

Is Microsoft ActiveSync Enough to Manage Mobile Devices?

McAfee® Enterprise Mobility Management provides mobile device lifecycle management



Key Advantages

Microsoft Exchange ActiveSync manages only a small set of device security policies. McAfee EMM manages the whole lifecycle including:

- Self-service provisioning
- All policies and configurations
- Selective and full device wipe
- Strong authentication
- Compliance enforcement
- Mobile application enablement

Routinely, corporate IT is faced with having to do more with less, including enabling more of the business with limited budgets and fewer resources. McAfee Enterprise Mobility Management (McAfee EMM®) provides significant return on investment by leveraging Microsoft ActiveSync for email and personal information management (PIM) sync, while complementing ActiveSync by providing lifecycle management for the enterprise's mobile devices.

ActiveSync is a highly scalable protocol developed by Microsoft to sync devices with Microsoft Exchange email and PIM. Microsoft has licensed this protocol to device manufacturers and to many email server vendors. For example, IBM Lotus Notes uses ActiveSync to push email and PIM to Apple mobile devices like the Apple iPhone. ActiveSync also provides limited policy management capabilities as part of the protocol, and Microsoft Exchange leverages ActiveSync for basic policy management. However, Exchange's native capability is insufficient for supporting the lifecycle of enterprise mobile deployments.

Lifecycle Management, Device Wipe, Strong Authentication, and Compliance Enforcement

There are key differentiators when comparing the two solutions for managing a mobile workforce; the McAfee EMM solution provides full lifecycle management of the device, including self-service provisioning, policy and configuration management, device wipe, strong authentication, compliance enforcement, reporting, and mobile application enablement. Microsoft Exchange covers only a limited subset of the device lifecycle and focuses on some policy management and elements of compliance. For example, the McAfee EMM self-service provisioning fully configures the device for email, along with WiFi and VPN. Microsoft Exchange, using ActiveSync, can exercise partial control over the device only after Exchange has been configured. It is worth noting that initial device configuration is complicated, but with McAfee EMM device configuration is made easy.

Another difference between McAfee EMM and Microsoft Exchange ActiveSync is the usefulness of the solutions in terms of wiping corporate data. Microsoft Exchange ActiveSync is able to only do full device wipe, while McAfee EMM can selectively wipe parts of the device (for example Exchange synced email, contacts, and calendars) in addition to the whole device (user data, configurations, and credentials). This is key when an organization allows employee-owned devices on the network, where IT might want to wipe the corporate email/data only and leave personal information or photos in place.

Further, McAfee EMM puts a client certificate on the mobile device so the device strongly authenticates itself to the network for email access. This is important as most large enterprises require strong or two-factor authentication to gain access to the corporate data and many are bending their policies to permit push email with only username and password. Unlike a VPN, McAfee EMM provides push email with strong authentication with no impact on performance, latency, or battery life, and without the need for or the complexity of a VPN.

Enterprise Mobile Device Risk

Mobile OS vendors recognize the need for device security and management beyond the scope of Microsoft Exchange ActiveSync. Apple iOS4 and Google Android 2.2 include mature mobile device management frameworks that need McAfee EMM for security management. Both Apple and Google demonstrate that enterprise mobile device security management requires a full mobility management solution for scale, security, compliance, and reporting.

Finally, enterprises need to ensure that only devices that satisfy their security properties are able to connect to their network. Microsoft Exchange’s ability to enforce compliance and gather mobile device data is limited. McAfee EMM ensures that only authenticated, managed, and secured devices can connect to the network. For example, McAfee EMM can block compromised (jailbroken) mobile devices and collects a variety of device and meta data as well as real-time information about the device and provides reports on this information. A useful McAfee EMM report tracks the compliance status of devices and can report on noncompliant devices. This report can be used to help IT guide users to remediate their devices back to compliance.

Organizationally, many enterprises do not want to use Microsoft Exchange to manage their mobile devices. The enterprise does not use Exchange to manage their laptops, and they do not want to risk the availability of email by managing these powerful mobile devices. Viewed as small computers, mobile devices like the iPhone and iPad should be properly managed by the endpoint group and not as appendages to the messaging group.

Secure, Easy, and Scalable Enterprise Mobility

McAfee EMM delivers security by providing the most comprehensive and robust compliance management automatically while offering the same level of control, visibility, and protection of mobile devices enjoyed by laptops. With McAfee ePolicy Orchestrator® integration, enterprises have unified policy management and compliance reporting across all endpoints, from data center servers to smartphones and other mobile devices.

For more information visit www.mcafee.com/mobilesecurity/emm.



Figure 1. Lifecycle management of McAfee EMM.

