

Androids in the Enterprise

Using Google Android Devices with McAfee® Enterprise Mobility Management and McAfee VirusScan® Mobile



Androids are invading the enterprise, and IT leaders need a strategy for managing them. On top of the basic functions available already, McAfee is expanding its support for Android use, and keeping pace with the maturation of enterprise features in the underlying platform, such as remote management, encryption, and other crucial minimum requirements.

Every enterprise user is also a consumer: they bring their personal devices to work and want to bring their work to their personal devices. Last year, it was the iPad. This year, it is the Android. Next year, who knows? If your users are clamoring to use their Androids to access your enterprise applications, here's what you need to know about securing and managing these devices, and how McAfee® Enterprise Mobility Management (McAfee EMM™) and McAfee VirusScan Mobile can help.

Key Points

The McAfee Enterprise Mobility Management solution ensures the success of your enterprise deployment by focusing on lifecycle tasks:

- **Manage**—Track and manage the mobile device lifecycle
- **Provision**—Deploy and decommission smartphones and tablets
- **Secure**—Transparently secure smartphones and tablets, their corporate data, and the IT network they access
- **Support**—Minimize IT support costs and maximize user productivity
- **Audit**—Support enterprise IT and policy compliance reporting requirements

We leverage core platform and device capabilities to provide the security, management, scale, and control you need—and the transparent user experience users demand.

Start with the Basics

An open source oriented platform like the Android gives developers a lot of creativity, but all that independence makes control—the byword of security and compliance—a constant challenge. Google ships the device operating system (OS) to individual device manufacturers who loosely follow the Google blueprint as they build their individual devices, customized for their target markets. There can be several releases of a device OS in commercial production at the same time, with multiple device configurations using each release. We know, because we have been leading the effort to securely connect consumer devices to the enterprise. The McAfee EMM platform integrates smartphones, PDAs, and tablets into enterprise networks with the same level of security protection enjoyed by laptops and desktops. McAfee VirusScan Mobile protects Android devices by scanning and cleaning malware from files, memory cards, applications, Internet downloads, text messages, and attachments. Always-on protection identifies and removes viruses, Trojans, worms, and other malicious applications and content.

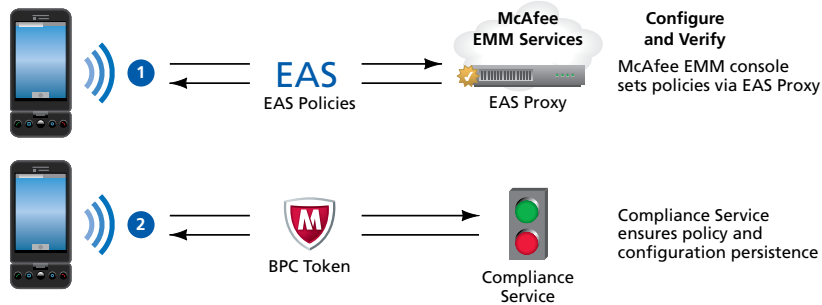
It usually takes several releases for device manufacturers and platform vendors to deliver products with the security and manageability required by enterprise IT and compliance leaders. For example, what happens to the customer contacts on a device if the salesperson loses it? Android 2.2 is the first Google release to offer a password screen, the bare minimum security control for data protection. Many enterprises worry that without encryption, the customer database in the example can still be compromised by a determined thief. What about Microsoft Exchange support? Many Android devices don't offer it. For most enterprise users, though, it's just a gadget until it supports Microsoft email. Regardless, McAfee VirusScan Mobile is designed to provide protection at all vulnerable points. Inbound email, outbound email, text messages, applications, and Internet downloads are protected with both on-access and on-demand scanning.

Today, the McAfee EMM* platform and McAfee VirusScan Mobile offer critical core security functions to Android users, including the requirement of a password or PIN to unlock, remote wipe, and always-on protection that identifies and removes viruses, Trojans, worms, and other malicious applications and content. Today, if you don't trust an Android device that is trying to connect to your network, you can lock it by disabling the password and then delete, or wipe, its sensitive data and restore to factory settings.

*McAfee EMM capabilities are based on each Android device's ability to understand and enforce policies, such as "turn on password screen" or "initiate remote wipe," therefore not all Android devices are supported.

Microsoft ActiveSync and Beyond

Prior to the Android 2.2 platform, the ActiveSync protocol allowed McAfee EMM to manage native policy enforcement capabilities. Policies are created using a web-based console and pushed to Android platforms. Policy pushes are acknowledged by the native client and persistently enforced via the McAfee EMM Compliance Service. As an operation performed natively on the device, rather than by an extra agent, policy enforcement is real time, low latency, and low power.



Key Benefits

McAfee VirusScan Mobile is designed to provide protection at all vulnerable points. Inbound email, outbound email, text messages, applications, and Internet downloads are protected with both on-access and on-demand scanning.

- *Easy to use*—Managing protection for your mobile device should be easy. Download, set up, and activate McAfee VirusScan Mobile directly to your mobile device. It works in the background to protect your smartphone or Android tablet from the many ways malware can attack.
- *Up-to-date protection*—Get the confidence of always active, always up-to-date security with 24/7 worldwide virus outbreak monitoring provided by McAfee Global Threat Intelligence™
- *With McAfee, you don't have to worry*—McAfee VirusScan Mobile automatically updates silently in the background—and our unmatched security expertise ensures that you always have the latest protection

When Google released Android 2.2, it enabled minimum policy management functions without the overhead of ActiveSync. McAfee is now leveraging this infrastructure to support a range of Android devices running Android 2.2 or later, while exploring ways to implement more robust minimum features.

Fulfilling Enterprise Expectations

The McAfee EMM platform blends mobile device management with policy-managed endpoint security, network access control, and compliance reporting features in a seamless system. To achieve this, we require certain core capabilities within the native device platform, such as strong authentication, hardware-based encryption, policy-based resource control, and reporting. Google is now enabling some of these capabilities natively, while others may be implemented by device manufacturers eager to differentiate their platforms. None of these features are available natively in Android V2.2.

McAfee VirusScan Mobile was designed for mobile devices to run with minimal memory resources, avoiding any service interruptions while protecting you against malware. With more than 10 years of experience in mobile security and more than 150 million handsets protected today, McAfee VirusScan Mobile is unmatched in ease of use, low power consumption, and rapid file scanning.

Learn More

The device landscape changes quickly. As one of the market's most successful device platforms, Android has our development team's full attention. Our Android support is gated only by the platform's ability to meet enterprise security expectations with embedded security functions. Stay tuned as Google Android capabilities—and McAfee EMM and McAfee VirusScan Mobile capabilities—expand to seize the market opportunity presented by avid consumers and mobile enterprises. Keep pace with us at www.mcafee.com.

