

McAfee Enterprise Mobility Management

Answers to your most frequently asked questions

Device Management	2
Which devices do you currently support?	2
Why shouldn't I use Microsoft Exchange, Apple iPCU, or other device management solutions?	2
What control do I have over the firmware and applications on the device?	2
Can I detect a device that has been "jailbroken?" If yes, what can I do about it?	2
Data Encryption and Wipe Operations	2
Do you support data encryption on phones and other devices, including encryption of an SD card?	2
When and how can I implement wipe operations? Are there any limitations?	2
What happens if the SIM is removed before a device is wiped?	3
Getting Started	3
What is the setup process for the administrator?	3
How do you provision users and applications?	3
What happens when a user wants to activate a different device?	3
Can I control who can provision devices?	3
Applications and Personal Content	3
Can I blacklist certain applications?	3
How can I provide access to in-house developed applications?	3
What if the device already has personal content and applications installed?	3
Does McAfee EMM have access to personal email or other personal information on the device?	3
Compliance	4
What assistance do you offer to help us ensure and maintain device compliance?	4
What happens when a noncompliant device tries to connect?	4
Are there any compliance-specific reports?	4
Secure connection, authentication, and communication	4
How does your product secure communications from the IT network to the mobile device?	4
How does a user authenticate and connect?	4
What sort of strong authentication can I require?	4
Do you support use of WiFi?	4
What are your plans for integration with McAfee ePolicy Orchestrator® (McAfee ePO™)?	4
Where can I learn more about McAfee EMM?	4

Device Management

Q: Which devices do you currently support?

A: McAfee® Enterprise Mobility Management (McAfee EMM®) offers extensive support for Apple iPhone/iTouch/iPad and Microsoft Windows Mobile devices, and basic support for platforms with less capable security and management functions, including Google Android, Symbian, and HP webOS smartphones and tablets. “Basic support” means we can require use of a password or PIN to unlock, and perform a remote wipe (restore factory settings). We support specific devices within each platform release and are expanding our support as the platforms mature, so please ask your sales representative for the most up-to-date list of tested devices.

Q: Why shouldn't I use Microsoft Exchange, Apple iPCU, or other device management solutions?

A: Enterprise-class support requires control across the entire lifecycle of the device, not just password/PIN unlock and remote wipe. We provide features that allow you to scale to the service levels and devices your users require and enforce the policies your business demands:

- Self-service device activation, including a user agreement process
- Group-based policy configuration (tied to Microsoft Active Directory or Lotus Domino LDAP)
- Automatic and personalized configuration of enterprise services, including VPN, email, and WiFi
- Strong authentication
- Encryption management
- Over-the-air push updates of security policies and configurations

Exchange and other device-specific management tools offer subsets of these functions for specific applications and devices. We offer a comparable minimum feature set—pin unlock and remote wipe—for all supported platforms, plus more capability where feasible.

Q: What control do I have over the firmware and applications on the device?

A: You can block devices that are noncompliant with your policies, including those without approved versions of the firmware, and exert some control over the resources and

applications on the device, such as turning off the camera or Bluetooth. On Apple devices you can ban certain native applications such as YouTube, Safari, and iTunes. Once the device is active, you can block installation of any additional applications, leaving existing applications and personal data in place.

Q: Can I detect a device that has been “jail-broken?” If yes, what can I do about it?

A: Yes. Jailbroken phones can be blocked. You can monitor iPhones that are out of compliance and set additional policies, such as “block jailbroken phones,” “block if policies are out of sync,” or “block phones prior to version 3GS.”

Data Encryption and Wipe Operations

Q: Do you support data encryption on phones and other devices, including encryption of an SD card?

A: We encourage use of encryption and, to assure high performance and data integrity, we work with native hardware-based encryption rather than providing this function ourselves. For Windows Mobile, McAfee EMM encrypts the entire phone, including the SD card, and you can turn encryption on and off. For Apple, every device released after the 3GS is natively encrypted with hardware-based encryption (includes iPads and latest iPod Touches). We can detect and block devices that are not using encryption. We expect to extend our encryption support to other platforms as the capability ships within each device. Note, if encryption is important, IT must dictate the devices that can be used.

Q: When and how can I implement wipe operations? Are there any limitations?

A: EMM supports two kinds of wipe: full wipe and selective wipe.

- Full wipe takes the device back to factory settings for firmware and applications. It is ideal when the user loses a device. It works even if encryption is active.
- Selective wipe allows IT to manage enterprise data (email, contacts, and calendars) on the phone, but leaves intact the user's personal information and content (such as an iTunes library and photos). You cannot uninstall applications.

Q: What happens if the SIM is removed before a device is wiped?

A: Even if the SIM is removed, the device is protected with the PIN. If the password is entered too many times, the device can be set to auto-wipe. However, if you do not use encryption, then the SD card itself might be read before the wipe is performed, allowing a thief access to sensitive information on the SD card.

- Updates to security policies and configurations are pushed in real time to the device over-the-air, including selective and remote wipe if the device is lost or stolen

Getting Started

Q: What is the setup process for the administrator?

A: Our installer configures all prerequisite software for you, typically in less than half an hour, then EMM helps you configure, enforce, and manage native device security settings for the devices we support.

- Set up the roles-based console to use Active Directory (AD) or Domino LDAP credentials and leverage directory security groups
- Create a group in the directory, populate that group, and associate that group with the “role” of system administrator. You can define policies for each user based on the type of device used and the security appropriate to each user’s role.
- Create policies, assign policies to groups, and associate groups with policies
- Finally, define the types of connections and services users/groups can access, including VPN, WiFi, messaging, and line of business applications

Q: How do you provision users and applications?

A: Once you are satisfied with the policies, users can provision their own devices over-the-air from a self-service interface.

- End-users can check to see if their service accounts exist and if one does not, request the creation of a new account. If the account is disabled, a user will not be able to provision a device to the environment.
- For iPhones, users go to the AppStore, download the EMM agent, enter email credentials (Exchange or Domino user name and password), and agree to the corporate policy. IT services are provisioned automatically. The EMM solution pushes them using an encrypted profile.

Q: What happens when a user wants to activate a different device?

A: Just provision the new one, and they can keep both. Or, if only the new device is to be used, IT can use the management console to explicitly retire or wipe the old device using an administrative password.

Q: Can I control who can provision devices?

A: You can pre-populate (whitelist) selected users that are allowed to provision, or you can allow all users.

Applications and Personal Content

Q: Can I blacklist certain applications?

A: On Apple devices you can ban (blacklist) certain native applications such as YouTube, Safari, and iTunes explicitly.

Q: How can I provide access to in-house developed applications?

A: To distribute your own application, you have two options: place it on the Apple iTunes store, or physically tether the device and download the application directly to each device, then configure it with the platform utility, such as the iPhone Configuration Utility (iPCU).

Q: What if the device already has personal content and applications installed?

A: Once the device is active, you can “secure the image” to block installation of any additional applications, leaving existing applications in place.

Q: Does McAfee EMM have access to personal email or other personal information on the device?

A: Although we can delete personal data with a selective or total remote wipe, we do not backup or restore that data. We cannot download personal information from the device to the enterprise server.

Compliance

Q: What assistance do you offer to help us ensure and maintain device compliance?

A: You can manage policies and devices and get reports through any Silverlight-enabled web browser. Our console allows you to monitor who is trying to connect.

- You can use automatic policy enforcement to ensure that only authorized devices from authorized users can connect to enterprise applications and services
- You can require that devices are registered, secured, and up to date with respect to policies, configurations, and operating system versions before allowing a connection
- When you update a policy (usually per user or group), the policy is applied to the device when the device checks in
- Windows Mobile users can limit exposure using a policy that declares “if a device has not logged on for 15 days, it should automatically wipe”

Q: What happens when a noncompliant device tries to connect?

A: You can monitor which devices are attempting to access the enterprise, mark any noncompliant (or unapproved) devices, and use these details to work with the user to get, use, or maintain an appropriate device.

Q: Are there any compliance-specific reports?

A: Some audit reports are provided to get you started, including device status, noncompliant device list, and an audit log that notes changes in the console, pending actions, and device health. You can see device details, such as user, email, phone number, security policy applied, and device state.

Secure connection, authentication, and communication

Q: How does your product secure communications from the IT network to the mobile device?

A: Each device is issued a unique digital certificate to strongly authenticate it to the enterprise network. All communications are performed using the Secure Sockets Layer (SSL) protocol.

Q: How does a user authenticate and connect?

A: We offer several options for user authentication:

- Standards-based certificates
- VPN on demand
- SSL VPN

Q: What sort of strong authentication can I require?

A: We rely on certificates on each device for access and for use with encryption. In addition, to sync email, you can require strong authentication—username and password plus the device certificate.

Q: Do you support use of WiFi?

A: Yes. WiFi is one of the resources you can control on a device using policies. EMM can provision the WiFi settings so that the SSID and the passphrases do not need to be given to the users.

Q: What are your plans for integration with McAfee ePolicy Orchestrator (McAfee ePO)?

A: We are integrating the web-based EMM console within McAfee ePO. Initially, compliance management and reporting allows you to audit and report policy violations, application inventory, compliance tracking, and lost devices. You can report device hardware, operating system, compromised phone status, and policy and configuration status.

Q: Where can I learn more about McAfee EMM?

A: You can learn more about McAfee EMM on our website (www.mcafee.com) or by calling us on 1.888.847.8766.

