McAfee® Enterprise Mobility Management (McAfee EMM™) 12.0

Frequently Asked Questions

Q. What types of mobile devices does McAfee® Enterprise Mobility Management (McAfee EMM™) support?

A. McAfee EMM supports:

- Apple iOS devices, such as the Apple iPhone and Apple iPad.
- Google Android smartphones and tablets made by a host of vendors, including Samsung, HTC, and others.
- Microsoft Windows smartphone devices.

Q. What are the primary features?

A. McAfee EMM can be used to:

Secure devices and data to insulate corporate networks from risk:

- Centrally manage anti-malware (McAfee VirusScan® Mobile Security) on Android devices, including enforcing the use of McAfee VirusScan Mobile Security and blocking devices that carry malware.
- Secure Android devices with app reputation through McAfee Global Threat Intelligence (McAfee GTI).
- Provide a secure workplace by segregating corporate email, contacts, and calendars and applying cut, paste, reply, and forwarding restrictions.
- Distribute apps and blacklist apps.
- Block jailbroken or rooted devices.
- Enforce authentication (including optional one-time tokens), authorization, and encryption
- Restrict device access by device type or operating system (OS) version.
- Enforce password restrictions, including strength and number of password attempts before devices are locked.
- Remotely lock or wipe lost or stolen devices (selectively wipe corporate data and full wipe).
- Enforce restrictions, such as blocking app store downloads (iOS), camera, Apple iCloud backup, and more.
- Deliver VPN and/or Wi-Fi profiles, including optional use of certificates (PKI).
- Monitor and report on the mobile enterprise, including mobile policy compliance, threat events, app reputation, reasons for noncompliance, and a host of other metrics.

Manage and secure all endpoints with a single pane of glass:

- Smartphones and tablet policies and security are managed, along with PC, laptop, server, virtual, Mac, and Linux endpoints, with McAfee® ePolicy Orchestrator™ (McAfee ePO™) software.
- Include mobile threat events into broader endpoint event reporting and alerting for comprehensive security analysis and automated remediation

Q. What is included in the McAfee EMM license?

A. McAfee EMM is similar to a suite in that it includes licenses of McAfee EMM, McAfee Secure Container for Android, McAfee VirusScan Mobile Security for Android, and McAfee ePO software for management. McAfee Secure Container is available on the Google Play store but requires the purchase and use of McAfee EMM to work.

Q. Is McAfee EMM included in any suites?

A. Yes. McAfee Complete Endpoint Protection—Business (CEB) and McAfee Complete Endpoint Protection—Enterprise (CEE) customers receive license entitlement rights to deploy mobile anti-malware and device management. A McAfee VirusScan Mobile (VSM) node and a McAfee EMM node are provided at no extra charge. Customers are entitled to use McAfee EMM on one mobile device for every CEB/CEE license.

Q. What is McAfee Secure Container for Android?

A. McAfee Secure Container (SC) for Android is part of the McAfee EMM product. It can be downloaded separately from Google Play but needs McAfee EMM to work. McAfee Secure Container provides an encrypted container for corporate email, contacts, and calendar. It also enables secure document viewing inside the container. Policy can be established for passwords and restrictions, such as blocking cut and paste and save outside the container. It also assists the help desk by providing a single email client across Android devices.

McAfee Secure Container offers these additional capabilities:

- Inline editing.
- Out-of-office settings.
- Pinch and zoom.
- GAL lookup.
- Dial phone numbers from emails and calendar events, including conference call IDs.
- One-touch dialing for Meeting Place and Adobe conference calls.
- Caller ID.
- Separate notifications for new email and calendar events.

McAfee Secure Container helps keep personal and business data separate to support "bring your own device" (BYOD). In the event a device is lost or stolen or when an employee leaves the company, just the business data can be remotely wiped, keeping the personal data intact. The device can also be remotely fully wiped or locked (not a McAfee Secure Container feature per se).

Q. What is McAfee VirusScan Mobile Security for Android?

A. Since Google's Android OS is open source and very popular, it is experiencing more malware than other platforms. McAfee VirusScan Mobile Security for Android protects against malware by leveraging mobile specific signatures and backed by McAfee Global Threat Intelligence.

Q. What's new in McAfee EMM 12.0?

A. **Managed McAfee VirusScan Mobile Security**

- Administrators can enforce the use of McAfee VirusScan Mobile Security (VMS) for Android. McAfee VirusScan Mobile Security comes with McAfee EMM but has historically been a stand-alone, unmanaged product. With McAfee EMM 12.0, customers can centrally configure settings like turning on real-time scanning, and configuring the scan and .DAT update intervals. They can optionally enforce the use of virtual machines (VMs) to sync corporate email and block devices with malware, out-of-date scans, or out-of-date .DATs.

App reputation

- McAfee EMM 12 supports automated reputation queries to the McAfee mobile cloud for Android apps. If enabled, and users download apps, McAfee EMM can get a trust score (malicious, suspicious, clean, or unrated). Administrators can establish policies to block devices with malicious and/or suspicious apps or simply generate threat events in McAfee ePO software for devices that contain apps that McAfee deems malicious and/or suspicious. A local whitelist is provided to override the McAfee score, as well as a local blacklist to provide control to administrators. Blacklisting is available as a standard policy for Android or iOS.

iOS7 MDM enhancements

- *Managed open-in*—This allows administrators to specify the apps that a user can use to open attachments. This way, only "managed" apps can be used to open corporate attachments. Apps are managed by being distributed via McAfee EMM to Apple devices. Normally, these are public apps that the company approves or a corporate app.
- *Single sign-on*—Apple introduced this concept for iOS7. Users can enter their passwords once for several managed apps or URLs. A common use case is various corporate Intranet sites that each require a login.
- *Device lock message*—IT can put a message on devices when they are locked. For example, "This device belongs to XYZ company. Please contact ABC if found."
- *Touch-ID restriction*—iOS7 introduced the concept of using a fingerprint to unlock an iPhone. IT can choose to disable the option so that a traditional passcode is required to unlock a device, making it easier for IT to troubleshoot problems.

PKI

- Certificate management and distribution for iOS VPN and Wi-Fi profiles for two-factor authentication and easier access to corporate resources by employees.

Threat events

- Enhances situational awareness and security posture assessment. Events such as jailbroken/rooted devices, blacklisted app detected, malicious or suspicious app detected, and malware detected are now McAfee ePO software threat events. They can be rolled into broader threat event logs and reports with other endpoints which opens up more reporting and automation.

Compliance notifications

- A host of new compliance capabilities are included in McAfee EMM 12.0, such as those associated with managed McAfee VirusScan Mobile, app reputation, and blacklisting. Users receive alerts and remediation information on compliance events. Administrators can see reasons for noncompliance when viewing a user's device in the McAfee ePO software system tree.

Q. Is McAfee ePO software included with McAfee EMM?

A. Yes.

Q. Which versions of McAfee ePO software work with McAfee EMM?

A. McAfee ePO software 4.6.7 through McAfee ePO software 5.1.

General

Q. Can I block devices that contain malware?

A. Yes, administrators can optionally enforce a policy to restrict devices from synching corporate data until file identified by McAfee VirusScan Mobile Security as malware is removed.

Q. Will I receive alerts for mobile threat events?

A. McAfee ePO software automation allows you to configure automated email-based alerts for threat events. These can be applied to mobile events as well, including malware detected, suspicious or malicious app detected, device jail broken/rooted, and blacklisted app detected.

Q. How are users notified when they are out of compliance?

A Users receive automated push messaging notices or pop-up notices explaining why they are out of compliance (for example, they have a blacklisted or malicious app on their device), and they are given remediation steps via prompts or messaging automatically. Once the compliance event is cleared, the user is able to sync mail again. The user notifications are designed to allow the user to regain compliance without calling the IT help desk. If, however, the user does contact IT, administrators can view the reason the device is not compliant in the device details within the McAfee ePO console.

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

A. For iOS 5 and higher devices, McAfee EMM provides controls to enable administrators to block the forwarding of corporate email out to a personal email account. For Android devices that use the McAfee Secure Container, administrators can place cut and paste restrictions on content within the container.

Q. Can I distribute and manage apps?

A. For iOS and Android devices, McAfee EMM can push apps (IPA/APK file for corporate apps, link to app store for public apps, or Webclip) to users based on their Microsoft Active Directory group. On iOS, users simply tap to accept the install of an app. On Android, apps appear in the recommended apps area of the McAfee EMM app/agent on the device. McAfee EMM can be used to distribute app updates as well. When an employee leaves the company or the device is no longer managed, iOS and Android apps that have been pushed to devices can be removed remotely, along with their associated data.

McAfee has also partnered with Apperian (www.apperian.com) for Mobile Application Management (MAM). Apperian offers a complete end-to-end mobile app lifecycle management service and an enterprise app store. Apperian's solution includes app wrapping, app policies, usage monitoring, analytics, and more. Through our partnership, Apperian's EASE platform is integrated into McAfee ePO software, allowing joint customers to launch Apperian from McAfee ePO software via single sign-on and also do reporting and analytics in McAfee ePO software.

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

A. 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. 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 device but leaves intact the user's personal information and content (such as an iTunes library and photos). You cannot uninstall applications. Selective wipe is supported for Android devices using McAfee Secure Container (included with McAfee EMM).

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.

Q. Can I blacklist or whitelist applications?

A. For iOS and Android devices, application blacklisting is available. Application whitelisting is handled both as an override for McAfee app reputation for Android and via McAfee EMM package management, which is used to push apps to devices.

Q. What support is there for VPN and Wi-Fi profiles?

A.

- iOS VPN profiles include the optional use of certificates and support L2TP, PPTP, IPSec (Cisco), Cisco AnyConnect, F5 SSL, Juniper SSL and custom SSL connection types, and proxy configuration.
- iOS Wi-Fi profiles include optional use of certificates and support WEP, WPA/WPA2, any (personal) WEP Enterprise, WPA/WPA2 Enterprise, and any (enterprise) security types and password.
- Wi-Fi profiles on Android devices support SSID, hidden network, WEP, WPA/WPA2 security types, and password.

Server Components and Network Architecture

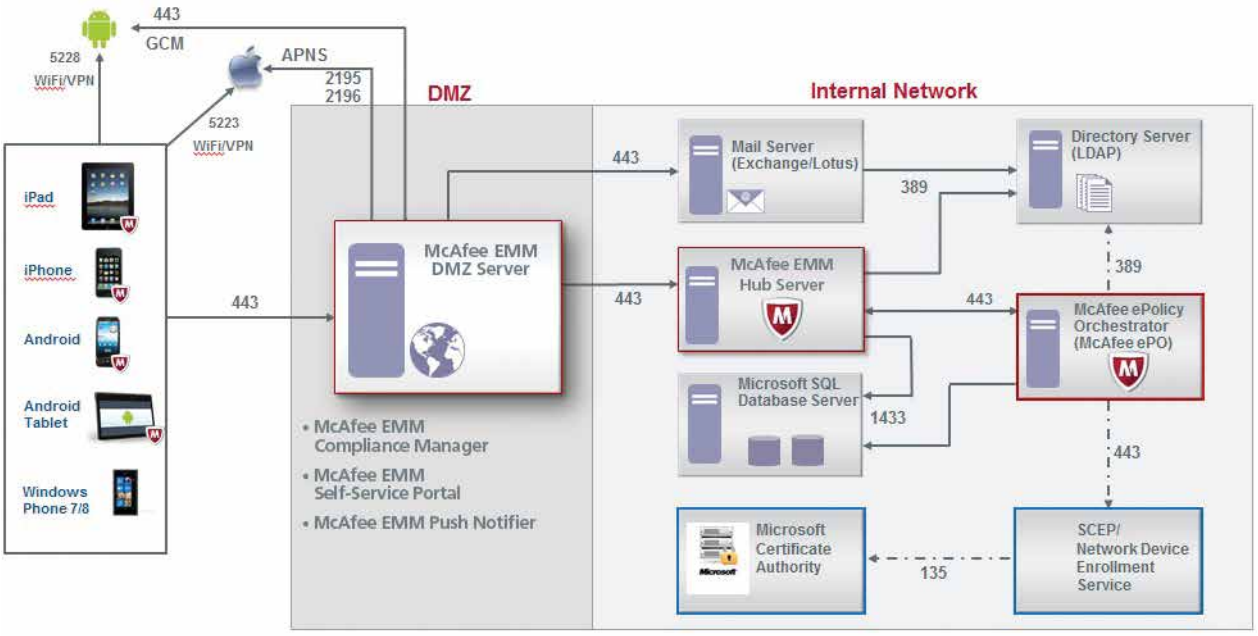
Q. What are McAfee EMM's components and what does each do?

A.

- *McAfee ePolicy Orchestrator (McAfee ePO) software*—Management infrastructure used to establish and enforce policies, generate reports and dashboards, take administrative action (wipe), manage mobile inventory and check compliance status.
- *McAfee Enterprise ActiveSync (EAS) Proxy and Compliance Filter*—This IIS application resides in the DMZ and proxies ActiveSync traffic to the email servers. It enables McAfee EMM to control access to enterprise resources on the DMZ server before reaching the internal network.
- *McAfee EMM hub*—Manages communications between McAfee EMM components and allows secure communications between McAfee EMM modules across the firewall (between the DMZ and the internal network).
- *McAfee EMM push notifier*—Allows push notifications to be sent to devices. It is usually installed in the DMZ so it can communicate with Apple and Android push notification services

Q. Is there a network diagram that shows where these components fit?

A. See the diagram below.



Q. What ports need to be open?

A. See the chart on the next page.

Configuration	Allow traffic on this port	From	To
Enhanced security configuration (dual servers)	443	Internet	McAfee EMM DMZ server
	443	McAfee EMM DMZ	Email servers providing ActiveSync server or Notes Traveler
	443	McAfee EMM DMZ server	McAfee EMM internal server
	389	McAfee EMM DMZ server	LDAP server
	88	McAfee EMM DMZ server	LDAP server
	1433 (or dynamic SQL port)	McAfee EMM DMZ server	SQL server where the McAfee EMM database is installed
	25	McAfee EMM DMZ server	SMTP server
Basic security configuration (single server)	443	Internet	McAfee EMM server
	443	McAfee EMM server	Email servers providing ActiveSync or Notes Traveler
	389	McAfee EMM server	LDAP server
	88	McAfee EMM internal server	LDAP server
	1433 (or dynamic SQL port)	McAfee EMM server	SQL server where the McAfee EMM database is installed
	25	McAfee EMM internal server	SMTP server
iOS devices	2195	McAfee EMM server (DMZ in enhanced security mode)	Apple Push Notification service at gateway.push.apple.com
	2196	McAfee EMM server (DMZ in enhanced security mode)	Apple Push Notification service at gateway.push.apple.com
	5223	Devices connected to Wi-Fi	Internet
Android devices	443	McAfee EMM server (DMZ in enhanced security mode)	Google Cloud Messaging service at android.googleapis.com
	5228	Devices connected to Wi-Fi	Internet
	443 (to enable app protection)	Devices	McAfee McAfee Global Threat Intelligence server at https://appcloud.mcafee.com/aa

Note: For outbound connections to Apple and Google push services, do not set IP-specific firewall restrictions because the IP addresses are subject to change.

McAfee
An Intel Company

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

61011faq_emm_0314_wh