

Microsoft Endpoint Manager

CLOUD MANAGEMENT WITH INTUNE

Topics

- What is Microsoft Endpoint Manager?
- What is Intune (and the other features around it)?
- Things you should think about.
- How is Bellarmine using Endpoint Manager?
- 🖱️ Demos 🖱️

Who am I?

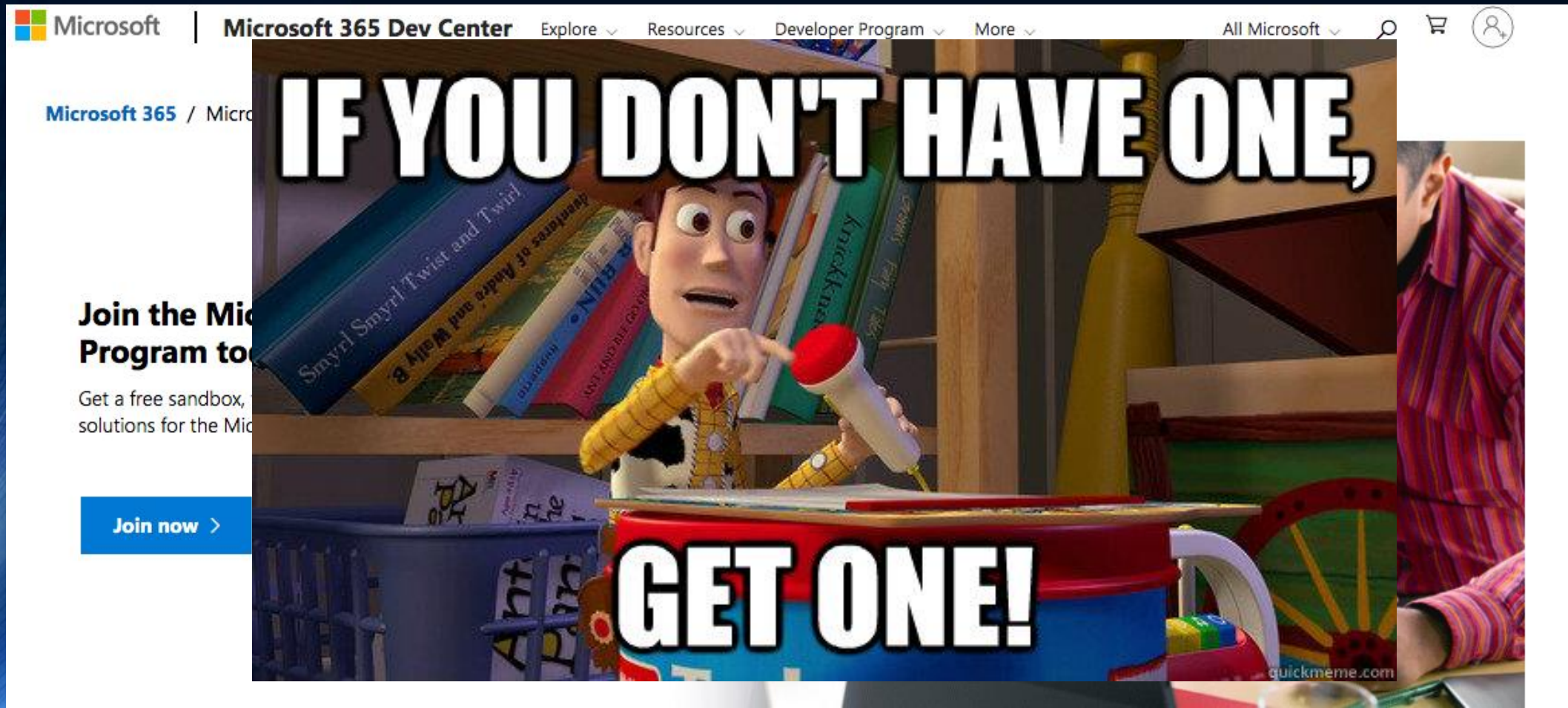
- Tony Morrow
 - @a_gizm0
 - <https://lookanotherblog.com>
- Principal Solutions Architect @ Bellarmine University
- 12 years working at Bellarmine (10 in the Infrastructure Team)
- Focus
 - Networking
 - Wireless
 - Servers/Virtualization
 - Systems integration
 - AD & AAD management
 - Microsoft Endpoint (Intune & System Center)
 - VoIP

Disclaimer 😊

- I am not a Microsoft MVP or Partner
- All technologies showcased are using free, trial, or paid licenses
- All the opinions here are my own
- Nobody is paying me for this presentation
- Nobody has reviewed or approved this presentation before hand

(Tangent) Get a Development Environment

- <https://developer.microsoft.com/en-us/microsoft-365/dev-program>



The image shows a screenshot of the Microsoft 365 Dev Center website. The page features a navigation bar with the Microsoft logo, "Microsoft 365 Dev Center", and menu items like "Explore", "Resources", "Developer Program", and "More". There are also utility icons for search, shopping cart, and user profile. The main content area includes a heading "Microsoft 365 / Micro" and a sub-heading "Join the Microsoft 365 Dev Program to". Below this is a paragraph: "Get a free sandbox, solutions for the Micro". A prominent blue button with the text "Join now >" is visible. A large meme is overlaid on the right side of the page, featuring Woody from Toy Story pointing at a red pushpin on a desk. The text "IF YOU DON'T HAVE ONE," is written in large white letters at the top of the meme, and "GET ONE!" is written at the bottom. The meme also includes a "quickmeme.com" watermark in the bottom right corner.

Microsoft Endpoint Manager

- Microsoft's device management platform
 - Mobile/Desktop/Virtual device management
 - Desktop analytics
 - Device auto configuration
- Includes
 - AzureAD
 - Configuration Manager
 - Intune
 - Autopilot/Autoenrollment

Microsoft Endpoint Manager Licensing

Information Worker Plans

USD ERP per user per month	Microsoft 365				Office 365			Enterprise Mobility + Security	
	E3	E5	E5 Security Add-on	E5 Compliance Add-on	E1	E3	E5	E3	E5
	\$32	\$57	\$12	\$12	\$8	\$20	\$35	\$8.80	\$14.80

Endpoint and app management

	E3	E5	E5 Security Add-on	E5 Compliance Add-on	E1	E3	E5	E3	E5
Microsoft Intune	•	•						•	•
Mobile Device Management	•	•			•	•	•	•	•
Microsoft Endpoint Manager	•	•						•	•
Mobile application management	•	•						•	•
Windows AutoPilot	•	•						•	•
Group Policy support	•	•				•	•		
Shared computer activation for M365 Apps	•	•				•	•		
Endpoint Analytics	•	•						•	•
Cortana management	•	•							

¹ Windows must be licensed separately

Configuration Manager

- Microsoft's On-prem desktop management platform
 - Started as Systems Management Server in 1994
- Configuration compliance
- App deployment
- OS imaging
- Windows Updates

- Wait... wrong presentation

Intune (Cloud MDM Buffet)

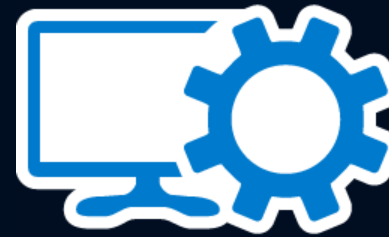
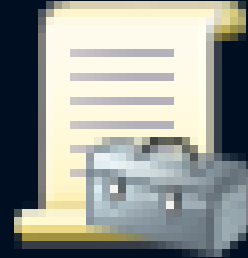
- Microsoft's cloud-based device and application management platform
- Supports Windows, MacOS, iOS, iPadOS, Android devices
- Push software to devices
- Define settings pushed to devices
- Compliance Policies to enable verify security settings
 - Some settings will remediate. Others require configuration profiles
- Manage Updates (Windows & iOS/iPadOS)
- Execute scripts

Intune Application Deployment

- Supports Windows MSI/MSIX & EXE installers or Store apps
 - EXE feels like Configuration Manager application script deployment types
 - Store Apps require getting the URL and logo from browser
- MacOS requires manual package building
- Easy support for iOS/iPadOS
 - App store search built into Endpoint Manager
- Android deployment the same as Windows Store apps

Configuration Profiles

- AKA
 - Intune's equivalent for GPOs
 - Intune's equivalent to WICD ppkg files
 - Intune's equivalent to Apple mobileconfig files
- Apply application and devices settings on a per user or per machine basis



Configuration Profiles (iOS/macOS)

- Can use the templates provided
 - Certificates
 - VPN
 - WiFi
 - Device Restrictions
- OR import your own mobileconfig files
 - ProfileCreator: <https://github.com/ProfileCreator/ProfileCreator>
 - Awesome open-source application for creating custom configs



Configuration Profile (Windows)

- Many prebuilt templates
 - Device restrictions
 - Edition upgrade
 - Kiosk Mode
 - Certificates
 - WiFi
- Settings Catalog (Preview): **All Windows 10 Administrative Templates!!!**
- Custom profiles
 - (If you can figure out the OMA-URI)

Autopilot

- A solution for automatic enrollment into MDM
 - Easily configure the Out-of-Box-Experience
 - Control device ownership throughout its lifecycle
-
- Manufacturer support varies
 - Existing devices can be enrolled if desired

MacOS & iOS Autoenrollment

- Look at Apple Business Manager
 - Devices purchased by the organization can be automatically enrolled into an MDM solution
 - <https://www.apple.com/business/it/>
 - <https://www.apple.com/education/k12/it/> (Apple School Manager)

MacOS Management *(Well, Bless Your Heart)*

- Intune could be a great replacement for Apple Profile Manager
- The challenges:
 - App deployment requires applications and installers to be signed + notarized + OSCP stapled.
 - [Mac Admins Talk: The Loyal Order of Notaries – Cannonball \(tombridge.com\)](#)
 - [Notarization Follow-Up and Video – Cannonball \(tombridge.com\)](#)
 - [Notarization and macOS, what it does, why you need it – Tom Bridge - YouTube](#)
 - Configuration profiles can disappear without warning.
 - OR profiles are not removed when desired.
 - No cloud authentication mechanism offered (JAMF Connect is an alternative).

Things you should think about

- Organization
 - Directory structures are not a concept in AzureAD or MEM.
 - A very hard computer science problem? j/k
 - How are you going to group devices and users for Intune assignments?
 - How are you going to name the dozens-hundreds of configuration profiles and applications you are deploying across four different operating systems?
- What devices will you manage?
 - AD joined computer?
 - AAD joined computers?
 - Company mobile devices?
 - Employee personal computers and mobile devices?

Topics Not Covered

- Device Protection: <https://docs.microsoft.com/en-us/mem/intune/protect/device-protect>
- Compliance policies: <https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>
- Conditional Access: <https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access>
- App protection policies: <https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview>
 - Control what data can be shared between apps
 - Require additional security to access apps
- Defender/Endpoint protection: <https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection>

Topics Not Covered

- RBAC for Intune Management: <https://docs.microsoft.com/en-us/mem/intune/fundamentals/role-based-access-control>
- Windows update management: <https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure>
- PowerShell and Graph API tools for managing Intune: <https://github.com/Microsoft/Intune-PowerShell-SDK/> & <https://docs.microsoft.com/en-us/mem/intune/developer/intune-graph-apis>

DEMO!!!

Intune Apps

Home > Apps > Android >

Add App

Android store app

✓ App information ✓ Assignments ③ Review + create

Name * ⓘ Microsoft Outlook

Description * ⓘ Outlook

Publisher * ⓘ Microsoft

Appstore URL * ⓘ <https://play.google.com/>

Minimum operating system * ⓘ Android 7.0 (Nougat)

Category ⓘ 0 selected

Show this as a featured app in the Company Portal ⓘ Yes No

Home > Apps > Windows >

Add App

Windows MSI line-of-business app

1 App information 2 Assignments 3 Review + create

Select file * ⓘ [googlechromestandaloneenterprise64.msi](#)

Name * ⓘ Google Chrome

Description * ⓘ Google Chrome

Publisher * ⓘ Enter a publisher name

App install context ⓘ User Device

Ignore app version ⓘ Yes No

Command line arguments

Home > Apps > iOS/iPadOS >

Add App

iOS store app

✓ App information 2 Assignments 3 Review + create

Select app * ⓘ [Search the App Store](#)

Name * ⓘ Microsoft Outlook

Description * ⓘ Outlook lets you bring all your email accounts and calendars in one convenient spot. Whether it's staying on top of your inbox or scheduling the next big thing, we make it easy to be your most productive, organized, and connected self.

Publisher * ⓘ Microsoft Corporation

Appstore URL <https://apps.apple.com/us/app/microsoft-outlook/id951937596?uo=4>

Minimum operating system * ⓘ iOS 8.0

Applicable device type * ⓘ 2 selected

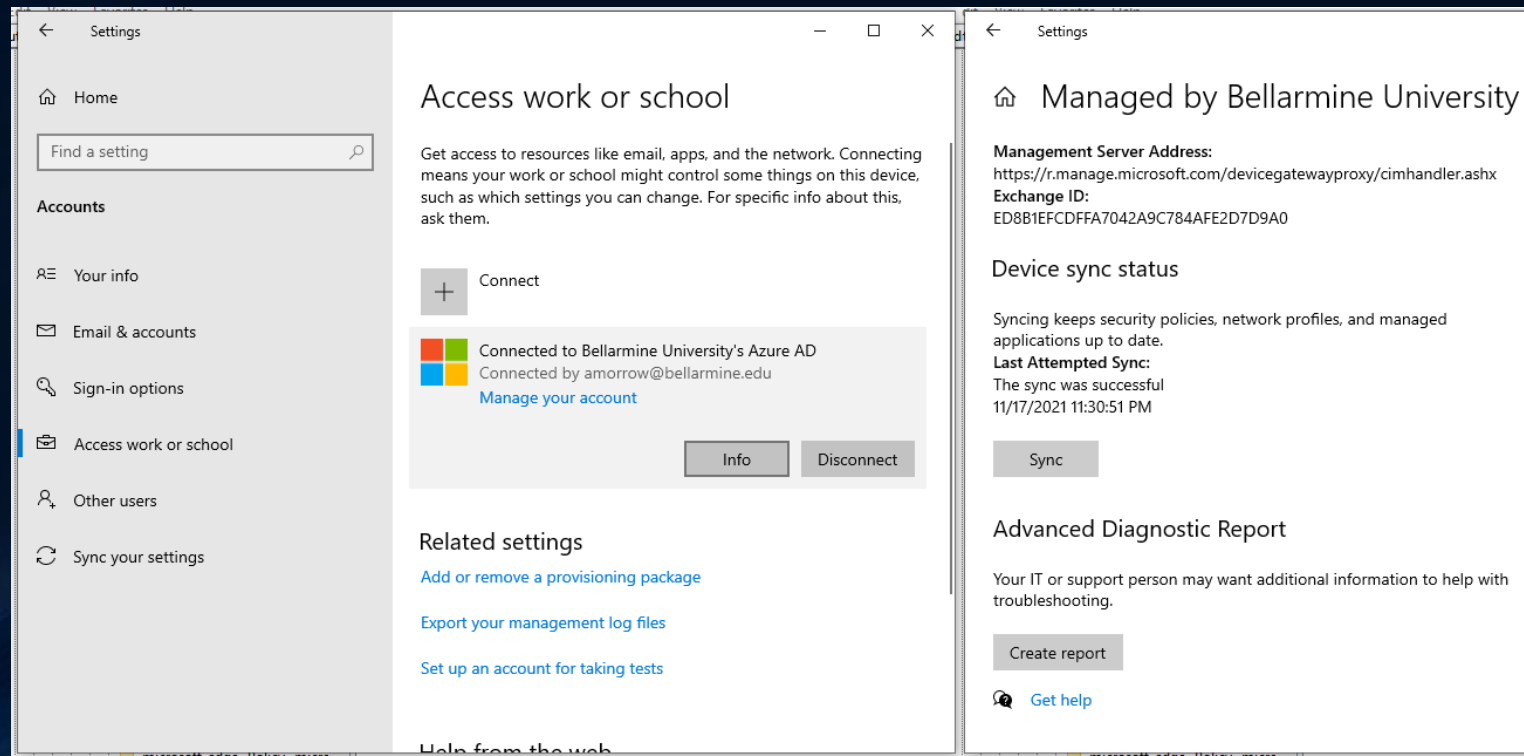
Category ⓘ 0 selected

Custom ADMX Based Profiles

- <https://docs.microsoft.com/en-us/windows/client-management/mdm/understanding-admx-backed-policies>
- Chrome basic example:
<https://support.google.com/chrome/a/answer/9102677?hl=en#zippy=%2Cstep-ingest-the-chrome-admx-file-into-intune>

Troubleshooting

- Settings > Accounts > Access work or school > Info > Advanced Diagnostic Report > Create report



Troubleshooting

- Event Viewer > Applications and Services Logs > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider > Admin

The screenshot shows the Windows Event Viewer interface. The left pane displays the navigation tree with 'DeviceManagement-Enterprise-Diagnostics-Provider' expanded to 'Admin'. The right pane shows a list of events with the following data:

Level	Date and Time	Source	Event ID
Information	11/17/2021 11:25:36 PM	DeviceManagement-...	361
Error	11/17/2021 11:25:36 PM	DeviceManagement-...	454
Error	11/17/2021 11:25:36 PM	DeviceManagement-...	454
Error	11/17/2021 11:25:36 PM	DeviceManagement-...	404
Information	11/17/2021 11:25:36 PM	DeviceManagement-...	202

The details for Event 454 are shown below:

Event 454, DeviceManagement-Enterprise-Diagnostics-Provider

General Details

MDM ConfigurationManager: Command failure status. Configuraton Source ID: (0E00098D-6752-4A31-8522-1DD025D7200F), Enrollment Type: (MDMDeviceWithAAD), CSP Name: (Policy), Command Type: (Clear: first phase of Delete), Result: (./Device/Vendor/MSFT/Policy/ConfigOperations/ADMXInstall/Chrome/Policy/ChromeAdmx).

Troubleshooting

- Registry\Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\current\device

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\current\device\Chrome~Policy~googlechrome_recommended~Startup_recommended

Name	Type	Data
(Default)	REG_SZ	(value not set)
RestoreOnStartup_recommended_ADMXInstanceData	REG_SZ	Software\Microsoft\PolicyManager\providers\0E0...
RestoreOnStartup_recommended_Container	REG_DWORD	0x00000001 (1)
RestoreOnStartup_recommended_ProviderSet	REG_DWORD	0x00000001 (1)
RestoreOnStartup_recommended_WinningProvider	REG_SZ	0E00098D-6752-4A31-8522-1DD025D7200F
RestoreOnStartupURLs_recommended_ADMXInstanceData	REG_SZ	Software\Microsoft\PolicyManager\providers\0E0...
RestoreOnStartupURLs_recommended_Container	REG_DWORD	0x00000001 (1)
RestoreOnStartupURLs_recommended_ProviderSet	REG_DWORD	0x00000001 (1)
RestoreOnStartupURLs_recommended_RestoreOnStartupURLsDesc_ListSet	REG_SZ	1• http://one.bellarmino.edu
RestoreOnStartupURLs_recommended_WinningProvider	REG_SZ	0E00098D-6752-4A31-8522-1DD025D7200F
ShowHomeButton_recommended_ADMXInstanceData	REG_SZ	Software\Microsoft\PolicyManager\providers\0E0...
ShowHomeButton_recommended_Container	REG_DWORD	0x00000001 (1)
ShowHomeButton_recommended_ProviderSet	REG_DWORD	0x00000001 (1)
ShowHomeButton_recommended_WinningProvider	REG_SZ	0E00098D-6752-4A31-8522-1DD025D7200F