Good for Enterprise™
Good Dynamics™

International Legal Technology Association
What are Good for Enterprise and Good Dynamics?
Good is far more than just MDM

Good delivers greater value and productivity through application data security

Low Business Value
Device Mgmt.

Medium Business Value
Integrated Secure Email, PIM

High Business Value
Secure Intranet Apps & Portals
Integrated Document Mgmt.

Good for Enterprise

Good Dynamics
Good’s Platform

Good for Enterprise™/Good for Government™

- Mobile Security Suite
  - Device Management
  - Secure Email/PIM/Calendar
  - Secure Browser
  - Secure Documents
  - Application Management

Good Dynamics™

- Enterprise Apps
- 3rd Party Apps

Good’s Mobile Data Security Platform
End-to-end comprehensive security

- Encrypted enterprise data
- Application password enforcement
- Data loss prevention policies
- Remote erase

Devices with Good

Network Operations Center

Wireless Network

Network Operations Center

Wireless Network

Enterprise Applications

Good Servers

Intranets

SharePoint

Web-enabled Apps

Internal Security

Perimeter Security

Transport Security

Handheld Security

Control traffic by:
- Access list
- Domain name
- Detect jailbroken/rooted malware infected devices

- Outbound connection
- No firewall holes
- No VPN
- Role-based admin
- Policy groups

- Guaranteed delivery
- AES encryption
- FIPS 140-2 certificate
- Authorized device check

- Encrypted enterprise data
- Application password enforcement
- Data loss prevention policies
- Remote erase
Provisioning a mobile device/user

- IT provision or self-provision – fully OTA
- Fully integrated with Active Directory/LDAP
- Users receive activation email
- Download client app from app stores (Apple, Google, Amazon)
- Run app and enter in credentials received in email
- Synchronization begins immediately
Self-Provisioning Portal

Good Mobile Control

Sign in to Good Mobile Control

Username: 
Password: 
Domain: 

Remember my username and domain

Sign In
## Self-Provisioning Portal

### Welcome brobison

<table>
<thead>
<tr>
<th>Your Handhelds</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Mobile Pocket PC MAC:001DFED693E4</td>
<td>![Lock handheld]</td>
</tr>
<tr>
<td>iOS 8a184e40749c3ea1de05c4e358a7d6e331b1d55</td>
<td>![Lock handheld]</td>
</tr>
<tr>
<td>iOS 7aaa7b7c4eb4d049991c218bb6700d592be2695</td>
<td>![Lock handheld]</td>
</tr>
<tr>
<td>5555551212 Android ESN:GD55555551212</td>
<td>![Lock handheld]</td>
</tr>
</tbody>
</table>
Quickly add single users or bulk import users from file using first and last name
On device setup

Good Technology

Welcome to Good for Enterprise!

Before you begin, make sure you have strong network coverage.

You will need your email address and PIN included in the welcome message sent by your IT administrator.

Tap "Start" to set up Good for Enterprise.
- Implement *application level* security in real-time to prevent data loss

- Separate “personal” from “business”

- Apply policies consistently across multiple mobile platforms – even when underlying platform doesn’t provide security controls
Enterprise App Store - Custom Software Distribution

- Deploy Apps On:
  - Apple iOS
  - Android
  - Windows Phone
  - Windows Mobile
  - Symbian
  - Palm OS

- Integration with other App Stores

- Recommended Apps
Application Management and/or Deployment

- Application Blacklist
- Compliance based “required” apps
- Third party apps “recommended”
- Deploy in-house/ custom apps

Add compliance rule
Platform: iOS
Check to Run: Connectivity Verification
Conditions: Client Version Verification
Application Name: Hardware Model Verification, Jailbreak/Rooted Detection, OS Version Verification
Description:
Failure Action: Quit Good for Enterprise
Check Every: 12 hours

Enterprise Applications
Add application enforce policy

<table>
<thead>
<tr>
<th>Application</th>
<th>Version</th>
<th>Platform</th>
<th>Type</th>
<th>Allow iTunes/iCloud Sync</th>
<th>Auto-Uninstall</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Good Dynamics™ - Services

- **Secure Storage**
  - Encrypted file system (including file and directory names)
  - Encrypted SQL storage

- **Enterprise Secure Connectivity**
  - Transparent access to Enterprise App Servers
  - TCP socket level connection
  - Web services calls/REST calls

- **Container Management & Policies**
  - Provisioning, de-provisioning, lock, wipe
  - Compromised device detection, password policy

- **Push Services**
  - Push data Service: any type of message, token-based
  - Also used internally to push Policies to the client
Enterprise Data/Document Storage

- Fully encrypted document repository within the Good for Enterprise app
- Allows files to be opened or edited in IT approved apps
- Secure apps powered by Good Dynamics
Good Dynamics is a security SDK that allows app developer to take advantage of Good’s security platform

GD powered apps can securely communicate with each other and Good for Enterprise

Apps are now fully managed by IT, features by policy, remote wipe of app and data

Box for Good Technology

Description

Specially designed for the Good Dynamics mobile application platform, Box for Good Technology provides simple, secure sharing from anywhere – letting you easily store files online, send big files fast, access content from your iPhone or iPad and collaborate with colleagues while on the go. It offers advanced enterprise security and management features from Good Technology, such as added encryption, remote wiping and policy requirements.

If you are not a Good Technology user, you can download Box for iPhone and iPad at: http://itunes.apple.com/app/box-for-iphone-and-ipad/id290853822.

Box.net, Inc. Web Site  Box for Good Technology Support
End-to-end workflow with no data exposure!

1. Receive work email with attachment via GFE
2. Open, view, edit document in “Quickoffice for Good”
3a. Send to GFE
3b. Save to GFE file repository
3c. Sync to Box
Removal of data/wiping devices

- Good for Enterprise is focused on protecting customer sensitive data – not necessarily managing the device
  - App level wipe allows IT to have confidence when removing sensitive data and does not impact personal data or apps
  - Encrypted container to protect and separate corporate email/PIM and other sensitive data from personal data
  - Rather than restrict, Good enables the personal use of iCloud, iTunes, social media and document sharing apps
  - Device level wipe is available through MDM features if desired
Help Desk Console/Issues Management

- Helpdesk staff is notified by end-user of difficulty or notified by Good Mobile Control reports of issues

- Issues that are common
  - Users lose pin and require IT to resend
  - Users want to provision a new device
  - Users email is not being sent to device
    - View device’s connectivity status (4 hours – 24 hours)
    - View Exchange/Domino configuration states and run mailbox diagnostics
    - Work with Good support and can easily send logs directly
Most enterprise organizations utilize the Good API’s to access data directly and integrate with other consoles.

**Built-in reporting and live (filtered) views**
- Devices by Policy Sets
- Devices by Server (Exchange/Domino server)
- Devices by Compliance (in or out)
- Devices with Roaming (enabled or disabled)
- Devices by Platform
- Devices by Carrier
- Devices by Department

**Exports of data (CSV)**
- Software installed, connection statistics, paused devices and compliance
Device Deprovisioning Process

- IT or end user can “remove/delete” a device from the Good Mobile Control console
- Within seconds the user will be logged out of Good for Enterprise or any other app controlled app
  - User sees a message stating that they no longer have access to this data
  - Data is immediately wiped
  - User can then remove app from device
Full Compliance Manager built-in to Good Mobile Control

Rule based mechanism

- Checks to run
  - Client version verification – keep GFE clients updated
  - Connectivity verification – device connected at least once in period
  - Hardware model verification – officially certified devices
  - Jailbreak/Rooted detection
  - OS version verification

- Failure actions
  - Quit Good for Enterprise
  - Force application download
  - Wipe enterprise data
  - Send report only

- Check Every
Compliance checks are run when Good for Enterprise or Good powered app is accessed

No separate useless “compliance” app

No use of “location/GPS” required – saves battery!!!

No requirement of cell radio or Wi-Fi – works when in airplane mode

Compliance rule values are updated by Good

- New device, OS version, or jailbreak/rooted detection mechanisms
- Example: iOS 5.1 showed up as soon as Apple released the IPSW on March 7th
Not high priority for our customers

- Device Remote Control
- Utilize GPS location or keep track of GPS logs
- Download phone call or SMS usage
Good does not provide device Anti-Virus/Malware

Good keeps sensitive data safe from malware
- Encrypted container goes above and beyond the default security (if available) – if device security compromised data is still secure
- App to app security provides protection for data leaking malware or even poorly designed apps
  - Example: IT decides what fields are sent to device’s contact list from corporate list – name and number for caller-id to work
- Secure “behind-the-firewall” architecture does not require VPN – limits exposure to network if device is infected
Good for Enterprise includes email/PIM functionality

Has features that do not exist in “native” apps and is getting better!
- Out of office
- Free/busy scheduling
- Integrated conference call dialing
- Integrated meeting location mapping

Usability enhancements coming soon
- MUCH faster email synchronization upon launch
- Notification enhancements – controlled by IT
- Further integration with “default” apps – send a photo to Good
- Corporate instant messaging, tasks and notes
- Proxy support for Secure Browser

Same user experience across platforms
- Less training, fewer “variations” to support, lighter helpdesk load
HIPAA
PCI
SOX
FIPS-140-2 certified compliant cryptography
Currently undergoing Common Criteria EAL 4 testing
Tested by DISA – developed STIG for implementing
US Army granted Good Certificate of Networthiness and Authority to Operate
US Air Force – Good is the only approved alternative to Blackberry
US Air Force Communications Agency – listed on the iTRM Approved Products List
Good Provides More Value Than MDM: Security

- Not limited by MDM controls at a device-level
  - Device password – may require complex password
  - Selective wipe can only remove email or apps pushed – full device wipe
  - Relies on default device/OS security – easily circumvented
  - Restricts/disables native features that could leak sensitive data (iCloud/iTunes/Box/DropBox etc.)

- Provides security enhancements at both the device and app level
  - Encrypted container to protect and separate corporate email/PIM and other sensitive data from personal data
  - App level password does not impact personal use of device
  - App level wipe allows IT to have confidence when removing sensitive data and does not impact personal data or apps
  - Rather than restrict, Good enables the personal use of iCloud, iTunes, social media and document sharing apps
Good Provides More Value Than MDM

- Higher Mobile Productivity
  - Fully protected end-to-end business workflow
    - Receive email attachment -> Open/Edit document in Quickoffice for Good -> Save in secure repository -> email reply/fwd new version

- Lower Overall TCO
  - Provides a single, cross-platform user experience – lower training/helpdesk or mobile device app costs
  - Allows for organization to disable EAS – lowers risk and IT management costs
  - Secure Browser – removes additional cost of VPN and IT management costs
  - Good Dynamics – internal and commercial apps: more secure
Questions?
Contact us:
- http://www.good.com
  - Videos – Beyond MDM
  - BYOD Whitepapers

Download your own 30-day free trial
- LOW TOUCH!! EASY!
Thank you!

International Legal Technology Association