Exploiting Mobile Technologies to Run a More Profitable Business

Steve Metzman • iBusiness Technologies

This session is eligible for 1.5 Continuing Education Hours.

To earn these hours you must:
– Have your badge scanned in and out at the door
– Attend 90% of this presentation
– Fill out the online evaluation for this session:
  www.necanet.org/NNSurvey2017

Copyright 2017 • iBusiness Technologies. Unauthorized use in full or part prohibited.
Let’s Demystify Mobile Device Management

Learn about deploying devices, methods to protect your assets and proprietary content.

Remote Management

Learn about managing devices; protecting your assets and proprietary content; restricting features, Apps and purchases; remote wiping of lost/stolen devices; company-issued vs. BYOD; location tracking.

Content

Identify the top MDM software companies, differences and prices starting at free. Also learn how to create multiple Apple IDs for device deployments without tying a credit card to each.

Integrating Device Management

Exploiting mobile technologies has become essential for any field-based business.

Remotely Wipe Sensitive Data

Remote lock and wipe in the event customer sensitive data is left on a job site!

Unified, Central Control

Manage your fleet of devices from one dashboard allowing you granular control.

Enforce Security Protocols

Deploy devices securely over the air — everything from passwords to location based security. You can even preload wifi and email settings.

Restrict Device Functions

Over the air device management, allowing everything from app removal to locking down the camera on devices.
Start Smart!

It is estimated that over 50% of IT projects fail due to poor planning. – CIO.com, 2016

“If you don’t know where you’re going, how can you expect to get there?” – Basil S. Walsh

Executive Support
Develop and communicate a clear and strategic plan before deploying.

Establish Clear Objectives
Design decisions, good and bad, are amplified with scale.

Basic Firm Requirements
Determine the needs of the firm and isolate those requirements from the wants.

Where to Start?

Plans are worthless. Planning is essential. – Dwight D. Eisenhower

1. Understand the deployment goals, develop a scope.
2. Define and communicate expected outcomes, make a plan for future communication.
3. Assess the existing infrastructure: LAN/WiFi density, VPN, server/storage resources, internet bandwidth.
4. Plan for user support and rollout – pilot users, what happens when it breaks?
5. Identify device policies, users & groups: Who gets the devices in what order? Training? Who purchases applications? What is the device backup strategy?
6. Purchase devices, order accessories and applications – if Apple, purchase via VPP.
7. Prepare for physical rollout: Unpack, check and initialize devices, transmit configuration payloads, verify.
9. Conduct device training – articulate deployment plan, goals and expected outcomes.
10. Expand distribution to remaining devices.
11. Verify deployment through dashboard.
12. Monitor to ensure program fidelity.
Process Overview

This example depicts a basic deployment of a Mobile Device Management server.

- A Configuration Profile containing Mobile Device Management server information is sent to the device. The user is presented with information about what will be managed and for whom by the server.
- The user installs the profile to opt in to the device being managed.
- Device enrollment takes place on the profile if it is installed. The server monitors the device and allows access.
- The server sends a push notification prompting the device to check-in for tasks or queries.
- The device connects directly to the server via HTTPS. The server sends commands or requests information.

iOS Deployment

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation</td>
<td>Associating a brand new device</td>
</tr>
<tr>
<td>Enrollment</td>
<td>Associating a device to an account to bring it under management.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Applying settings to a device via Configuration Profiles.</td>
</tr>
<tr>
<td>Security Management</td>
<td>Locking, resetting of a passcode, or wiping data from a device.</td>
</tr>
<tr>
<td>App Distribution</td>
<td>Making App Store or in-house apps available to end users.</td>
</tr>
<tr>
<td>eBook Distribution</td>
<td>Making iBookstore or in-house eBooks available to end users.</td>
</tr>
<tr>
<td>Inventory</td>
<td>Gathering a device's hardware, software or settings.</td>
</tr>
<tr>
<td>App Updates</td>
<td>Updating the apps on a device.</td>
</tr>
<tr>
<td>Backups</td>
<td>Backing up data from an iOS device to a computer.</td>
</tr>
<tr>
<td>Restore</td>
<td>Restoring an iOS device to a previous state.</td>
</tr>
<tr>
<td>iOS Updates</td>
<td>Updating the device to a newer version of iOS.</td>
</tr>
</tbody>
</table>
Compare & Contrast

Unified, Central Control
Restrict Device Functions

Device Functionality (iOS):
- Allow FaceTime
- Disallow sharing of managed documents with AirDrop
- Allow in-app purchases

Cross-Platform Restrictions:
- Allow use of camera
- Allow installing apps
- Allow screen capture

Security and Privacy:
- Allow automatic updates to certificate trust settings
- Allow user to accept untrusted TLS certificates
- Force encrypted backup

Enforce Security Protocols

Device Functionality (iOS):
- Allow app removal
- Allow configuring restrictions
- Allow “Erase All Content and Settings”

Windows Phone Specific:
- Allow WiFi
- Allow Bluetooth
- Allow use of external storage card
- Encrypt device internal storage

Additional Security:
- Enable “Single App” mode
- Enable Global HTTP proxy
- Enable web content filter
The Secret of Apple IDs with No Credit Card

Workaround via the App Store
Volume Purchase, Simplified Distribution of Apps

Questions

iBusiness Technologies
www.iBusiness-Tech.com
Steve.Metzman@iBusiness-Tech.com
877-565-3261

Up Next: Lunch on Event Lawn 1

Breakouts resume at 1:30

Don’t forget to fill out the online evaluation at
www.necanet.org/NNSurvey2017

Copyright 2017 • iBusiness Technologies. Unauthorized use in full or part prohibited.