Sharing *(our)* biggest mistakes from implementing Microsoft Intune

Lessons learned from implementing many Microsoft Intune environments

Agenda

- Hardware
- Application Deployment
- Assignments
- Compliancy
- Change Management
- Settings Catalog challenges
- Know your sources
- Re-learn
- RBAC
- BYOD
- Cleaning Up
- Licensing

Think about your Hardware Configuration before you start rollout

- Hardware Configuration:
  - Secure Boot
  - TPM
  - Virtualization
  - Do not allow boot from external media
  - BIOS Password
  - Firmware updated
- Newest OS (and not 2 feature updates behind, breaking AutoPilot f.e.) – enforce using Enrollment Restrictions (minimum OS version)
- Devices that support Windows 10 don't necessarily support Windows 11 / 12
- We have seen Windows 10 deployments on devices not having UEFI enabled

Your device must be running Windows 10, version 2004 or later, to upgrade. Free updates are a

Processor	1 gigahertz (GHz) or faster with 2 or more cores on a compatible 64-bit processor or System
RAM	4 gigabyte (GB).
Storage	64 GB or larger storage device Note: See below under "More information on storage space to
System firmware	UEFI, Secure Boot capable. Check here for information on how your PC might be able to meet
TPM	Trusted Platform Module (TPM) version 2.0. Check here for instructions on how your PC mig
Graphics card	Compatible with DirectX 12 or later with WDDM 2.0 driver.
Display	High definition (720p) display that is greater than 9" diagonally, 8 bits per color channel.
Internet connection and Microsoft account	Windows 11 Pro for personal use and Windows 11 Home require internet connectivity and a M Switching a device out of Windows 11 Home in S mode also requires internet connectivity. Le For all Windows 11 editions, internet access is required to perform updates and to download a

VBS requires the following components be present and properly configured.

Please notice that TPM is not a must requirement, but we highly recommend to implement TPM.

Hardware requirement	Details
64-bit CPU	Virtualization-based security (VBS) requires the Windows hypervisor, which is only supported on 64-bit IA processors with virtualization extensions, including Intel VT-X and AMD-v.
Second Level Address Translation (SLAT)	VBS also requires that the processor's virtualization support includes Second Level Address Translation (SLAT), either Intel VT-X2 with Extended Page Tables (EPT), or AMD-v with Rapid Virtualization Indexing (RVI).
IOMMUs or SMMUs (Intel VT-D, AMD-Vi, Arm64 SMMUs)	All I/O devices capable of DMA must be behind an IOMMU or SMMU. An IOMMU can be used to enhance system resiliency against memory attacks.
Trusted Platform Module (TPM) 2.0	TPMs, either discrete or firmware, will suffice. For more information, see Trusted Platform Module (TPM) 2.0.
Firmware support for SMM protection	System firmware must adhere to the recommendations for hardening SMM code described in the Windows SMM Security Mitigations Table (WMST) specification. The WSMT specification contains details of an ACPI table that was created for use with Windows operating systems that support VBS features. Firmware must implement the protections described in the WSMT specification, and set the corresponding protection flags as described in the specification to report compliance with these requirements to the operating system.
Unified Extensible Firmware Interface (UEFI) Memory Reporting	UEFI firmware must adhere to the following memory map reporting format and memory allocation guidelines in order for firmware to ensure compatibility with VBS. • **UEFI v2.6 Memory Attributes Table (MAT)** - To ensure compatibility with VBS, firmware must cleanly separate EFI runtime memory ranges for code and data, and report this to the operating system. Proper segregation and reporting of EFI runtime memory ranges allows VBS to apply the necessary page protections to EFI runtime services code pages within the VBS secure region. Conveying this information to the OS is accomplished using the EFI_MEMORY_ATTRIBUTES_TABLE. To implement the UEFI MAT, follow these guidelines: 1. The entire EFI runtime must be described by this table. 2. All appropriate attributes for EfiRuntimeServicesData and EfiRuntimeServicesCode pages must be marked. 3. These ranges must be aligned on page boundaries (4KB), and can not overlap. • **EFI Page Protections** -All entries must include attributes EFI_MEMORY_RO, EFI_MEMORY_XP, or both. All UEFI memory that is marked executable must be read only. Memory marked writable must not be executable. Entries may not be left with neither of the attributes set, indicating memory that is both executable and writable.
Secure Memory Overwrite Request (MOR) revision 2	Secure MOR v2 is enhanced to protect the MOR lock setting using a UEFI secure variable. This helps guard against advanced memory attacks. For details, see Secure MOR implementation.
Memory integrity-compatible drivers	Ensure all system drivers have been tested and verified to be compatible with memory integrity. The Windows Driver Kit and Driver Verifier contain tests for driver compatibility with memory integrity. There are three steps to verify driver compatibility: 1. Use Driver Verifier with the **Code Integrity compatibility** checks enabled. 2. Run the Hypervisor Code Integrity Readiness Test in the Windows HLK. 3. Test the driver on a system with VBS and memory integrity enabled. This step is imperative to validate the driver's behavior with memory integrity, as static code analysis tools simply aren't capable of detecting all memory integrity violations possible at runtime.

Windows 11: Half of enterprise workstations don't meet the new system requirements, says survey

Windows 11 could be a very slow and heavy-lifting rollout for enterprise organizations.

Written by **Liam Tung,** Contributing Writer on Oct. 1, 2021

About “Kenneth van Surksum”

Focus

Modern Workplace Consultant, Microsoft Certified Trainer, Co-founder and organizer at Workplace Ninja User Group Netherlands

Secure At Work

Experts Live Netherlands

From

The Netherlands

My Blog

https://www.vansurksum.com

Certifications

Microsoft 365 Certified Enterprise Administrator

Microsoft Certified Azure Solutions Architect

Hobbies

Cooking on my Kamado Joe & Sports

Contact

kenneth@vansurksum.com

https://twitter.com/kennethvs

https://www.linkedin.com/in/kennethvansurksum

About “Peter Daalmans”

Focus

Modern Workplace Consultant, Microsoft Certified Trainer, Co-founder and organizer at Workplace Ninja User Group Netherlands, Organizer Workplace Ninja Summit

From

Breda, The Netherlands

Professional info

Microsoft Certified Trainer

Microsoft MVP

Hobbies

Australia, (watching) soccer

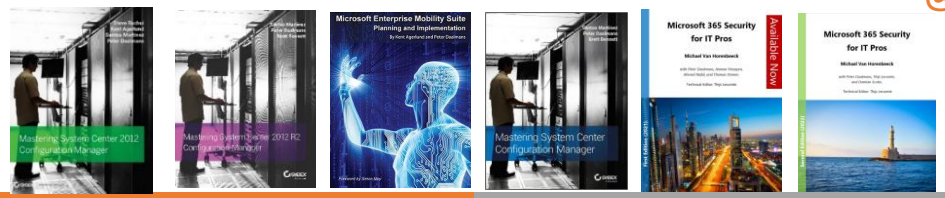
My Blog

https://peterdaalmans.com

Contact

peter@daalmansconsulting.com

@pdaalmans



App deployment

Consistent Application Deployment

- Win32 versus MSI/Built in Apps from Microsoft
- Mandatory in Autpiilot? (configure in ESP)/what comes later
- Prefer available over assigned
- Use AppDeployToolkit
- Make Stores available for users? (Windows Store/Office Store/Teams Store/Extensions in your browsers?)
- Enable logging in your installers if possible (write to known folder which can be picked up by collecting diagnostics)
- Make sure that users understand what they see in the Company Portal (no technical names shall be used), use logo/reference to documentation, clear versioning and more ….

Collect diagnostics from a Windows device

- Don’t use **%temp%**

- [Collect diagnostics from a Windows device - Microsoft Intune | Microsoft Learn]

Files:

- %ProgramData%\Microsoft\DiagnosticLogCSP\Collectors*.etl
- %ProgramFiles%\Microsoft EPM Agent\Logs*.*
- %ProgramData%\Microsoft\IntuneManagementExtension\Logs*.*
- %ProgramData%\Microsoft\Windows Defender\Support\MpSupportFiles.cab
- %ProgramData%\Microsoft\Windows\WlanReport\wlan-report-latest.html
- %ProgramData%\USOShared\logs\system*.etl
- %ProgramData Microsoft Update Health Tools\Logs*.etl
- %temp%\CloudDesktop*.log
- %temp%\MDMDiagnostics\battery-report.html
- %temp%\MDMDiagnostics\energy-report.html
- %temp%\MDMDiagnostics\mdmlogs-<Date/Time>.cab
- %temp%\MDMDiagnostics\msinfo32.log
- %windir%\ccm\logs*.log
- %windir%\ccmsetup\logs*.log
- %windir%\logs\CBS\cbs.log
- %windir%\logs\measuredboot*.*
- %windir%\logs\Panther\unattendgc\setupact.log
- %windir%\logs\SoftwareDistribution\ReportingEvent\measuredboot*.log
- %windir%\logs\WindowsUpdate*.etl
- %windir%\system32\config\systemprofile\AppData\Local\mdm*.log
- %windir%\temp%computername%*.log
- %windir%\temp\officeclicktorun*.log
- %TEMP%\winget\defaultstate*.log

Assignments

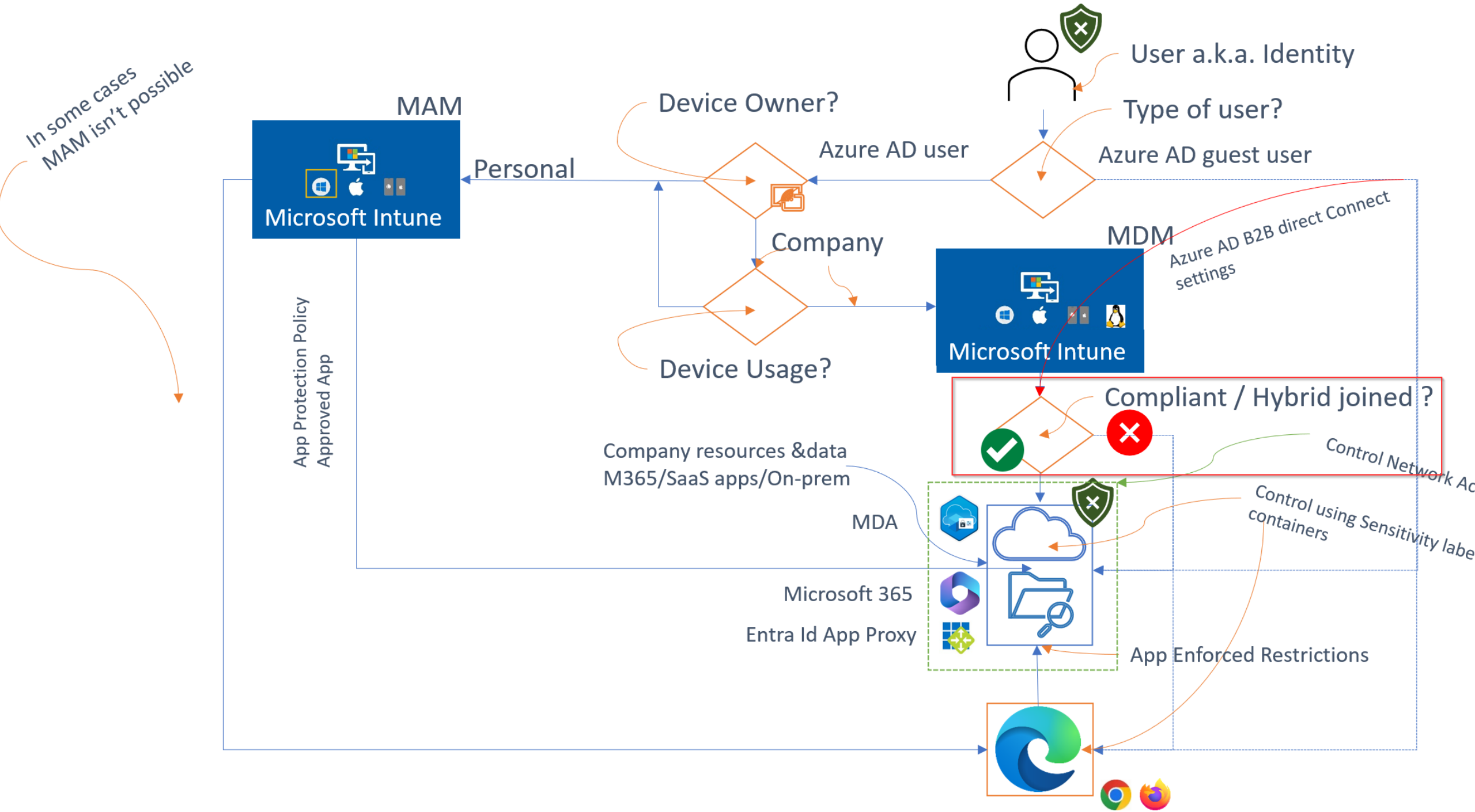
Have an assignment plan and stick to it

- Be careful with assigning to devices (can cause reboots during AutoPilot)
- We prefer to deploy to user groups (Intune = User Centric) – only deploy to devices when it concerns deployment profiles or if you deploy to “device” scenarios like Pre-Provisioning/Kiosk/Shared Devices etc..
  - Use Filters when needed
- Some functionality has not been updated in a long time (like policy sets)/ transition to other techniques

Compliance

Make sure that devices are compliant after the rollout

- Because Compliancy is used within Conditional Access to allow/deny access
- Install Company Portal App (so that users can check compliancy themselves)
- During mass-rollout you can “relax” policies temporarily
- Divide your Compliancy Policies by functionality
  - So that f.e. without BitLocker device is non-compliant immediately
  - So that f.e. when Defender is not up to date, the device becomes non-compliant after 1 day

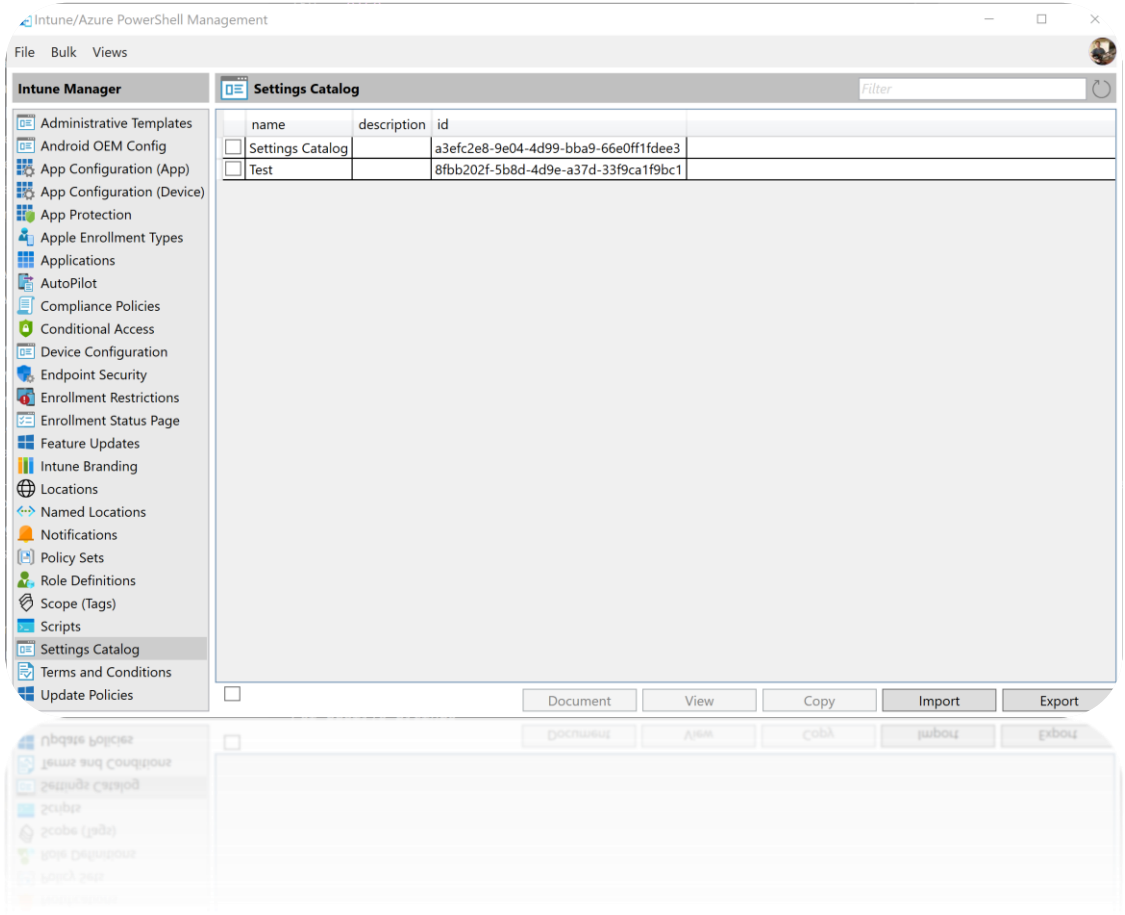

In some cases
MAM isn't possible
MAM
Microsoft Intune
Personal
Device Owner?
Azure AD user
Company
Device Usage?
User a.k.a. Identity
Type of user?
Azure AD guest user
MDM
Microsoft Intune
Azure AD B2B direct Connect settings
App Protection Policy
Approved App
Compliant / Hybrid joined ?
Control Network Ac
Company resources &data
M365/SaaS apps/On-prem
MDA
Control using Sensitivity labe
containers
Microsoft 365
Entra Id App Proxy
App Enforced Restrictions

Change management

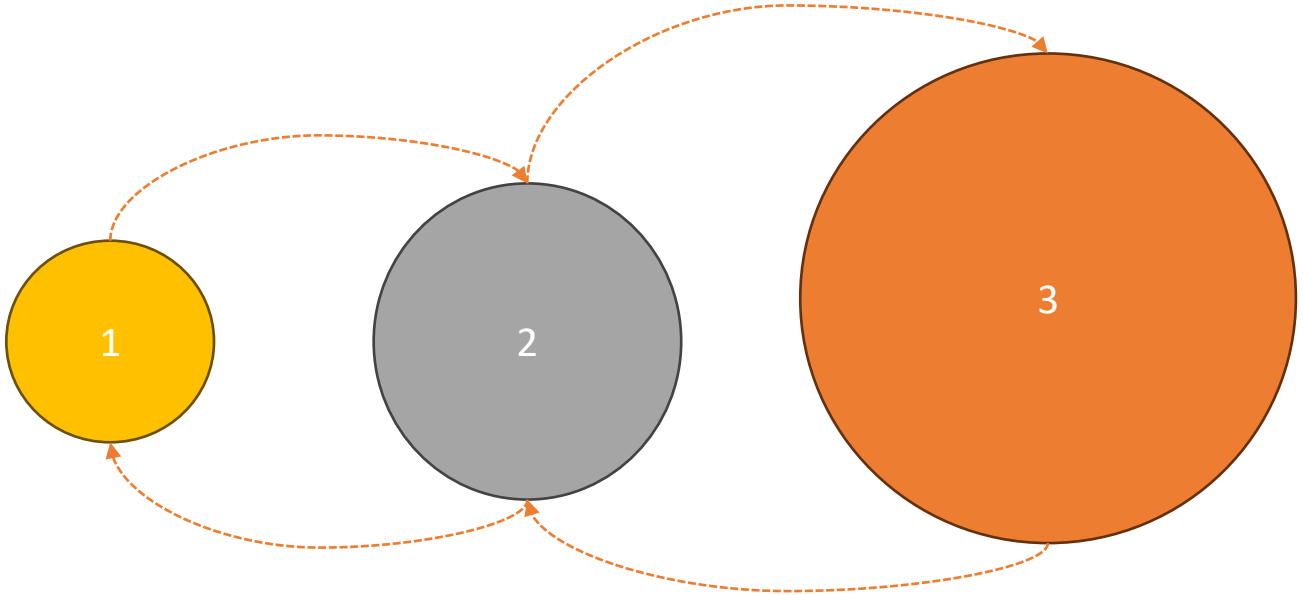
How to safely test in Production?

- Use Update Rings
- Make backup (IntuneManagement tooling) – https://github.com/Micke-K/IntuneManagement
- 4 eyes principle (Apps & Scripts /admin approval)
- Document your environment on a regular basis
- Do not modify existing policies while in status production

- Built your own test environment (Developer subscription) – E5 functionality without Defender



Release- and Change Management



Update Ring 1

- Small Group of Users
- Receive MS updates on day of release
- Run M365 Current Channel
- Run Microsoft Edge Current
- Defender updates first
- New configuration first

Update Ring 2

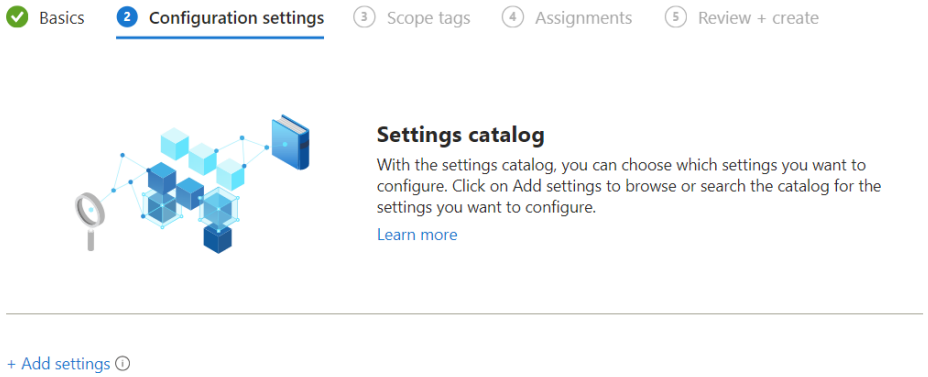
- Small Group of “Business” Users
- Receive MS updates after 3 days
- Run M365 Current Channel
- Run Microsoft Edge Current
- Defender updates second
- New configuration second

Update Ring 3 (Default)

- Rest of Users
- Receive MS updates after 7 days
- Run M365 Monthly Enterprise
- Run Microsoft Edge Stable
- Defender updates third
- New configuration third

Settings management

The challenge with the Settings Catalog



- Settings catalog combines native CSP and ADMX settings (what about WMI bridge?)
  - Sometimes a local GPO is set
    - Some GPO settings are tattooing (provide example)
  - Sometimes a native CSP

- Start replacing your “legacy” policies with the Settings Catalog alternative
- Be careful with double negatives (allow versus block)
- DeviceConfig/README.md at main · IntunePMFiles/DeviceConfig (github.com)
- okieselbach/SyncMLViewer: A small real time SyncML protocol Viewer (github.com)

Don’t just believe every solution on Google/Bing

- Most blogs are written on test environments, not necessarily your environments situation
- Blogs are point solutions, and don’t necessarily fit in your total solution
- Only more and more information is added to the internet, blogs from 5 years ago are probably not relevant anymore, or at least require some updates based on new technology/best practices
- Best practices also change !!

- AppLocker/SCCM examples
- Blogs based on public preview material
- Be critical and understand first

Think modern

Don’t rebuild your legacy configuration in Intune

- Force wallpaper
- Lock down start menu
- Migrate all current GPOs to Setting Catalog
- **VPN solutions** (new solutions coming Entra Id Private Access – VPN is now even mentioned as “legacy”)
- Deploy 100+ apps on your Modern Workplace
- Hybrid AD Join

- Autopilot is not holy/OSD is still relevant (SCCM/MDT/OSDCloud)

Demo

Microsoft Entra Private Access

Role based implementation challenges

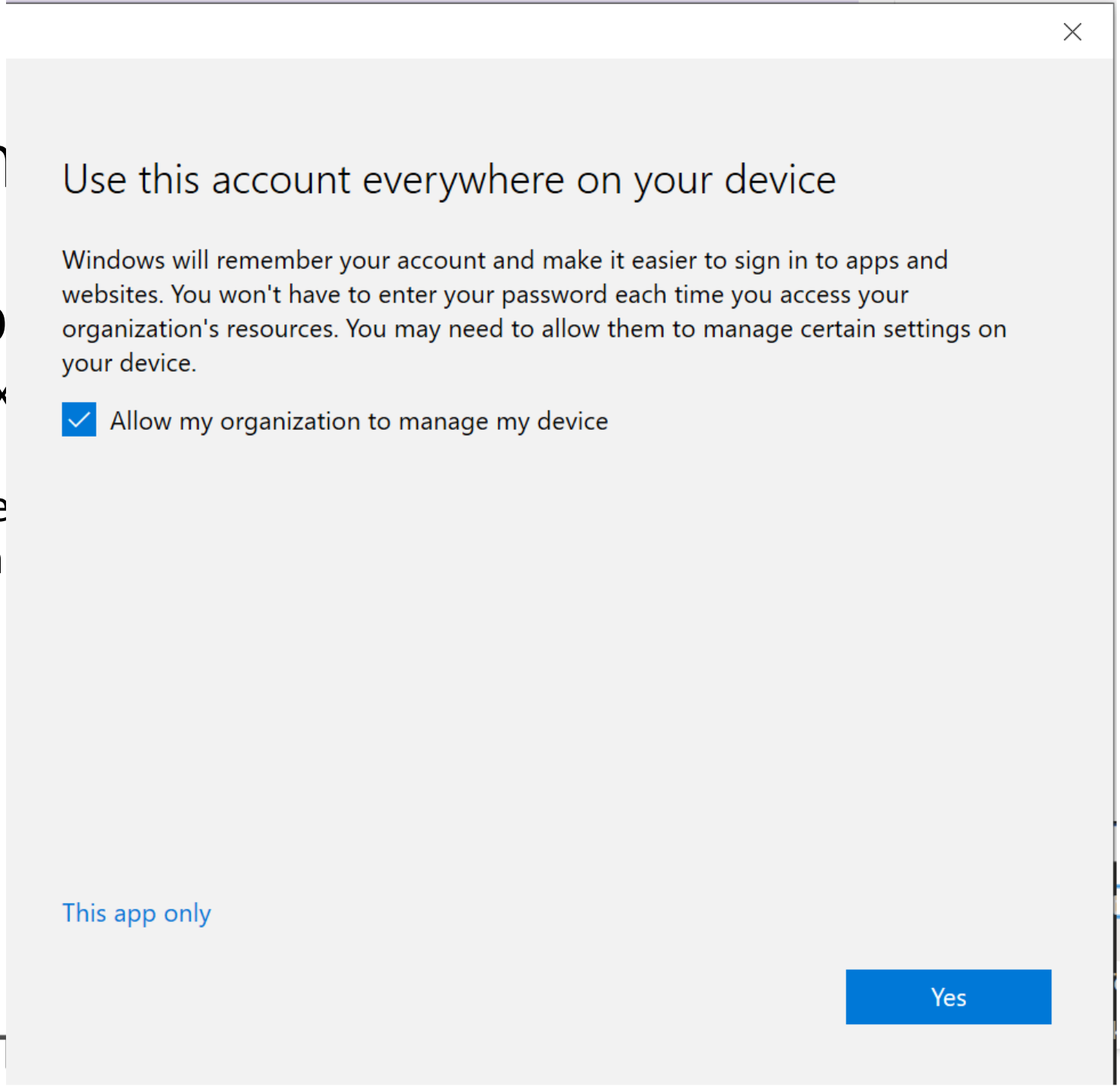
“With Global Administrator rights we now for sure it will work”

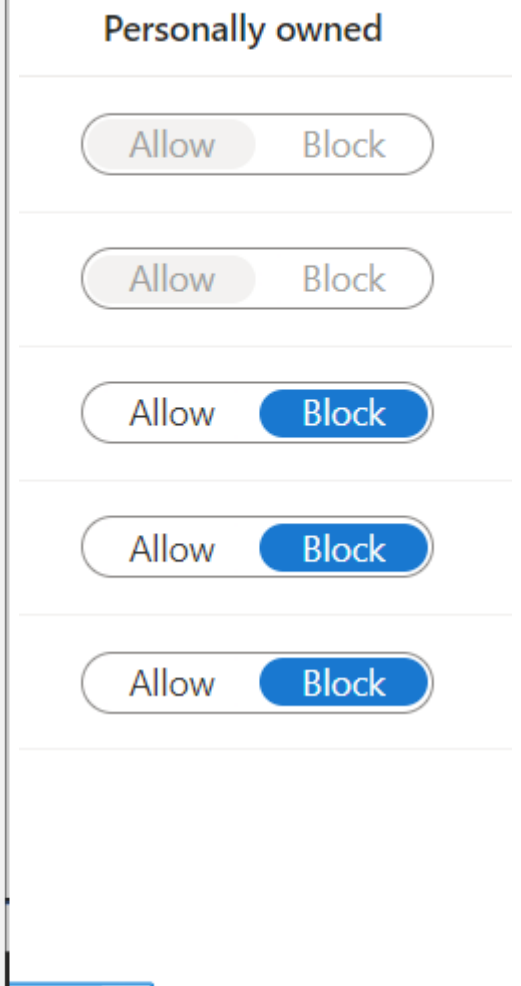
Why give 24x7 rights, if you only need them 8x5 or even less?

- Microsoft Entra Id Privileged Identity Management (PIM) (P2)
  - Privileged Access Groups for Intune and other related roles
  - Distinct between Operational/Change roles

Enrollm

- Block BYO
  - Work ex
  - Default must be enrollm
  - Provide
- Company





Clean up

- Cleanup old devices
  - Intune automatically but do not forget AAD/Entra Id
- Cleanup old configuration (but backup just in case, use IntuneManagemenTooling bulk export)
- Old apps

- Users/Guest users… (Scope AAD)

Licensing challenges and issues

- No App Protection Policies if user is not licensed
- No Autopilot/Intune policies if user is not licensed
- Use group based licensing

Do you have an NDA with Microsoft?

Yes?

Join the Microsoft Customer Connection

https://aka.ms/joinccp

Please provide feedback

Yellenge