Mobility & Storage

17.15 – 17.40

IBM Endpoint Manager for Mobile Devices

Alessandra Pecorari – Tivoli Client Technical Professional

17.45 – 18.10

Simplify and optimize storage infrastructure in the cloud era

Carlo Anello – Italy Tivoli Storage Sales Leader & Business Development

18.10 - 18.30

Integrated platform for network management

Alessandro Proia - Tivoli Client Technical Professional

IBM Endpoint Manager for Mobile Devices

Alessandra Pecorari
Tivoli Client Technical Professional
alessandra.pecorari@it.ibm.com

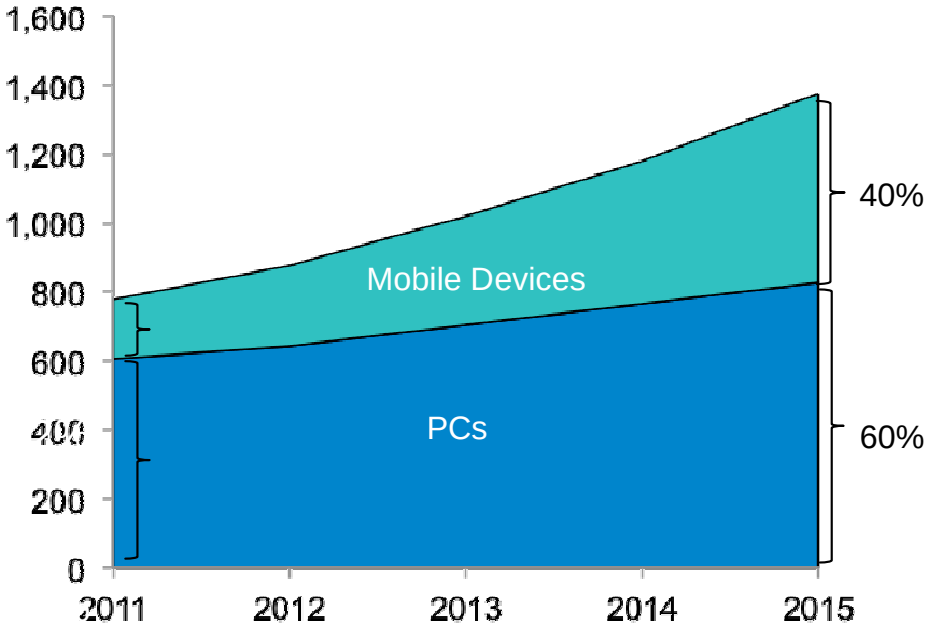
PCTY2012
Pulse Comes to You

Optimizing the World's Infrastructure
15/05/2012 Rome

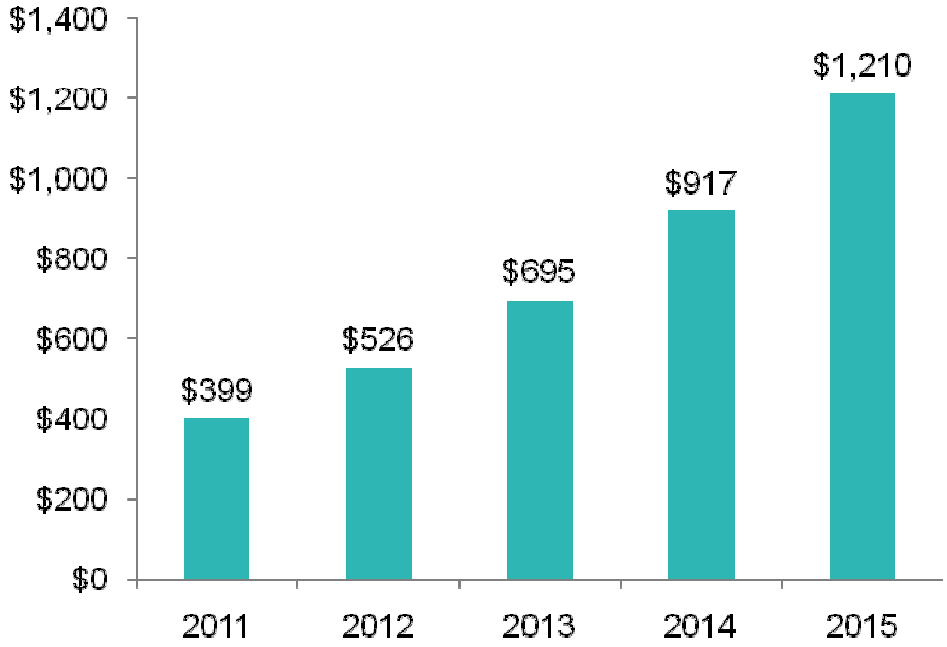
© 2012 IBM Corporation

Mobile device growth

Growth in Enterprise Devices by Type[1]



Enterprise MDM Market Size (millions)[2]



[1] Gartner Forecast: PCs, All Countries (Annual Data) 1Q11; IDC, Worldwide Business Use Smartphone 2010-2014 Forecast, 9/2010; Gartner Forecast: Connected Mobile Consumer Electronics, Worldwide, 2008-2014, 4Q10 Update;
[2] IDC, Worldwide Mobile Device Management Enterprise 2011-2015 Forecast; August 2011

Note: Enterprise devices defined as PCs, smart phones, and media tablets (iPad, RIM PlayBook, etc)

IBM Endpoint Manager for Mobile Devices Summary

- IBM Endpoint Manager for Mobile Devices
  - New product released on March 2012
- Background
  - Smartphones and tablet usage continues to grow
  - Mobile devices (owned by employees or organization) access company data and resources
  - Enterprises do not have the tools to properly manage mobile devices
  - Old methods of managing devices (email-based management) do not give enterprises sufficient control of the devices
- Unique management console
  - IBM Endpoint Manager for Mobile Devices (built on the **BigFix**) platform provides fully-integrated, single-pane-of-glass **Unified Endpoint Management**

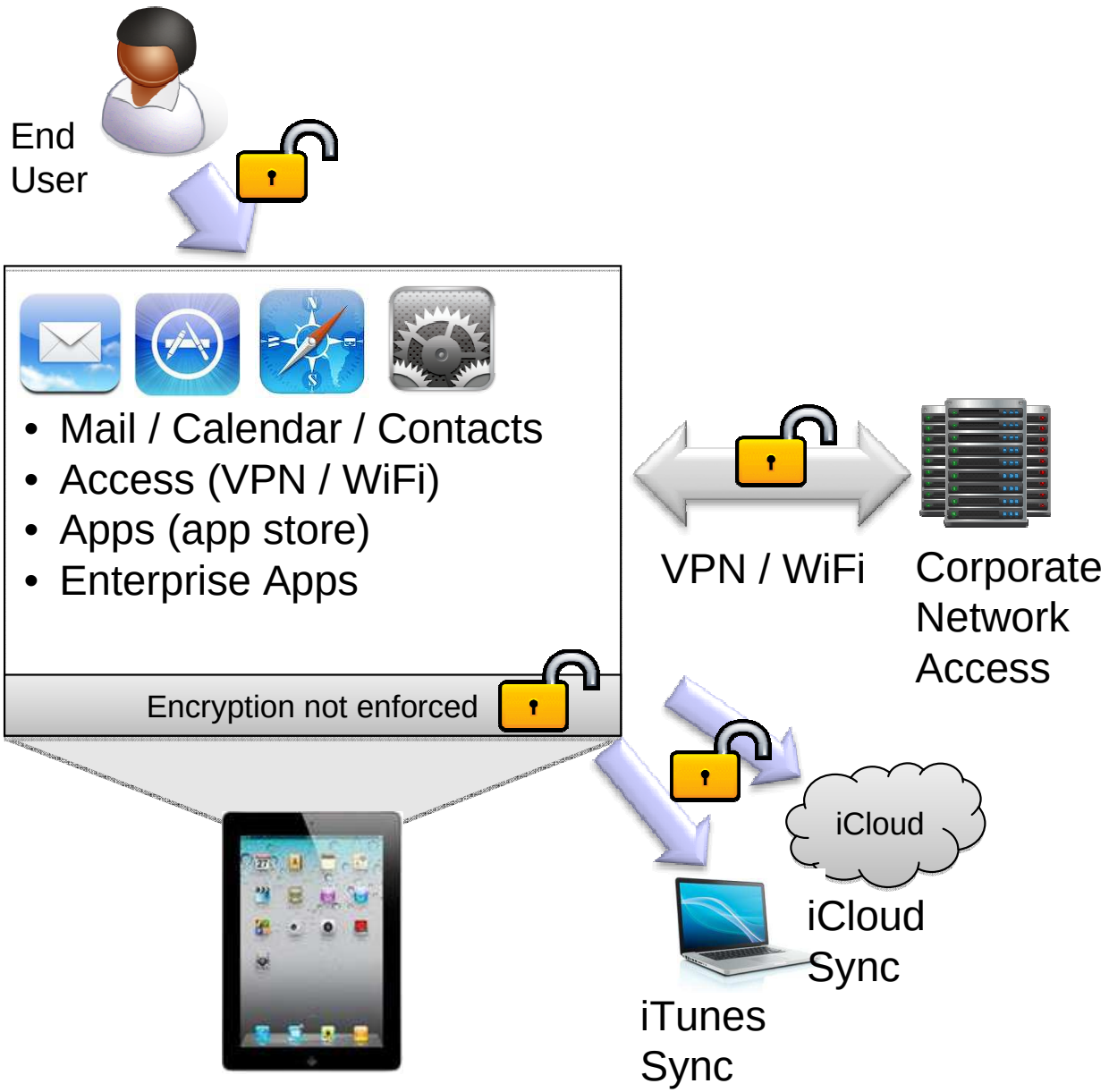
Mobile Devices Create New IT Challenges

Traditional Mgmt Model	New Device Mgmt Paradigm
Enterprises provide all equipment	Employees bring personal devices (BYOD)
Small set of supported platforms / models	Many different manufacturers / models
IT initiates and manages upgrades	OS/app upgrades managed by carriers, OEMs, users
IT tightly controls apps and security	Users control their own devices

Options for IT departments

- ✗ Don't allow mobile devices because they are too hard to manage ✗
- ✗ Allow unmanaged and insecure mobile devices ✗
- ✓ Invest in tools to secure and manage devices ✓

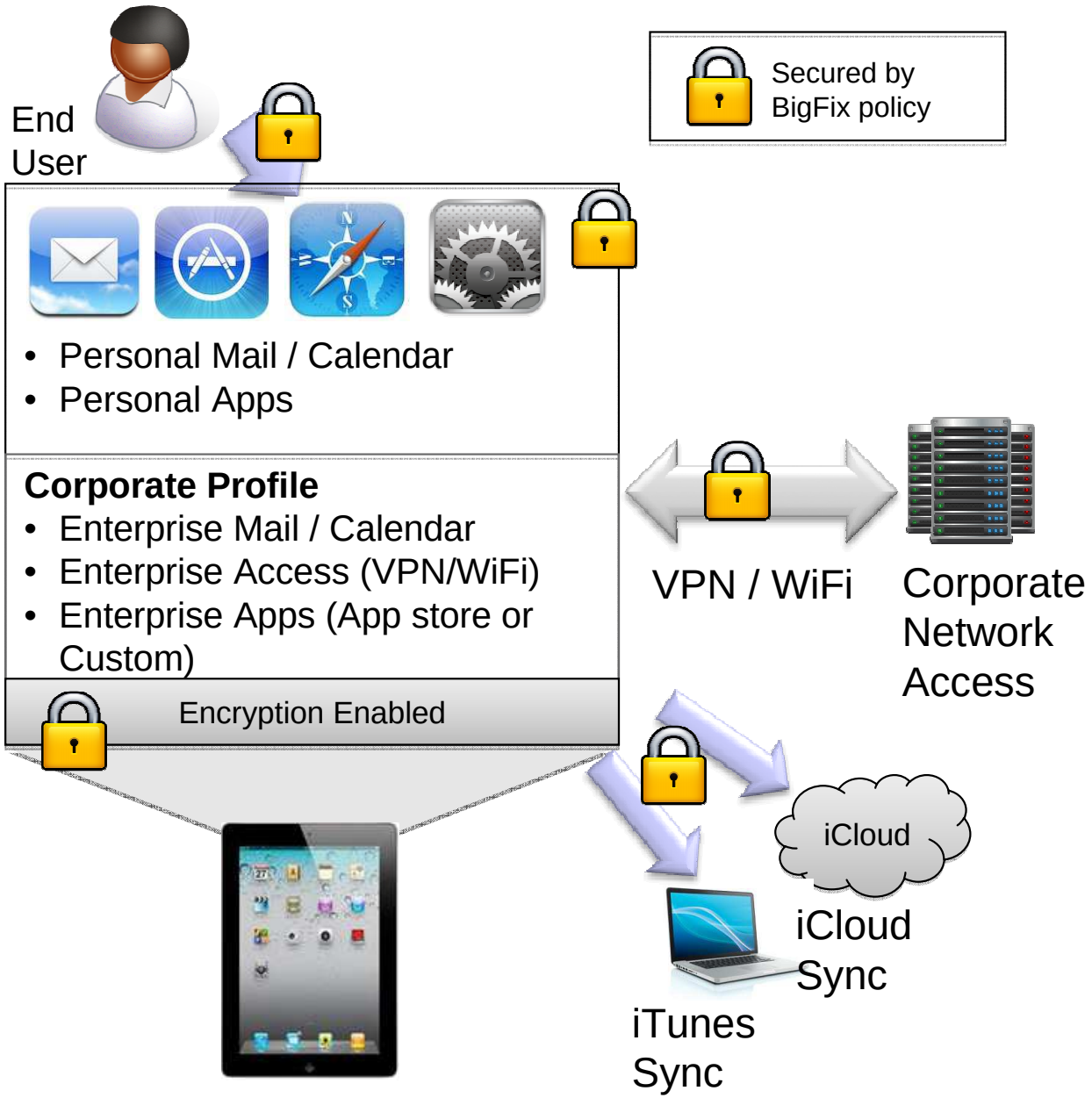
Managing Mobile Devices – The Problem



Security/Mgmt Problems

- Potential Unauthorized Access (lost, stolen)
- Insecure devices connecting to network
- Lack of encryption
- Corporate data leakage

Managing Mobile Devices – The Solution



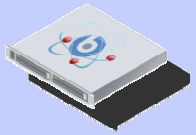
Endpoint Manager for Mobile Devices

- Enable PW Policies
- Enable Device Encryption
- Force encrypted backup
- Disable Sync
- Corporate Access, email access, and App access contingent on Policy Compliance!
- Wipe if lost / stolen
- Wipe corporate data if employee leaves company (selective wipe)

PCs and mobile devices have many of the same management needs

Traditional Endpoint Management

- OS provisioning
- Patching
- Power Mgmt
- Anti-Virus Mgmt



Mobile Device Management

- Device Wipe
- Location info
- Jailbreak/Root detection
- Enterprise App store

- Device inventory
- Security policy mgmt
- Application mgmt
- Device config (VPN/Email/Wifi)
- Encryption mgmt
- Roaming device support
- Integration with internal systems
- Scalable/Secure solution
- Easy-to-deploy
- Multiple OS support
- Consolidated infrastructure

IEM MDM Functionality Overview

Category	Tivoli Endpoint Manager Capabilities
Platform Support	Apple iOS, Google Android, Nokia Symbian, Windows Phone, Windows Mobile
Device Inventory	Model, manufacturer, carrier, free space, battery details, serial numbers
Management Actions	Selective wipe, full wipe, deny email access, remote lock, user notification
Application Management	Application inventory, enterprise app store, whitelisting, blacklisting
Policy & Security Management	Password policies, device encryption, jailbreak & root detection
Location Services	Track devices and locate on map
Enterprise Access Management	Configuration of Email, VPN, Wi-fi

How does IEM manage mobile devices?

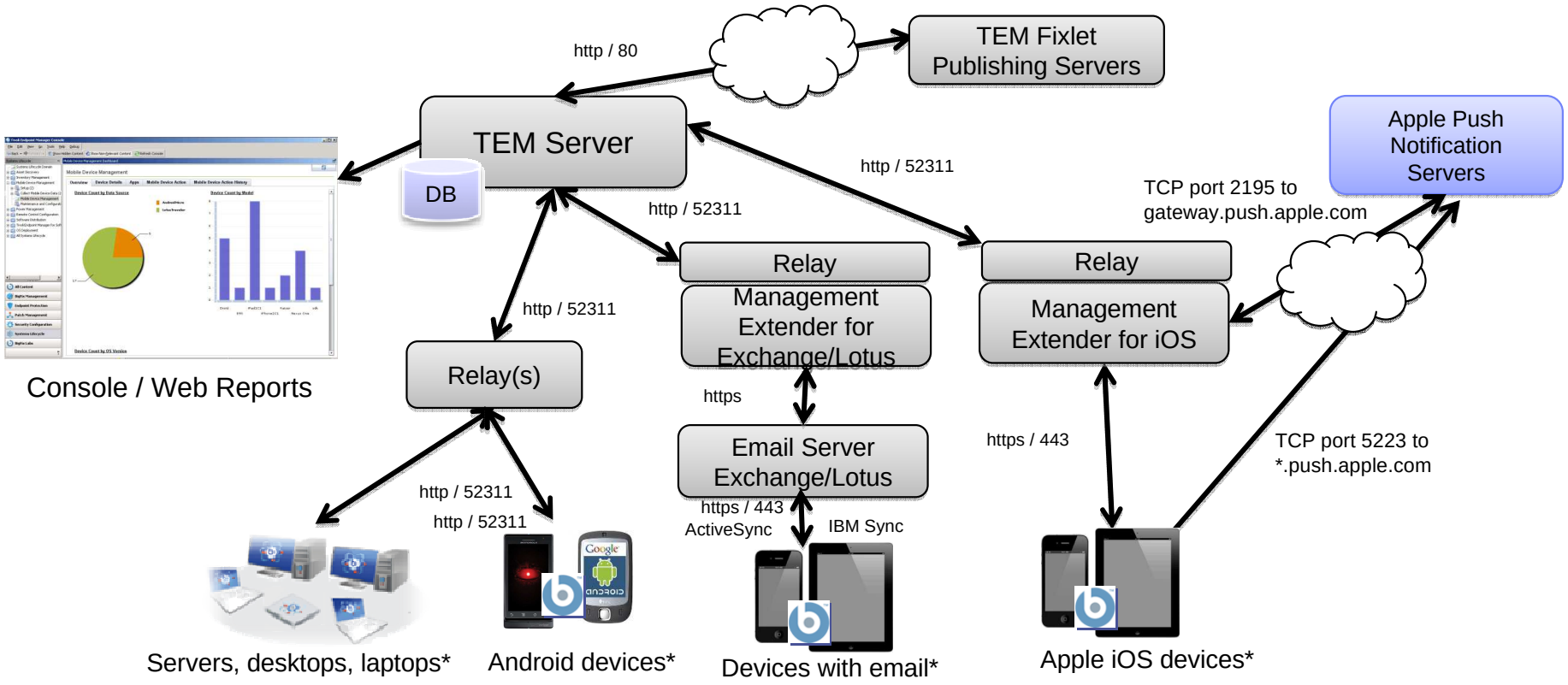
- Agent-based Management
  - Complete set of management functionality
  - Supported OSes
    - Android – Native BigFix Agent (95%+ shared code)
    - Apple iOS – Apple MDM APIs

- Email-based management through Exchange (ActiveSync) and Lotus Traveler (IBMSync)
  - Minimal management functionality (security policies + wipe)
  - Supported OSes
    - iOS
    - Android
    - Windows Phone
    - Symbian

Microsoft® Exchange Server

Lotus. Notes

MDM Architecture



* Managing devices that are not connected to the internal network requires opening the management port to the Internet (HTTP 52311 for Laptops and Android or HTTPS 443 for Apple iOS devices)

MDM Component – Android Agent

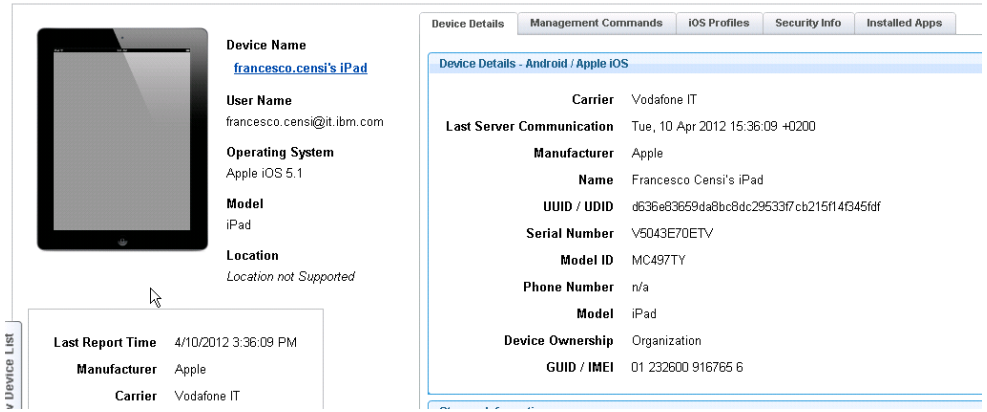
- Android agents are built from Linux agent
- Deployed through an App available on Google Play
- They act very similar to any other BigFix Agent (e.g., registering, gathering, evaluating Fixlets, relay selection, etc)
- Android Agent can:
  - Inspect hardware, apps, security policies, network, location, battery
  - Wipe the device
  - Change security policies
  - Detect if device is “rooted”
- Android Agent cannot:
  - Silently install apps (but can “offer” apps)
  - Silently uninstall apps (but can message user with notifications)
  - See or delete other app’s info

MDM Component – Email-based Management

- Almost all devices can be managed by Activesync protocol (or “IBMSync”)
- Email-based management is fairly easy to setup
  - Install mgmt extender and immediately get access to all devices
- Email-based management has limited capabilities
  - Allowed: Wipe, deny email access, password policies
  - Not allowed: device info (hardware, network, manufacturer, location, apps, etc.)
  - Not allowed: “selective wipe”, clear password, “offering apps”

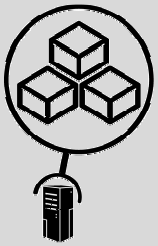
MDM Component – Apple iOS

- Deployed through an App available on the Apple Store
- Apple MDM APIs allow many functions:
  - Advanced inventory (device HW, apps, user, VPN info, email info, etc.)
  - Configuring security policies (passwords, encryption, etc.)
  - Configuring “enterprise access” (wifi, email, vpn)
  - Restrictions (camera, bluetooth, appstore, etc.)
  - “Managed Apps” (associating apps with profile) – new to iOS5
  - Complete device wipe
  - “Enterprise container” / “Selective Wipe” – Grouping & removing calendar / contacts / email / VPN / Wifi / managed apps
- Apple iOS App still needed for full mgmt
  - Jailbreak detection
  - “Recommended Apps”
  - Facilitated enrollment



IBM Mobile Platform – Platform for Managing Devices and Apps

IBM Mobile Platform

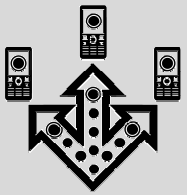


Build mobile applications

Connect to, and *run* backend systems in support of mobile

Manage mobile devices and applications

Secure my mobile business



Extend existing business capabilities to mobile devices

Grow the business by creating new opportunities

IBM Endpoint Manager for Mobile Devices

- IBM Mobile Platform brings together Mobile Enterprise Application Platform (Worklight) with Mobile Device Management (BigFix)
- Enterprises can now build, manage, and secure internal enterprise apps and the devices that they run on

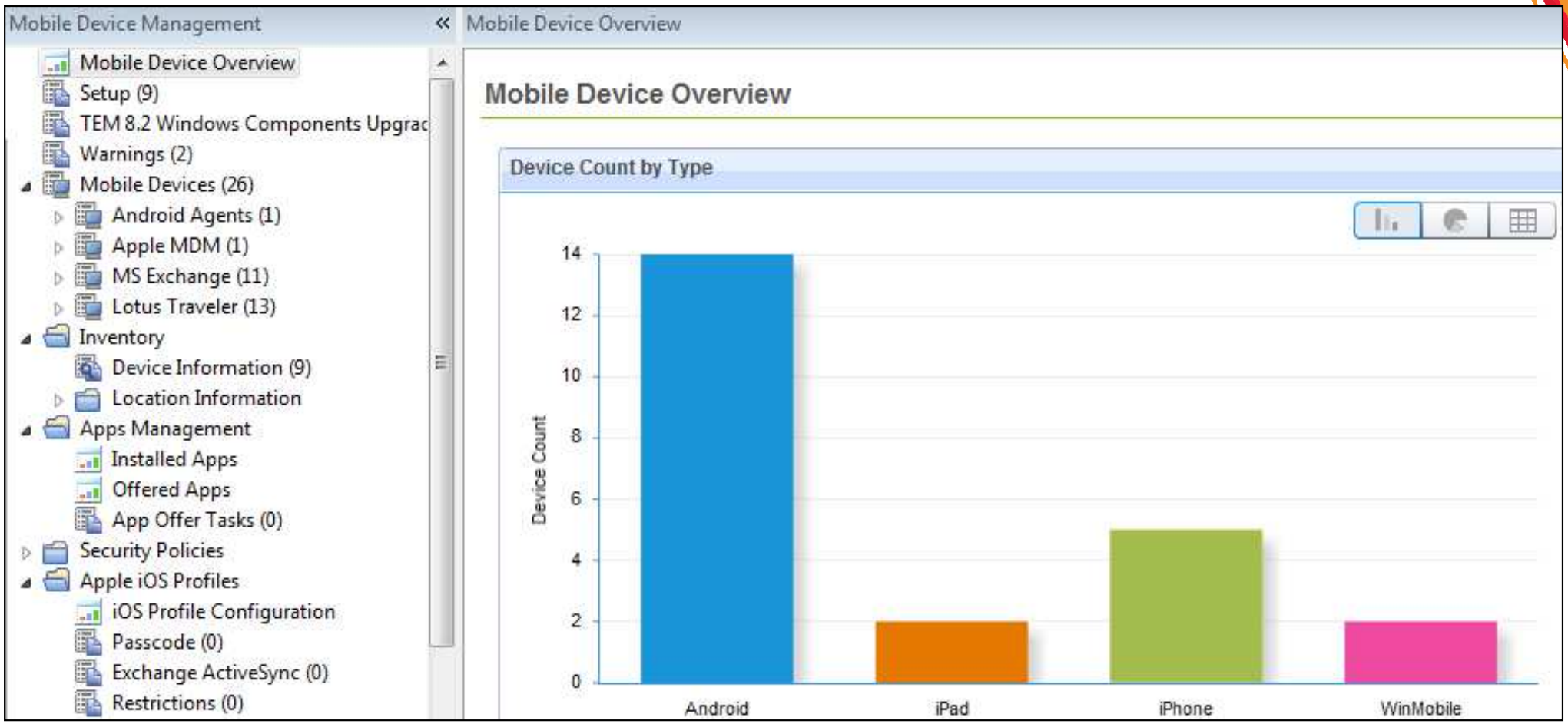
IBM Endpoint Manager for Mobile Devices

Product Demo

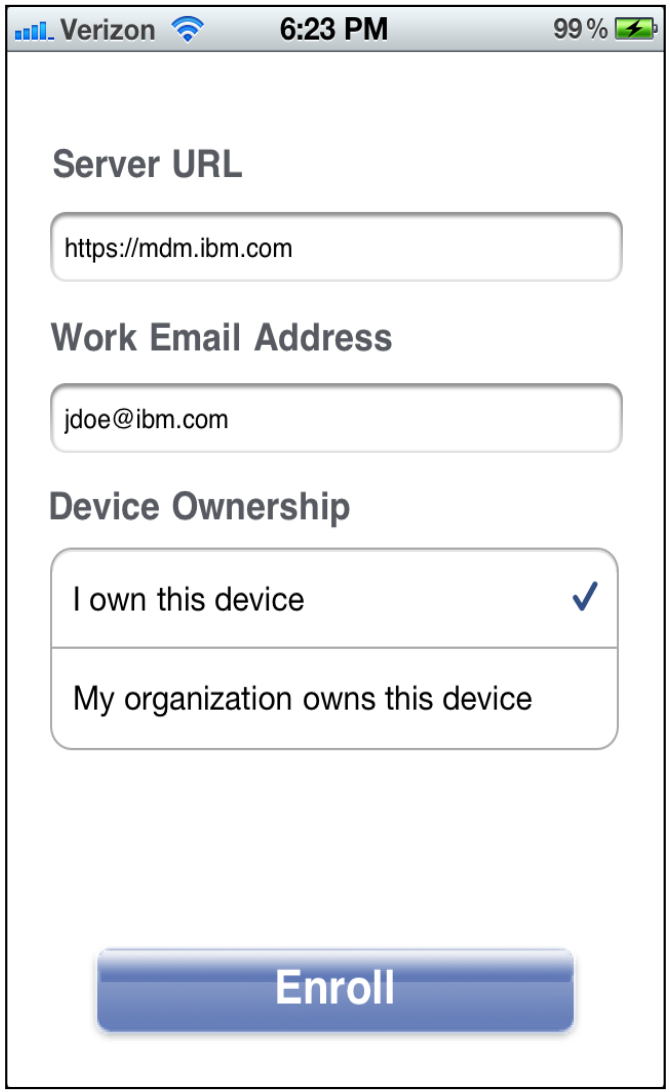
Optimizing the World's Infrastructure
15/05/2012 Rome

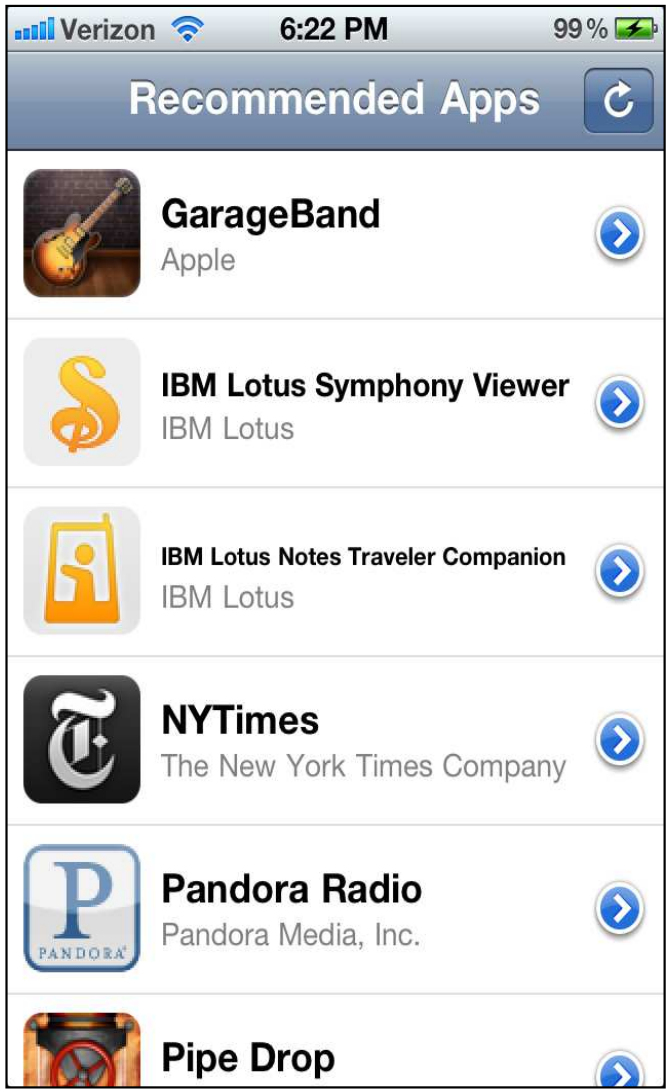
© 2012 IBM Corporation

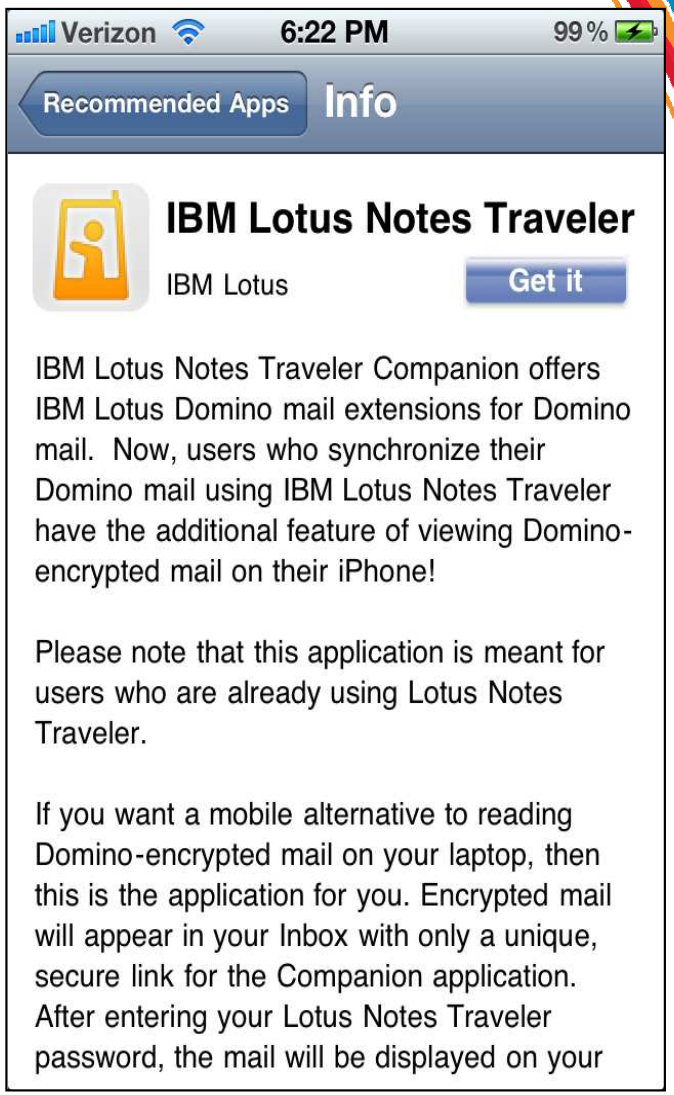
Endpoint Manager for Mobile Devices Dashboard



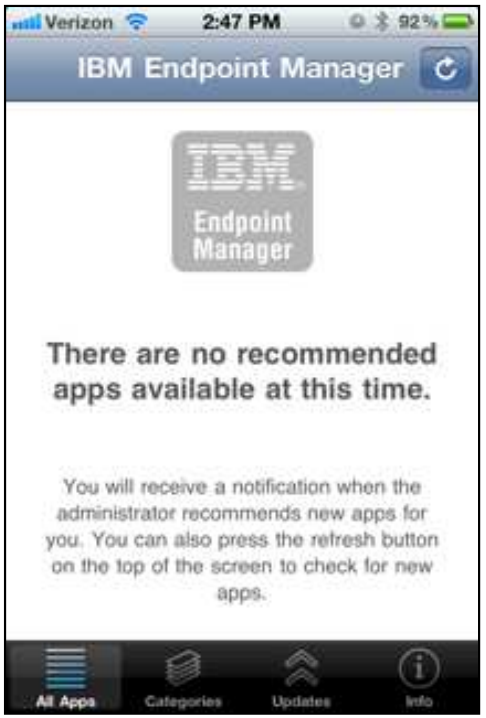
An on-device app can be used to distribute enterprise apps and detect whether an iOS or Android device is jailbroken or rooted

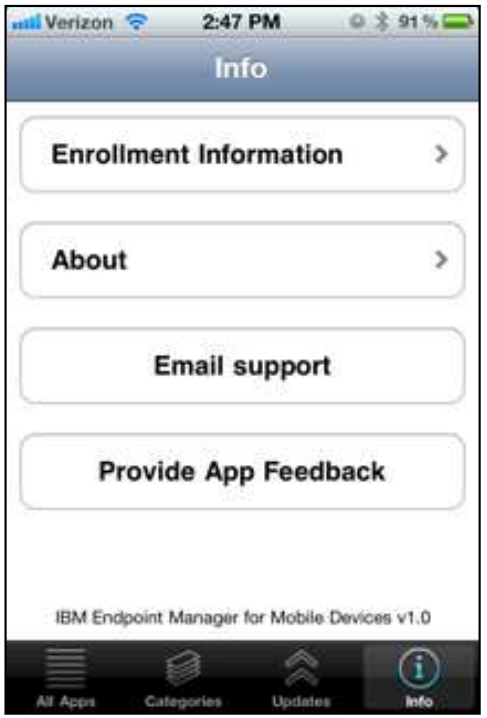




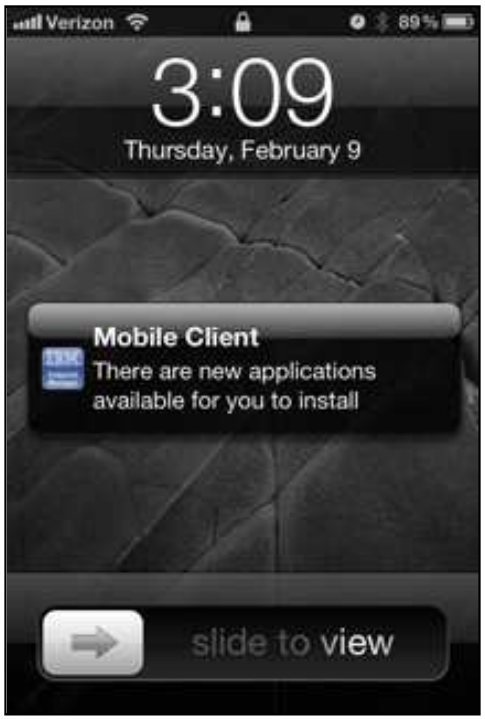


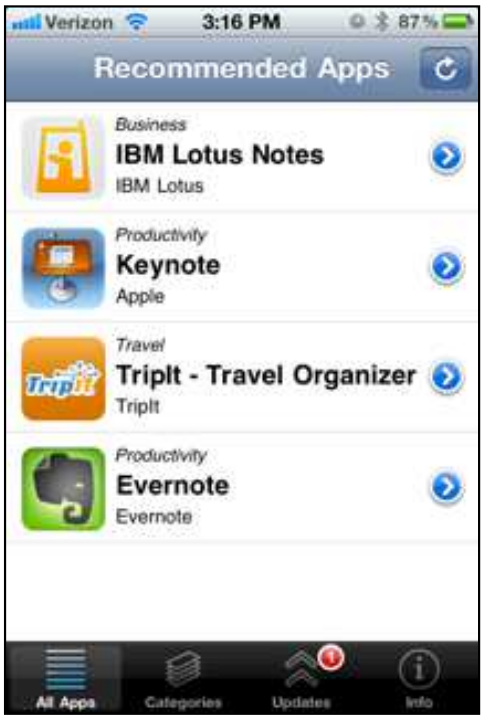
iOS Enrollment

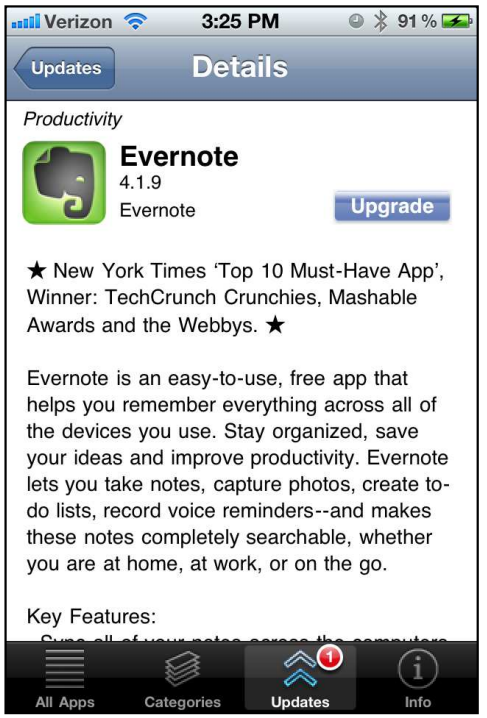




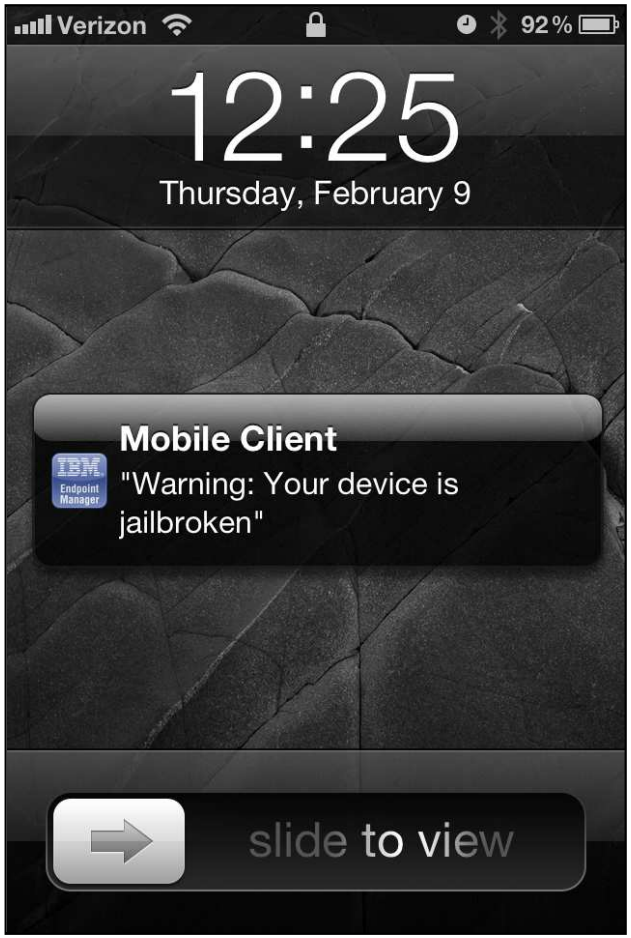
App Management



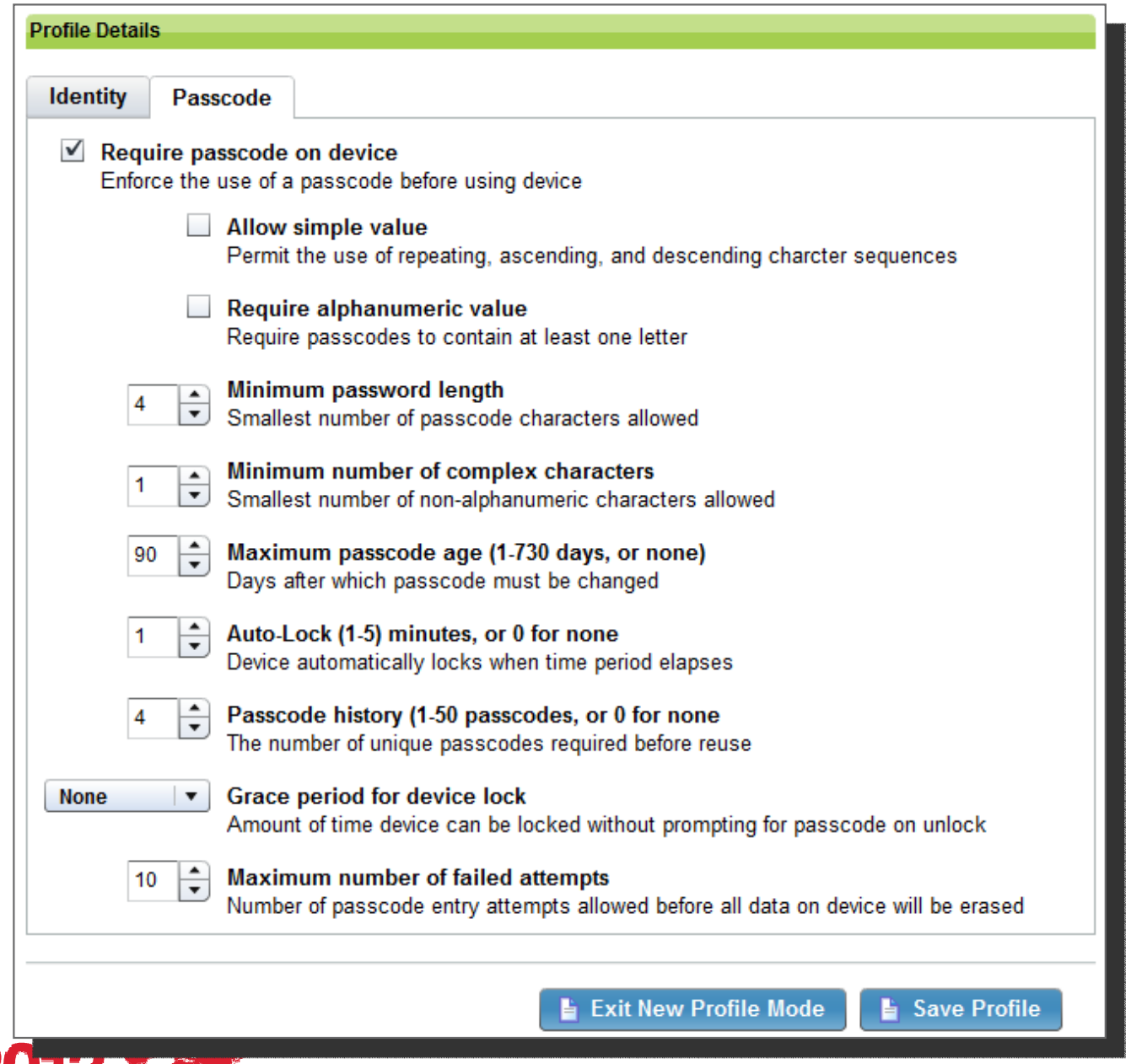




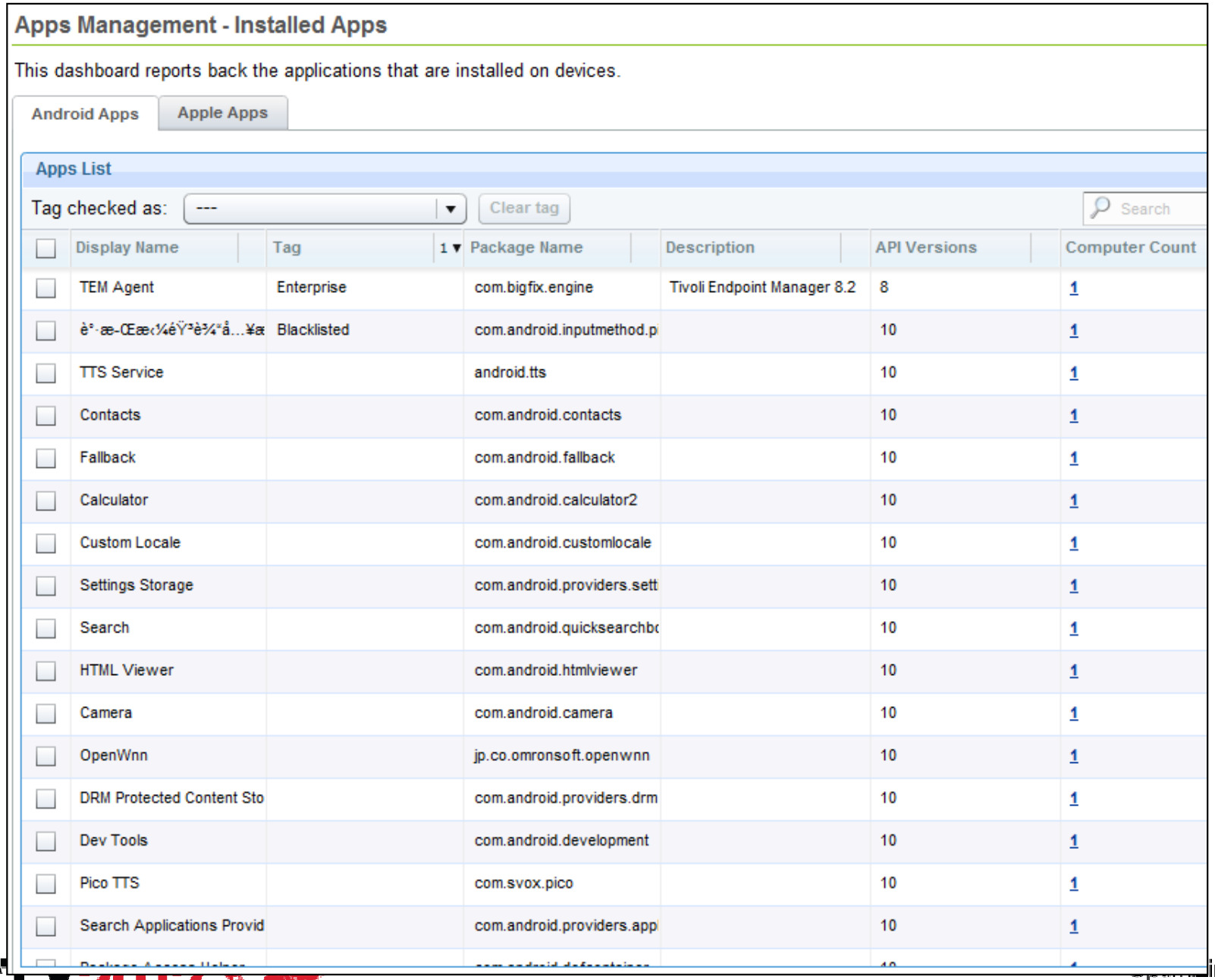
iOS Jailbreak Notification



A user-friendly iOS Profile Configuration Wizard exposes all of the configuration capabilities exposed by Apple's MDM APIs



View installed apps on Android and iOS devices



Apps Management - Installed Apps

This dashboard reports back the applications that are installed on devices.

Android Apps | Apple Apps

Apps List

Tag checked as: --- | Clear tag | Search

Display Name	Tag	Package Name	Description	API Versions	Computer Count
TEM Agent	Enterprise	com.bigfix.engine	Tivoli Endpoint Manager 8.2	8	1
è°·æ-Œæ‹¼éŸ³è¾“å…¥æ	Blacklisted	com.android.inputmethod.p		10	1
TTS Service		android.tts		10	1
Contacts		com.android.contacts		10	1
Fallback		com.android.fallback		10	1
Calculator		com.android.calculator2		10	1
Custom Locale		com.android.customlocale		10	1
Settings Storage		com.android.providers.sett		10	1
Search		com.android.quicksearchbo		10	1
HTML Viewer		com.android.htmlviewer		10	1
Camera		com.android.camera		10	1
OpenWnn		jp.co.omronsoft.openwnn		10	1
DRM Protected Content Sto		com.android.providers.drm		10	1
Dev Tools		com.android.development		10	1
Pico TTS		com.svox.pico		10	1
Search Applications Provid		com.android.providers.appl		10	1

Q & A

Thank You!

Acknowledgements, disclaimers and trademarks

© Copyright IBM Corporation 2012. All rights reserved.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this publication to IBM products, programs or services do not imply that they will be made available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results. All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information concerning non-IBM products and services was obtained from a supplier of those products and services. IBM has not tested these products or services and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products and services. Questions on the capabilities of non-IBM products and services should be addressed to the supplier of those products and services.

All customer examples cited or described are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer and will vary depending on individual customer configurations and conditions. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

IBM, the IBM logo, ibm.com, Tivoli, the Tivoli logo, Tivoli Enterprise Console, Tivoli Storage Manager FastBack, and other IBM products and services are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml