

Ensuring Persistent Policy Compliance

Protect noncompliant devices with McAfee Enterprise Mobility Management

Today, there is an explosion of mobile devices accessing the corporate network, many of them employee-owned and configured. Despite this device diversity, IT must guarantee that corporate security and data usage policies are enforced. McAfee® Enterprise Mobility Management (McAfee EMM®) performs an automatic, real-time compliance check before allowing devices to access the corporate network, ensuring that required policies and configuration profiles are present and persistent at each connection. Integration with McAfee ePolicy Orchestrator® (McAfee ePO™) allows compliance status and policy violations to be monitored and remediated efficiently, aggregating detailed device data into the larger landscape of enterprise reporting.



Key Advantages

- Automatic compliance check detects noncompliant devices and denies network access to jailbroken, compromised, or manually configured devices
- Supports strong authentication through integration with the Microsoft Certificate Authority, authenticating both the device and user before access to email and corporate resources; supports one-time password tokens for two-factor authentication
- Presents mobile device status and details within the unified McAfee ePO platform for convenient monitoring and streamlined audit and compliance reporting
- Full and selective* remote wipe help protect sensitive data if a device is lost or stolen

*Not yet available for Android devices.

Unlike PCs and laptops, mobile device owners have the ability to hard reset and manually configure their devices and still access the corporate network. Security controls from McAfee EMM can protect the enterprise by detecting noncompliant and jailbroken devices and preventing them from accessing corporate resources and data.

McAfee EMM assures that your mobile workforce is compliant with regulatory requirements and fully secures and protects your critical data. A lost mobile device managed by McAfee EMM will not jeopardize your business or your industry reputation.

Provisioning mobile devices

McAfee EMM provides secure and easy user self-service provisioning, installing protection without altering the native device capabilities or the user's experience. The system interacts with Microsoft Active Directory (AD) or Domino LDAP to validate users and ensure that only authorized users are able to provision their devices. The McAfee EMM Enterprise App Store offers a secure, efficient way to recommend applications based on devices or user role. The applications can be custom, links to third-party app stores, or web clips.

Configuring mobile devices

McAfee EMM configures and manages the device over the air using Microsoft ActiveSync and device-specific configuration policies. ActiveSync policies govern a subset of features—such as email synchronization—while McAfee EMM harnesses the device's mobile device management (MDM) capabilities to do more thorough and granular configuration and policy setting, such as VPN, WiFi, and strong authentication.

McAfee EMM combines these two management approaches—ActiveSync and device-specific—into a single device management solution that uses group-based policy management. A device is associated with a user who is then associated with a group.

Connecting mobile devices to the corporate network

McAfee EMM bootstraps a mobile device that is not known to and does not know of the enterprise data center into a fully managed endpoint that mobilizes applications and services from the data center.

Compliance Enforcement for Jailbroken Devices

McAfee EMM policy compliance enforcement is also able to detect jailbroken devices. Jailbreaking is a process that allows a user to run any code on their device, as opposed to only code that is authorized by Apple, for example. McAfee EMM denies access to devices compromised in this way.

Step 1: Upon activating the mobile device with their service provider, users are instructed by IT to download McAfee EMM from the Apple App Store, Android Marketplace, or other app store. Once downloaded, McAfee EMM locates the corporate EMM server based on the users' credentials and validates them against the enterprise directory, such as Microsoft AD.

Step 2: McAfee EMM then uses the Microsoft Certificate Authority to distribute a digital certificate to the mobile device. This certificate validates the device and user for single sign-on to corporate resources. It also provides strong authentication to prevent rogue devices from accessing the network and ensures policy compliance.

Step 3: Configuration profiles are dynamically generated by the McAfee EMM server based on the users' credentials and group-based membership (Microsoft AD or Domino LDAP). For example, the configuration profile sets up the users' email accounts on Microsoft Exchange.

Step 4: Upon setup, the device initiates a connection to Exchange that is intercepted by the McAfee EMM Exchange ActiveSync proxy. McAfee EMM uses device-specific MDM features and ActiveSync to configure user policies. For example, users are prompted to set up their passcodes to protect mobile devices if they are lost.

Step 5: Users are now connected to the corporate network and compliant with corporate policies. McAfee EMM ensures that all MDM and ActiveSync policies and configuration profiles are persistent and enforced.

Enterprise-wide visibility and compliance reporting

Integration with McAfee ePO provides centralized reporting, policy management, and role-based access control for administrative and help desk personnel. McAfee EMM monitors compliance status within a McAfee ePO dashboard and reports details such as policy violations, application inventory, compliance tracking, and lost devices. Roll up McAfee EMM data with data from a BlackBerry BES server and other McAfee ePO results to create unified, custom reports across devices. By automating processes and unifying data streams across mobile, endpoint, network, audit, and compliance solutions, your team can manage compliance most efficiently.

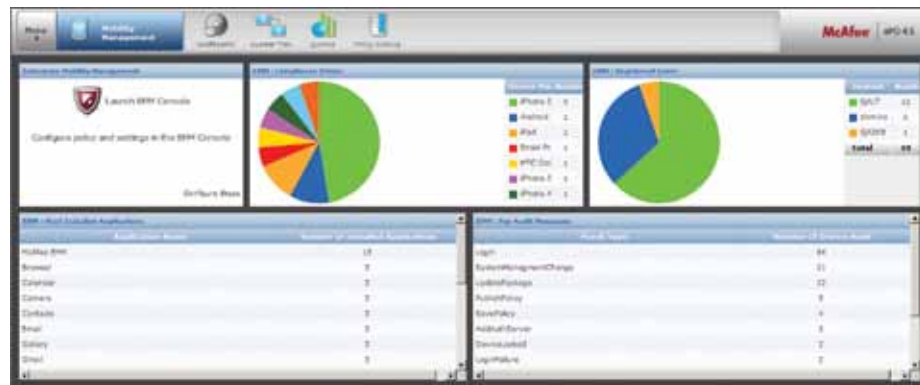


Figure 1. McAfee ePO integration allows mobile device compliance monitoring within the context of day-to-day operations.

Policy compliance enforcement

Once a mobile device is configured with McAfee EMM, a compliance check is performed before the mobile device is able to enter the corporate network; this ensures that policies and configuration profiles remain persistent.

McAfee EMM scans the mobile device to ensure the specified configuration profile is present and the device isn't compromised. The McAfee EMM policy compliance process provides an added layer of compliance enforcement, specifically, if a device is hard-reset and then manually configured, McAfee EMM will detect this state. The mobile device will be ruled noncompliant and prevented from accessing corporate systems and syncing with email. Compliance decisions can be made based on device hardware, device compromise status, user authenticity, strong certificate-based authentication, and policy and configuration status.

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

