



**Exploiting Mobile Technologies to Run a More Profitable Business**

Steve Metzman  
*President*  
*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](http://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 that 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.

◀ --- ▶

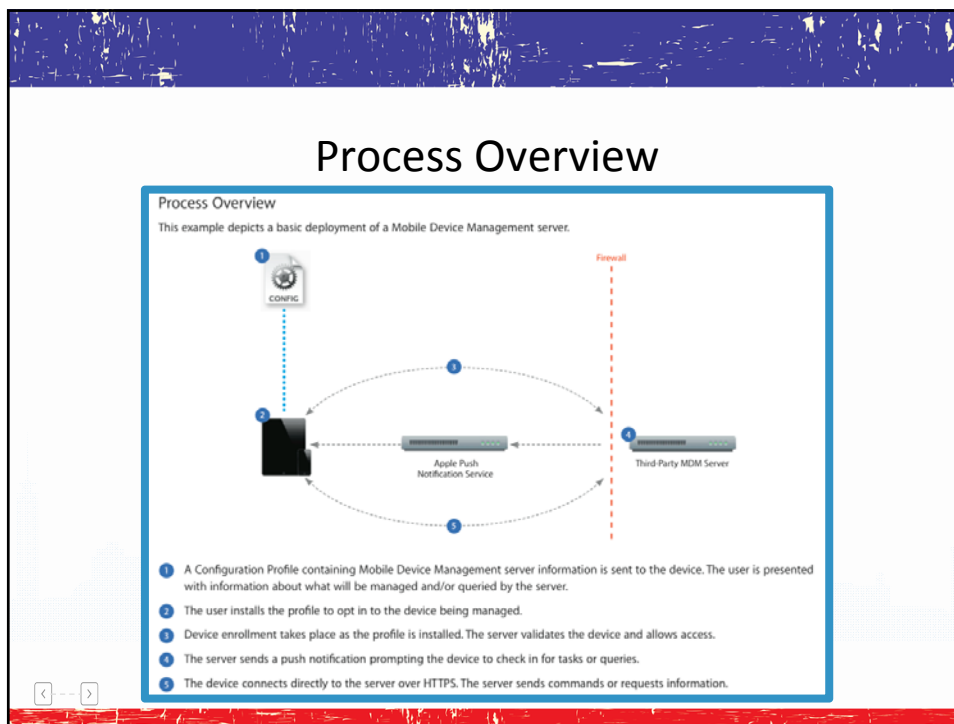
## Where to Start?

*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.
8. Distribute devices with sign-out documents.
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.



◀ --- ▶



## iOS Deployment

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

## Compare & Contrast

### MDM Comparison Chart

MOBI Wireless Management

**Enterprise mobile device management (MDM) software** is primarily a policy and configuration management tool for mobile handheld devices, such as smartphones and tablets based on smartphone OSs. It helps enterprises manage the transition to a more complex mobile computing and communications environment by supporting security, network services, and software and hardware management across multiple OS platforms. This is especially important as bring your own device (BYOD) initiatives become the focus of many enterprises. It can support corporate-owned as well as personal devices, and helps support a more complex and heterogeneous environment. The primary delivery model is on-premises, but it can also be offered as software as a service (SaaS) or through the cloud. Although some MDM vendors also support PCs, this Magic Quadrant focuses only on mobile capabilities.

	MobileIron	AirWatch	Fiberlink	Zenprise	Good	BoxTone	IBM	SAP	Symantec	Netify	McAfee	Sophos	SCIT	Tingee	LANDesk
<b>MOBI Supported</b>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<b>PACKAGING</b>															
SaaS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Appliance	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
Windows Software	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mac Software	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Unix Software	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Virtual Machine	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Retailer Theming	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
<b>LICENSING</b>															
Perpetual License	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
Recurring License	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

## Unified, Central Control

The screenshot displays a dashboard interface for mobile device management. At the top, there are navigation tabs for 'Business Technologies', 'Systems Manager', and 'Tag: All'. A search bar is present on the right. Below the navigation, there is a notification banner: 'New in Dashboard: ICMP Layer 3 Firewall Rules. Read more.' The main section is titled 'Client list' and shows a table with 495 clients. The table has columns for: #, Status, Name, Enrollment Date, Model, Connected, Connectivity, User, SSID, Serial, Battery, Phone #, Tags, Location, OS, Location (Selected), and Carrier network. The first row shows a client with ID 1, Status 'Enrolled', Name 'iPad mini', Enrollment Date 'Apr 11 2016', Model 'iPad mini', Connected 'Yes', Connectivity 'Wi-Fi', User '...', SSID '...', Battery '...', Phone # '...', Tags '...', Location 'Binghamton', OS 'iOS', Location (Selected) 'Binghamton', and Carrier network '...'.

## 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

The screenshot shows the Apple ID account management page. The 'Payment' link is circled in red. The page is divided into sections: Account, Security, Devices, and Payment. The Account section shows the Apple ID (11111@stevemetz.com) and Reachable At (11111@stevemetz.com). The Security section shows Password (Change Password...), Security Questions (Change Questions...), Rescue Email (Add a Rescue Email...), and Two-Step Verification (Add an extra layer of security to your account. Get Started...). The Devices section shows View Details. The Payment section shows Payment Method (credit card number, mm/yyyy, security code), Billing Address (Bob, Ginz), and a note: 'This payment method will be used when you make purchases in the iTunes Store, App Store, Apple Online Store, and more.' There are Cancel and Save buttons.

## Workaround via the App Store

The screenshot shows the 'Provide a Payment Method' form in the App Store. The form includes a 'Payment Type' section with buttons for VISA, MasterCard, American Express, PayPal, and None. Below this is a section for redeeming a code or gift certificate with an 'Enter Code' field. The 'Billing Address' section includes fields for Title, First name, Last name, Street, Apt., suite, box, City, State, Zip, and United States, as well as Area code and Phone. A note at the bottom states: 'Apple uses industry-standard encryption to protect the confidentiality of your personal information.'

## Volume Purchase, Simplified Distribution of Apps

**Business Store**  
Volume Purchase Program for Business

The Volume Purchase Program allows businesses to purchase iOS apps in volume and distribute the apps to their users. You can learn more about the program [here](#). To find an app, search for its name or App Store URL.

Purchase History DUNSF Sign Out

[Back to Store](#)

Payment Information Edit Payment Information

Recent Purchases

Latest Purchase. This is your most recently made purchase.

Order Date	Order	Name	Type	Order Total	Licenses	Codes
08/02/12	NGYLWZG45	<a href="#">Contact Wheel</a>	App	\$99.00	100 Codes	<a href="#">Download Spreadsheet</a>

## Questions

iBusiness Technologies  
[www.iBusiness-Tech.com](http://www.iBusiness-Tech.com)  
[Steve.Metzman@iBusiness-Tech.com](mailto: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](http://www.necanet.org/NNSurvey2017)

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