

McAfee Enterprise Mobility Management Securing Mobile Applications



An overview for MEEC



The User is Evolving



facebook

amazon.com

WebMD
Better information. Better health.



iTunes



You Tube

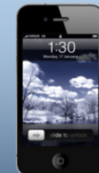
flickr

citi

Bank of America



The User is Evolving



IT's Challenge with Mobile Devices

Web 2.0, Apps 2.0, Mobility 2.0



Requirements for Secure Application Enablement



Required:

- Data Protection
- Compliance
- Authentication

- Security Policy Management
- Self-Service Provisioning
- Enterprise App Management

Empowering Enterprise Mobility



- **Secure**

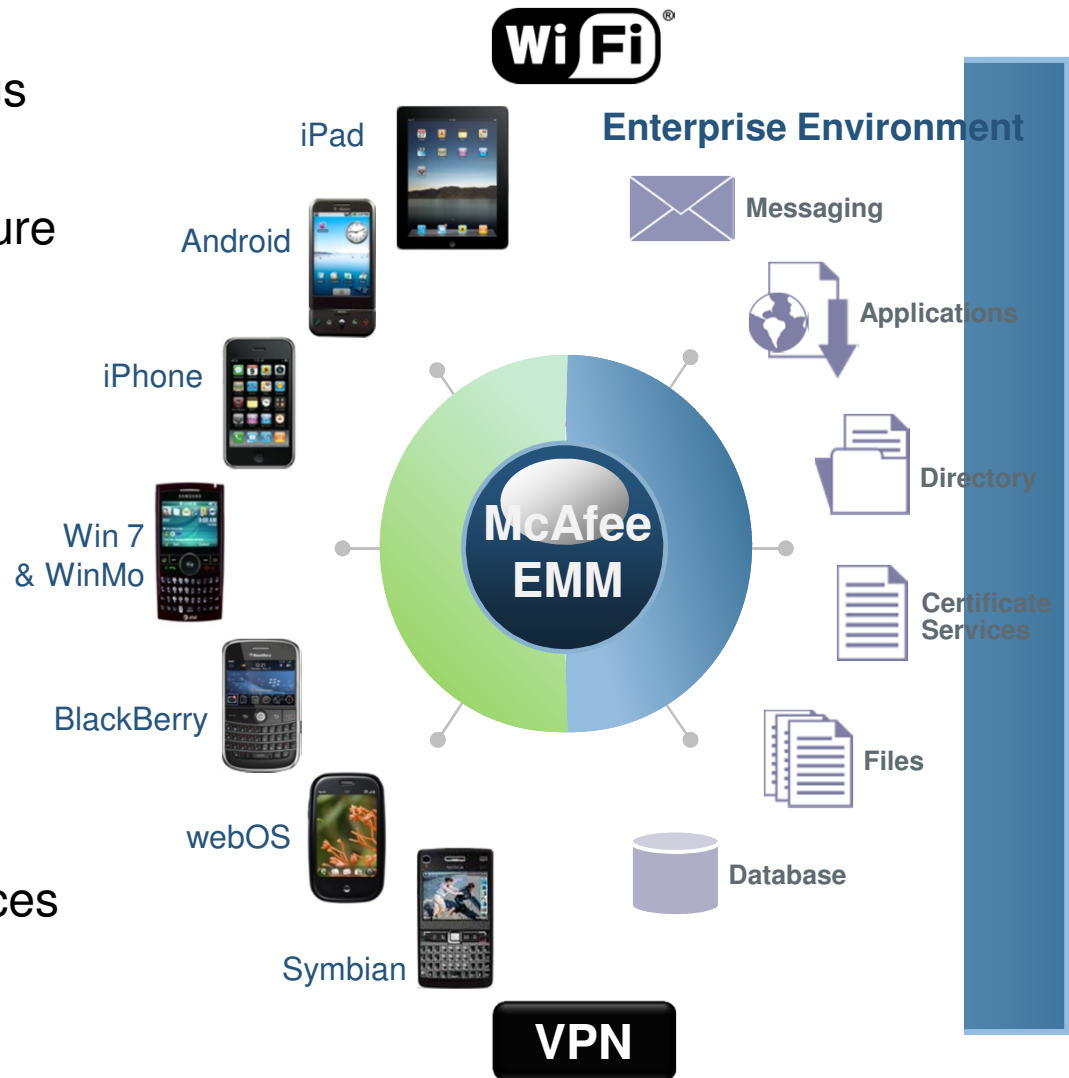
- Manages native security settings
- Enforces device compliance
- Extends the security infrastructure via ePO
- Integrates with the data center

- **Easy**

- Simple administration and reporting via ePO
- User self-service provisioning
- Device personalization for user productivity

- **Scalable**

- Scales to 10s of 1,000s of devices
- Supports HA and DR configurations



The Right Life Cycle for Mobile Device Management



Enterprise Application Management

Make apps available in a **secure, role-based way**. Offer apps for download, links to third-party app stores, and web links.

Provisioning

Define security policies, network connectivity, and resources; users self-service provision for automatic device personalization.

IT Operations Support

Visualize and manage devices centrally through McAfee ePO integration.

Security and Authentication

Enable devices to strongly authenticate against Microsoft CA. Supports two-factor authentication.

Compliance

Automatically check devices prior to network access.

Policy Management

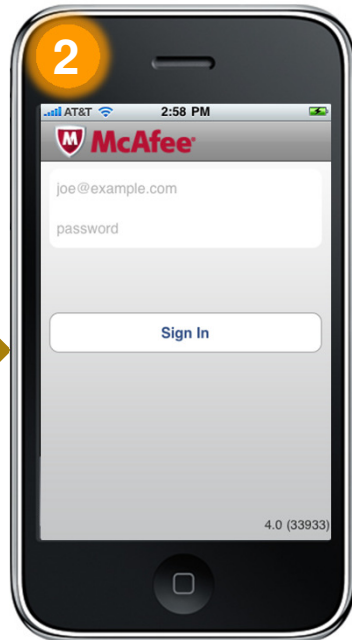
Remotely perform helpdesk tasks and push security policies and configuration updates over-the-air.



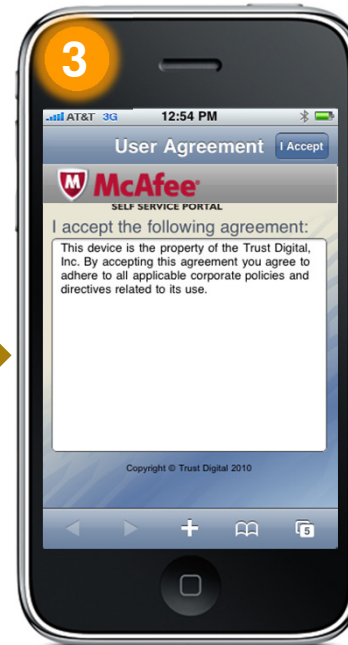
Self-Service Provisioning for iPhone



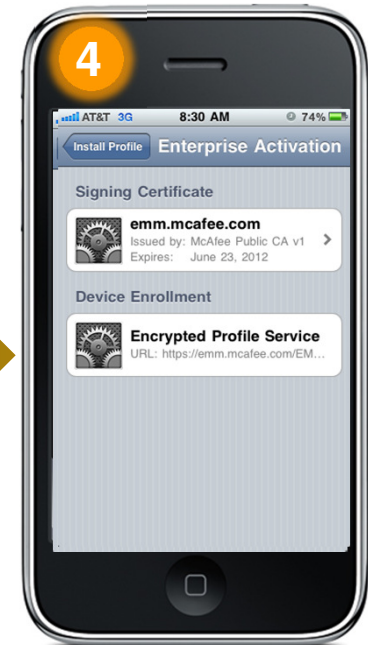
Go to the App Store



Enter Your Email Credentials



Agree to Corporate Policy



IT Services are Auto-Provisioned

Easy, Secure, Automated

optional

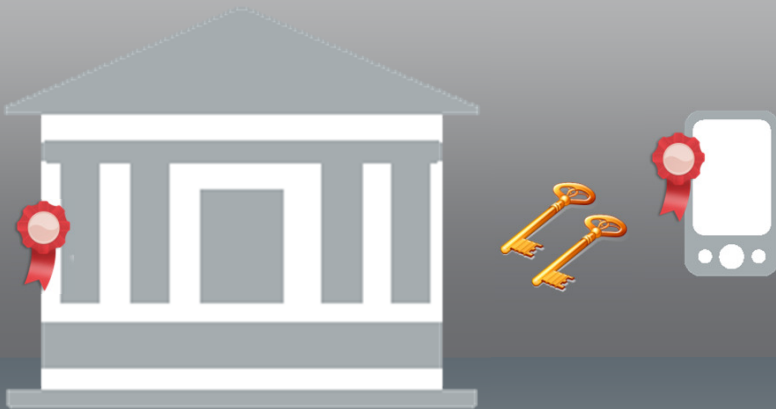


Self-Service Provisioning for Android



Easy, Secure, Automated

Industry-Standard Security: Microsoft Certificate Authority



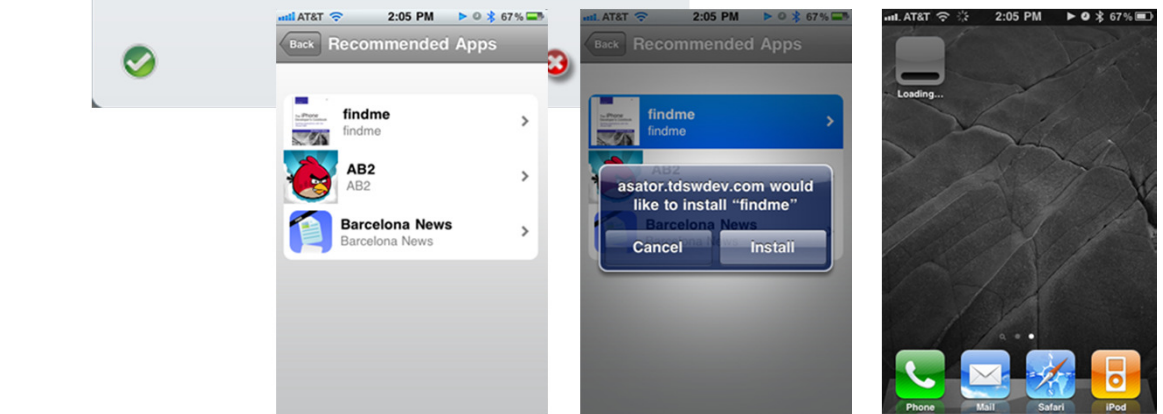
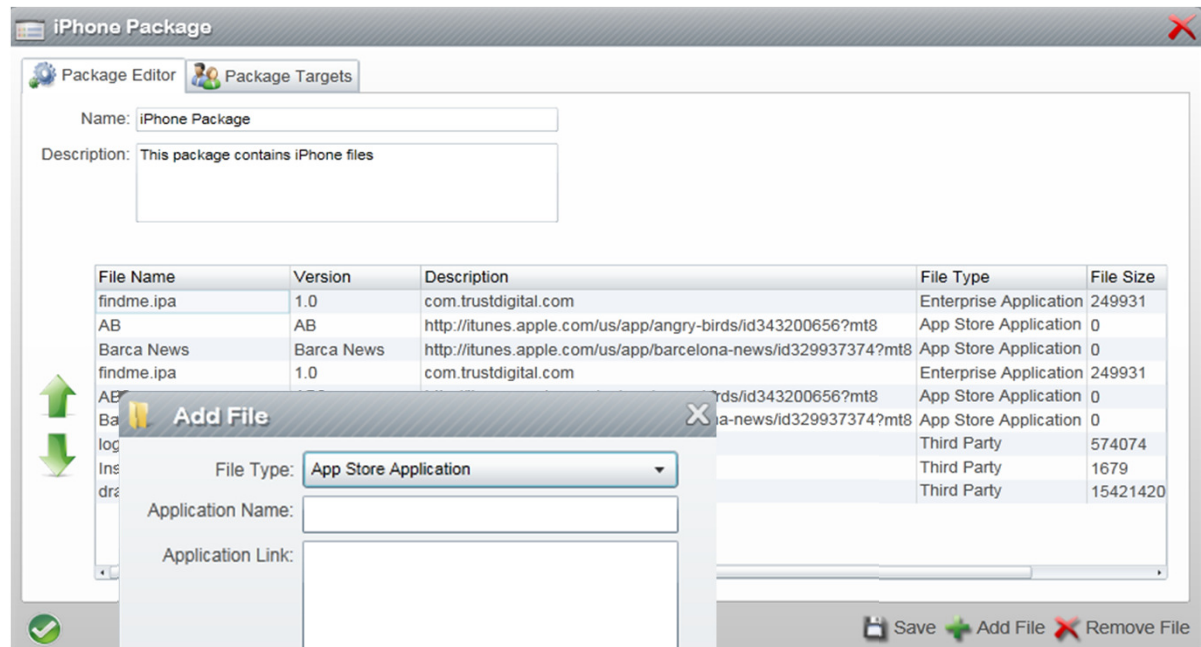
Benefits:

- Industry-standard security
- Strong authentication for secure access to communications services such as Wi-Fi and VPN
- Strong authentication for secure push email and other applications
- Single sign on for enhanced user experience
- No impact on battery life

Enterprise Application Store



- Recommend and make applications securely available based on group, role, or device type.
 - Custom corporate applications
 - Third-party applications (Apple App Store or Android Marketplace)
 - Webclips
- Device application inventory, audit, and policy management



Centralized Visibility and Control with ePO



The screenshot displays the McAfee ePO interface. At the top, there is a navigation bar with icons for Detected Systems, Dashboards, System Tree, Queries & Reports, Policy Catalog, Server Tasks, Client Task Catalog, and Host IPS Catalog. Below this, a 'Subnet Status' section shows 'Covered Subnets: 35.7%' and '28 Covered'. A large red arrow points from this section to a detailed 'Overall System Status' window. This window features a green header with 'Compliant Systems: 94.3%'. Below the header is a table with the following data:

Category	Count
Managed	56,340
Rogue	8,756
Exceptions	6,904
Inactive	1,720

Below the table is a button labeled 'Import/Export Exceptions'. To the right of the 'Overall System Status' window, a 'Compliance Status' pie chart is visible, with a legend for iPhone 3GS/4 (green), HTC Touch Pro RAPH800 (blue), and iPhone 4 (orange). A red callout box with a white arrow points to the 'Managed' row of the table, containing the text: 'Compliance reports are based on systems we know about'. The bottom of the interface shows a list of systems with columns for IP address, name, last seen, and vendor, along with an 'Ignore' button and an 'Actions' dropdown menu.

Centralized Visibility and Control with ePO



The screenshot displays the McAfee ePO dashboard. At the top, there are navigation tabs: Dashboards, System Tree, Queries & Reports, Policy Catalog, Server Tasks, Client Task Catalog, and Host IPS Catalog. The main content area is divided into several sections:

- Detected Systems:** A summary card showing "Overall System Status" with "Compliant Systems: 94.3%". Below this, a table lists system categories: Managed (56,340), Rogue (8,756), Exceptions (6,904), and Inactive (1,720). There is also a "52 Uncovered" summary and an "Add Subnet" button.
- Detected System Interfaces by Subnet:** A table listing detected interfaces with columns for Computer Name, IP Address, and Last Detected Time.

Computer Name	IP Address	Last Detected Time
3700	192.168.1.1	12/13/10 2:29:38 PM
DLINKNAS	192.168.1.4	12/13/10 2:30:09 PM
BRN001MFC7440N0	192.168.1.3	12/13/10 2:29:09 PM
Rogue iPad	192.168.1.204	12/13/10 1:54:39 AM
	192.168.1.8	12/13/10 3:26:43 AM

Two red arrows point from a text box to the "Rogue" and "Exceptions" categories in the Overall System Status table, and to the "Rogue iPad" entry in the Detected System Interfaces table.

What we don't manage is where compliance status is unknown

Centralized Visibility and Control with ePO



EMM : Compliance Status

- iPhone 3GS/4
- HTC Touch Pro RAPH800
- iPhone 4

Total

OS Platform ▲	Organization Name
Linux	NETGEAR
Linux	D-Link Corporation
Printer	BROTHER INDUSTRIES, LTD.
Unknown	Apple
Unknown	MITUMI ELECTRIC CO., LTD.

Subnet: 10.70.14, 172.16.5, 161.69.8, 192.166., 10.0.0.0

Bob's iPhone

SERVER01

Ignore Actions 15 items Deploy Agent

Bringing all endpoints into compliance status view is critical to assessing risk and prioritizing actions

McAfee WaveSecure for User Device Management



Lock Your Phone Remotely to Prevent Unauthorized Access

Track your Phone's Location and SIM Changes in the Phone

Backup and Restore the Data on Your Phone

Remotely Wipe Your Phone Data and Memory Card

The screenshot displays the 'My Device' management interface. On the left, a vertical menu lists various actions: Lock (with a padlock icon), Track (with a location pin icon), Location (with a Wi-Fi icon), Backup (with a folder icon), Wipeout (with a radiation symbol icon), and Restore (with a circular arrow icon). Below this is the 'My Data' section, which includes options for Contacts, SMS, Call Logs, and Media. On the right, a section titled 'Track the location on my device' features a magnifying glass icon, a 'Last tracked on' timestamp of 'Jan 14, 09:43 AM', and a 'Show current location' button. Below this is a map showing a street grid with a red location pin and a yellow circle indicating the current location. The map includes street names like 'Delaware Ave', 'Chapin Pkwy', and 'W Delaware Ave', and a route marker '384'.

All Part of McAfee Security Connected



Security Management

- Policy Management
- Security Reporting
- Mobile Management
- Vulnerability Management
- Risk Management
- Compliance



Network Security

- Next Generation Firewall
- Network Intrusion Prevention
- NAC Gateway
- Network User Behavior Analysis
- Network Threat Behavior Analysis
- Network Threat Response



Content Security

- Email Gateway
- Web Gateway
- Data Loss Prevention
- Encryption



Endpoint Security

- Mac, UNIX/Linux AV
- Virtual Desktop
- Virtual Server
- Mobile Devices
- Anti-Virus & Anti-Spyware
- Host Intrusion Prevention
- Endpoint Encryption
- Application Whitelisting
- Desktop Firewall
- Device Control
- Policy Auditing
- NAC Endpoint
- Email Server AV & Anti-Spam
- SharePoint Protection
- Website Reputation



Delivery

Software

Appliance

SaaS

Virtualized

Open Security Platform

Security Innovation Alliances

Global Strategic Alliances

McAfee Connected

Security Alliances

Security Solutions for Consumerization of IT



Consumerization of IT

