

Intune Misconfigurations in the Wild: What We See, What You Should Fix

Janic Verboon & Nicola Suter



*Workplace Ninja
Summit 2025*



Thank you Sponsors

www.wpninjas.eu
#WPNinjaS

Diamond Sponsor



Microsoft

Platinum Sponsors

2Pint



PATCH MY PC



RECAST SOFTWARE

glueck kanja

Gold Sponsors



nerdio

baseVISION
SECURE & MODERN ENDPOINT MANAGEMENT

Rimo3

SOFTWARE
CENTRAL

eido

EPIC FUSION
BRING IT ALL TOGETHER

Silver Sponsors

APENTO

PROACT

control UP
UMB creating time®

water
IT Security & Defense



About Janic Verboon

www.wpninjas.eu
#WPNinjaS

Focus

Endpoint Management, Entra ID

From

Switzerland

My Blog

-



Certifications

Some Microsoft
Android Enterprise Expert
Certified Beer Lover

Hobbies

Concerts, running, football

Contact



/janic-verboon-04b11b114



/Janic1904



About Nicola Suter

www.wpninjas.eu
#WPNinjaS

Focus

Security, ITDR

From

Switzerland

My Blog

tech.nicolonsky.ch
nicolasuter.medium.com



Certifications

Various & Microsoft MVP

Hobbies

Cycling, running, mountaineering

Contact

hi@nicolasuter.ch



High-Level Agenda

www.wpninjas.eu
#WPNinjaS

- **Session Format**
- **(Mis) Configurations**
aka Simple Toggles to Flip
- **Remediation Guidance**
aka not so easy toggles to flip
- **Recap and resources**
- **Questions**

Format of this session





Storyline aka Disclaimer

www.wpninjas.eu
#WPNinjaS

- We do a lot of Intune & security assessment as part of daily biz
- We want to highlight some common 'misconfigurations' that we see the most
- Maybe there are valid reason why you have configured something different, our opinion is not 'the right opinion' only truth
- We want to give you some stats, a rationale and how to fix those in your environment.
- Most misconfigurations don't require a "fancy" configuration because it is built in....
- We will go through a list of common misconfigurations and will show
 - Excerpt, impact and rationale
 - (Live) Demo about how to identify the misconfiguration
 - Demo / Guidance how to remediate the misconfiguration

Reference to CIS Controls....

Reference to CIS Benchmarks....

Reference to Microsoft and deviating from framework recommendations.



CIS Critical Security Controls

www.wpninjas.eu
#WPNinjaS

CIS control help you to follow prioritized set of actions to protect your organization and data from cyber-attack vectors. An excerpt of the currently 18 available controls as part of v8.1:

- CIS Control 1: Inventory and Control of Enterprise Assets
- CIS Control 2: Inventory and Control of Software Assets
- CIS Control 4: Secure Configuration of Enterprise Assets and Software
- CIS Control 7: Continuous Vulnerability Management

We often face environments where (too many of) the right tools are available, but processes are missing or inadequate, and people are missing an overall view or understanding about their infrastructure and security posture.

Device registration and enrollment

Getting your device under Intune management





What do all these settings do?

Microsoft Entra join and registration settings

Users may join devices to Microsoft Entra ⓘ

AllSelectedNone

Selected
1 member selected

Users may register their devices with Microsoft Entra ⓘ

AllNone

Platform settings [Edit](#)

Type	Platform	Min	Max	Personally owned	Blocked manufacturers
Android Enterprise (work p...	Allow	14.0		Allow	
iOS/iPadOS	Allow	17.0		Allow	N/A
macOS	Allow	N/A	N/A	Block	N/A
Windows (MDM)	Allow			Block	N/A

Mobility (MDM and WIP) ...

+ Add applicationRefresh⚙️ Manage view ▾

Name ↑

- Microsoft Intune
- Microsoft Intune Enrollment

Microsoft Intune ...

MDM user scope ⓘ

☐ None☒ Some☐ All

Groups

1 group selected

MDM terms of use URL ⓘ

MDM discovery URL ⓘ

MDM compliance URL ⓘ

[Restore default MDM URLs](#)

Windows Information Protection (WIP) user scope ⓘ



Common Issues

www.wpninjas.eu
#WPNinjaS

- Users may join devices, MDM Scope Only apply to Windows 10 and later devices and user-driven scenarios
 - Inconsistency between groups makes leads to enrollment issues
- A lot of different and distinct groups are used
 - E.g. users allowed to enroll Android BYOD
 - Another BYOD User group
 - Policies, Apps and other configurations are inadequately targeted, but this is a topic for later 😊



Device Platform restriction & ownership

www.wpninjas.eu

#WPNinjaS

Platform Restrictions Apply for both		
Enrollment Restrictions Apply		Enrollment Restrictions do NOT Apply
Platform	Personal	Corporate
Windows	• OOBE • Work or school accounts	• Autopilot • Hybrid Join (GPO) • Co-Management • AVD • Bulk registration token
Android	• Android Device Administrator • AE pers with work profile	• All AE corp. owned scenarios • All AOSP methods • Android Device Administrator with corporate identifier)
iOS	• Apple user enrollment • Apple Device enrollment	• Apple Device enrollment (with corporate identifier) • Apple Automated Device enrollment
macOS	• Apple Device enrollment	• Apple Device enrollment (with corporate identifier) • Apple Automated Device enrollment



Enrollment restriction ordering

www.wpninjas.eu
#WPNinjaS

- Intune enrollment restrictions get applied to users based on Priority

Priority	Name	Assigned
1	Allow BYOD MDM enrollment	No
Default	All Users	Yes

Priority	Allow pers Android	Allow pers iOS	Assigned to
1	Allow	Allow	sg-intune-allowbyod
Default	Block	Block	All Users



Policies with a higher priority win over policies with a lower priority



Bundling enrollment restrictions with Tenant customizations

www.wpninjas.eu
#WPNinjaS

- If Administrators want to block enrollment prompts in the Company Portal app on Android & iOS they can do so by configuring the Device enrollment setting in the Tenant customization policy.

Configuration

Enrollment

Customize the setup experience in Company Portal for Android and iOS/iPadOS. [Learn more](#)

Device enrollment ⓘ

Unavailable

Priority	Device enrollment	Assigned to
1	Available with prompts	sg-intune-allowbyod
Default	Unavailable	All Users



Admins can create a maximum of 10 Tenant customization policies.



Entra ID Device settings

Require Multifactor Authentication to register or join devices with Microsoft Entra ⓘ

Yes

No

You already require Multifactor Authentication to register or join devices with Microsoft Entra in a Conditional Access policy. To correctly enforce the Conditional Access policy, set this to No. [See Conditional Access policies.](#)

Conditional Access

Grant

Control access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

- ☐ Require multifactor authentication ⓘ
- ☐ Require authentication strength ⓘ

CA006-Global-BaseProtection-RegisterDevice-AnyPlatform-MFA

Conditional Access policy

Delete View policy information View policy impact

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control access based on all or specific apps, internet resources, actions, or authentication context. [Learn more](#)

Name *

CA006-Global-BaseProtection-RegisterDevi...

Select what this policy applies to

User actions

Assignments

Users ⓘ

All users included and specific users excluded

Select the action this policy will apply to

☐ Register security information

☒ Register or join devices

Target resources ⓘ

1 user action included

Network **NEW** ⓘ

Not configured

Enable policy

Report-only

On

Off

Only "Require multifactor authentication" can be used in policies created for the "Register or join devices" user action. [Learn more](#)



Device registration and enrollment

www.wpninjas.eu
#WPNinjaS

Check	• Entra > Devices > Device Settings • Intune > Devices > Enrollment > Platform Restrictions
Rationale	Entra device settings & Intune enrollment restrictions apply to user-driven device enrollment and registration scenarios.
Impact	• Users are unable to enroll their devices into management • Malicious actors can enroll devices to gain persistence • Settings do not have the desired effect because they're misunderstood
Real-world-environment-distribution	8/10
Mitigation	• Configure MDM Scope and Entra Join settings • Configure Intune enrollment restrictions • Require MFA using Conditional Access
References	• CIS Critical Security Control 1: Inventory and Control of Enterprise Assets

Assignments





Assignments - Common issues

www.wpninjas.eu
#WPNinjaS

What we often see

Policy conflicts

- Overlapping groups / Devices in multiple groups
- Wrong dynamic queries in groups and filters

Not extensible

The environment doesn't allow future use-cases such as:

- Provisioning a device without any policies (e.g. for support cases or troubleshooting)
- Introducing or building a new client type (e.g., W365, Developer Clients,...)

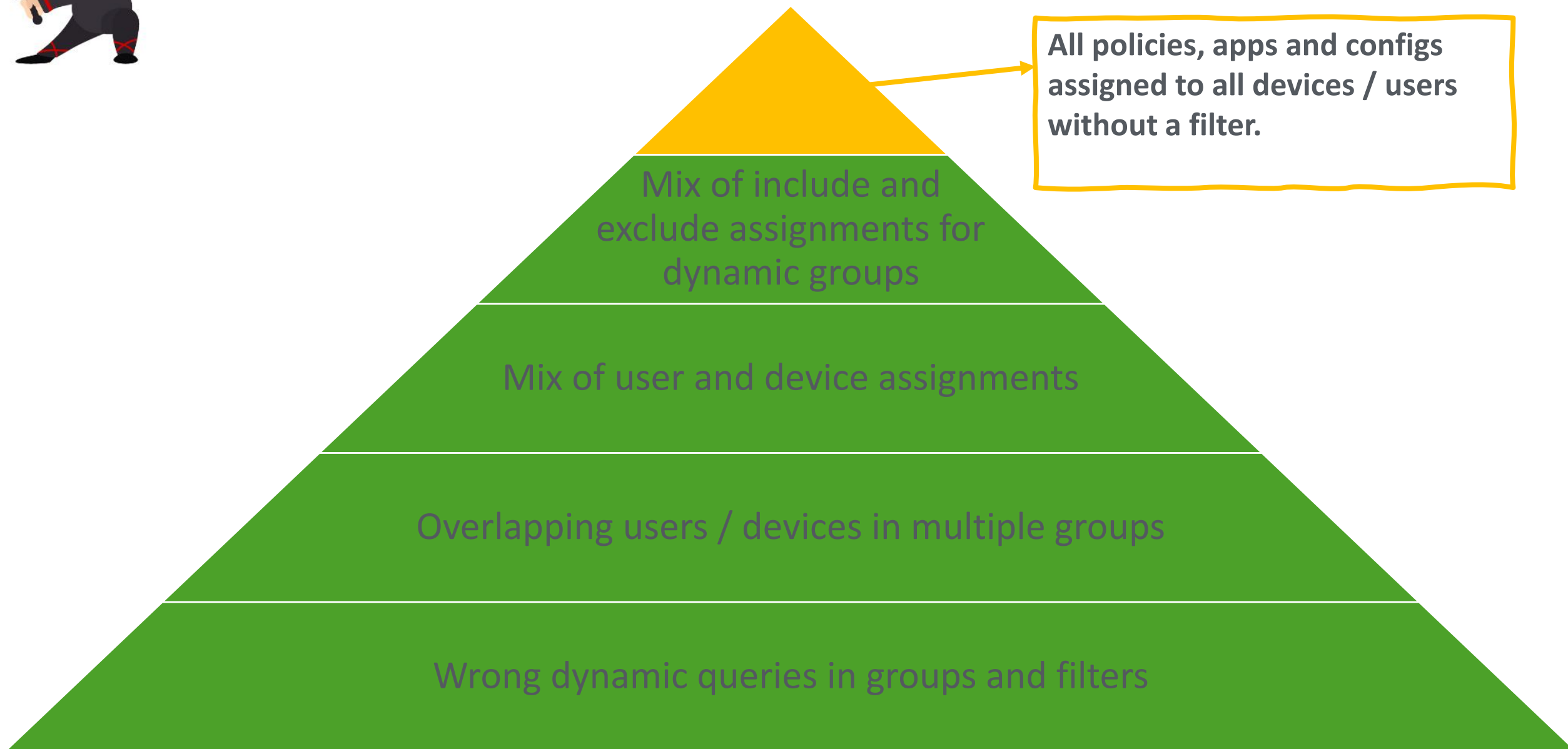
No assignment strategy

- Too many assignments, unintended installations...
- A little bit of try and error



Intune Assignment Pyramid of Pain

www.wpninjas.eu
#WPNinjaS



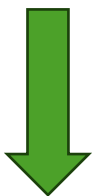


Intune Grouping and Targeting

www.wpninjas.eu
#WPNinjaS

Current config – 1 policy (without exception)

Policy 1: Device and Resource Redirection	
Do not allow COM port redirection	Enabled
Do not allow drive redirection	Enabled
Do not allow LPT port redirection	Enabled
Do not allow supported Plug and Play device redirection	Enabled



Included groups	All devices
Excluded groups	--

New config – with exception – 3 policies

Policy 1: Device and Resource Redirection	
Do not allow COM port redirection	Enabled
Do not allow drive redirection	Enabled
Do not allow LPT port redirection	Enabled



Included groups	All devices
Excluded groups	--

Policy 2: Device and Resource Redirection	
Do not allow supported Plug and Play device redirection	Enabled



Included groups	All devices
Excluded groups	Exclusion-Group1 (device group)

Policy 3: Device and Resource Redirection	
Do not allow supported Plug and Play device redirection	Disabled



Included groups	Exclusion-Group1 (device Group)
Excluded groups	

Approach (device based):

- First, create a new Entra group containing the devices which are excepted.
- Remove the respective setting from the current Policy 1.
- Create a new Policy 2 with the respective setting. Assign it to all devices but exclude the new Entra group.
- Create a new Policy 3 with the respective setting and assign it to the new Entra group.



Intune Grouping and Targeting - Bonus

www.wpninjas.eu
#WPNinjaS

Original Challenge

- Exclude a new device type from 200+ Intune policies and 300+ mobile applications.

Assumption

- A few lines of PowerShell will solve this easily.

Additional Challenges

- Intune assignments are handled differently depending on the configuration / policy type
- The Intune / Microsoft Graph API does not always provide the option to **add** an assignment, a HTTP **POST** to the */assignments* route will override existing assignments.

The Solution

- A quick and dirty PowerShell script that will do this job for you and back-up the assignments if the API doesn't support the add option.



Assignments – Facts and Figures

www.wpninjas.eu
#WPNinjaS

Check	• Intune Landing Page Stats • Devices > Monitor > Configuration policy assignment failures
Rationale	• Policy conflicts shall be avoided at all costs.
Impact	• Policy conflicts can cause undesired configurations on endpoints and lead to degraded security posture.
Real-world-environment-distribution	• Policy conflicts with severe impact: 2/10 environments • No assignment strategy or process: 6/10 environments
Mitigation	• Define a process for assignment handling • Regularly review for conflicts or even automate this 😊
References	• -



In case of a new policy conflict existing clients will block the new policy from being applied to ensure they retain the existing settings.

Local Administrator (Mis)Management

A wise man (Sami Laiho) once said: Admin Rights are not Human rights





Administrators everywhere?

www.wpninjas.eu
#WPNinjaS

- Users became local administrators by accident
- Users 'need' administrator permissions
- Helpdesk or IT staff 'needs' administrative access to each Intune device's C\$ share





What we often observe

Group Management

The built-in Administrators group is not overridden and thus managed by Intune and contains different members on existing clients.

- Device enrollments without Autopilot? Enrolling user became a built-in admin.
- Are Global Admins still part of your built-in admin group?

LAPS

Is LAPS really used for helpdesk and support scenarios? Or was it just deployed.

- Do you review local admin group changes or who's signing-in with local administrator permissions?

Additional Admins

A subset of users might still require administrative permissions, that's okay. Try to use EPM or similar solution(s), if not possible, try to grant those privileges carefully.



Local Administrator Management

www.wpninjas.eu
#WPNinjaS

Check	• Custom Intune Detection Script for Administrators Group • MDE Advanced Hunting Query: Who's signing in with administrator permissions
Rationale	• Windows and third-party security products and features can often be bypassed or tampered with local administrator permissions. Removing these permissions increases the attacker's cost.
Impact	• Especially for existing clients and Intune tenants there's a risk of undesired or historically present administrators on endpoints.
Real-world-environment-distribution	• Unmanaged Administrators Group: 5/10 environments
Mitigation	• Override the built-in administrator's group with an Intune Policy
References	• CIS Control 5: Account Management - 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts.

Security Baselines





Introduction

www.wpninjas.eu

#WPNinjaS

- Do you know, what the following Windows Security Features have in common?
 - LSA Protection
 - Windows LAPS
 - Windows Defender Exploit Guard Network Protection
 - Windows Defender Exploit Guard ASR
 - NTLM Auditing and NTLMv2 enforcement
- These settings are **not configured** or **not enabled** by default. Security Baselines help us to identify, enable and deploy these features and hardening measures to protect our enterprise assets such as Windows clients or servers.



Why use security baselines?

www.wpninjas.eu
#WPNinjaS



Remember: Security Baselines should still be seen as Guidelines; some settings might not work for you and your organization.



Security Baseline providers

www.wpninjas.eu
#WPNinjaS

Microsoft

Provided for Microsoft products such as:

- Microsoft Windows
- Microsoft Window Server
- Microsoft Edge
- Microsoft 365 Apps for Enterprise (Office)

CIS

Provides benchmarks for all sort of products, Windows, Browser, macOS, Android, Linux, iOS



DOD (STIG)

Provides benchmarks for all sort of products, Windows, Browser, macOS, Android, Linux, iOS

NIST

Provides benchmarks for all sort of products, Windows, Browser, macOS, Android, Linux, iOS



Of course there are lots of other different other providers.



Challenge

www.wpninjas.eu
#WPNinjaS

We often see one of the following scenarios at customers:

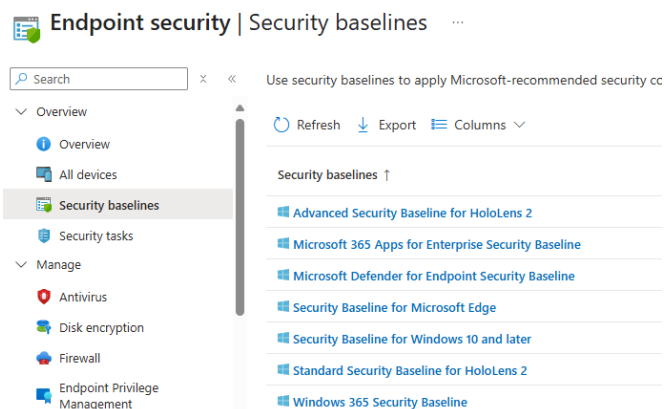
No Security Baseline

The customer is not using any security baselines at all.

Client settings are configured

Built-in Intune Baseline

The customer is using the built-in Security baseline within Microsoft Intune.



Baseline is in place but no documentation

The customer has adopted a security baseline but has not documented any deviations.

Having no documentation available makes the update of security baseline increasingly harder.



Why you should not use the built-in baseline

www.wpninjas.eu
#WPNinjaS

- **Error Prone:** The built-in Microsoft baseline proved to have some flaws during their last releases
Example: User right policies were released with the names of the groups instead of SID's I guess you can all guess how that turned out on non English Operating Systems ;)
- **Lack of documentation:** The built-in baselines don't come with proper Excel sheets, which help you to document deviations
- **Releases:** It takes a long time until Microsoft releases new versions of their baselines: Example Win11 24H2 was released in October 2024, the new built-in baseline got released in February 2025 → 5 months later
- **Exception management:** The built-in baseline does not allow you to remove a setting to implement a proper deviation.



Our recommendation: If you want to use the MS Security baseline framework, review the provided Excel sheets and build your own security baseline profiles using Settings Catalog & Endpoint Security



Security Baseline exception handling

www.wpninjas.eu
#WPNinjaS

Current config – 1 policy
(without exception)

Policy 1: Device and Resource Redirection	
Do not allow COM port redirection	Enabled
Do not allow drive redirection	Enabled
Do not allow LPT port redirection	Enabled
Do not allow supported Plug and Play device redirection	Enabled



Included groups All devices

Excluded groups --

New config – with exception – 3 policies

Policy 1: Device and Resource Redirection

Do not allow COM port redirection	Enabled
Do not allow drive redirection	Enabled
Do not allow LPT port redirection	Enabled



Included groups All devices

Excluded groups --

Policy 2: Device and Resource Redirection

Do not allow supported Plug and Play device redirection	Enabled
---	---------



Included groups All devices

Excluded groups Exclusion-Group1
(device group)

Policy 3: Device and Resource Redirection

Do not allow supported Plug and Play device redirection	Disabled
---	----------



Included groups Exclusion-Group1
(device Group)

Excluded groups

Approach (always device based):

- First, create a new Entra group containing the devices which are excepted.
- Remove the respective setting from the current Policy 1.
- Create a new Policy 2 with the respective setting. Assign it to all devices but exclude the new Entra group.
- Create a new Policy 3 with the respective setting and assign it to the new Entra group.



How you should document your SECB

www.wpninjas.eu
#WPNinjaS

- Ensure to keep the Excel sheets up to date

C	D	E	F	G
Intune Setting Name	Microsoft Recommendation	Customer Configuration	Justification	Intune Configuration Profile
Prevent enabling lock screen camera	Enabled	Enabled		Windows-SECB-SettingsCatalog-WindowsSecurityBaseline-Win11
Prevent enabling lock screen slide show	Enabled	Enabled		Windows-SECB-SettingsCatalog-WindowsSecurityBaseline-Win11
Apply UAC restrictions to local accounts on network logons	Enabled			Windows-SECB-SettingsCatalog-WindowsSecurityBaseline-Win11
Configure SMB v1 client driver	Disable driver			Windows-SECB-SettingsCatalog-WindowsSecurityBaseline-Win11
Configure SMB v1 server	Disabled			Windows-SECB-SettingsCatalog-WindowsSecurityBaseline-Win11

- Document:
 - The state of the setting in your environment
 - If you deviate from the recommendation, that's fine but state the reason why you deviated, add a comment or add the change nr to your ITSM solution.
 - Document in which Intune profile the setting is configured.



Keeping your documentation updated will help you in the long term.
Especially if you want to update your security baselines



Summary

www.wpninjas.eu
#WPNinjaS

Check	• Intune & Your Document location
Rationale	Define the to be used security benchmarks in your organization, maintain them and document them.
Impact	• Common security features are not enabled by default • Increased attack surface
Real-world-environment-distribution	8/10
Mitigation	• Implement Security Baselines • Maintain Security Baselines • Document Security Baselines
References	• Security baselines guide Microsoft Learn • CIS Benchmarks®

Patch Management





Introduction

www.wpninjas.eu
#WPNinjaS



It's the year 2025

And patch management can still be a burden!



Patch Management flavors

www.wpninjas.eu
#WPNinjaS

Security Updates

Monthly Security Updates

Feature updates

Released once a year



Driver and Firmware Updates

Released by the respective OEM's

Application Updates

M365 apps, Browsers, Business Apps etc..



Microsoft's Approach

www.wpninjas.eu
#WPNinjaS

- In the past we had WUfB and Windows Autopatch
- Now Microsoft unified those two approaches under the Windows Autopatch umbrella.
- Autopatch covers:
 - Quality Updates
 - Feature Updates
 - Driver & Firmware Updates
 - M365 apps updates



Regardless which solution you use, ensure that the devices are added to the Update rings!



Autopatch things to look out for

www.wpninjas.eu
#WPNinjaS

- Regularly review the not ready blade in Microsoft Intune and check why clients are not ready for Autopatch
- Intune > Reports > Windows Quality updates

Name ↑↓	Device count ↓	Up to date ↑↓	Not up to date ↑↓	In progress ↑↓	Not ready ↑↓	% of latest quality update ↑↓
> 	836	779	57	0	68	93%

- Intune > Devices > Monitor > Autopatch Group Membership will provide you additional information

Status

 Need attention

Conflicting Configuration

Description	Windows Autopatch has identified configurations that will prevent the device from receiving Windows updates, drivers, and firmware.
Registry keys	SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\DoNotConnectToWindowsUpdateInternetLocations
Recommended action	Remove the conflicting configuration from the device. Learn more about conflicting configuration .

Status

 Inactive

The device has not synchronized with Intune for the past 28 days.



- Review the Autopatch Tenant health status at: Intune Tenant Admin > Tenant Management

Search ⓘ			
Name ↑↓	Description	Severity ↑↓	Status ↑↓
Manage client broker	Install Windows Autopatch client agent to devices ...	📘 Informational	🔄 In progress



Firmware patching

www.wpninjas.eu
#WPNinjaS



There is one important rule

Only use ONE system to patch your drivers and firmware.

Either Windows Autopatch or the OEM solution



Third Party App Patching

www.wpninjas.eu
#WPNinjaS

- Ensure that processes are in place within your org to patch third party Apps
 - Release management
 - Roll back plans
- Look at awesome products like PatchmyPC to automate the patching process of third-party apps
- Know who the application responsible are to give green light for business-critical releases



Summary

www.wpninjas.eu
#WPNinjaS

Rationale	Patching still is one of the most important practices
Impact	• Unpatched devices are still a big security threat. • Known vulnerabilities can be exploited
Real-world-environment-distribution	8/10
Mitigation	• Ensure all devices are part of update rings • Control those update rings on a regular basis • Patch third party apps
References	• CIS Critical Security Control 7: Continuous Vulnerability Management

Connector management and Tokens





Intune Connectors and Tokens

www.wpninjas.eu
#WPNinjaS

Managed Google Play

Microsoft Configuration Manager

Defender for Endpoint

TeamViewer Connector

Apple APNS

Must be renewed every 365 days

Apple VPP Token

Must be renewed every 365 days

Apple ADE Token

Must be renewed every 365 days

T&C must be approved 1-3 times per year

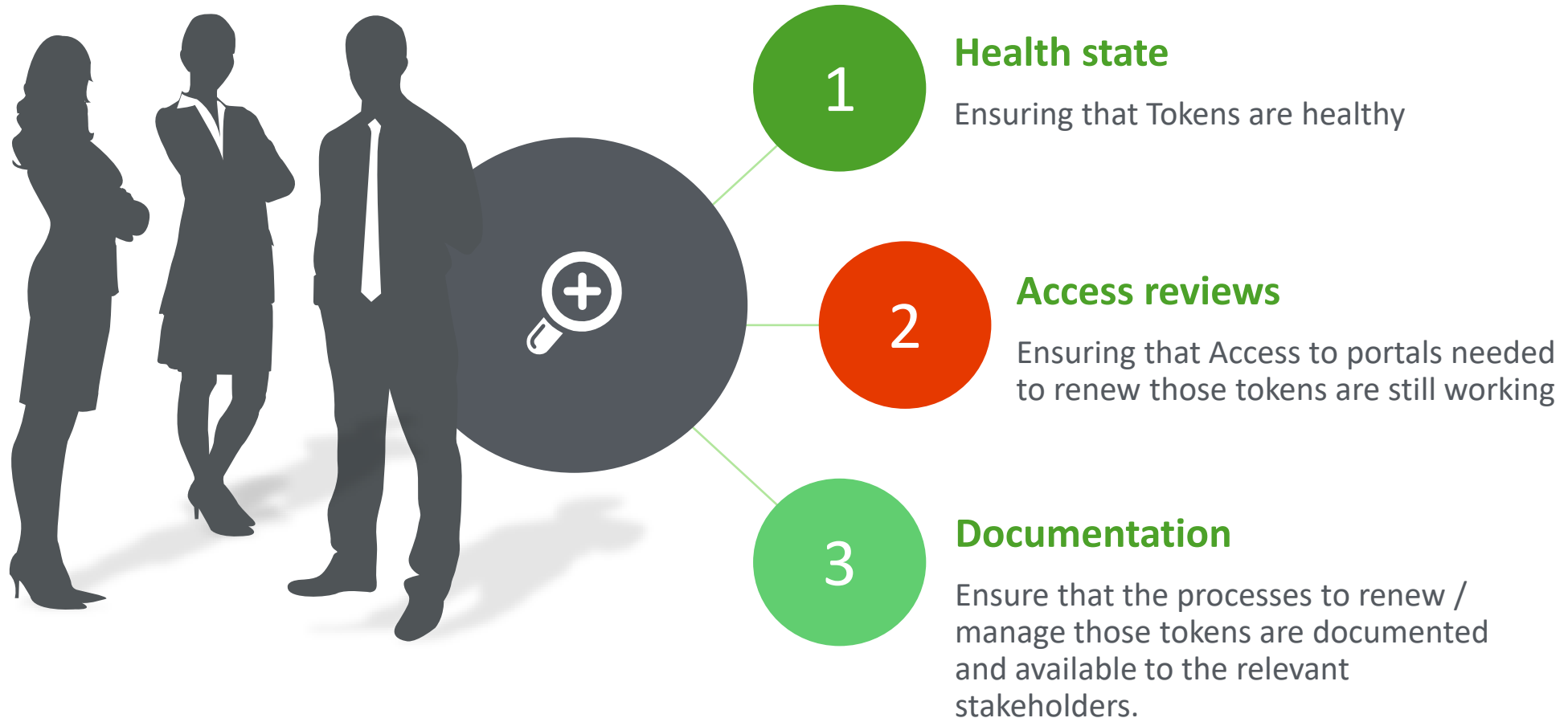
Intune Certificate Connector

NDES Certificates must be renewed from time to time



Aspects of Token Monitoring

www.wpninjas.eu
#WPNinjaS





Intune Certificate Connector

www.wpninjas.eu

#WPNinjaS

Check applies to:	Intune Certificate Connector
Rationale	The Intune Certificate Connector should be kept up to date. Versions are supported for 6 months after the release of a new versions.
Impact	Business continuity might be impacted if no certificates can be issued to devices / users
Real-world-environment-distribution	2/10
Mitigation	- Ensure that Auto upgrade is enabled - Check the version of the Connector regularly
References	Overview of Certificate Connector for Microsoft Intune - Azure Microsoft Learn Overview of Certificate Connector for Microsoft Intune - Azure Microsoft Learn

#Run the following command on your Intune Certificate Connector server to verify that Auto Upgrade is enabled:

Test-NetConnection -ComputerName autoupdate.msapproxy.net -Port 443

```
PS C:\> Test-NetConnection -ComputerName autoupdate.msapproxy.net -Port 443
```

```
ComputerName      : autoupdate.msapproxy.net
RemoteAddress     : 52.149.186.68
RemotePort        : 443
InterfaceAlias    : Wi-Fi
SourceAddress     : 10.10.3.143
TcpTestSucceeded  : True
```

#Check the version of the Intune Cert Connector using the browser dev tools

The screenshot shows the Intune Certificate Connector console. On the left, the 'Connection status' is 'Active' with a green checkmark. Below it, 'Last connected' is '08.09.2025, 21:19:57'. At the bottom, the 'Name' is 'jvms002'. On the right, the 'Preview' tab of the browser dev tools shows a JSON response. The 'connectorVersion' field is highlighted with a red box and contains the value '6.2406.0.2002'.

Name	Headers	Preview	Response	Initiator	Timing
33dbc651-3fce-4447-b7f9-bd...		<pre>{ "@odata.context": "https://graph.microsoft.com/beta/\$metadata", "connectorVersion": "6.2406.0.2002", "displayName": "jvms002", "enrolledDateTime": "0001-01-01T00:00:00Z", "id": "33dbc651-3fce-4447-b7f9-bdee89382d63", "lastConnectionDateTime": "2025-09-08T19:19:57.8334296Z", "machineName": null, "roleScopeTagIds": [], "state": "active" }</pre>			



Managed Google Play

www.wpninjas.eu
#WPNinjaS

Check applies to:	- Managed Google Play - Google Developer Accounts
Rationale	IT admins should ensure that at least two administrators accounts are added to the Managed Google Play Organization and that both accounts can still sign in to play.google.com/work
Impact	If access to the accounts is lost, this won't have an immediate impact, since the connection with Intune doesn't need to be renewed, but might have an impact on future activities.
Real-world-environment-distribution	2/10
Mitigation	- Ensure that two administrative accounts have access the Managed Google Play organization - Ensure that access credentials are shared within the team
References	Connect Intune account to managed Google Play account - Microsoft Intune Microsoft Learn



Apple Token Monitoring

www.wpninjas.eu
#WPNinjaS

Check applies to:	• Apple APNS Portal • Apple Business Manager
Rationale	Administrators should ensure that access to ABM and the APNS portal is given at any time. APNS access credentials should be present for multiple employees.
Impact	• If access to the APNS portal is lost, companies are at risk to loose management over devices. • If access to the ABM portal is lost VPP&ADE can't be renewed and T&C can't accepted.
Real-world-environment-distribution	7/10
Mitigation	• Use a Managed Apple ID in ABM for the APNS certificate • Ensure that multiple admin accounts exist.
References	• Connect Intune account to managed Google Play account - Microsoft Intune Microsoft Learn



Automate the Monitoring of your Apple Infrastructure

www.wpninjas.eu
#WPNinjaS

- The following script Automates the monitoring of:
 - APNS expiration
 - ADE Token expiration
 - ADE Token T&C approval
 - VPP Token expiration
 - VPP apps free licenses
 - LOB provisioning certificate



More information about the Automation can be found here: [WPNinja25-FromManualtomagical/Scripts/Intune Apple Monitoring at main · JanicVerboon/WPNinja25-FromManualtomagical](#)

Alert! Apple Management requires Attention

ADE Tokens at Risk

The following ADE Tokens are at risk, check if they haven't expired yet or if the new T&C must be accepted within Apple Business Manager

Token Name	Token Expiration	Last Successful Sync
Janic Verboon Intune	05/02/2026 10:22:55	09/07/2025 02:35:46

VPP Tokens at Risk

Please ensure that the following VPP Tokens get renewed before they expire!.

Token Name	Expiration Time
Janic Verboon	09/02/2025 14:16:36

VPP Licenses

The following VPP apps are about to run out of licenses, sign in to Apple Business Manager and acquire more licenses

VPP App Name	Associated Token	Free Licenses
Apple Configurator	Janic Verboon	49
Edubase Reader	Janic Verboon	10
Google Chrome	Janic Verboon	10
Netflix	Janic Verboon	9
TeamViewer QuickSupport	Janic Verboon	23



- Be aware about device restrictions and enrollment capabilities and how much of a security assurance they are (?)
 - Stay on top of havoc by having a clear assignment strategy
 - Explicitly manage your Administrators group
 - Even when your patch management is automated it still needs to incorporate checks for gaps in terms of endpoints missing patches
 - Monitor your Intune tenant for token expiration. Expired tokens can cause a lot of trouble
- > Be sure to check out the handout on sched. Which also includes useful references and links to helpful community tools.



We love Feedback

<https://wpninjas25.sched.com/>



Great Session!



Okay Session!



Not so okay Session!



Workplace Ninja
Summit 2025



Thank You



*Workplace Ninja
Summit 2025*