

Contrasting the McAfee Enterprise Mobility Management Solution with the Apple iPhone Configuration Utility

McAfee simplifies corporate deployment without sacrificing personalization



A commonly asked question is: “what’s the difference between the McAfee® Enterprise Mobility Management (McAfee EMM®) solution and the Apple iPhone Configuration Utility?” The iPhone supports a Microsoft ActiveSync client that actively enforces protocol policies. However, ActiveSync policies currently only govern a subset of the iPhone and Apple iPod Touch. This includes enforcement of 12 policies for defining how device passwords are used and controlling the use of the device camera. In addition, the ActiveSync protocol supports remote wipe of the device.

Apple differentiates the iPhone from other smartphones by providing a better way for IT to configure devices via the iPhone Configuration Utility (iPCU). Configuration profiles are XML files that quickly load device configuration and authorization information. Apple provides the iPCU to help administrators create and personalize configuration profiles (for example, email, VPN, and WiFi 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.

In contrast, the McAfee Enterprise Mobility Management (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 set on the device.

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

Ensuring Configuration Persistence

Without a method to ensure compliance enforcement, iPhone users can easily remove IT configurations on their iPhone, including password-protected configuration profiles, by simply hard resetting their device. The McAfee EMM solution includes bonded policy compliance (BPC), a patent-pending feature that ensures the persistence of iPhone configurations after they are installed on the device.

BPC installs a token on the iPhone that is placed in the ActiveSync stream between the iPhone and the data center. This approach leverages the iPhone email application, a privileged application running in the background, to report user compliance with IT policy.

McAfee EMM performs a compliance check on all iPhones before they enter the corporate network to ensure that ActiveSync policies and configuration profiles installed on the device by IT are present. The presence of the BPC token is an indicator that the appropriate configuration policy is in place. If a user

Technical Brief Contrasting the McAfee Enterprise Mobility Management Solution with the Apple iPhone Configuration Utility

hard resets the device, the token will not be present in the ActiveSync stream and the device will be deemed noncompliant and prevented from accessing corporate email. Policy compliance enforcement by the EMM platforms considers all the device information known about the iPhone, 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.

Use Case: IT Activation of Personal iPhones

Increasingly, enterprises are adopting policies that permit employees to use their personal iPhones for business. IT wants to automate the activation process that allows employees to connect their personal devices to the corporate network so as not to burden the IT helpdesk. Automation typically includes the configuration of basic services such as email and access (WiFi or VPN). For the iPhone, these capabilities are configured via configuration profiles.

The McAfee EMM solution bootstraps an iPhone 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. The McAfee EMM solution follows the Apple iPhone enrollment process, including the use of simple certificate enrollment protocol (SCEP) to deploy digital certificates to the iPhone. This capability enables the secure deployment of iPhone configuration profiles used to configure IT services and applications, while McAfee compliance management ensures their persistence.

The McAfee EMM solution makes the iPhone enterprise ready by providing users with an automated and secure way to connect their iPhones to the corporate network while following corporate IT policies and without taxing IT resources.

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

