Mobile Device Management with Microsoft System Center Configuration Manager and Windows Intune

Roger Morell
Four sessions this week on unified device management

- Infrastructure Setup
  - PCIT-B216 – Infrastructure Deployment for Mobile Device Management with Microsoft System Center Configuration Manager and Windows Intune

- Settings and Enrollment
  - PCIT-B317 - Enrollment and Management of Mobile Devices with Microsoft System Center Configuration Manager and Windows Intune

- Application Management
  - PCIT-B323 - Application Management with Microsoft System Center Configuration Manager and Windows Intune

- Data Protection
  - PCIT-B325 - Protecting Your Corporate Data with Microsoft System Center Configuration Manager and Windows Intune
Session Objectives And Takeaways

Session Objective:
- Outline System Center 2012 R2 Configuration Manager and Windows Intune support for mobile device management
Agenda

- Getting started
- Signing into Windows Intune service
- Active Directory, DirSync and ADFS
- Creating Configuration Manager objects
- Setting up a lab or POC environment
- Troubleshooting
Empowering people-centric IT

Mobile Device Management

Desktop Virtualization

Hybrid Identity

Access and information protection
Facing the challenges in keeping users productive while protecting company information
Users

Devices

Apps

Data

Realitywant
Mobile Device Management

Unify your environment
On-premises and cloud-based management of devices within a single console.
Simplified, user-centric application management across devices
Comprehensive settings management across platforms, including certificates, VPNs, and wireless network profiles

Enable users
Access to company resources consistently across devices
Simplified registration and enrollment of devices
Synchronized corporate data

Protect your data
Protect corporate information by selectively wiping apps and data from retired/lost devices
A common identity for accessing resources on-premises and in the cloud
Identify which mobile devices have been compromised
Selecting the Management Platform

Unified Device Management
System Center 2012 R2 Configuration Manager with Windows Intune

Build on existing Configuration Manager deployment
Full PC management (OS Deployment, Endpoint Protection, application delivery control, rich reporting)
Deep policy control requirements
Scale to 300,000 devices
Extensible administration tools (RBA, PowerShell, SQL Reporting Services)

Cloud-based Management
Standalone Windows Intune

No existing Configuration Manager deployment
Simplified policy control
Less than 28,000 devices and 7,000 users
Simple web-based administration console
Windows Intune integrated with System Center 2012 R2 Configuration Manager

- Windows PCs (x86/64, Intel SoC), Windows to Go, Windows Embedded
- Mac OS X
- Windows 8 RT, Windows 8.1, Windows Phone 8.x
- iOS, Android

IT

Single Admin Console

Microsoft System Center 2012 R2 Configuration Manager

Windows Intune
Integration points of Configuration Manager and Windows Intune

- Windows Intune provides cloud based infrastructure to provide settings management and software distribution to mobile devices
- All administrative tasks are performed via Configuration Manager console
Platform Support

“Modern” Platforms

- Windows 8 RT
- Windows Phone 8 (and 8.1)
- iOS (5.x, 6.x, 7.x)
- Android (2.3+ via EAS)
- Android (4.0+ via native agent)
- Windows 8.1 (x86/x64 and RT)

*Highlighted items available only in System Center 2012 R2 Configuration Manager*

Features fully integrated into ConfigMgr

- Over the air device enrollment
- Available user targeted applications
- User and device settings management
- Device inventory
- Remote device retirement
- Remove device wipe (full and selective)
- Company branding
- Web apps and remote apps
- Required application deployment
- VPN/Wi-Fi/certificate profiles
- Additional settings
## Platform Support in ConfigMgr R2

<table>
<thead>
<tr>
<th>OS Platform</th>
<th>Management Agent</th>
<th>End User Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows 8.1 PC</strong></td>
<td><strong>ConfigMgr Agent</strong></td>
<td><strong>Software Center/Application Catalog / ConfigMgr Company Portal app</strong></td>
</tr>
<tr>
<td></td>
<td>Or <strong>Management Agent (OMA-DM)</strong></td>
<td><strong>Windows Intune Company Portal app</strong></td>
</tr>
<tr>
<td>Windows PC (Win8,Win7,Vista,XP)</td>
<td>ConfigMgr Agent</td>
<td>Software Center/Application Catalog</td>
</tr>
<tr>
<td>Windows RT</td>
<td>Management agent (OMA-DM)</td>
<td>Windows Company Portal app</td>
</tr>
<tr>
<td>Windows Phone 8.x</td>
<td>Management agent (OMA-DM)</td>
<td>Windows Phone 8 Company Portal app</td>
</tr>
<tr>
<td><strong>iOS</strong></td>
<td>Apple MDM Protocol</td>
<td><strong>Native iOS Company Portal App</strong></td>
</tr>
<tr>
<td><strong>Android</strong></td>
<td><strong>Android MDM agent (OMA-DM)</strong></td>
<td><strong>Native Android Company Portal App</strong></td>
</tr>
<tr>
<td>Mac</td>
<td>ConfigMgr Agent</td>
<td>Limited self service experience</td>
</tr>
<tr>
<td>Linux/Unix</td>
<td>ConfigMgr Agent</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Getting Started
Overview of Process
1. Create Windows Intune Account
2. Add Public DNS details
3. Verify Public Domain UPNs for users
4. AD Federation Services (ADFS 2.0)
5. AD Directory Synchronization
6. Connect Configuration Manager to Windows Intune
Create Windows Intune Account

- This can be performed as a Volume License agreement, through those normal channels.
- If your company does not have a volume license agreement for Configuration Manager you may create a Windows Intune subscription directly from www.WindowsIntune.com.
- Once complete, use the newly created admin account to login to the Windows Intune Account Portal account.manage.microsoft.com.
Create Verifiable Public Domain

- To ensure users will synchronize correctly, create a verified public domain within Windows Intune Account Portal.
  - This is a public domain for the company, something like company1.com
  - This domain must be able to be verified as a registered domain by an external source

- For device enrollment ensure you have a public DNS CNAME record directing EnterpriseEnrollment to manage.microsoft.com
Verify User Details and Perform AD User Discovery

Ensure users that will be managed have this Public Domain as their primary User Principal Name (UPN) in Active Directory.

To add UPNs for each user, either edit via ADSI or script, similar to that shown in here: [http://blogs.technet.com/b/heyscriptingguy/archive/2004/12/06/how-can-i-assign-a-new-upn-to-all-my-users.aspx](http://blogs.technet.com/b/heyscriptingguy/archive/2004/12/06/how-can-i-assign-a-new-upn-to-all-my-users.aspx)

Once confirmed, perform AD User Discovery in Configuration Manager
Deploy and Configure AD Federation Services

Not required but strongly recommended!

- When you set up single sign-on (also known as identity federation), your users can sign in with their corporate credentials to access the services in Windows Intune.

- Follow the Steps outlined in the Windows Intune Account Portal, under Users.


Deploy and Configure AD Directory Synchronization

• Next, configure the on-premise AD Directory Synchronization with Microsoft Online.

• To deploy and configure DirSync follow the steps outlined in the Windows Intune Account Portal (account.manage.microsoft.com).

• Select Users, and then select the option to Setup Active Directory® synchronization. This will allow Intune to retrieve the user details from Microsoft Online.

• TechNet series on DirSync that outlines the entire set of steps needed.

• DirSync Password Synchronization is available as an alternative for those who want a single password for on-prem and cloud, but can’t or don’t want to implement ADFS (http://technet.microsoft.com/en-us/library/dn246918.aspx)
Reset User Microsoft Online Password

- Once configured, AD DirSync will happen immediately and then every 3 hours.
  - User should then be visible in the Windows Intune Account Portal (in the Users node) – shown in previous slide

- If not using ADFS, need to set a Microsoft Online password for each user:
  - In order for the users to be able to login into the Windows Intune service (and Microsoft Online), they need a Microsoft Online/Azure AD password set
  - You may perform these activities for an individual user or in bulk via the Windows Intune Account Portal. Or leverage PowerShell to programmatically activate them. Details in the link below
  - [http://aka.ms/aadposh](http://aka.ms/aadposh)
Connecting to Windows Intune Account Portal

Jim Dempsey
Creating Configuration Manager Objects
Functions of Configuration Manager Windows Intune Objects

Windows Intune Subscription, used by admin to:
1. Retrieve certificate needed by connector to connect to Windows Intune Service (background process)
2. Define User Collection that enables members to enroll mobile devices
3. Define and configure mobile platforms organization wants to support

Windows Intune Connector
- Connects to Windows Intune Cloud Service
  - Sends policy for Settings Mgt and Software Distribution
  - Receives state/status messages back from clients

Windows Intune Service (not visible to admin)
- Contains DMP like functionality
  - MP with local DB for storage of Policies
  - Gateway/Proxy to communicate to Mobile Devices
## Platforms and Certificates/Keys

<table>
<thead>
<tr>
<th>Platform</th>
<th>Certificates or keys</th>
<th>How you obtain</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>*Not required for domain-joined Windows Enterprise computers</td>
</tr>
<tr>
<td>iOS</td>
<td>Apple Push Notification service certificate</td>
<td>To enable app management for iOS, you must follow these steps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Download a Certificate Signing Request from Windows Intune. This certificate signing request lets you apply to Apple's certification authority for an Apple Push Notification service certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Request an Apple Push Notification service certificate from the Apple website.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To Download a Certificate Signing Request from Windows Intune</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In the Configuration Manager console, click Administration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In the Hierarchy Configuration, right-click Windows Intune Subscriptions and select Create APNs certificate request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Select a location and then click Download.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In the Windows Intune sign in page, enter your organizational account and password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• After you sign in, the certificate signing request is downloaded to the location that you specified.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To request an Apple Push Notification service certificate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Connect to the Apple Push Certificates Portal.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sign in and continue in the wizard.</td>
</tr>
<tr>
<td>Android</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
Creating Windows Intune Subscription & Connector in Configuration Manager

Jim Dempsey
Lab Considerations and Troubleshooting
Setting up a Lab

Things to consider when deploying a lab environment

- Sign up for Windows Intune trial account (30 days)
- AD DirSync is still needed
- Default domain is Onmicrosoft.com, modify on-prem UPN
- Download Support Tool for Windows Intune Trial Management of Window Phone 8
Lab Setup

Jim Dempsey
Basic Troubleshooting

- **Users:**
  - Log: CloudUserSync.log

- **Policies:**
  - Log: DMPUploader.log

- **Registration/Compliance:**
  - Log: DMPDownloader.log

- **Content:**
  - Log: OutgoingContentManager.log
Scenario: Fail to sign in for subscription

• Errors on sign in popup or blank page:
  • Verify that IE trusts manage.microsoft.com and login.microsoftonline.com
  • Make sure JavaScript is allowed for above pages

• Credentials/User not recognized
  • Make sure credentials are correct and the account is the tenant admin

• Access denied popup
  • Management authority was already set to Intune

• This account is already managed
  • This account is already on-boarded. Continuing will invalidate the previous environment!
Scenario: Nobody can enroll

- **Connector components are not working**
  - Forgot to install connector role after creating subscription?
  - Make sure the machine with the connector role has internet access
  - Make sure correct device platforms in subscription are enabled
  - Check DMPUploader.log for errors
  - Check that users are enabled for MDM (Cloud user group not empty, etc.)
    - Tenant admin should always be able to enroll

- **Auto-Discovery is not working**
  - Make sure CName was created, use browser/dnslookup to validate

- **WinPhone8, WinRT fail to enroll**
  - Make sure active authentication is allowed for your account
Scenario: Specific user cannot enroll

- User is not set to MDM licensed in Intune
  - Check if users is synced to account.manage.microsoft.com
  - Check if UPN is correct
  - Check if user is discovered in ConfigMgr with correct UPN
  - Check if user is in cloud user collection used in subscription
  - Check CloudUserSync.log for errors for this user

- User already enrolled 10 devices
  - Use ConfigMgr console or portal.manage.microsoft.com to delete unused devices

- User was just created/synced
  - Make sure that user has Intune license in IAP
  - Run collection evaluation for cloud user collection in ConfigMgr
  - There is a potential delay between users showing up in IAP and in Intune DataCenter
Scenario: Enrolled devices don’t show up

• Registration message is invalid
  • Check DMPDownloader.log for RDX messages, errors
  • Check DDM.log for failures
  • Check if user has CloudUserID and it matches with RDX message

• Messages get lost
  • If you just onboarded (1 day) and used the account previously somewhere else, make sure that old connector was uninstalled
Scenario: User cannot get application

- Make sure that app is deployed to the correct users and content is distributed to manage.microsoft.com
- Check for content was uploaded in outgoingcontentmanager.log
- Check for content policy was uploaded in dmpuploader.log
Wrap Up
How can my customer get this for Configuration Manager 2007?

- Deploy a stand-alone primary site (ConfigMgr 2012)
- Configure unified device management integrated with Windows Intune on the new site
- ConfigMgr 2007 and ConfigMgr 2012 console can be installed side by side on the same computer
- When ready to move completely to ConfigMgr 2012, deploy additional servers (if necessary) and perform migration
In Review: Session Objectives And Takeaways

**Session Objective:**
- Outline System Center 2012 R2 Configuration Manager and Windows Intune support for mobile device management

**Key Takeaways:**
- A better understanding of the configuration requirements to manage mobile devices
- Knowledge of setup procedures required to deploy the solution
**Mobile Device Management Review**

**Unify your environment**
- On-premises and cloud-based management of devices within a single console.
- Simplified, user-centric application management across devices
- Comprehensive settings management across platforms, including certificates, VPNs, and wireless network profiles

**Enable users**
- Access to company resources consistently across devices
- Simplified registration and enrollment of devices
- Synchronized corporate data

**Protect your data**
- Protect corporate information by selectively wiping apps and data from retired/lost devices
- A common identity for accessing resources on-premises and in the cloud
- Identify which mobile devices have been compromised
Enterprise Mobility Suite

EMS will enable customers with:

**Hybrid Identity Management**

*Enabled via Azure Active Directory Premium:*
- Group management & Self Service Password Reset
- Security audit reports & MultiFactor Authentication
- Connection between AD / Azure AD

**Mobile Device Management**

*Enabled via Windows Intune:*
- Mobile device settings management
- Mobile app management
- Selective wipe

**Data Protection**

*Enabled via Azure Rights Management Service:*
- Information protection
- Connection to on-premises assets

Enterprise Agreement Prices starting at $4 per user per month*

* Limited time EA Level A promo pricing. Requires 250 seat minimum purchase and underlying CAL Suite license (CoreCAL/ECAL/BridgeCAL)
## Breakout Sessions

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FDN02</td>
<td>Enabling Enterprise Mobility with Windows Intune, Microsoft Azure, and Windows Server</td>
<td>Mon, May 12 11:00 AM</td>
</tr>
<tr>
<td>PCIT-B311</td>
<td>What's New in Enterprise Management with Microsoft System Center Configuration Manager and Windows Intune</td>
<td>Mon, May 12 1:15 PM</td>
</tr>
<tr>
<td>PCIT-B215</td>
<td>What's New in Microsoft System Center 2012 R2 Configuration Manager Infrastructure</td>
<td>Mon, May 12 3:00 PM</td>
</tr>
<tr>
<td>PCIT-B410</td>
<td>Microsoft System Center 2012 Configuration Manager: MVP Experts Panel</td>
<td>Mon, May 12 4:45 PM</td>
</tr>
<tr>
<td>PCIT-B216</td>
<td>Infrastructure Deployment for Mobile Device Management with Microsoft System Center Configuration Manager and Windows Intune</td>
<td>Tue, May 13 8:30 AM</td>
</tr>
<tr>
<td>PCIT-B317</td>
<td>Enrollment and Management of Mobile Devices with Microsoft System Center Configuration Manager and Windows Intune</td>
<td>Tue, May 13 1:30 PM</td>
</tr>
<tr>
<td>PCIT-B320</td>
<td>Microsoft System Center Configuration Manager Community Jewels</td>
<td>Tue, May 13 5:00 PM</td>
</tr>
<tr>
<td>PCIT-B323</td>
<td>Application Management with Microsoft System Center Configuration Manager and Windows Intune</td>
<td>Wed, May 14 8:30 AM</td>
</tr>
<tr>
<td>PCIT-B325</td>
<td>Protecting Your Corporate Data with Microsoft System Center Configuration Manager and Windows Intune</td>
<td>Wed, May 14 10:15 AM</td>
</tr>
<tr>
<td>PCIT-B340</td>
<td>What's New with OS Deployment in Configuration Manager and the Microsoft Deployment Toolkit</td>
<td>Wed May 14 5:00 AM</td>
</tr>
<tr>
<td>PCIT-B336</td>
<td>Managing Mac OS X Clients and Linux Servers Using Microsoft System Center Configuration Manager</td>
<td>Thu May 15 8:30 AM</td>
</tr>
<tr>
<td>PCIT-B339</td>
<td>How Microsoft IT Manages Their Microsoft System Center Configuration Manager Application Lifecycle with Zero Touch</td>
<td>Thu, May 15 10:15 AM</td>
</tr>
<tr>
<td>PCIT-B333</td>
<td>How Microsoft IT Solves BYOD Using Microsoft System Center 2012 R2 Configuration Manager and Windows Intune</td>
<td>Thu, May 15 1:00 PM</td>
</tr>
</tbody>
</table>
## Related content

### Instructor Led Labs

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Time</th>
</tr>
</thead>
</table>
| PCIT-IL200 | Introduction to Microsoft System Center 2012 R2 Configuration Manager | Mon, May 12 3:00 PM  
              |                                                                  | Wed, May 14 5:00 PM          |
| PCIT-IL201 | Upgrading from Configuration Manager 2012 SP1 to Microsoft System Center 2012 R2 Configuration Manager | Thu, May 15 10:15 AM          |
| PCIT-IL300 | Deploying Windows 8.1 to Bare Metal Clients                          | Wed, May 14 1:30 PM  
              |                                                                  | Thu, May 15 1:00 PM          |
| PCIT-IL305 | Basic Software Distribution with Microsoft System Center 2012 R2 Configuration Manager | Tue, May 13 5:00 PM  
              |                                                                  | Wed, May 14 3:15 PM          |
| PCIT-IL306 | Implementing Endpoint Protection in Microsoft System Center 2012 R2 Configuration Manager | Tue, May 13 10:15 AM  
              |                                                                  | Thu, May 15 8:30 AM          |
| PCIT-IL307 | Managing Microsoft Software Updates in Microsoft System Center 2012 R2 Configuration Manager | Tue, May 13 1:30 PM  
              |                                                                  | Wed, May 14 8:30 AM          |
| PCIT-IL308 | Migrating from Configuration Manager 2007 to Microsoft System Center 2012 R2 Configuration Manager | Wed, May 14 10:15 AM         |
# Related content

## Hands On Labs

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCIT-H302</td>
<td>Deploying a Microsoft System Center 2012 R2 Configuration Manager Hierarchy</td>
</tr>
<tr>
<td>PCIT-H303</td>
<td>Deploying Microsoft System Center 2012 R2 Configuration Manager</td>
</tr>
<tr>
<td>PCIT-H304</td>
<td>Deploying Windows 8.1 to Bare Metal Clients</td>
</tr>
<tr>
<td>PCIT-H309</td>
<td>Implementing App-V 5.0 in Microsoft System Center 2012 R2 Configuration Manager</td>
</tr>
<tr>
<td>PCIT-H310</td>
<td>Implementing Endpoint Protection in Microsoft System Center 2012 R2 Configuration Manager</td>
</tr>
<tr>
<td>PCIT-H311</td>
<td>Implementing Linux Clients in Microsoft System Center 2012 R2 Configuration Manager</td>
</tr>
<tr>
<td>PCIT-H312</td>
<td>Implementing Role-Based Administration in Microsoft System Center 2012 R2 Configuration Manager</td>
</tr>
<tr>
<td>PCIT-H314</td>
<td>Managing Clients with Microsoft System Center 2012 R2 Configuration Manager</td>
</tr>
<tr>
<td>PCIT-H315</td>
<td>Managing Content in Microsoft System Center 2012 R2 Configuration Manager</td>
</tr>
<tr>
<td>PCIT-H316</td>
<td>Managing Software Updates in Microsoft System Center 2012 R2 Configuration Manager</td>
</tr>
</tbody>
</table>
Resources

Channel 9

Sessions on Demand
http://channel9.msdn.com/Events/TechEd

TechNet

Resources for IT Professionals
http://microsoft.com/technet

Learning

Microsoft Certification & Training Resources
www.microsoft.com/learning

msdn

Resources for Developers
http://microsoft.com/msdn
Complete an evaluation and enter to win!
Evaluate this session

Scan this QR code to evaluate this session.