Modernize your Windows Management with Microsoft Intune

Presented by Max Fritz & Doug Wilson
Systems Consultants, Now Micro
Now Micro is a Consulting & Device Life Cycle Management company

Now Micro’s Consulting Practice focuses on helping organization deliver the best end user experience by designing and implementing the most robust Systems Management, Cloud Productivity, and Identity Management solutions available.
Microsoft 365

Vision: Unified management across users, devices, apps and services.
Microsoft Education
Empowering students today to create the world of tomorrow

Enabling the right environment for better learning outcomes
An affordable and accessible learning platform
Modern tools for classroom collaboration
Experiences that spark creativity
Bridging the Classic & Modern Workplaces
The Promises of Modern Management

Modern Workplace
- Work from anywhere
- Choose the device you want or bring your own
- Quick, friendly out-of-box experience
- Self-service

Cloud IT
- Integrated and cloud-based security
- Simpler application delivery through Store/SaaS
- Data intelligence for better business insights

Lower TCO
- Minimize on-prem infrastructure costs
- Unified identity, device and app management
- Self-service deployment without imaging
Simplify Windows 10 management and lower TCO with EMS

**Simplified management & security**
Embrace cloud-based management and transition at your pace while staying in control.

- Agentless
- Unified identity, device and O365 ProPlus mgmt.
- Office 365 ProPlus MGMT
- Integrated data protection

**Self-service deployment**
Make any new PC enterprise-ready via a simple self-service experience.

- Sign in with contoso.microsoft.com
  - email@contoso.com
  - Next

- Automatically configure devices when your users log in with their company credentials.

**Always up to date**
Deliver the latest features and security.

- Cloud updates mean you don’t need to have on-premise update servers.
- Control what updates are deployed, to whom and when.

**Proactive insights**
Get ongoing proactive insights to diagnose and fix issues before they happen.

- Use cloud intelligence to upgrade Windows 10 and Office 365 ProPlus with confidence.
Paths to Modern Management

Cloud-first

Big Switch Transition

Group by Group Transition

Iterative ("Co-management")
Co-Management Architecture With ConfigMgr and Intune

- Azure portal
- ConfigMgr console
- ConfigMgr Site Servers
- Mobile devices
- Windows 10 AD Domain-joined & AAD Joined
- Windows 7/8.x
How to get to co-management

Existing ConfigMgr managed devices

- ConfigMgr agent
- AD Domain Joined

- ConfigMgr agent
- AD Domain Joined
- AAD Joined

- ConfigMgr agent
- Intune MDM
- AD Domain Joined
- AAD Joined

New devices

- AutoPilot

- Intune MDM
- AD Domain Joined
- AAD Joined

- ConfigMgr agent
- Intune MDM
- AD Domain Joined
- AAD Joined
Bridging to Modern Management

Adopt & Connect
- ConfigMgr Content Delivery to Cloud Content Delivery
- Win32 to Modern Apps
- Kerberos to Modern Auth
- GPO to MDM Policy
- Imaging to Signature Image
- WSUS to WUfB

Transition to Modern
- Adopt Windows 10
- Adopt Office 365/ProPlus
- AD/AAD connect

Modernizing with a co-management bridge
Bridging to Modern Management

Adopt Windows 10
Adopt Office 365/ProPlus
AD/AAD connect

GPO to MDM Policy
Imaging to Signature Image
WSUS to WUfB
Kerberos to Modern Auth
Win32 to Modern Apps
ConfigMgr Content Delivery to Cloud Content Delivery

Modernizing with a co-management bridge

Today
1/2020
From Domain Joined to Azure AD Joined Devices

AD Domain Joined
- Extend your on-premises directory with Azure AD.
- Azure AD Join your AD domain-joined devices
- AD + Azure AD Join new devices through Auto Pilot

Hybrid Azure AD Joined
- Transition GPO to MDM
- Pilot Azure AD Join to identify AD auth dependencies
- Gradually move traditional management tools that rely on computer identity to their cloud equivalents or AAD enlightened versions (e.g. ConfigMgr with CMG, WSUS to WUfB)
- AAD Join new devices (AD Joined machines remain AD joined until retired)

Azure AD Joined
- Eliminate PC dependency on domain controllers
- Better battery life and performance of the device
- Extend your on-premises directory with Azure AD
- Azure AD Join your AD domain-joined devices
- Users sign-in conveniently and securely with Windows Hello for Business
Demo: Co-Management
Apps

Your apps are located in Software Center. Open Software Center to get these apps.

Software Center

SCCM PG On-Premises Dogfood

Applications

All Required

Filter: All Sort by: Most recent

Search

Updates
Operating Systems
Installation status
Device compliance
Options

MSIT AutoVPN package - MSIT and SCCM Dogfood 1.0
Company Portal (x64)
Virtual Smart Card Certificate Manager
Bridging to Modern Management

Adopt Windows 10
Adopt Office 365/ProPlus
AD/AAD connect

GPO to MDM Policy
Kerberos to Modern Auth
Imaging to Signature Image
WSUS to WUfB

ConfigMgr Content Delivery to Cloud Content Delivery
Win32 to Modern Apps

Transition to Modern
Modernizing with a co-management bridge

Today
1/2020
Windows AutoPilot
TRADITIONAL DEPLOYMENT:
THE OLD WAY

1. Build & maintain custom image, gathering everything else that’s necessary to deploy

2. Wipe original OEM Windows image and replace with custom image

Time

Money
Employee driven Self-Deployment

- Custom imaging – expensive, limits HW choice, impairs talent acquisition
- Windows EULA – employees not permitted to accept on org-owned devices
- Non-trivial decision making (Personal vs Org Owned disambig, Privacy Settings, OEM Registration) generates Helpdesk calls
- OOB account is always Admin – majority of enterprises want standard accounts on corp-owned devices
INTRODUCING
WINDOWS AUTOPILOT

Employee unboxes device, self-deploys

Windows AutoPilot Service

Hardware Vendor

Upload Device IDs

Configure AutoPilot Profile

IT Admin

Device IDs

Ship

Deliver direct to Employee

Self Deploy
INTRODUCING

WINDOWS AUTOPILLOT

Hardware Vendor

Upload Device IDs

Configure AutoPilot Profile

Ship

Device IDs

IT Admin

Deliver direct to Employee

Employee unboxes device, self-deploys

Self Deploy
Windows AutoPilot

Microsoft 365 powered device

Lenovo
Microsoft Surface
HP
Panasonic
TOSHIBA
FUJITSU
Co-Management using Windows AutoPilot

Intune

AAD

Policies

Apps

Updates

Reporting

Config Manager

INTERNET

INTRANET
Adopt Windows 10
Adopt Office 365/ProPlus
AD/AAD connect

Today

1/2020

Transition to Modern

ConfigMgr Content Delivery to Cloud Content Delivery
Win32 to Modern Apps
Kerberos to Modern Auth
GPO to MDM Policy
Imaging to Signature Image
WSUS to WUfB

Modernizing with a co-management bridge
Windows Update for Business
What needs to change

Traditional deployment (every 3-5 years)

Windows as a service (twice per year)
<table>
<thead>
<tr>
<th>Windows Server Update Services</th>
<th>System Center Configuration Manager</th>
<th>Windows Update for Business</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>On-Prem</strong></td>
<td><strong>On-Prem</strong></td>
<td><strong>Cloud</strong></td>
</tr>
<tr>
<td>Upgrades are deployed when you approve them</td>
<td>Choice of task sequence-based upgrades or (with vNext) software update capabilities</td>
<td>Upgrades can be deferred</td>
</tr>
<tr>
<td>Content distributed from WSUS servers</td>
<td>Content distributed from ConfigMgr DPs</td>
<td>Builds on top of Windows Update</td>
</tr>
<tr>
<td>Requires KB3095113</td>
<td>BranchCache to reduce bandwidth</td>
<td>Uses Windows Update for content</td>
</tr>
<tr>
<td>BranchCache to reduce bandwidth</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Thinking through deployment strategy

1. **Configure** Insider PCs
   - Lab or secondary PCs
   - Enough to explore new features, measure compatibility

2. **Identify** special PCs
   - Deploy Windows 10 Enterprise LTSB
   - Limited numbers (we hope)

3. **Recruit** volunteers for pilots
   - Willing participants who will provide feedback
   - Cover the broadest set of apps and devices possible

4. **Divide** broad population of PCs
   - Standard deployment best practice
   - Focus on risk reduction, minimizing disruption
Bridging to Modern Management

Adopt & Connect
- Windows 10
- Office 365/ProPlus
- AD/AAD

Transition to Modern
- ConfigMgr Content Delivery to Cloud Content Delivery
- Win32 to Modern Apps
- Kerberos to Modern Auth
- GPO to MDM Policy
- Imaging to Signature Image
- WSUS to WUfB

Modernizing with a co-management bridge
MDM Migration Analysis Tool for IT Admins

- An easy-to-use tool which quickly shows you MDM support for the Group Policies your organization uses today.

MDM Migration Analysis Tool (MMAT) User Manual

Executive Summary

What is this thing called MMAT?

More and more organizations want to move to mobile device management (MDM) to manage their devices including PCs. Windows 10 Creators Update, Microsoft is adding functionality to the Group Policy tool to make transitioning to MDM easier. See additional documentation for more background.

Transferring from Group Policy to MDM can be challenging. Some organizations have Group Policies that have been in place for over a decade and which may not be fully inventoried, never mind understood.

Furthermore, MDM does not have a 1:1 mapping for all legacy Group Policies. While it is possible for an IT administrator to manually review Group Policy and cross reference MDM documentation on MSDM to determine the support level, this would be labor intensive and error prone.

Microsoft created the MD Migration Analysis Tool (aka MMAT) to help. MMAT determines which group policies have been set for a target user/computer and cross-reference against its built-in list of supported MDM policies. MMAT will then generate both XML and HTML reports indicating the level of support for each Group Policy in terms of MDM equivalents.

If you have a Group Policy targeting Minimum Password Length, for instance, MMAT will detect this and tell you that MDM also support this policy.
Check out the 1703 MDM security baselines here: https://aka.ms/mdm1703baselines
Bridging to Modern Management

Adopt Windows 10
Adopt Office 365/ProPlus
AD/AAD connect

Transition to Modern
- ConfigMgr Content Delivery to Cloud Content Delivery
- Win32 to Modern Apps
- Kerberos to Modern Auth
- GPO to MDM Policy
- Imaging to Signature Image
- WSUS to WUfB

Modernizing with a co-management bridge
Application Management
Application Management

- Move applications to Microsoft Store for Business. Use Desktop Bridge.
- Legacy apps:
  - Manage traditional applications with ConfigMgr through co-management
  - Basic MSI support in Intune
  - Intune Management Extension for PowerShell script deployments in environments without ConfigMgr
Thank you!

Come ask us questions!

Other Now Micro Sessions

Tuesday:
- Dealing with Hardware – Overcoming Challenges with Windows 10
- A Hitchhiker's Guide to Azure Active Directory
- Microsoft Enterprise Mobility & Security Suite