



**The Iam Lotus User Group**

# Choosing a Mobility Device Management (MDM) solution – it's not simple as pie

**Barb Skedel, Sherwin-Williams, Mobile Integration Administrator**  
**Gregg Eldred, NextStep Technologies, President**

*© 2013 by the individual speaker*





The Iam Lotus User Group



IamLUG 2013 Sponsors

© 2013 by the individual speaker



# What We'll Cover ...

---

- **What exactly is MDM?**
- **Review of Traveler**
- **MDM Objectives**
- **Cloud, on-premises, hybrid?**
- **Evaluating vendors**
- **Voice and data cost considerations**
- **Internal and External Applications**
- **Provisioning of devices**
- **Support considerations**
- **Self service considerations**
- **Observations from Sherwin Williams MDM project**
- **Conclusions**

# What exactly is MDM?

---

- **Policy Management**
- **Inventory Management**
- **Security Management**
- **Service Management**
- **Software Distribution**
- **Telecom Management**
- **Content Management**

# Quick review of Traveler

---

## Lotus Traveler 8.5.3

- **Has “MDM Features” but is NOT an MDM**
- **Could be “good enough”**
- **Features continue to move forward**

# Quick review of Traveler

**Lotus Traveler Device Settings : Default**

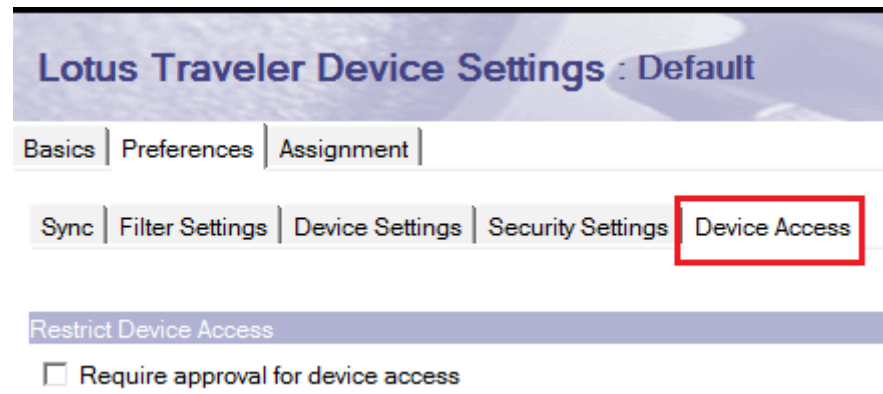
Basics | Preferences | Assignment |

Sync | Filter Settings | Device Settings | Security Settings | Device Access |

Windows Mobile | Nokia | Apple | Android |

Device Security		Violation Action
<input checked="" type="checkbox"/> Require device password		Enforce
<input type="checkbox"/> Prohibit ascending, descending and repeating sequences		
<input type="checkbox"/> Require alphanumeric value		
Minimum password length:	6	
Minimum number of complex characters:	0	
Auto lock period (maximum):	60 minutes	
Password expiration period:	0 days	
Password history count:	0	
<input checked="" type="checkbox"/> Wrong passwords before wiping device	6	
<input checked="" type="checkbox"/> Prohibit unencrypted devices		
<input type="checkbox"/> Prohibit camera		Enforce
<input checked="" type="checkbox"/> Prohibit devices incapable of security enablement		Enforce

# Quick review of Traveler



The screenshot shows the 'Lotus Traveler Device Settings : Default' page. It features a series of tabs for configuration: Basics, Preferences, Assignment, Sync, Filter Settings, Device Settings, Security Settings, and Device Access. The 'Device Access' tab is highlighted with a red rectangular border. Below the tabs, there is a section titled 'Restrict Device Access' which contains a single checkbox labeled 'Require approval for device access', which is currently unchecked.

Lotus Traveler Device Settings : Default

Basics | Preferences | Assignment |

Sync | Filter Settings | Device Settings | Security Settings | **Device Access**

Restrict Device Access

☐ Require approval for device access

# Traveler 9

Edit Settings Cancel

## Notes Traveler Device Settings : Default

Basics | Preferences | Assignment |

Sync | Filter Settings | Device Settings | Security Settings | Device Access |

Windows Mobile | Windows Phone | Nokia | Apple | Android | BlackBerry |

### Device Security

### Violation Action

☐ Require device password

Enforce

☐ Prohibit camera

Enforce

☐ Prohibit download of attachments

☐ Prohibit devices incapable of security enablement

Enforce



# Traveler 9

Save & Close Cancel

## Notes Traveler Device Settings : Default

Basics | Preferences | Assignment |

Sync | Filter Settings | Device Settings | Security Settings | Device Access |

### Synchronization Options ↑

### How to apply this setting:

Synchronize:



- ☒ Email
- ☒ Calendar
- ☒ ToDo
- ☒ Contacts
- ☒ Journal

☐ Lock value on device

### Auto Sync Options

### How to apply this setting:

Schedule:

Peak sync type	Every 15 minutes ▾	<input type="checkbox"/> Lock value on device
Off-peak sync type	Every 15 minutes ▾	<input type="checkbox"/> Lock value on device
Peak days	<input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input type="checkbox"/> Saturday <input type="checkbox"/> Sunday	<input type="checkbox"/> Lock value on device
Peak start time	08:00 AM 	<input type="checkbox"/> Lock value on device
Peak end time	05:00 PM 	<input type="checkbox"/> Lock value on device
Disable sync when battery low:	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Lock value on device
Connect when roaming:	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Lock value on device

# User and IT expectations for mobility

---

- **What does the user want?**

- Access PIM data, documents, applications
- Access at anytime from anywhere
- Freedom of choice

- **What does IT want?**

- Ability to secure corporate data on the device
- Business agility
- Lower costs
- Competitive advantage

# Defining your objective when looking for an MDM

**Your strategy should be to optimize the functionality and security of a mobile communication network while minimizing cost and downtime. The goals of each organization's mobile-device management deployment will vary and there is no one size fits all solution.**

**Developing a list of enterprise objectives:**

- **Define must have objectives**
- **Define nice to have objectives**
- **What devices am I going to support**

**Some examples of objectives:**

- 1. Ability to secure corporate data on device**
- 2. Functionality**
- 3. Reputation/reliability of vendor**
- 4. Vendor support, and not just from the pre-sales engineer**
- 5. Management capabilities**
- 6. Availability of a complete solution**
- 7. Flexibility to manage IT and user needs**
- 8. Reporting**

# What devices do I support today?

---

## What's your existing mobile device inventory look like today?

- BlackBerry
- iOS phones
- iOS tablets
- Android phones
- Android tablets
- Symbian
- Win Mobile

## What type of management am I providing to these devices today?

- Mail and PIM
- Applications
- Security

## Are these devices corporate-liable or individual liable?

# Corporate liable and/or BYOD considerations

---

## Corporate liable considerations:

- Will your organization be purchasing the devices for the user; how many are they allowed to request
- Configuration of the device will be handled by corporate IT
- What access will these devices be allowed
- Corporate mail and PIM
- Applications purchased by IT for use on devices (such as Pages, Numbers, PocketCloud)
- Access to internal websites

# Corporate liable and/or BYOD considerations

---

## BYOD considerations:

The challenge here is that most devices were designed for consumer market and not enterprise.

- Will individual be liable for the purchase cost and data plan cost or will a stipend be provided
- What involvement will IT have in configuration of the device(s)
- What support will IT provide to the user
- What access will these devices be given

# Corporate liable and/or BYOD considerations

---

**Different policies for corporate liable vs. individual liable devices? Some examples of individual liable rules:**

- Corporate devices are allowed access to internal corporate websites**
- Individual liable must sign off on corporate compliance document**
- If the person signs off on the corporate compliance document, they can also get their mail and PIM info on their devices**
- IT has the right to enterprise and/or remote wipe the device if it does not meet the compliance rules**
- Individual must agree to surrender the device if required for e-discovery or internal security audit**

# Who needs to be involved in defining the need of a MDM

---

- **Security**
- **Network**
- **Messaging**
- **Application development**
- **Procurement**
- **Human Resources**
- **Legal**



# What device platforms are involved?

---

- **iOS**
- **Android**
- **Symbian**
- **Windows Mobile**
- **BlackBerry**

# What about security?

- Boils down to device compliance
- If the user does x on the device, what actions should be performed
  - Remove rights to mail/PIM
  - Remove MDM application itself (including the mail, applications, etc. that were sent down to the device via the MDM)
  - Notify the user
  - Combination of the above
- Do you care about jailbroken devices
- Can a user copy/paste from corporate mail to a personal mail account
- What features of the device should be disabled; can this vary depending on different user profiles
- Required applications/blacklisted applications
- Are you going to limit what device models and/or OS can be used
- Get your security folks involved in setting up your compliance



# Cloud, on-premises, or combination of both

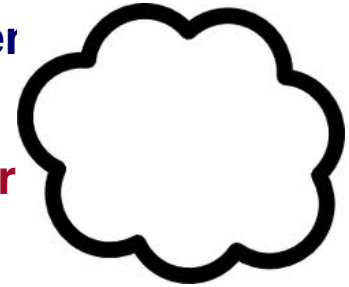
- **Cloud (aka software as a service) – hosted environment**

- **PROS:**

- **Updates are done by provider; no need for hardware**

- **CONS:**

- **Updates are done by provider on their schedule**



- **On premises**

- **PROS:**

- **You determine when to do updates**

- **CONS:**

- **Need hardware; administrator to manage system.**



- **Some MDM solutions provide a hybrid solution when some components are cloud and others are in your data center**

# What directory service should I use?



- Most MDMs provide you an option of where user information is pulled from
- Used for enrollment/authentication into the system
- Options can be self-contained within the MDM itself, integration with Active Directory, Open LDAP, or the Domino Directory
- Does the directory you choose cause you to add additional server components to your MDM environment
- How secure is the solution (what ports do I need to have open and what's the potential exposure into your directory environment from the outside)
- Are the enrollment/authentication requests into your directory structure encrypted?
- How does your security group feel about this if it is hosted solution

# Evaluating vendors

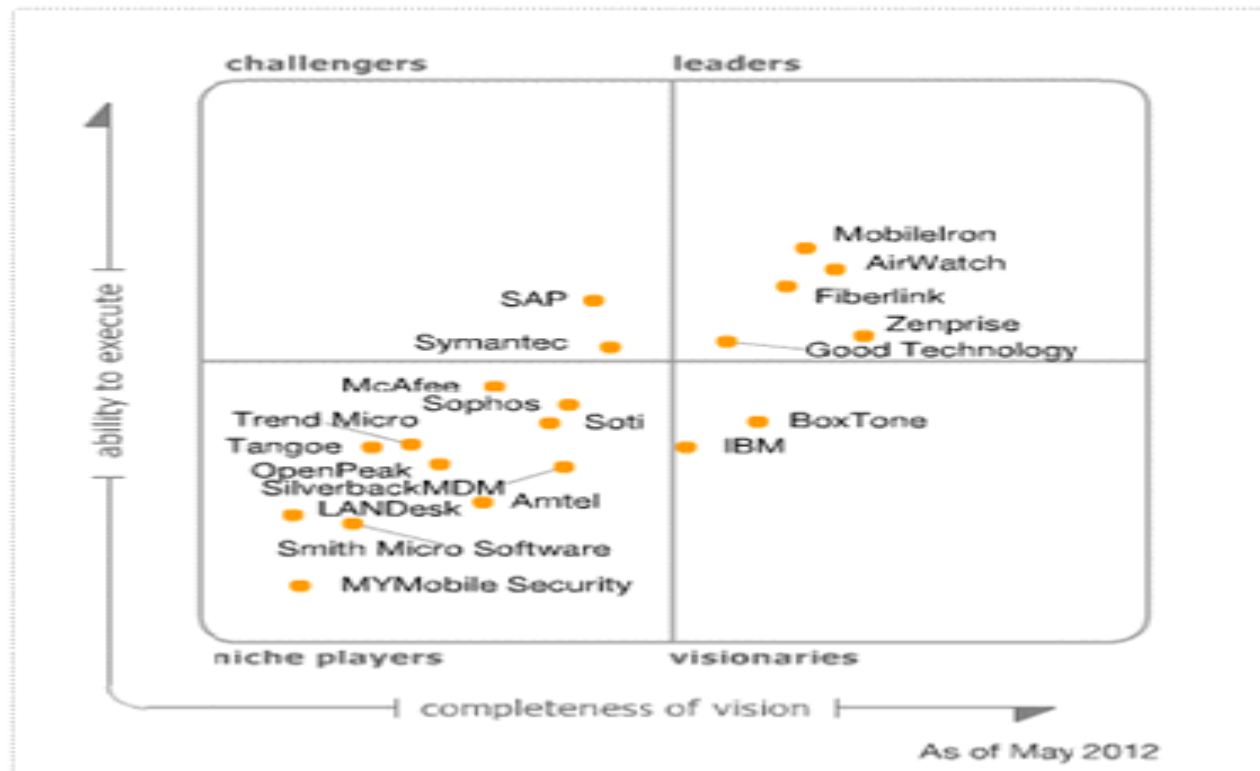
- **Gartner, peers, carriers**
- **Cloud, on-premises, hybrid**
- **Pilot each with a small set of users**
- **Involve potential MDM Administrators**
- **Do Not Forget to test support**
- **Numbers don't lie – create matrix, weight scores, tally scores**



# Evaluating Vendors

## Magic Quadrant

**Figure 1.** Magic Quadrant for Mobile Device Management Software



Source: Gartner (May 2012)

# Voice and data cost considerations

---

- **Able to see/manage voice and data**
- **Most MDM's allow control of roaming**
- **BYOD may transfer costs to employees**
- **Fewer corporate owned devices may affect corporate plan**
- **SMS may not be covered**



# Access to internal applications

## Corporate devices – Part of deployment plan

### BYOD:

- Determine need
- Deploy VPN client
- Consider wireless needs
- Consider authentication requirements
- Decide BYOD has no access





# Use of external applications

- **Create Policies to manage iTunes/Play applications**
- **Will you allow file sharing (Dropbox, Box.net)?**
- **Will you allow streaming?**
- **Slingbox, HBO, NFL/MLB/NBA/NHL/Soccer?**
- **Deploy a set of common apps (Angry Birds, Calculator, Weather)**
- **Create alerts. Discuss with appropriate resources**



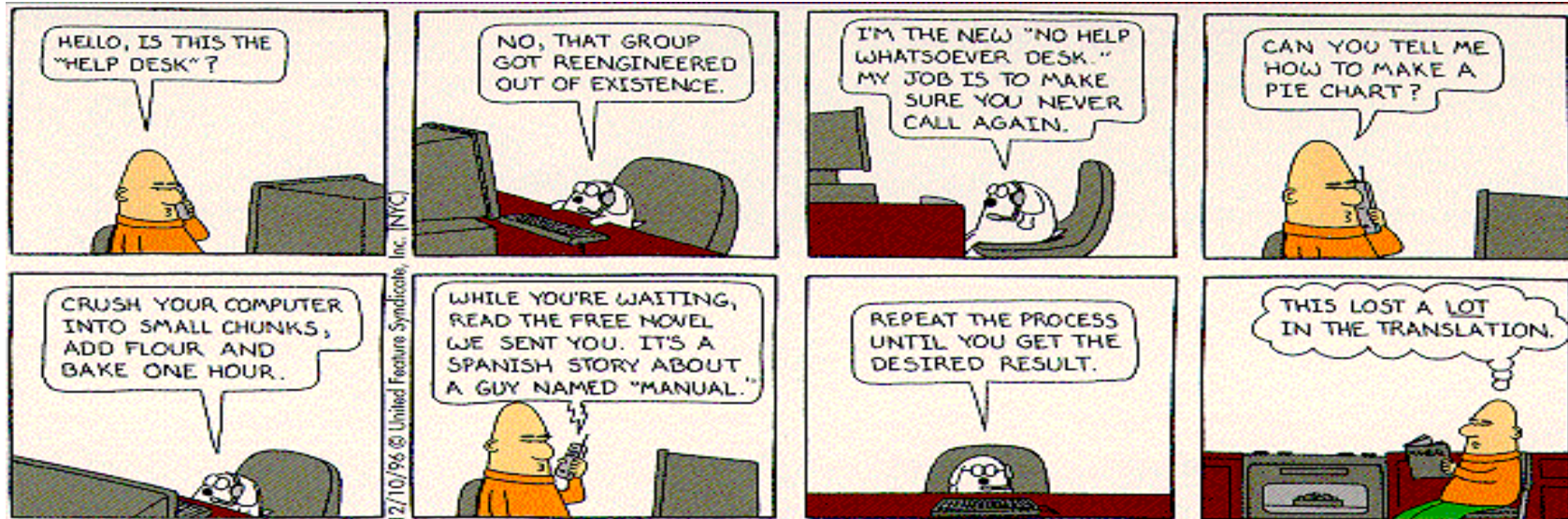
# Provisioning of devices

- Will IT be provisioning the device for the user or will you have the end-user provision their own device
- What information do you need to provide the user if provisioning themselves
- Does the user have to download the application from an App Store or can you push the application to the device as part of the MDM
- What if the user already has profiles on their device for mail, wifi, etc.
- What level of support will IT offer the user when provisioning their device
- Does the user have to add an additional data plan from their carrier depending on the MDM chosen?



# Helpdesk support considerations

- Will addition to staff be needed
- Training your helpdesk
- Determine what rights your helpdesk staff should have in the MDM
- What level of support will the helpdesk provide
- What hours of support will be available to the user



# Self service considerations



- **Will you provide the end-user the ability to manage their devices**
- **What can the end-user do**
  - **Enroll their own devices**
  - **Change profiles**
  - **Submit a support request**
  - **Lock their device**
  - **Find a device**
  - **Clear the password**
  - **Wipe enterprise data/wipe entire device**

# Observations from Sherwin Williams MDM project

- The best laid plans never work as you think they should
- Get everyone involved ASAP (security, networking, HR, legal, procurement)
- I can't put enough emphasis on piloting the choices because you really don't know how well they match your requirements until you do
- Avoid scope creep – make sure everyone is aware of the requirements you defined and stick to that plan
- Educate the support staff as well as the end user



# Conclusions

---

- **Users want flexibility and choice**
- **The line between personal and corporate data on a device is getting blurry**
- **Mobile users increase business agility, competitiveness and productivity**
- **Users will find a way to use their personal devices anyway, thus increasing the risk if not managed**
- **Educate your users**
- **If BYOD, measure ROI**

# Q&A



"Harris, when I said 'any questions' I was using only a figure of speech."

# Resources

---

## **Mobile Device Management – not what it used to be**

[http://www.biztechmagazine.com/sites/default/files/108281-wp-mobile\\_device-df\\_1.pdf](http://www.biztechmagazine.com/sites/default/files/108281-wp-mobile_device-df_1.pdf)

## **Gartner: Cloud-based mobile device management (MDM) getting hot**

<http://www.networkworld.com/news/2012/060612-gartner-mdm-259900.html>

## **Surveying the landscape of today's mobile device security risks**

<http://www.computerweekly.com/news/2240146347/Surveying-the-landscape-of-todays-mobile-device-security-risks>

## **Airwatch**

Mobile Device Management – Where are we heading

Mobile IT scorecard



# Follow Up



**Barbara Skedel**

**Email:** [bskedel@sherwin.com](mailto:bskedel@sherwin.com)

**Twitter:** [@babsskedel](https://twitter.com/babsskedel)

**LinkedIn:** <http://www.linkedin.com/pub/barb-skedel/0/778/463>

**Gregg Eldred**

**Email:** [gregg.eldred@ns-tech.com](mailto:gregg.eldred@ns-tech.com)

**Twitter:** [@geldred](https://twitter.com/geldred)

**LinkedIn:** <http://www.linkedin.com/in/geldred>