Enterprise Mobility Management Migration

Migrating from Legacy EMM to an ePO Managed EMM Environment

Paul Luetje

Enterprise Solutions Architect

Table of Contents

Welcome 3

Purpose of this document 3

Legacy EMM compared to ePO Managed EMM 3

Management Differences 3

EMM Enhancements 4

Legacy EMM (10.x) Architecture 5

ePO Managed EMM (12.x) Architecture 6

Client Side Changes 7

Migration to ePO managed EMM 8

Parallel EMM Infrastructure 8

Portal SSL Certificate 9

Apple MDM Certificate 9

DNS Server Changes 9

Client-side experience 9

Welcome

Purpose of this document

McAfee's release of a McAfee ePolicy Orchestrator (ePO) managed version of Enterprise Mobility Management (EMM) brings the goal of ubiquitous end point management another step closer. Taking the leap into ePO involves significant transparent client side changes as well as some slight architectural or infrastructure changes. The goal of this document is to outline and explain moving from a legacy stand-alone EMM environment to an ePO managed EMM environment.

Many enhancements and improvements have been made to EMM as a result of ePO becoming the management platform along with changes that have been made regarding device profiles. However, there is no direct upgrade from EMM 10.2 or earlier to EMM 12.x (ePO Managed version of EMM). This document describes the changes and offers best practices for migrating from a legacy stand-alone EMM environement to an ePO managed EMM environment.

Legacy EMM compared to ePO Managed EMM

The largest change when moving from Legacy EMM to an ePO Managed EMM is the administrative interface. Aside from requiring a McAfee ePO Server and less EMM server components, the overall basic architecture is identical to that of a Legacy EMM implementation.

The EMM DMZ server running the EMM Portal, Proxy, and Push Notifier components is still required. The internal EMM server now runs only the EMM Hub component and the McAfee ePO Console replaces the older EMM Console.

Management Differences

The following table outlines where management logistics have changed between the Legacy EMM Console and the McAfee ePO Console.

EMM Console	McAfee ePO Console
Query	Actions->Agent->Wake Up Agents
Wipe	Actions->Mobile->Wipe
Delete Email & PIM Data	Actions->Mobile->Wipe Corporate Data
Uninstall	Actions->Mobile->MDM Uninstall
Lock	Actions->Mobile->Lock
Reset Password	Actions->Mobile->Unlock
Compliance Override	ePO Policy setting
Change Ownership	ePO Tags
Delete	Action->Directory Management->Delete
Unlock Users	Menu->User Management->Locked Users
Reports	ePO Queries and Reports
Policy Settings	ePO Policy Catalog

EMM Enhancements

Several improvements and enhancements have been made to EMM since moving to ePO as the management platform. For example, policies and administrative permissions are more granular, and policy changes no longer require end user interaction as profiles are now asynchronous (see Client Side Changes below).

Key features of McAfee EMM 12.0 include:

Android Security Enhancements

- ✓ Managed McAfee VirusScan Mobile Security (VMS).
  - Optionally enforce the use of VMS in order to sync corporate data and block devices with malware, or out of date scans or DATs.
  - Malware events are reported as Threat Events in ePO.
- ✓ Android app reputation, using the McAfee Mobile Cloud and Global Threat Intelligence (GTI), provides an extra layer of protection against malicious and suspicious Android apps. EMM 12 gives the enterprise total control with report only capabilities, and local white and black lists.

iOS Enhancements

- ✓ IT can specify which apps can be used to open attachments to corporate email on iOS devices, providing security and separation of personal and work data on the device
- ✓ Certificate management and distribution (PKI), for iOS VPN and WiFi profiles makes connecting to corporate networks more secure and easy.
- ✓ Single sign-on to corporate managed apps or URLs simplifies the end user experience when connecting to corporate assets by allowing them to type in their credentials just one time in order to access multiple apps or URLs.

New mobile Threat Events for improved situational awareness and remediation

- ✓ Mobile events such as a jailbroken or rooted device, malware detection, malicious, suspicious, or blacklisted app detected are now ePO Threat Events so they can be rolled into broader Threat Event Logs, dashboards, and reports along with other endpoint events and take advantage of ePO automation.

Improved user experience

- ✓ End users receive more specific alerts and remediation information on compliance events. Administrators can now see the reason for non-compliance when viewing a user's device details in the ePO system tree.

Continuing Benefits from the May 2013 EMM 11.0 release include:

- ✓ Policy management , configuration, and security of mobile devices, laptops, and desktop PCs in the same console (ePO)
- ✓ Granular policy options including per user, device, and operating system
- ✓ Flexible, role-based administration including mobile specific permissions
- ✓ Drag-and-drop dashboards for mobile or all managed systems (standard and custom) for inventory management, situational awareness, compliance reporting, and IT audits
- ✓ Over-the-air enrollment and policy delivery
- ✓ Enforcement of authentication and encryption.

- ✓ Partial or full wiping of lost or stolen devices to prevent corporate data loss.
- ✓ Remote device locking for lost devices
- ✓ Hosting and distribution of commercial and enterprise apps, including support for Apple's Volume Purchase Program.

Legacy EMM (10.x) Architecture

The architecture outlined in Figure 1 is a typical high level Enhanced Security Model deployment of EMM 10.x. The design of this architecture scales horizontally to accommodate redundancy, scaling, or both by placing either the EMM DMZ or EMM Hub servers behind one or more network load balancers.

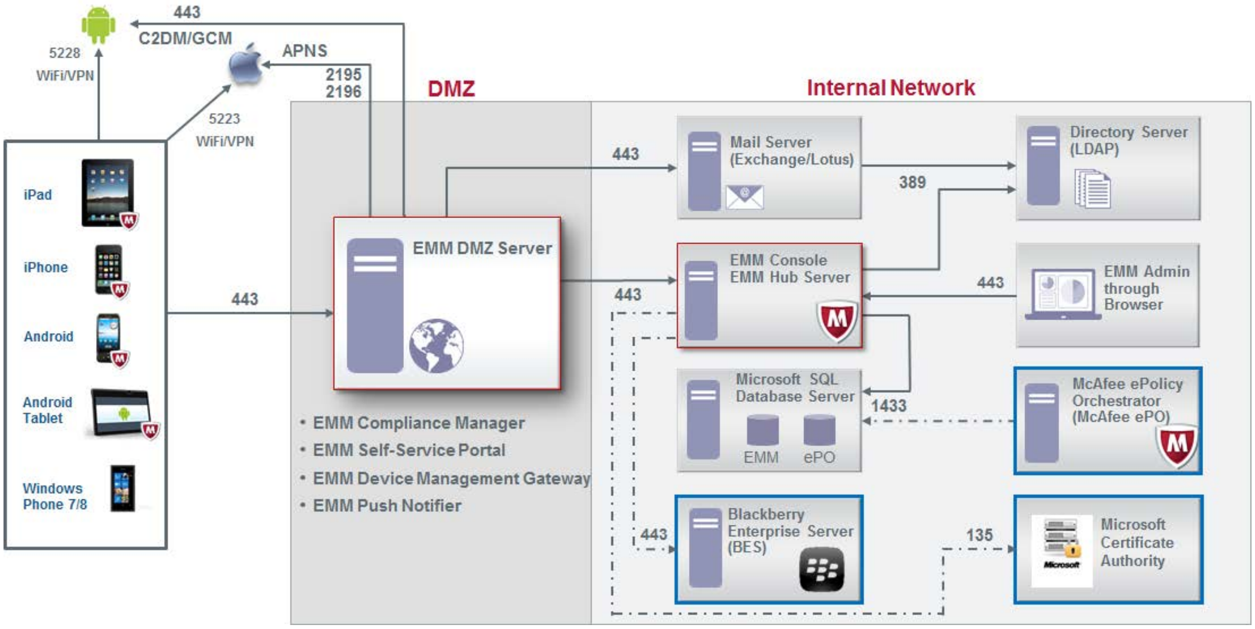

Figure 1 McAfee Enterprise Mobility Management Legacy Architecture (Enhanced Security Model)

ePO Managed EMM (12.x) Architecture

Deploying an ePO managed EMM environment, such as EMM 12.x, is not that different from a legacy EMM environment when it comes to the number of servers and where they sit in the network. Comparing Figure 2 to Figure 1, you will notice there is still an EMM DMZ and Hub Server deployed in the Enhanced Security Model. The biggest difference between each deployment is that now EMM does require a McAfee ePO server, which replaces the EMM Console.

Policies are now created, stored, and assigned from within the ePO Console and communicated to the McAfee EMM Hub server for delivery to the devices. Reporting data is now stored inside the ePO database. In order to accomplish all of this, there is trusted bi-directional communication between the McAfee ePO and EMM Hub server.

EMM 12.x also introduces a PKI extension installed into McAfee ePO. Connecting EMM to an internal PKI infrastructure is now done through a registered Simple Certificate Enrollment Protocol (SCEP) server in ePO which requires a Microsoft NDES server to connect to.

Communication to and from smartphones or tablets remains the same leveraging established messaging services such as Apple Push Notification Service (APNS) and Google Cloud Messaging (GCM). Google deprecated their Cloud-to-Device Messaging (C2DM) service in 2012. EMM no longer supports C2DM and therefore requires a GCM Sender ID and Token in order to connect to Google.

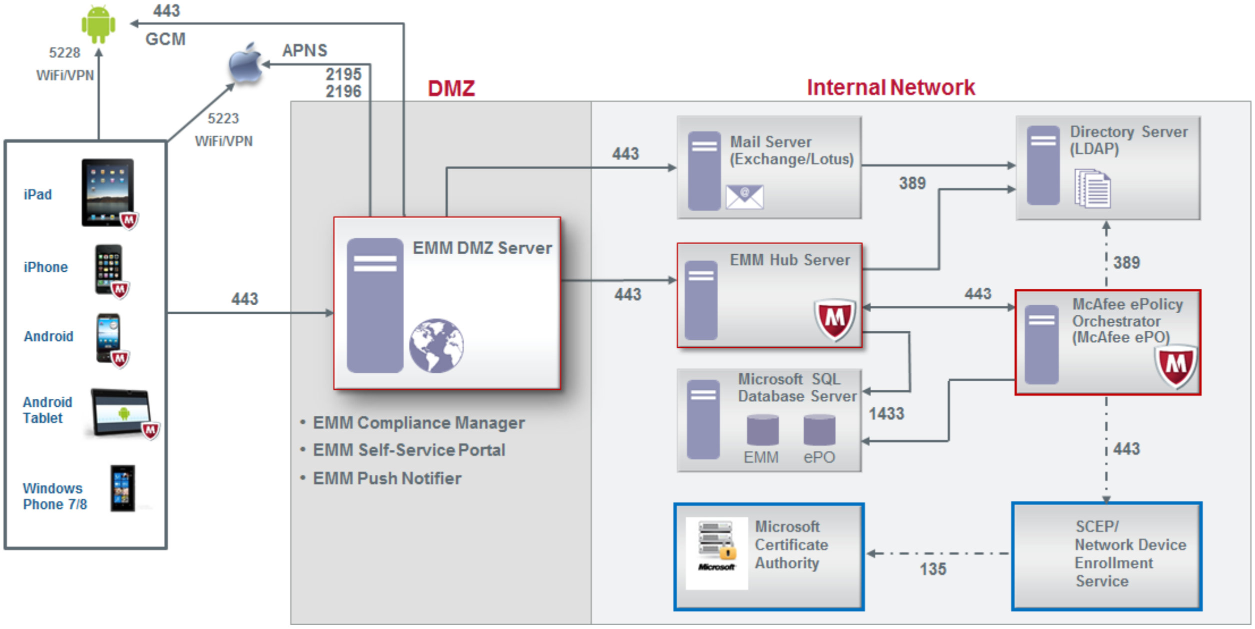

Figure 2 McAfee Enterprise Mobility Management ePO Managed Architecture (Enhanced Security Model)

Client Side Changes

McAfee EMM still requires the McAfee EMM App from the Google Play Store or Apple App Store to enroll a device. There are some notable differences in the client side experience when moving from Legacy EMM to an ePO Managed EMM. For the most part these changes are transparent to the user, but are still important to understand.

McAfee has addressed some client-side challenges such as policy changes removing email from a device as well as forcing a device re-enrollment every time the Portal SSL certificate was renewed/replaced.

Changes are most noticeable on Apple iOS devices. Previously, iOS devices had a Mobile Device Management profile along with one single Enterprise Activation Profile which contained several configuration profiles (See Figure 3).

The ePO Managed EMM enrollment process now generates a profile signing certificate unique to every iOS device at the time of enrollment. The Mobile Device Management profile still exists, but now EMM delivers asynchronous managed config profiles for individual settings such as Passcode, Restrictions, Email, and more (See Figure 4). These managed config profiles are signed using the profile signing certificate.

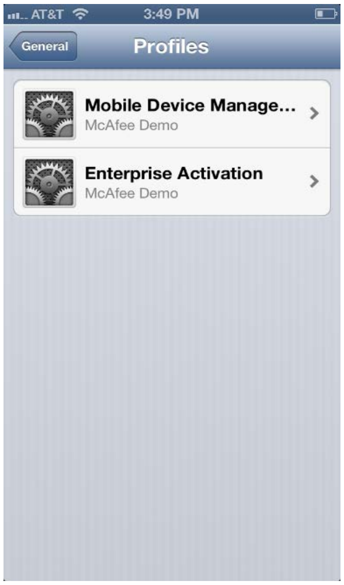

Figure 3 Legacy EMM iOS Profiles

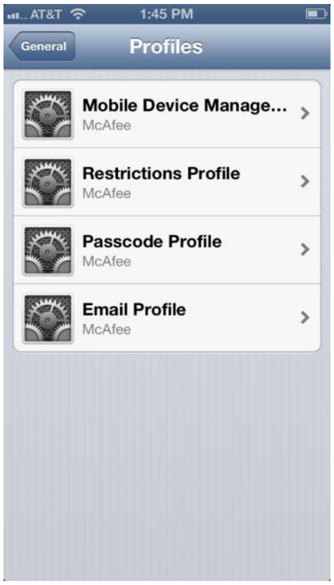

Figure 4 ePO Managed EMM iOS Profiles

By signing and delivering these individual managed config profiles, it is now possible to make a change to one security settings, such as making the Passcode stronger, and it will not adversely affect the Email profile. As a result of these changes, it is now possible to update and renew the Portal SSL certificate without requiring the re-enrollment of every iOS device.

Additionally, McAfee has improved the messaging around non-compliance to Android and iOS devices. Better communication to the user of the device will reduce Helpdesk calls and allow the users to resolve their non-compliance issues.

In order to take advantage of these new enhancements, it will be necessary for devices currently enrolled in a Legacy EMM environment to re-enroll their device into the new ePO managed EMM environment. The steps will be outlined later in this document.

Migration to ePO managed EMM

Due to the significant changes outlined in this document for both server and client components, McAfee recommends migrating from a Legacy EMM environment to a McAfee ePO Managed EMM environment by deploying a parallel EMM environment running the latest McAfee EMM product offering.

Once deployed, devices that are enrolled into the new McAfee EMM environment will re-send device information which will now be stored into ePO. Security and compliance settings defined in a McAfee EMM ePO policy will be enforced and delivered to the device.

Moving to the new McAfee ePO managed EMM environment will require a bit of planning before bringing it online and enrolling devices. Here are some recommended steps to follow:

- Obtain new SSL certificate (if necessary) to reflect new external connection
- Build out a parallel EMM environment
- Modify 'My Default' EMM policies for each mobile OS platform in McAfee ePO to match default policy settings from the Legacy EMM environment
- Test a few devices to ensure everything is working
    - Requires entering new EMM Server URL into the McAfee EMM App during enrollment
- Once testing is completed, modify SRV record in DNS to reflect new URL
- Instruct users to re-enroll devices

Parallel EMM Infrastructure

Building out a parallel McAfee ePO managed EMM environment is fairly straight forward. External communications to push messaging services are the same, so firewall rules will still apply. Common servers such as ActiveSync\Traveler, Active Directory\Notes Directory, and SQL can be used by both environments at the same time (See Figure 5).

Communication from devices will need to be directed to a new external URL (i.e.; emm2.company.com) in order to enroll into the new EMM environment. During any pilot or testing phase this may require manually entering this URL into the EMM Server field of the McAfee EMM App until the SRV record(s) are changed in DNS.

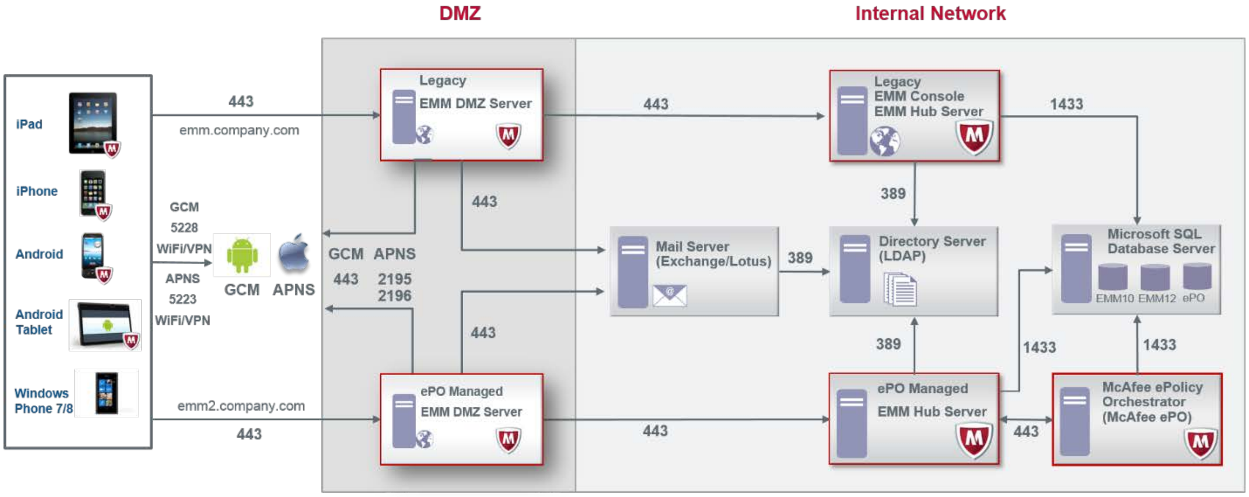

Figure 5 McAfee Enterprise Mobility Management Parallel Architecture

Devices that are still enrolled into the Legacy EMM environment will continue to receive email and report into the previous EMM servers until the user performs a device re-enrollment.

Portal SSL Certificate

If your organization is currently leveraging a wild card SSL certificate securing the external EMM connection, it may not be necessary to obtain a new SSL certificate. You can reuse the wild card certificate in the parallel EMM environment assuming you a copy of the certificate in PFX format complete with the full chain and private key. Reference the PFX file during the installation of the new EMM DMZ server components.

If you are not using a wild card certificate, every SSL certificate is unique to the common name specified at the time of generating the Certificate Signing Request (CSR). This field typically is the URL for which devices are going to resolve. For this reason, it will be necessary to obtain a new SSL certificate for the secondary URL (i.e., emm2.company.com).

Apple MDM Certificate

The current Apple MDM certificate can be reused in the new McAfee ePO Managed EMM environment. There is no need to regenerate a new certificate request. Make sure you have the Apple MDM certificate in PFX format ready at the time of installation.

DNS Server Changes

The McAfee EMM App running on iOS and Android devices leverages a DNS Service Record (SRV) associated with the email domain of the user that enrolled the device. This is done to automatically direct the connection of the device towards the EMM DMZ Server for device enrollment. Every time a user signs into the McAfee EMM App it will look up this record and reference that URL specified in the SRV record. By changing this, it will allow any new device enrollments to begin being directed to the new EMM environment.

Client-side experience

Device enrollment into the new McAfee ePO Managed EMM environment will require existing devices to re-enroll. The steps for these users are simple and easy to follow.

iOS Users:

1. Remove the MDM Profile
    a. Click on Settings->General->Profiles->Mobile Device Management
    b. Click Remove
2. Click Home Button
3. Launch McAfee EMM App and sign-in
4. Click ‘Update Configuration’
5. Follow the prompts to enroll the device

Android Users:

1. Launch McAfee EMM App and sign-in
2. Click ‘Update Configuration’
3. Follow the prompts to enroll the device

Windows Phone Users:

1. Modify the ‘Server’ setting of the Exchange ActiveSync account to now reflect the new EMM Proxy URL (i.e.;mdm2.company.com)

2. Alternatively, the user can delete the account on the device and create a new Exchange ActiveSync account referencing the new EMM Proxy URL in the ‘Server’ field.