

Designing and building your Microsoft Endpoint Manager/Intune environment for Operations

By Kenneth van Surksun – 16 December 2021





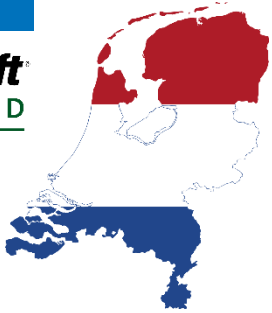
About “Kenneth van Surksun”

Focus

Modern Workplace Consultant at Insight24, Microsoft Certified Trainer, Co-founder and organizer at Windows Management User Group Netherlands, Workplace Ninja User Group Netherlands



Microsoft
CERTIFIED
Trainer



From

The Netherlands

My Blog

<https://www.vansurksun.com>



Certifications

Microsoft 365 Certified Enterprise Administrator

Microsoft Certified Azure Solutions Architect



Hobbies

Cooking on my Kamado Joe & Sports



Contact

kenneth@vansurksun.com

<https://twitter.com/kennethvs>

<https://www.linkedin.com/in/kennethvansurksun>



Azure AD Conditional Access Whitepaper version 1.3

October 2021 edition, 95 pages of Conditional Access goodness. Written by: Kenneth van Surksum

Available at: <https://www.vansurksum.com>



MVP Microsoft
Most Valuable
Professional

wpnijas.nl



Our topics for Today!

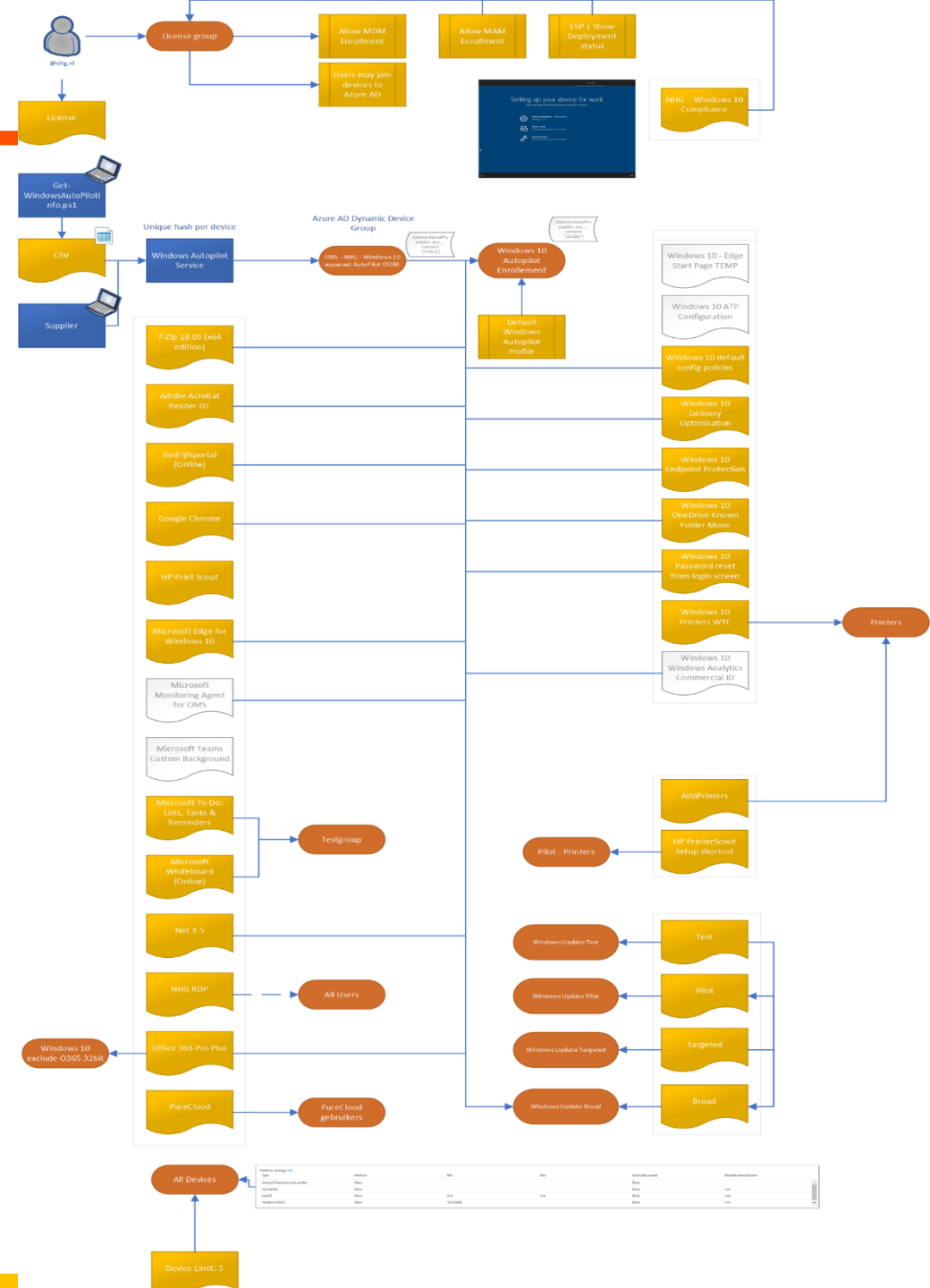


- **Problem statement**
Of course, I mean “Challenge”
- **Assigning to users or devices?**
- **My way of doing it**
- **Key takeaways**
- **DEMO's**



Problem statement

- **No structure**
 - Sometimes Applications are assigned to user groups, sometimes to all devices and sometimes to a device group without any logical reasoning behind it
 - Configuration profiles assigned to device groups, user groups, all devices, all users without any logical reasoning behind it
 - Not all devices have the same settings applied for unspecific reasons
- **Conflicting and errors for settings applied**
 - When investigating devices have errors or receive conflicting settings
- **Enrollment fails for unspecified reasons in some circumstances**
 - When device limit for “accounts used to test” are reached
 - When a group membership necessary for the solution to work is forgotten to be added



Goals for success and designing for Operations



- The requirements of the customer are met
- Device configuration is consistent and error free
- People administering the solution after being handed over know what to do and have a stable environment
- There is a process in place, to introduce changes in a controlled way into the environment.



Endpoint Management North Star



A framework for Windows endpoint management transformation

Assigning to users or devices?

Assigning to users

- Use user groups when you want your settings and rules to always go with the user, whatever device they use.

Assigning to devices

- If you want to apply settings on a device, regardless of who's signed in, then assign your profiles to a devices group. Settings applied to device groups always go with the device, not the user.
- Use device groups when you don't care who's signed in on the device, or if anyone is signed in. You want your settings to always be on the device.

Also see: [Intune: Choosing whether to assign to User or Device Groups](#)

Assignment options

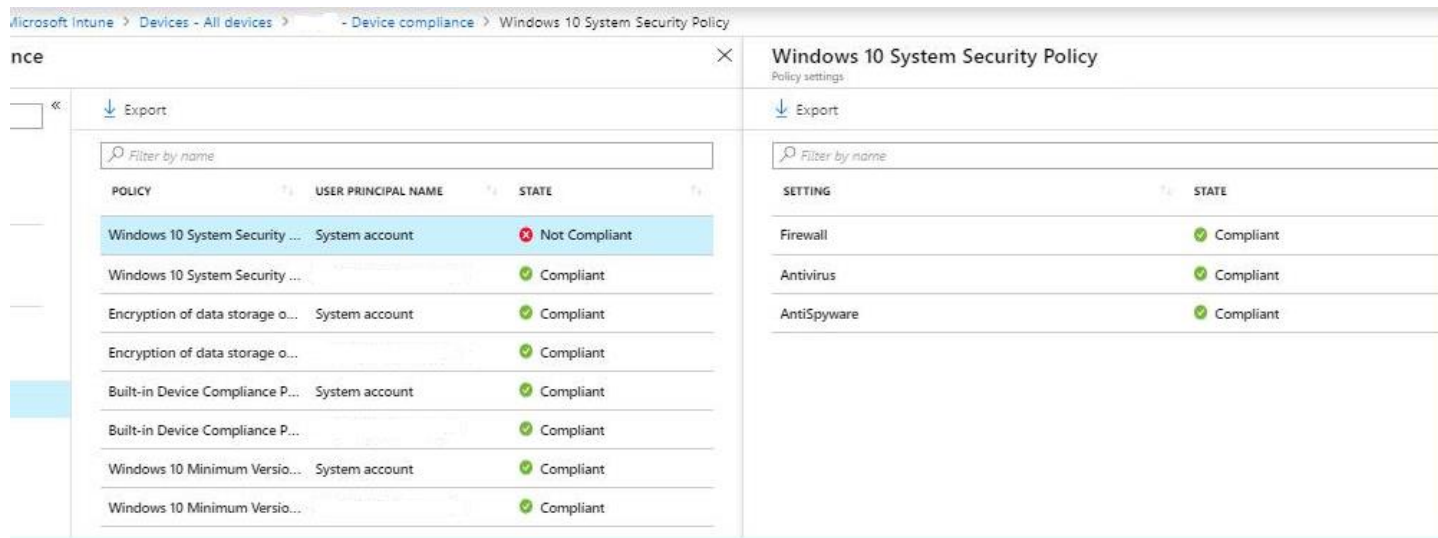
| <div>Include</div> <div>Exclude</div> | Assigned User | Assigned Device | Dynamic User | Dynamic Device |
|---------------------------------------|---------------|-----------------|--------------|----------------|
| | Assigned User | Assigned Device | Dynamic User | Dynamic Device |
| Assigned User | ✓ | | ✓ | |
| Assigned Device | | ✓ | | ✓ |
| Dynamic User | ✓ | | ✓ | |
| Dynamic Device | | ✓ | | ✓ |

Demo

Challenges with the Configuration Profile - Device Restrictions template

Challenges

- Assign wallpaper to device group, gives error when applying to “System” account
- Assigning Compliance Policy to device group could cause the device to become non-compliant because of the “System” account as well



The screenshot shows the Microsoft Intune console with the path: Microsoft Intune > Devices - All devices > Device compliance > Windows 10 System Security Policy. The main pane displays a table of policy compliance for the 'System account'.

| POLICY | USER PRINCIPAL NAME | STATE |
|--|---------------------|---------------|
| Windows 10 System Security Policy | System account | Not Compliant |
| Windows 10 System Security Policy | | Compliant |
| Encryption of data storage on the device | System account | Compliant |
| Encryption of data storage on the device | | Compliant |
| Built-in Device Compliance Policy | System account | Compliant |
| Built-in Device Compliance Policy | | Compliant |
| Windows 10 Minimum Version | System account | Compliant |
| Windows 10 Minimum Version | | Compliant |

Setting error

SETTING

PersonalizationDesktopImageStatus

STATE

Error

SOURCE PROFILES

Source Profile

W10 - Wallpaper

ERROR CODE

0x87d10000

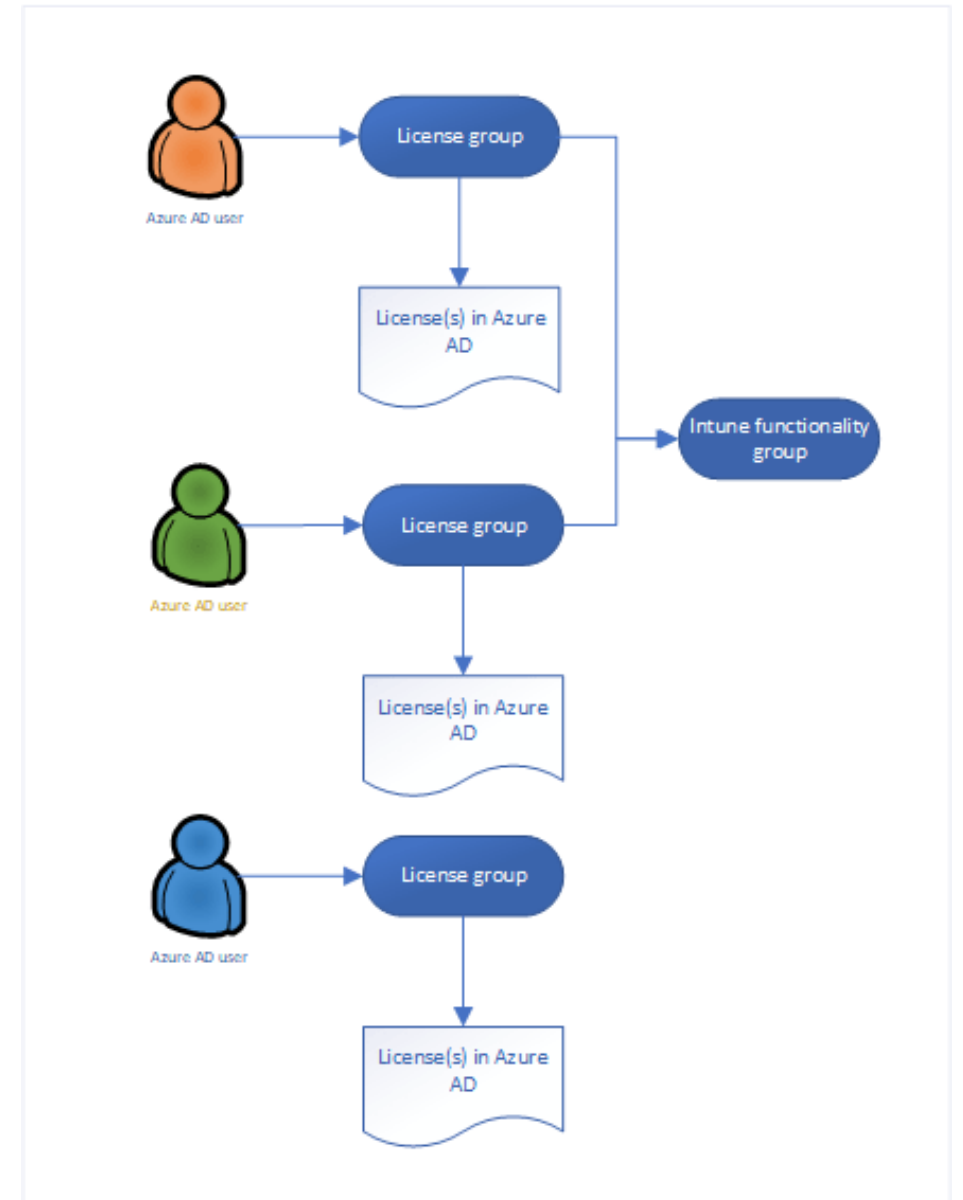
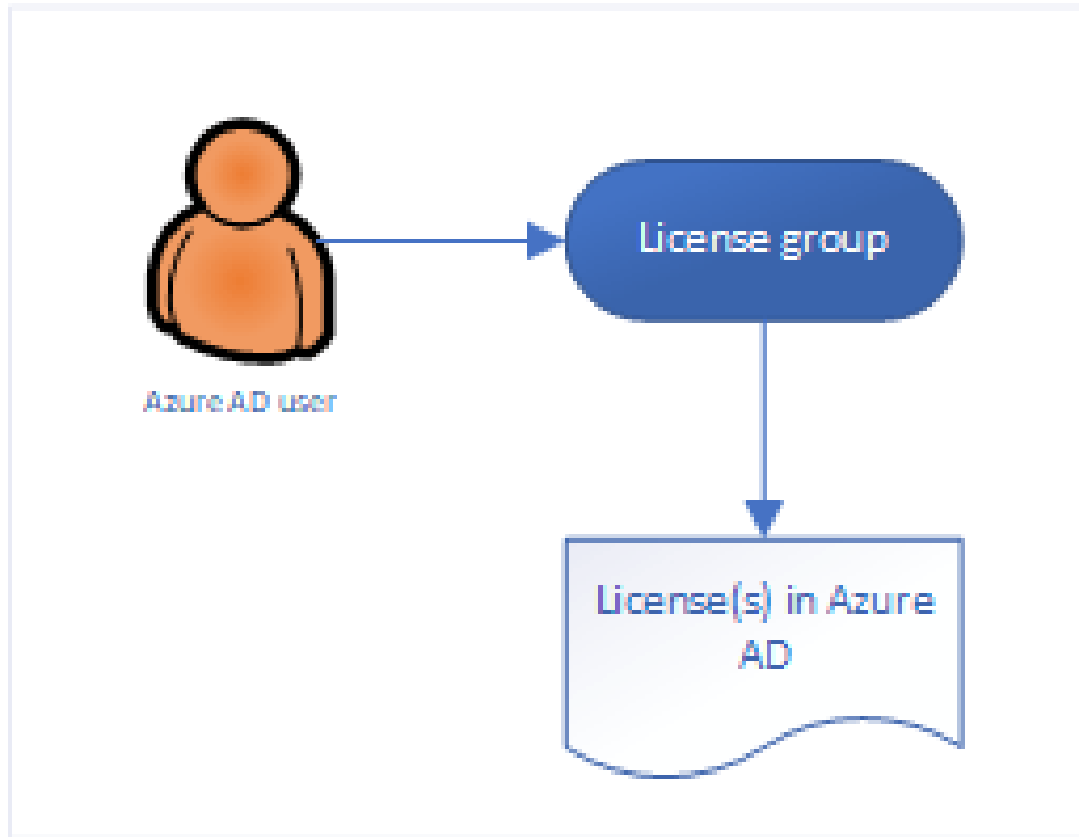
ERROR DETAILS

No error code

| Where | Functionality | Options | Option | Assignment types | Option2 | Assignment types2 |
|-----------------------|-----------------------------------|-------------------|----------------------|------------------|--|-------------------|
| Azure AD | Allow MDM Enrollment | None/Some/All | Some | UG/DG | | |
| | Allow MAM Enrollment | None/Some/All | Some | UG/DG | | |
| | Users may join devices to Azure A | None/Selected/All | Selected | UG/DG | | |
| MEM\Devices | Device Type Restrictions | Default | Include groups | UG/DG | | |
| | Device Limit Restrictions | Default | Include groups | UG/DG | | |
| | Enrollment Status Page | Default | Include groups | UG/DG | | |
| | Deployment Profile | | Included groups | UG/DG/AD | Excluded Groups | UG/DG |
| | Compliance Policy | | Included groups | UG/DG/AU | Excluded Groups | UG/DG |
| | Scripts | | Included groups | UG/DG | | |
| | Configuration Profiles | | Included groups | UG/DG/AU/AD/AUD | Excluded Groups | UG/DG |
| | Feature Updates | | Included groups | UG/DG | Excluded Groups | UG/DG |
| | Update Rings | | Included groups | UG/DG/AU/AD/AUD | Excluded Groups | UG/DG |
| | Policy sets | | Included groups | UG/DG/AU/AD/AUD | Excluded Groups | UG/DG |
| | Applications | | Required (Incl/Excl) | UG/DG/AU/AD | Available for enrolled devices (Incl/Exc | UG/DG/AU |
| | | | | | Uninstall (Incl/Excl) | UG/DG/AU/AD |
| | Policies for Office apps | | Included groups | UG/DG/Anonymous | | |
| | S mode supplemental policies | | Included groups | UG/DG/AU/AD/AUD | Excluded Groups | UG/DG |
| MEM\Endpoint Security | Security Baselines | | Included groups | UG/DG | Excluded Groups | UG/DG |
| | Anti-Virus | | Included groups | UG/DG/AU/AD/AUD | Excluded Groups | UG/DG |
| | Disk Encryption | | Included groups | UG/DG/AU/AD/AUD | Excluded Groups | UG/DG |
| | Firewall | | Included groups | UG/DG/AU/AD/AUD | Excluded Groups | UG/DG |
| | Endpoint detection and response | | Included groups | UG/DG/AU/AD/AUD | Excluded Groups | UG/DG |
| | Attack surface reduction | | Included groups | UG/DG/AU/AD/AUD | Excluded Groups | UG/DG |
| | Account protection | | Included groups | UG/DG/AU/AD/AUD | Excluded Groups | UG/DG |

You can [download the spreadsheet from my Github page](#).

Use Group Licensing



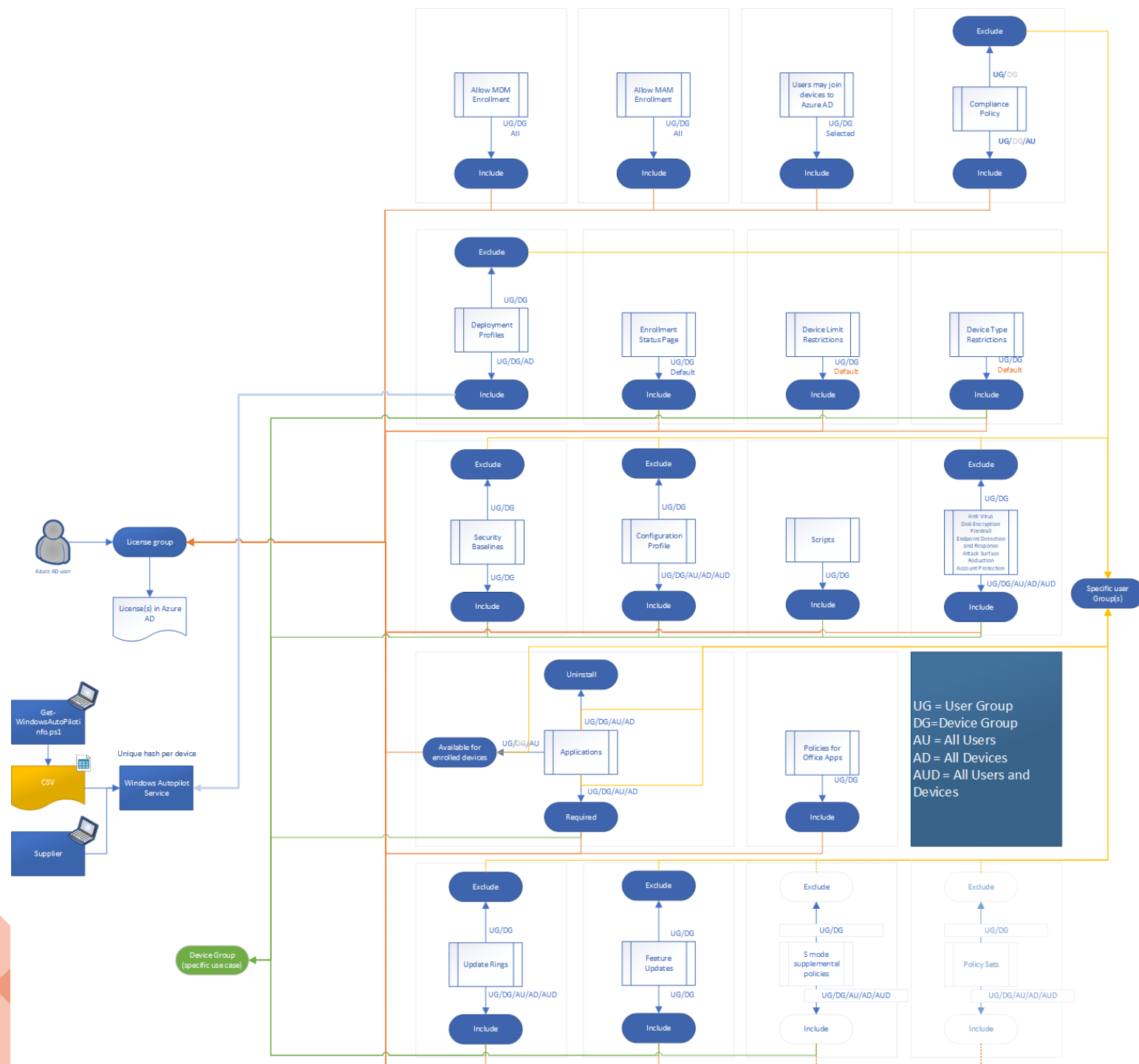


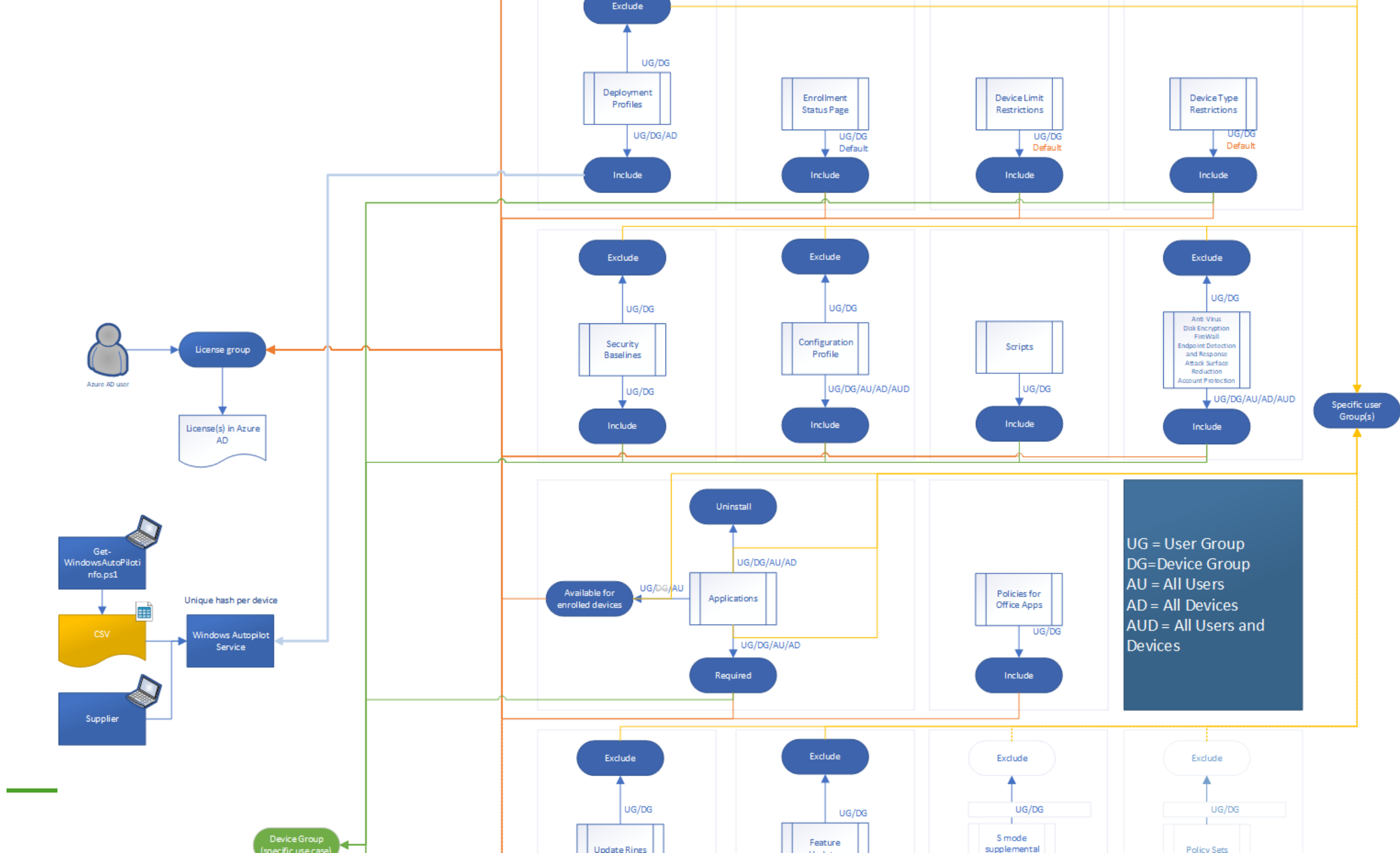
Group Nesting

📌 Important

We don't currently support:

- Adding groups to a group synced with on-premises Active Directory.
- Adding Security groups to Microsoft 365 groups.
- Adding Microsoft 365 groups to Security groups or other Microsoft 365 groups.
- Assigning apps to nested groups.
- Applying licenses to nested groups.
- Adding distribution groups in nesting scenarios.





Demo

How I implement Microsoft Endpoint Manager



Key takeaways

- Doing it different is not WRONG, there are multiple ways to implement MEM
 - <https://www.itpromentor.com/devices-or-users-when-to-target-which-policy-type-in-microsoft-endpoint-manager-intune/>
- Consistency is key!
- Understand how things work (f.e. the ESP and Required Apps)
 - <https://techcommunity.microsoft.com/t5/intune-customer-success/selecting-required-apps-for-your-enrollment-status-page/ba-p/2200381>
- I version all my Microsoft Endpoint Manager configuration
 - I24 - W10 - CP - Google Chrome Configuration - v1.0
 - I24 - Windows 10 Compliance Policy - v1.0
- Create Deployment Rings
 - ~~Eat your own dog food~~/Drink you own champagne
 - Use relevant business users
- Each choice has consequences
 - When applying to user groups for example, it's hard to make exceptions for certain devices (use test accounts)
- I consider my implementation successful when
 - The device configuration is consistent and simple to understand (and therefore manage)
 - Device configuration on a device is successful and there are no errors or conflicts