsoft has continued to expand the ActiveSync protocol's security policies in both Exchange 2007 and Exchange 2010. However, if you are using (or plan to use) ActiveSync to manage mobile devices it is important to understand the management features and security policies that are available to you.

The security policies that can be supported are a function of:

- The security policies supported by the ActiveSync server (your messaging infrastructure)
- The security policies supported by the ActiveSync clients on your mobile devices
- The mobile devices supported by the ActiveSync client software required by your messaging infrastructure vendor

Most mobile devices come with an Exchange ActiveSync client pre-installed. Other messaging platforms require installation of their own ActiveSync mobility client such as Lotus Notes Traveler or Novell Data Synchronizer Connector for GroupWise. These clients may not run on all mobile device platforms.

For example:

- Windows Mobile versions 6.1 and 6.5 are the only mobile device operating systems that support all the ActiveSync security policies. Not even Windows Phone 7 (Microsoft's latest mobile operating system) supports all the ActiveSync security policies.
- Companies that use Lotus Notes for messaging must deploy the Lotus Notes Traveler client software to their mobile devices. Support for Android 2.x mobile devices is available only in Notes Traveler 8.5.2.1 and 8.5.2.2.

Without understanding these nuances it is impossible to develop comprehensive and effective policies and procedures for securing and managing your mobile devices. To help you with this critical analysis, we have compiled links to the relevant resources that you will need to understand the ActiveSync security policies supported by your messaging platform and the ActiveSync security policy support on the major mobile device platforms.

- Microsoft Exchange
  - Exchange 2003 ActiveSync Mailbox Policies
  - Exchange 2007 ActiveSync Mailbox Policies
  - Exchange 2010 ActiveSync Mailbox Policies
  - Comparison of Supported Features and Policies of Exchange ActiveSync Clients

- Lotus Notes
  - Notes Traveler 8.5.1
  - Notes Traveler 8.5.2

- Novell GroupWise
  - Data Synchronizer Connector for GroupWise 8.0
The Role of EAS in MDM

Understanding ActiveSync’s Strengths

ActiveSync is most effective at providing access to corporate email, contacts, calendar, and tasks from mobile devices. The ActiveSync protocol provides a secure and efficient means of synchronizing this information between mobile devices and your corporate messaging infrastructure.

ActiveSync is broadly supported across most major messaging platforms and mobile device platforms. This insures that most of your mobile users will be able to access their corporate email from the mobile device of their choice. ActiveSync is also supported by legacy devices based on Symbian and Windows Mobile.

ActiveSync collects basic inventory data from the mobile devices that are partnered with your Exchange environment, but the accuracy of the data can vary based on the device’s ActiveSync client implementation. The richness of the device data collected is limited by the ActiveSync protocol itself. For example, ActiveSync provides no ability for a device to report network or location information.

ActiveSync provides basic device management functions, like Remote Wipe and Device Block, but lacks more sophisticated features like Selective Wipe and Device Lock that are required to effectively manage mobile devices. Access to these device management features is through the Exchange Management Console and cannot be easily delegated to IT personnel that are not trained on this technology.

Understanding the Mobile Device Management Gaps

Microsoft Exchange is a collaboration platform and ActiveSync is a protocol. They are not intended or designed to be a full mobile device management platform. As a result, there are shortcomings in the workflows for the administration of mobile devices through Exchange ActiveSync, as well as, the actual device management and device security capabilities that must be understood.

Recent mobility trends, like the use of personal devices for access to corporate email and the use of multiple mobile devices, highlight these shortcomings even more. To illustrate these points, let’s examine the most fundamental administrative workflow, provisioning a mobile device, and the most important security function, assigning security policies.

ACTIVESYNC PROVISIONING AND QUARANTINE

Enabling a mobile device to access an Exchange mailbox via ActiveSync is a difficult administrative task to perform efficiently without exposing your company to potentially significant security risks.

The most efficient way to set up this partnership is to enable ActiveSync on the server and let each mobile user configure the partnership between their mobile device and their Exchange mailbox. This satisfies the mobile user because they will have immediate access to their email and calendar. However, in Exchange 2003 and 2007 environments there are no easy ways for your IT team to discover the existence of these partnerships.

Your organization could be exposed to significant risks if a mobile device is lost or stolen. To further complicate the situation, the Exchange Management Console provides no simple way to view or generate a list of mailboxes with a device partnership. You must individually inspect the properties of each mailbox through the Exchange Management Console, or get smart on PowerShell. This is simply not feasible in organizations with more than a small number of mailboxes or those without PowerShell scripting expertise.

To mitigate this risk, companies will enable ActiveSync on their servers but disable it on each mailbox, thus implementing a type of poor man’s quarantine. This prevents devices from accessing email without the knowledge and approval of IT. However, it requires that IT first manually enable ActiveSync for each requested mailbox, and only then can the mobile user establish the partnership from their mobile device to enable access to email. This addresses the security risks but imposes higher administrative costs on IT and limits the productivity
of the mobile user until IT has completed the approval.

Unfortunately, even instituting this manual workflow to control mobile device access to Exchange does not eliminate the security risk. Once ActiveSync is enabled on a mailbox for an approved device, the mobile user can establish partnerships from additional mobile devices without any type of block or quarantine. If these devices would not pass the device approval process then any security or control gained as a result of the original quarantine process is circumvented.

MAILBOX POLICY MANAGEMENT
Due to its legacy as a messaging platform, Exchange manages security policies at the mailbox level. Security policies are assigned to a mailbox, and these policies are then sent to any mobile device partnered with this mailbox. This may seem innocuous but the recent appearance of mobile users that carry multiple mobile devices (think tablet and smartphone) is exposing the profound security and management challenges that result from this legacy.

Let’s assume that you have a mobile user who has both an iPad tablet and Android smartphone. This user naturally wishes to access Exchange from both devices. It is simple enough to establish a partnership between each device and the mailbox to get email access but configuring appropriate security policies for each device is a challenge.

Since the iPad supports on-device encryption it is desirable to enable encryption to guarantee that the data accessed via Exchange is secure. Since the Android phone does not support encryption it is desirable to prevent attachments from being accessed from this device. The Encryption policy and Attachment policy are defined at the mailbox level and are applied to all devices partnered with the mailbox.

Since policies cannot be assigned to each device individually, the only way to guarantee the security of attachments on both devices is to turn off encryption and turn off access to attachments in the policies assigned to the mailbox. This results in a worst-case scenario in which each security policy must be set to satisfy the least capable device.

This is one simple example of the management and security challenges that result from the mailbox-level policy management architecture of Exchange ActiveSync.

FULL AND SELECTIVE WIPE
Mobile devices syncing corporate email will both access and store sensitive data. Eventually one of these devices will be lost or stolen. When this occurs it is imperative that a device wipe be performed as quickly as possible to remove stored data and block access to corporate email.

ActiveSync provides a full device wipe capability that essentially restores the device to its default state. While this does remove corporate data and remove access to corporate email it also deletes all other information stored on the device. Since these devices also serve a lifestyle purpose for your users, it is likely that non-corporate information (like pictures, music and social media) that is still valuable to them will also be deleted. The trend towards personally-owned devices complicates this situation even more.

A Selective Device Wipe addresses the need to remove corporate data and email access while leaving the other contents of the mobile device intact. This feature is critical to effectively manage personal devices with access to corporate email, but is not available through ActiveSync even though it is supported by most major mobile device platforms.
Ready to Move Beyond ActiveSync-based Mobile Device Management?

Exchange ActiveSync is a logical choice for most companies starting their enterprise mobility journey. It is the quickest and easiest way to provide the feature most important to your end users—access to corporate email, calendar, and contacts from their mobile devices.

However, as we have discussed in this paper, Exchange ActiveSync as a mobile device management platform has significant functional gaps, administrative inefficiencies, and architectural artifacts as a result of its messaging platform legacy that may impose serious constraints on the enterprise mobility initiatives of your company. These include:

- End user choice of mobile devices is limited to those supported by your messaging platform
- End users carrying multiple mobile device are difficult to manage securely because ActiveSync security policies are assigned to the user’s mailbox rather than each device
- Key administrative workflows, like device quarantine, are not supported (Exchange 2003/2007) and can be easily circumvented
- The Exchange Management Console is missing features that simplify the administration of your mobile devices, like device views (as opposed to mailbox view), real-time dashboards, and an audit trail to track the configuration changes and actions performed on mobile devices
- Important device inventory information is not available, such as corporate-owned versus personally-owned devices, network and carrier information, and installed software inventory

From an evolutionary perspective, organizations that are facing the following scenarios are typically ready to move beyond Exchange ActiveSync-based mobile device management.

- You need device level auto-quarantine
- You need more consistent and accurate device data and asset information
- You need a consistent way to deal with variations in device/vendor support
- You need more granular device management features like:
  - Selective Wipe
  - Device Lock
  - Change Device Passcode
  - Locate Device
- You need to delegate administrative activities to IT staff other than Exchange administrators
- You need an audit trail to satisfy compliance audits

The ideal solution would leverage (rather than replace) ActiveSync’s strengths: secure access to corporate email, calendar, and contacts; and address its shortcomings as a mobile device management platform. MaaS360 for Mobile Devices provides just such a solution.

MaaS360 Complements Exchange ActiveSync Mobile Device Management

That is what Fiberlink has designed MaaS360 to do. MaaS360 for Mobile Devices is a cloud-based Mobile Device Management platform that integrates with:

- Your ActiveSync infrastructure to simplify administration
- Your mobile devices to improve their security and management

MaaS360 provides administrators with real-time mobile device dashboards that identify the mobile devices accessing your ActiveSync infrastructure, and watch lists that alert you to situations that require administrative action, like devices waiting for IT approval.
The Role of EAS in MDM

MaaS360 protects your Exchange environment by preventing mobile devices from accessing Exchange until an administrator has approved the device in MaaS360 by inspecting the advanced device data collected for each mobile device.

MaaS360 Device View (rather than EAS mailbox view) provides administrators with the appropriate framework for policy management of personally owned devices and the multiple devices increasingly being carried by individual mobile users.

MaaS360 secures the mobile device by providing on-device policy enforcement, detailed device information such as network and software inventory information, and advanced administrative functions, like Selective Wipe and Device Lock, that are not available through Exchange ActiveSync.

Access to corporate email, calendar, contacts, and tasks continues to be performed where it is done best, by your corporate ActiveSync messaging infrastructure.

**Improved workflows and simplified administration for your messaging infrastructure**
- Block access from unapproved devices
- Block access from non-compliant devices
- Personal device approval workflows
- Simplified policy management
- Mobile device dashboards and reports

**Improved security and management for your mobile devices**
- Over-the-Air (OTA) email and networking provisioning
- Enforce on-device policies
- Full and selective (corporate) wipe
- Application delivery and updates
- Detailed device reporting
- Detailed software reporting

**USING MAA360 WITH OFFICE 365**
Office 365 offers baseline security settings for controlling access to email from mobile devices, which most companies will leverage. However, it is critical to monitor the status of all mobile devices receiving corporate email, enforce security standards prior to email delivery, and take action on a lost or compromised device. IT organizations that are managing mobile devices with Office 365 will want and need more advanced capabilities.
With MaaS360, IT can block access to corporate data from jailbroken and rooted devices, locate lost or stolen devices, disallow unsafe applications and provide advanced capabilities to manage mobile devices accessing corporate data on Office 365. As the first cloud-based, MDM solution providing support for Office 365, MaaS360 delivers the essential security features needed to protect confidential corporate data on mobile devices including:

- Improved workflows and simplified administration for your messaging infrastructure
  - Block access from unapproved devices
  - Block access from non-compliant devices
  - Personal device approval workflows
  - Simplified policy management
  - Mobile device dashboards and reports
- Improved security and management for your mobile devices
  - OTA email and networking provisioning
  - Enforce on-device policies
  - Perform full and selective (corporate) wipes
  - Application delivery and updates
  - Detailed device reporting
  - Detailed software reporting

Business Productivity Online Standard Suite (BPOS) to Office 365 Transition
With MaaS360, you can seamlessly transition device configuration profiles from BPOS to Office 365. It provides seamless OTA configuration of your devices without affecting the user’s experience or productivity.

- BPOS environment: MaaS360 supports the ability to configure and publish OTA ActiveSync profiles, and reports on any failed settings.
- Office 365 environment: MaaS360 supports the ability to update and publish OTA BPOS ActiveSync profiles to your new Office 365 profiles, and provides the additional essential security features outlined above that are needed to protect confidential corporate data on mobile devices.

TO LEARN MORE ABOUT HOW MAAS360 CAN HELP YOU IMPROVE YOUR ACTIVESYNC OPERATIONS OR MOVE BEYOND ACTIVESYNC-BASED DEVICE MANAGEMENT, CHECK OUT THE FOLLOWING:
Watch a webinar on optimized mobile device management with MaaS360 and ActiveSync.
http://trials.maas360.com/forms/register_service_m.php?id=258

Learn more about how MaaS360 can protect your ActiveSync infrastructure and advance your mobile device management capabilities.
http://trials.maas360.com/forms/register_service_m.php?id=121&A=EASMDM_whitepaper