

McAfee Enterprise Mobility Management

Frequently Asked Questions

Device Management

Q: Which devices do you currently support?

A: McAfee® Enterprise Mobility Management (McAfee EMM™) offers extensive support for Apple iOS, Google Android, and Microsoft Windows Phone, and basic support for BlackBerry 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, so please ask your sales representative for the latest list of tested devices.

Q: Why shouldn't I use Microsoft Exchange, Apple iPhone Configuration Utility (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, and is most efficient when device management integrates into other endpoint and security management processes. Our features allow you to scale support to the service levels and devices your users require and enforce the policies your business and regulators demand:

- 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 Wi-Fi
- Enterprise app store for recommended or required applications
- Strong authentication
- Encryption management
- Over-the-air push updates of security policies and configurations
- Compliance enforcement, visibility, and reporting
- Support across device platforms, directories, and email platforms
- Bulk provisioning to simplify and expedite McAfee EMM deployments while reducing support requirements

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 capabilities where feasible.

Q: I already use Microsoft Exchange to manage my devices. Why should I switch to McAfee EMM?

A: Microsoft Exchange, using ActiveSync, can exercise partial control over the device only after Exchange has been configured. Initial device configuration with Exchange is complicated, compared to the easy, automated process with McAfee EMM. Further, Exchange can provide only full wipe, not selective wipe. 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 vital 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. In addition, McAfee EMM uses a client certificate on the device to support strong or two-factor authentication, enabling push email without the performance overhead or complexity of a VPN. Finally, security administrators can use the same environment to report on compliance of laptops and mobile devices, without a dependency on email servers and email administrators.

Q: What is the role of Microsoft ActiveSync?

A: ActiveSync is a highly scalable protocol that provides limited policy management capabilities. McAfee EMM leverages Microsoft ActiveSync for email and personal information management (PIM) sync, while complementing ActiveSync by providing scalable, efficient lifecycle management for mobile devices. McAfee EMM manages the whole lifecycle including:

- Self-service provisioning
- All policies and configurations
- Selective and full device wipe
- Strong authentication
- Compliance enforcement, visibility, and reporting
- Mobile application enablement beyond email and PIM
- Support across device platforms, directories, and email platforms

Q: What's the difference between McAfee EMM and the Apple iPhone Configuration Utility (iPCU)?

A: The iPhone supports a Microsoft ActiveSync client that actively enforces protocol policies. However, ActiveSync policies currently govern only a subset of the Apple iPhone, Apple iPad, and Apple iPod Touch features. This includes enforcement of 12 policies for defining how device passwords are used.

Apple provides the iPCU to help administrators create and personalize configuration profiles (for example, email, VPN, and Wi-Fi settings) for individual user devices. However, the use of this tool makes it difficult to configure devices en masse since the burden of creating and storing a unique profile for each user lies with the administrator.

McAfee EMM combines Apple configuration profiles and ActiveSync policy management into a single device management solution that uses group-based policy management: a device is associated with a user who is associated with a group. This approach allows for one-to-many policy management that simplifies large-scale deployment of Apple devices while also configuring each device to meet the unique needs of each user.

The McAfee EMM solution provides a comprehensive profile service, automating the creation and secure distribution of configuration profiles without sacrificing the ability to personalize iPhones. This capability includes the dynamic creation of configuration profiles; group-based distribution and customization of configurations; and compliance enforcement to ensure the persistence of configurations once they are set on the device. Configuration profile policies can include:

- Administrative profile lock
- Maximum number of failure attempts before local wipe
- Require passcode
- Allow explicit content
- Require alphanumeric passcode
- Allow browser use
- Minimum passcode length
- Allow YouTube use
- Minimum number of complex characters
- Allow Apple iTunes music store
- Maximum passcode age (1 to 730 days, none)
- Allow installing apps
- Auto-lock (1 to 60 minutes, none)
- Allow use of camera
- Passcode history (1 to 50 passcodes, none)
- Allow screen capture

Q: Does McAfee EMM restrict users from forwarding an email on their mobile device out of a different account than the one it was received from, thereby bypassing corporate security?

A: For iOS 5 devices McAfee EMM does not allow users to forward corporate email out of a personal email account.

Q: What control do I have over the firmware and applications on the device when using McAfee EMM?

A: You can block devices that are noncompliant with your policies, including those without approved versions of the firmware, and you can exert some control over the resources and applications on the device, such as turning off the camera or Bluetooth. Application blacklisting is available on iOS and Android devices. On Apple devices, you can ban certain native applications such as YouTube, Safari, and iTunes, and for iOS 5 devices, you have the ability to block iTunes password caching and backing up corporate data to a user's personal Apple iCloud account.

McAfee EMM supports controlling for iOS:

- FaceTime with camera
- Screen capture
- In app purchases
- Automatic sync while roaming
- Multiplayer gaming
- Voice dialing
- Installing non-enterprise apps
- Browser auto fill, fraud warning, JavaScript, pop-ups, and cookies

Q: Can I detect an Apple device that has been "jailbroken?" If so, what can I do about it?

A: Yes. McAfee EMM performs a compliance check on all iOS devices before they enter the corporate network to ensure the presence of ActiveSync policies and configuration profiles installed on the device by IT. Jailbroken devices ("hard reset" devices where IT configurations have been removed) can be blocked. Policy compliance enforcement by the McAfee EMM platform considers all the device information known about the device, including hardware version (for example, ensuring that devices like the iPhone 3GS with native encryption are used and earlier unencrypted devices are blocked), software version, configuration profiles, and ActiveSync policies, as well as the authorization of users and of their iPhones. For iOS 5 devices, an immediate alert is sent to the administrator when a user removes the McAfee EMM Agent. You can monitor Apple iOS devices that are out of compliance and set additional policies, such as:

- Block jailbroken phones
- Block if policies are out of sync
- Block phones that are not encrypted

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 the use of encryption and, to assure high performance and data integrity, we work with native hardware-based encryption rather than providing this function in software. We can detect and block devices that are not using encryption. For Apple, every device beginning with 3GS is natively encrypted with hardware-based encryption (includes iPads and latest iPod Touches). For Android 3.0 and later, we take advantage of encryption capabilities provided within each device.

Note: If encryption is important, IT must dictate the specific devices that can be used.

Q: When and how can I wipe a device? Are there any limitations?

A: McAfee EMM supports two kinds of wipe: full 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. Selective wipe is not yet available for Android devices.

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, the SD card itself might be read before the wipe is performed, allowing a thief access to sensitive information on the SD card.

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 McAfee EMM helps you configure, enforce, and manage native device security settings for the devices we support. Here are the steps:

- Pre-install helper checks the environment to ensure all necessary software and firewall ports are open. The helper also creates the MDM certificate request for Apple.
- Set up the roles-based console to use Active Directory (AD) or Lotus Domino LDAP credentials and leverage directory security groups
- PKI users set up enrollment agents and certificate authorities
- 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.
- Using the bulk provisioning notification, the administrator can send a bulk email or SMS to a group of users with provisioning instructions. This simplifies and expedites the deployment of McAfee EMM while reducing the support requirements for an initial deployment.
- 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, Wi-Fi, messaging, and line of business applications

Q: Is there anything special I need to do to make McAfee EMM work with Apple MDM?

A: For Apple mobile devices, McAfee EMM installs an MDM profile at provisioning, keeping the device connected to the McAfee EMM server at all times.

Q: How do you provision users and applications?

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

- 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.
- Using the bulk provisioning notification, the administrator can send a bulk email or SMS to a group of users with provisioning instructions. This simplifies and expedites the deployment of McAfee EMM while reducing the support requirements for an initial deployment.
- We support several app store options where users can download McAfee EMM and approved or required applications:
 - » *McAfee Enterprise App Store*—The McAfee EMM Enterprise App store appears in the “Recommended App” tab of the McAfee EMM Agent. McAfee EMM can create a list of recommended apps based on attributes such as a user or group that can then be sent to individuals or groups. Administrators can provide a customized database of web clips and applications sourced from public app stores such as the Apple App Store or the Android Market. Administrators gain visibility into device application inventory, audit, and policy management, and users do not have to visit a public app store to locate a recommended app.
 - » *iTunes App Store*—Download the McAfee EMM agent, enter email credentials (Exchange, Domino, or Gmail user name and password), and agree to the corporate policy. IT services are provisioned automatically. The McAfee EMM solution pushes them using an encrypted profile.
 - » *Android Market*—Download the McAfee EMM agent, enter email credentials (Exchange, Domino, or Gmail user name and password), and agree to the corporate policy. IT services are provisioned automatically.
- 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

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. For iOS and Android devices a one-time password can be used for an added layer of security and to enforce the use of a single device per user.

Q: Can I control who can provision devices?

A: You can pre-populate (whitelist) selected users that are allowed to provision, and therefore connect to the corporate network, or you can allow all users.

Applications and Personal Content

Q: Can I blacklist or whitelist applications?

A: For iOS and Android devices, application blacklisting is available. The administrator has the ability to limit apps on phones that contain corporate data. This includes games, apps with adult content, or inappropriate file sharing. Application whitelisting is done through the enterprise app store.

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

A: To distribute your own application, you can:

- Place it in McAfee EMM's enterprise app store where it appears as a tab on the McAfee EMM device agent
- Upload it to the Apple App Store or Android Market
- 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: 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 back up or restore that data. We cannot download personal information from the device to the enterprise server.

Q: What capabilities can be personalized?

A: McAfee EMM can personalize the configuration of the device to enable user access to IT services. Automated activation includes these services:

- Configuration profile resource management
- Wi-Fi (SSID, hidden network, security type, password)
- VPN (configuration name, connection type, server, user account, authentication type, shared secret, proxy setup)
- Exchange (account name, host, use secure sockets layer, domain, email address, password, authentication credentials)

Apple profile configurations can also be imported to configure other services for the iPhone, including lightweight directory access protocol (LDAP), CalDAV, subscribed calendars and non-Exchange email, and credentials (PKCS1, PKCS12). Also, certain applications can be recommended by device type or role.

Q: Users are concerned that adding McAfee EMM to their smartphones will destroy their productivity and be a hassle. How do I reassure them?

A: McAfee EMM secures the user's device without being intrusive: it is transparent to the user. Users are required to enter a PIN or password to access the devices, but McAfee EMM uses the native email, contacts, and calendar applications on all supported devices to provide the best user experience. Users can answer calls without entering a PIN, and the McAfee EMM software does not affect device battery life or application performance.

Compliance

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

A: The McAfee EMM console provides centralized reporting, policy management, and role-based access control for administrative and help desk personnel. You can manage policies and devices and get reports through any Silverlight-enabled web browser, as well as access dashboards and reports through McAfee® ePolicy Orchestrator® (McAfee ePO™) software. This allows you to:

- Monitor who is trying to connect
- Use automatic policy enforcement to ensure that only authorized devices from authorized users can connect to enterprise applications and services
- Require that devices are registered, secured, and up to date with respect to policies, configurations, and operating system versions before allowing a connection
- Refuse a connection to jailbroken (hard reset) or compromised devices
- Ensure that when you update a policy (usually per user or group), the policy is applied to the device when the device checks in
- Monitor compliance status within a McAfee ePO dashboard and report details such as policy violations, application inventory, compliance tracking, and lost devices
- For iOS 5 the McAfee EMM server will auto alert the administrator if the McAfee EMM Agent is removed, eliminating the time a mobile device could be unmanaged without the administrator's knowledge

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. You can also block noncompliant devices from entering the network.

Q: Are there any compliance-related dashboards or reports?

A: McAfee ePO software integration allows centralized dashboards to aggregate mobile device status with other McAfee-secured endpoint status. Administrators can see compliance status and drill directly down to see why devices are not compliant. Report details can roll up with other McAfee ePO software results to create unified, custom reports across devices, endpoints, and network systems. We provide some audit reports 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 also see device details, such as user, email, phone number, device state, device ID, make and model, operating system, assigned security policies, and Active Directory or LDAP membership. A complete system audit log tracks all activity by all users of the McAfee EMM solution and all reports can be exported to Microsoft Excel.

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. McAfee EMM servers use encrypted secure sockets layer (SSL/HTTPS) connections to ensure that all data transmitted between mobile devices and servers is encrypted. iPhones that do not have native encryption (prior to the iPhone 3GS) can be blocked from accessing your network. For Android devices we offer an extra layer of authentication with the use of a one-time password. The administrator can choose to require this password for first-time provisioning.

Q: Do you support use of Wi-Fi?

A: Yes. Wi-Fi is one of the resources you can control on a device using policies. McAfee EMM can provision the Wi-Fi settings so that the SSID and the passphrases do not need to be given to the users. Additionally with iOS 5 devices the administrator has the ability to set an "auto join" option on EMM delivered Wi-Fi configurations.

McAfee ePolicy Orchestrator Integration

Q: How much integration exists with McAfee ePO software?

A: McAfee EMM software can be installed as an extension of McAfee ePO software. You can view reports and create a McAfee EMM dashboard from within McAfee ePO software. McAfee EMM launches directly from McAfee ePO software with a single sign-on, displaying data within the McAfee ePO dashboard using charts, tables, and other graphics. Integration of McAfee EMM Agent data within McAfee ePO dashboards unifies visibility across McAfee-secured endpoints and mobile devices. Enterprises gain efficiencies in operations and reporting and make mobile device management part of the day-to-day operational workflow within a familiar management environment.

Within McAfee ePO software, you can view device compliance status and drill down seamlessly to see details on noncompliant devices, and also integrate mobile device information in other McAfee ePO reports. Initially, compliance management and reporting allows you to audit and report policy violations, device and application inventory, compliance tracking, and lost devices. You can report device hardware, operating system, compromised phone status, and policy and configuration status.

Q: What are your future McAfee ePO software integration plans?

A: Integration plans include more extensive policy and management functions.

Q: What are some key features of the platform?

A: See table below for key McAfee EMM platform features.

Areas of Functionality	Features	iPhone	Android	WinPho7	BlackBerry
Enterprise activation and end-user personalization	Email configuration	•	•		
	VPN, Wi-Fi settings	•	•		
	Certificate distribution with McAfee EMM CA	•			
Unified policy management	Policies decoupled from email servers	•	•	•	
	OTA policy and profile distribution	•	•	•	
	Group-based policy management	•	•	•	
Compliance management	Policy compliance	•	•	•	
	Profile compliance	•	•	•	
	Hardware-based device compliance	•	• (v2.2 and higher)	•	
	OS level-based device compliance	•			
Centralized administration	Comprehensive visibility	•	•		•
	Help desk	•	•	•	•
	Self-service portal for end users	•	•	•	
	App recommendation and distribution	•	•		
Infrastructure	Exchange, Lotus, and Gmail support	•	•	•	• (Does not support Gmail)
	Email proxy	•	•	•	

Q: Where can I learn more about McAfee EMM?

A: You can learn more about McAfee EMM on our website (<http://www.mcafee.com/us/products/enterprise-mobility-management.aspx>) or by calling 1.888.847.8766.



2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee, the McAfee logo, McAfee EMM, ePolicy Orchestrator, and McAfee ePO are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2012 McAfee, Inc.
42407faq_emm_0212_fnI_ASD