Housekeeping for the modern endpoint management admin

Start 10:10

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Sprekers

Tim De Keukelaere

✉ Tim.De.Keukelaere@it-essence.be

𝕏 @Tim_DK

Peter Daalmans

✉ peter@daalmansconsulting.com

𝕏 @pdaalmans

Naming Conventions

What is in scope?

- Entra ID groups
- Devices
- Configuration Profiles
- Compliance
- Autopilot
  - Profile
  - ESP
- GroupTags

And probably some other things …

The perfect naming convention

… it does not exist!

Generic elements

Supported Platforms

Platform	Abbreviation
Windows	WIN
MacOS	MAC
IOS / IPadOS	IOS
Android	AND
Linux (any flavour)	LNX

Releases / Deployment Phases

Release / Phase	Abbreviation
Development	DEV
Test	TST
Acceptance	ACC
Production	PRD

Others?

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Examples - Entra ID Groups

SG_INT_%Scope%_%freeform%_%Release%

Element	Description	Mandatory	Format
SG	prefix for security groups in Entra ID	Yes	Fixed - 2 characters
INT	prefix for Intune related groups	Yes	Fixed - 3 characters
%Scope%	Refers to the scope of the group: user or device.	Yes	DVC – Device USR - User
%FreeForm%	Used to describe the Configuration Profile purpose	Yes	
%Release%	Refers to the release phase	No	*See generic elements*

- SG_INT_DVC_AllLinuxDevices_TST
- SG_INT_DVC_App_GoogleChrome

Examples – AP Profiles

AUT_%Platform%_%Mode%_%freeform%_%Release%

Element	Description	Mandatory	Format
AUT	prefix for Autopilot deployment profiles	Yes	Fixed - 3 characters
%Platform%	Refers to the platform the policy applies to	Yes	*See generic elements*
%Mode%	Deployment mode	Yes	Fixed – 2 Characters Possible values are UD – UserDriven SD - SelfDeployed
%FreeForm%	Used to describe the compliance policy purpose	Yes	
%Release%	Refers to the release phase	No	*See generic elements*

- AUT_WIN_UD_DefaultProfile_TST

Examples – Intune Compliance Policies

COM_%Platform%_%freeform%_%Release%

Element	Description	Mandatory	Format
COM	prefix for compliance policies	Yes	Fixed - 3 characters
%Platform%	Refers to the platform the policy applies to	Yes	*See generic elements*
%FreeForm%	Used to describe the compliance policy purpose	Yes	
%Release%	Refers to the release phase	No	*See generic elements*

- COM_WIN_DefaultCompliance_TST
- COM_WIN_DefaultCompliance_PRD
- COM_WIN_RebootIn30days_TST
- COM_MAC_DefaultCompliance
- COM_AND_MDECompliance

Examples – Device Categories

CAT_%Platform%_%Release%

Element	Description	Mandatory	Format
CAT	prefix for device categories	Yes	Fixed - 3 characters
%Platform%	Refers to the platform the policy applies to	Yes	See section 2.1 Platforms
%Release%	Refers to the release phase	No	See section 2.2 Releases

- CAT-WIN-TST
- CAT-WIN-PRD
- CAT-MAC-TST
- CAT-LNX-PRD

Demo

Naming Conventions

Release Management

Versioning

Consider adding versioning to your Intune profiles

Allows for:

- Change tracking
- Rollback

Test / Acceptance / Production

Separate Tenants

Pro:

- Maximum risk reduction
- Suitable for intrusive testing

Con

- Optimal setup requires everything duplicated – not only Intune (think Entra … MDE)
- Difficult to maintain parity with production environment
- Additional operations : export / import
    - Can be mitigated using tools
    - … or full automation (Devops…)

Naming Conventions

Pro

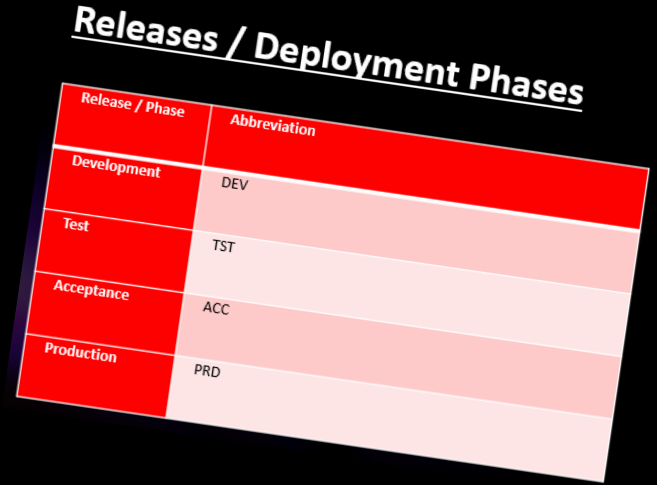
- Easy to implement
- Low(er) operational overhead

Con

Triple (or more) similar objects in one tenant

Staggered deployments - General

- Use naming convention for clear structure
- Works for a lot of policy types and other elements in Intune
- Also works for your assignment groups in Entra ID



Releases / Deployment Phases

Release / Phase	Abbreviation
Development	DEV
Test	TST
Acceptance	ACC
Production	PRD

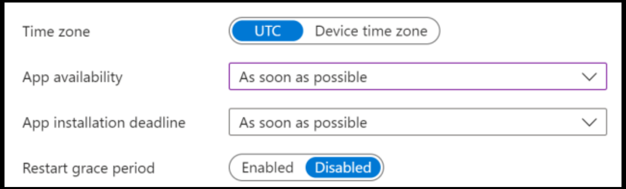
Staggered deployments – Updates too

Deployment Rings for Microsoft Updates

- Native policies support availability + deadline

3rd party updates

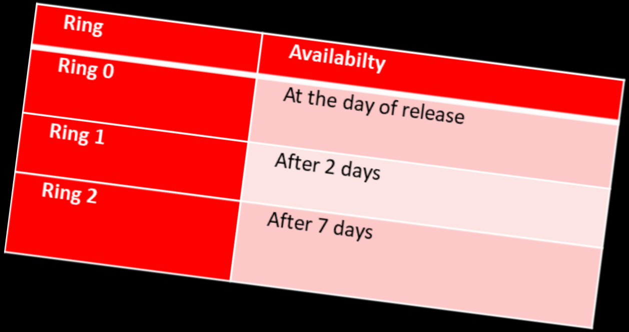
- Use the assignments of the app model



Time zone	[✓ UTC] Device time zone
App availability	As soon as possible
App installation deadline	As soon as possible
Restart grace period	Enabled [✓ Disabled]

Policies

- Manual or automated assignments to deployment rings



Ring	Availabilty
Ring 0	At the day of release
Ring 1	After 2 days
Ring 2	After 7 days

Monitoring & Reporting

Intune Auditing

Enabled by default in the Intune tenant

Built-in audit logs record change activities

- Create
- Edit
- Delete
- Assign
- Remote Actions

Accessible for

Global Administrators

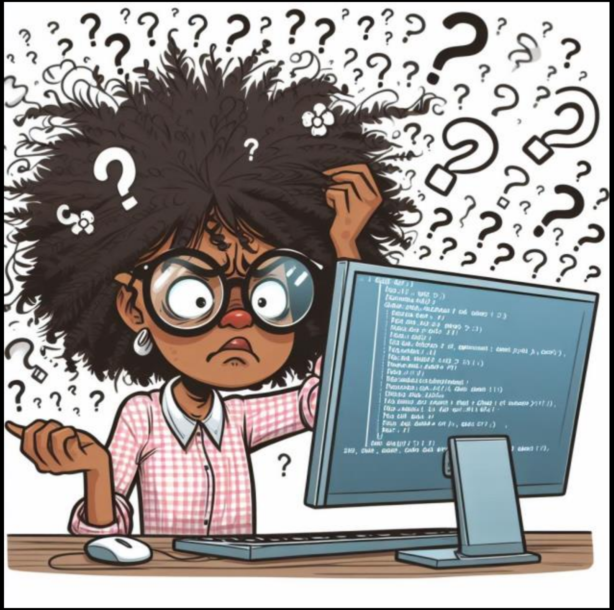
Intune Service Administrators

Intune custom role w Audit data read permissions

Get in to control via simple life hacks

Get in control via:

- Removing permissions ;)
- Implement RBAC (least privileged)
- Notification of (production) changes in Microsoft Intune
- Great examples by Peter Klapwijk; inthecloud247.com

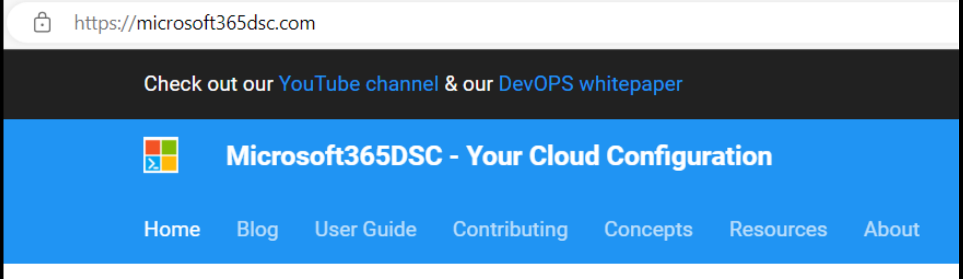


How to get in control and get rid of configuration drifts?

Desired State Configuration

Get in control via Desired State Config

Microsoft 365 DSC


https://microsoft365dsc.com

Check out our YouTube channel & our DevOPS whitepaper

Microsoft365DSC - Your Cloud Configuration

Great Blog by Intune PG; Configuration as code for Microsoft Intune:
https://techcommunity.microsoft.com/t5/intune-customer-success/configuration-as-code-for-microsoft-intune/ba-p/3701792

Simeon Cloud (paid commercial)

Demo

Monitoring & Reporting

Documenting

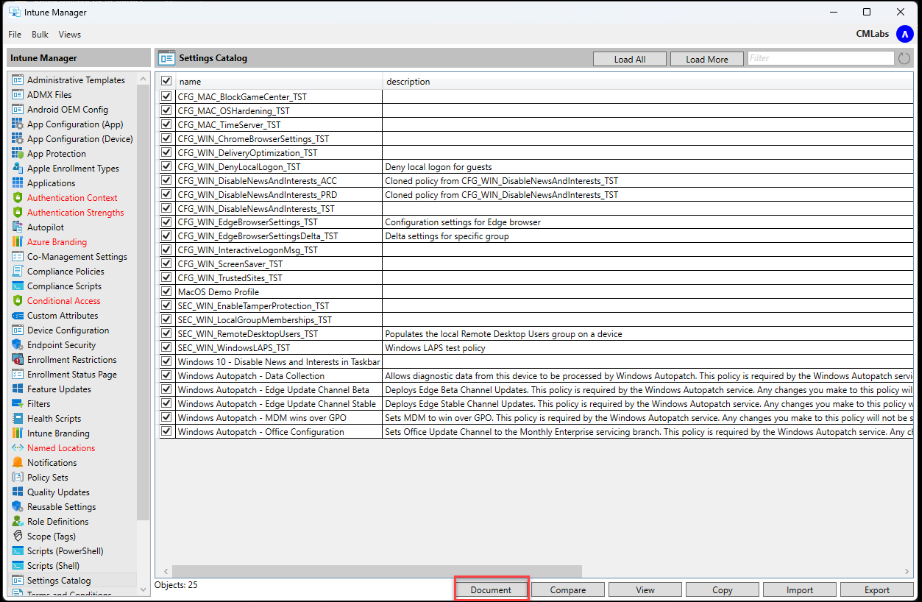
Different Approaches are possible

- Manually (you don’t want to do this)
- Semi-Automated - Intune Management Tool
- Fully Automated

Intune Management Tool

Community tool developed by Micke Karlsson

https://github.com/Micke-K/IntuneManagement



☑	name	description
☑	CFG_MAC_BlockGameCenter_TST	
☑	CFG_MAC_OSHardening_TST	
☑	CFG_MAC_TimeServer_TST	
☑	CFG_WIN_ChromeBrowserSettings_TST	
☑	CFG_WIN_DeliveryOptimization_TST	
☑	CFG_WIN_DenyLocalLogon_TST	Deny local logon for guests
☑	CFG_WIN_DisableNewsAndInterests_ACC	Cloned policy from CFG_WIN_DisableNewsAndInterests_TST
☑	CFG_WIN_DisableNewsAndInterests_PRD	Cloned policy from CFG_WIN_DisableNewsAndInterests_TST
☑	CFG_WIN_DisableNewsAndInterests_TST	
☑	CFG_WIN_EdgeBrowserSettings_TST	Configuration settings for Edge browser
☑	CFG_WIN_EdgeBrowserSettingsDelta_TST	Delta settings for specific group
☑	CFG_WIN_InteractiveLogonMsg_TST	
☑	CFG_WIN_ScreenSaver_TST	
☑	CFG_WIN_TrustedSites_TST	
☑	MacOS Demo Profile	
☑	SEC_WIN_EnableTamperProtection_TST	
☑	SEC_WIN_LocalGroupMemberships_TST	
☑	SEC_WIN_RemoteDesktopUsers_TST	Populates the local Remote Desktop Users group on a device
☑	SEC_WIN_WindowsLAPS_TST	Windows LAPS test policy
☑	Windows 10 - Disable News and Interests in Taskbar	
☑	Windows Autopatch - Data Collection	Allows diagnostic data from this device to be processed by Windows Autopatch. This policy is required by the Windows Autopatch servi
☑	Windows Autopatch - Edge Update Channel Beta	Deploys Edge Beta Channel Updates. This policy is required by the Windows Autopatch service. Any changes you make to this policy wil
☑	Windows Autopatch - Edge Update Channel Stable	Deploys Edge Stable Channel Updates. This policy is required by the Windows Autopatch service. Any changes you make to this policy w
☑	Windows Autopatch - MDM wins over GPO	Sets MDM to win over GPO. This policy is required by the Windows Autopatch service. Any changes you make to this policy will not be s
☑	Windows Autopatch - Office Configuration	Sets Office Update Channel to the Monthly Enterprise servicing branch. This policy is required by the Windows Autopatch service. Any c

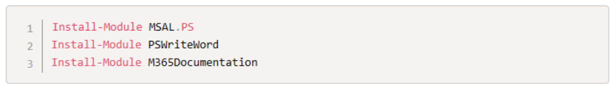
Objects: 25

Automatic Microsoft 365 Documentation

Community tool developed by Thomas Kurth

[Automatic Intune Documentation evolves to Automatic Microsoft 365 Documentation - Workplace Ninja's (wp]

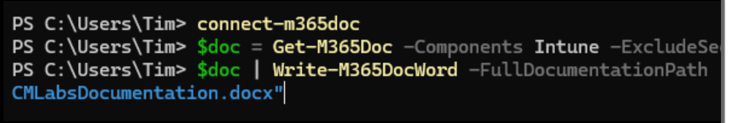
Install from PowerShell Gallery



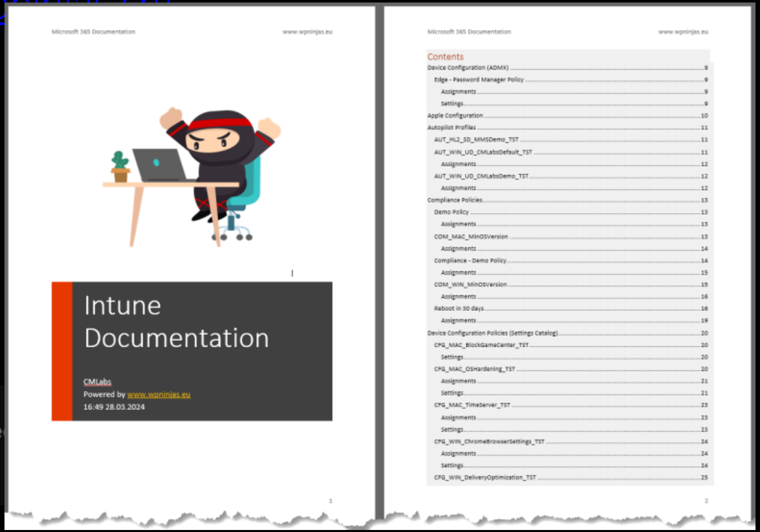
```
Install-Module MSAL.PS
Install-Module PSWriteWord
Install-Module M365Documentation
```

* Also install PSWriteOffice module for latest version

Run



```
PS C:\Users\Tim> connect-m365doc
PS C:\Users\Tim> $doc = Get-M365Doc -Components Intune -ExcludeSe
PS C:\Users\Tim> $doc | Write-M365DocWord -FullDocumentationPath
CMLabsDocumentation.docx"
```



Microsoft 365 Documentation www.wpninjas.eu

Intune Documentation

CMLabs
Powered by www.wpninjas.eu
16:49 28.03.2024

1

Microsoft 365 Documentation www.wpninjas.eu

Contents

2

Intune CD

Intune Continuous Delivery

Community Tool developed by Tobias Almen

[GitHub - almenscorner/IntuneCD at almenscorner.io]

IntuneCD
Intune as code

Separate Frontend available: IntuneCD Monitor

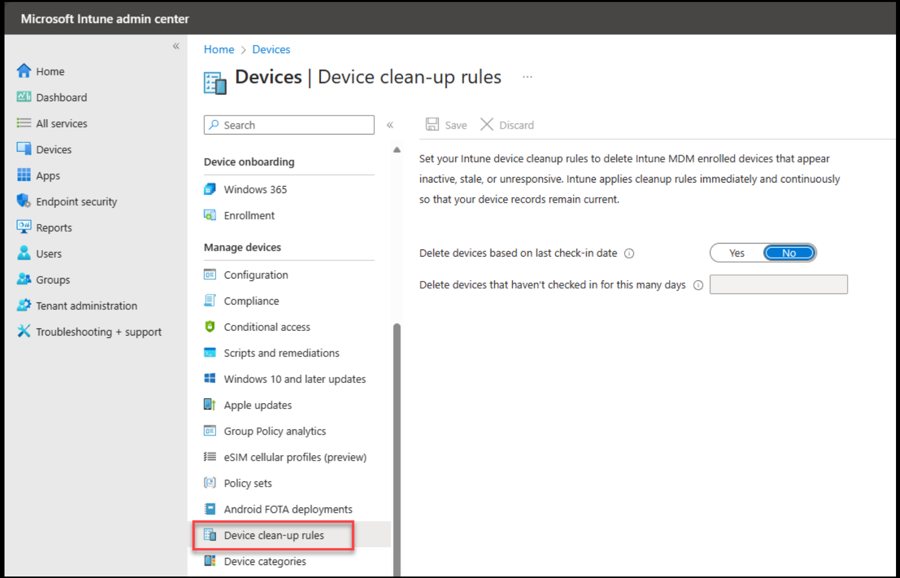
Demo

Documenting

Keeping it clean

Device Cleanup Rules

- Automatically delete stale and inactive devices
- Runs continuously
- Does not clean-up objects in Entra ID



Devices | Device clean-up rules

Set your Intune device cleanup rules to delete Intune MDM enrolled devices that appear inactive, stale, or unresponsive. Intune applies cleanup rules immediately and continuously so that your device records remain current.

Delete devices based on last check-in date: Yes [✓ No]

Delete devices that haven't checked in for this many days

Obsolete Objects

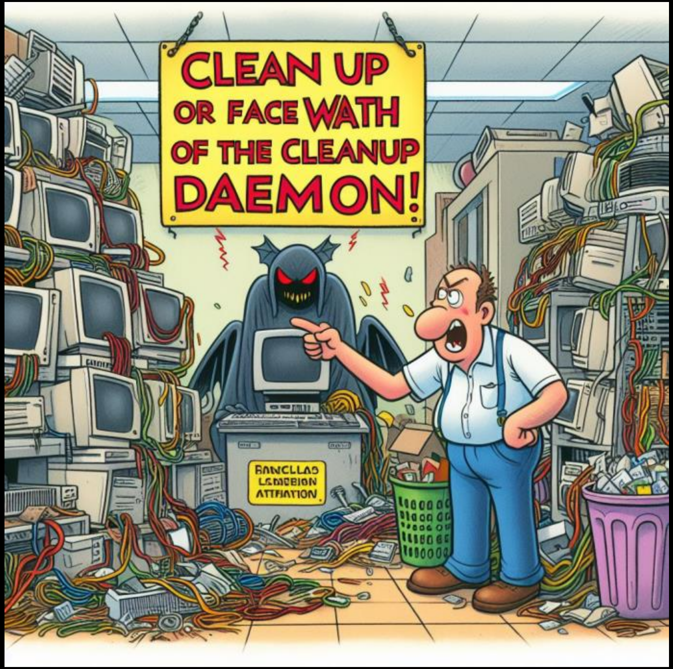
Cleanup your devices in Entra ID

Use Azure Automation to:

- Disable devices after X number of days
- Remove disabled devices after X number of days
- Monitor device disablement / detection

But what about:

- LAPS
- BitLocker keys



Other best practices

Optimize the offboarding process

Not only for Intune

- Entra
- MDE
- Others?

What to do with Emergency Offboarding?

- Disable login directly is difficult in a modern world
- Great blog: https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/zero-trust-rapid-offboarding-with-intune-and-microsoft-entra-id/ba-p/4067612 & https://www.inthecloud247.com/assign-deny-local-log-on-user-right-to-an-azure-ad-group-by-using-microsoft-intune/

Hygiene

Access to X is often given ad-hoc and are persistent.
And are a security risk….

Combine…

- Access Packages
- Access Reviews

…. to manage your groups

Demo

Hygiene

Please evaluate this session in the App.

THANK YOU

Are there any questions?