

# Security Baseline Management, How to...



*Workplace Ninja Australia Tour*



# Mirko Colemberg; Switzerland



## Focus

Managing Workplace Ninja Summit (try to manage the Ninjans who help to make the Summit success)

## From

Senior Expert Endpoint Consultant  
Workplace Sommelier



## Socials

X: @mirkocolemberg

Bluesky: @mirkocolemberg.bsky.social

Blog: <http://blog.colemberg.ch>



## Certification's



## Hobbies

Brewing Beer, and enjoy it :-P



## Contact

- Mail: [mirko@colemberg.ch](mailto:mirko@colemberg.ch)

Have you seen that you can create Security Baseline for Windows 11 24H2 in #MSIntune ??

This also means that you can use Settings catalog for configuring #Windows 11 24H2 policies.

The screenshot displays the Microsoft Intune admin center interface. The top navigation bar shows 'Home > Endpoint security'. The left sidebar contains a search bar and a list of navigation items: Overview, All devices, Security baselines (highlighted), Security tasks, Manage, Antivirus, Disk encryption, Firewall, and Endpoint Privilege Management. The main content area is titled 'Endpoint security | Security baselines' and includes a search bar. Below the title, there is a descriptive text: 'Use security baselines to apply Microsoft-recommended security configuration settings to your enrolled devices. [Learn more.](#)'. A table lists the available security baselines:

Security Baselines	↑↓	Version	↑↓
Security Baseline for Winc		Version 24H2	
Microsoft Defender for En		Version 24H1	
Security Baseline for Micr		Version 128	
Windows 365 Security Bas		Version 24H1	
Advanced Security Baseli		Version 1	
Standard Security Baseline		Version 1	
Microsoft 365 Apps for Er		Version 2306	

# Motivation for Security Baselines

Since the **security threat landscape** is constantly evolving, IT administrators must keep up with security threats and when needed, make changes to Windows, Microsoft 365 apps or 3rd party software **security settings** to help **mitigate** these **threats**.

# Motivation for Security Baselines

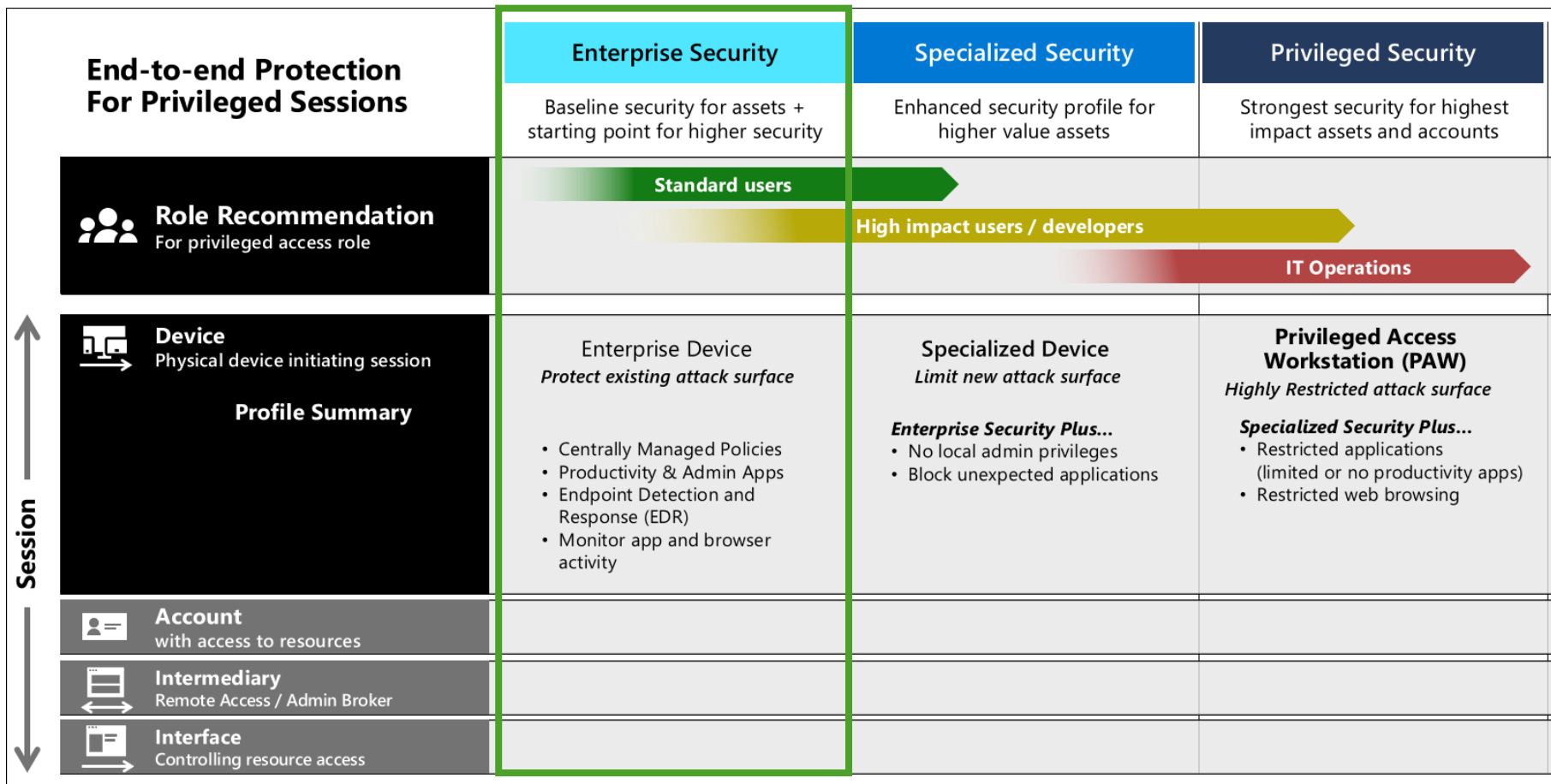
Do you know, what the following Windows Security Features have in common?

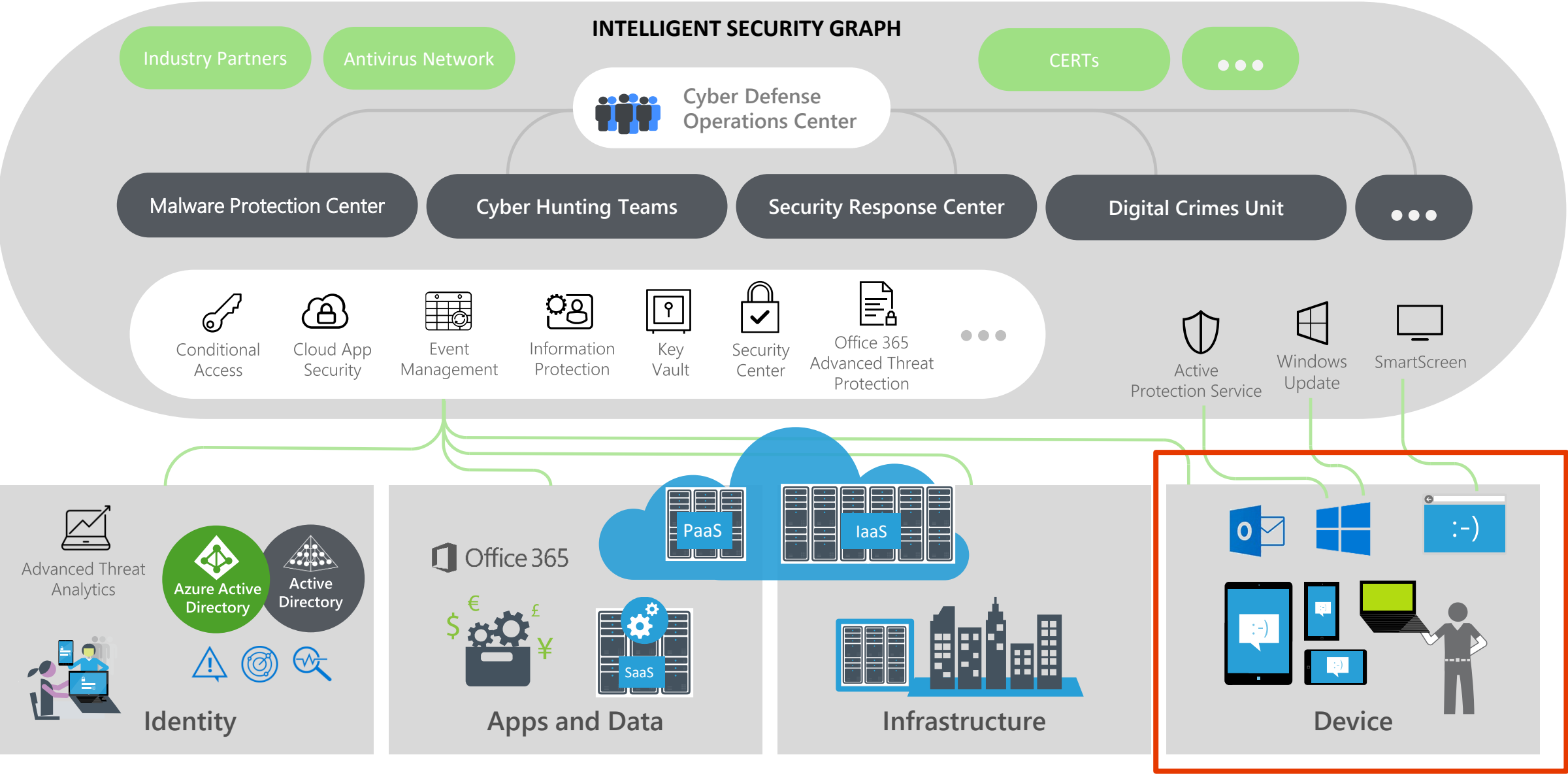
- LSA Protection
- Windows LAPS
- Windows Defender Exploit Guard Network Protection
- Windows Defender Exploit Guard ASR
- NTLM Auditing and NTLMv2 enforcement

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.

# Security Levels defined by Microsoft

By adopting and implementing security configuration baselines, organizations can achieve a stronger security posture, reduce the risk of cyber threats, and ensure compliance with relevant regulations and standards.







# Microsoft Threat Protection

1

**Identities:** Validating, verifying and protecting both user and admin accounts

2

**Endpoints:** protecting user devices and signals from sensors

3

**User Data:** evaluating email messages and documents for malicious content

4

**Cloud Apps:** protecting SaaS applications and their associated data stores

5

**Infrastructure:** protecting servers, virtual machines, databases and networks across cloud and on-premises locations



Azure Active Directory



Azure Advanced Threat Protection



Microsoft Cloud App Security



Microsoft Intune



Windows 11



Azure Security Center



Windows Defender Advanced Threat Protection



Office 365 Advanced Threat Protection



Office 365 Threat Intelligence



Windows Server Linux

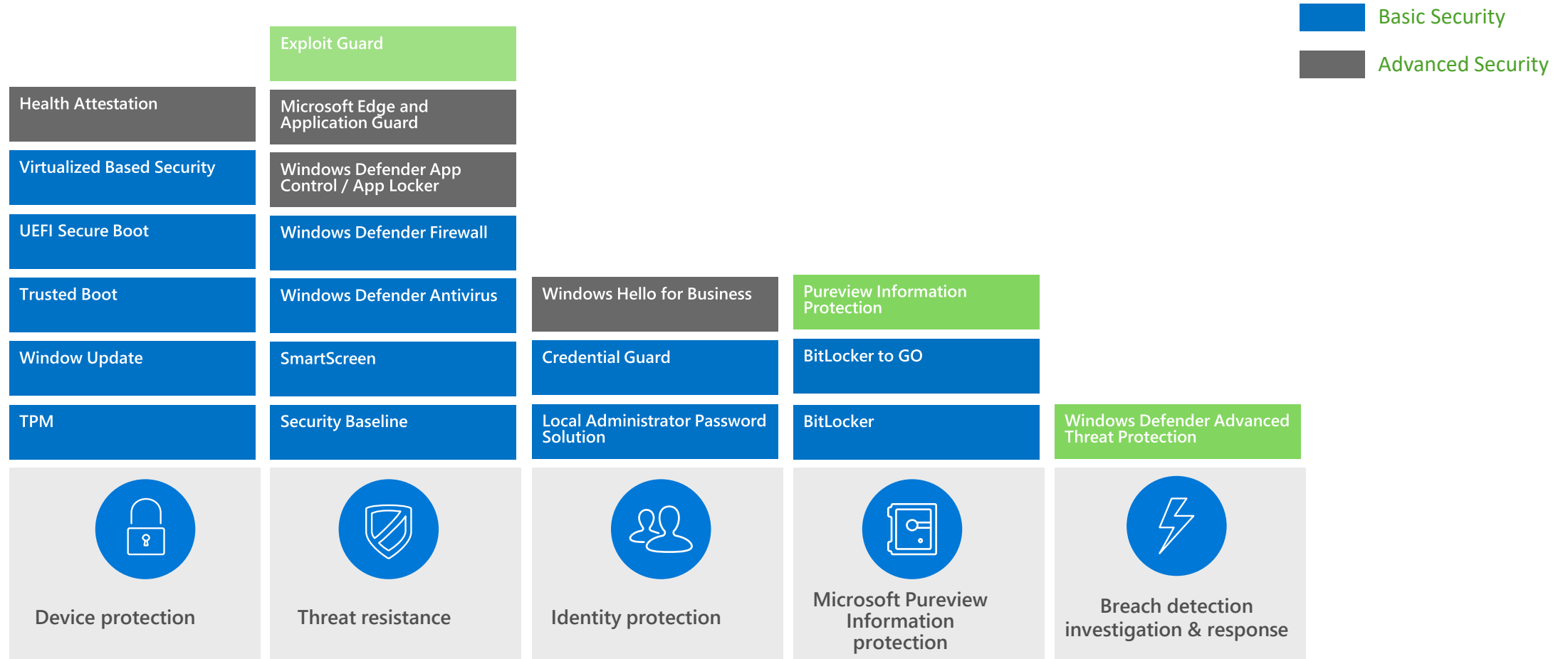


Exchange Online Protection



SQL Server

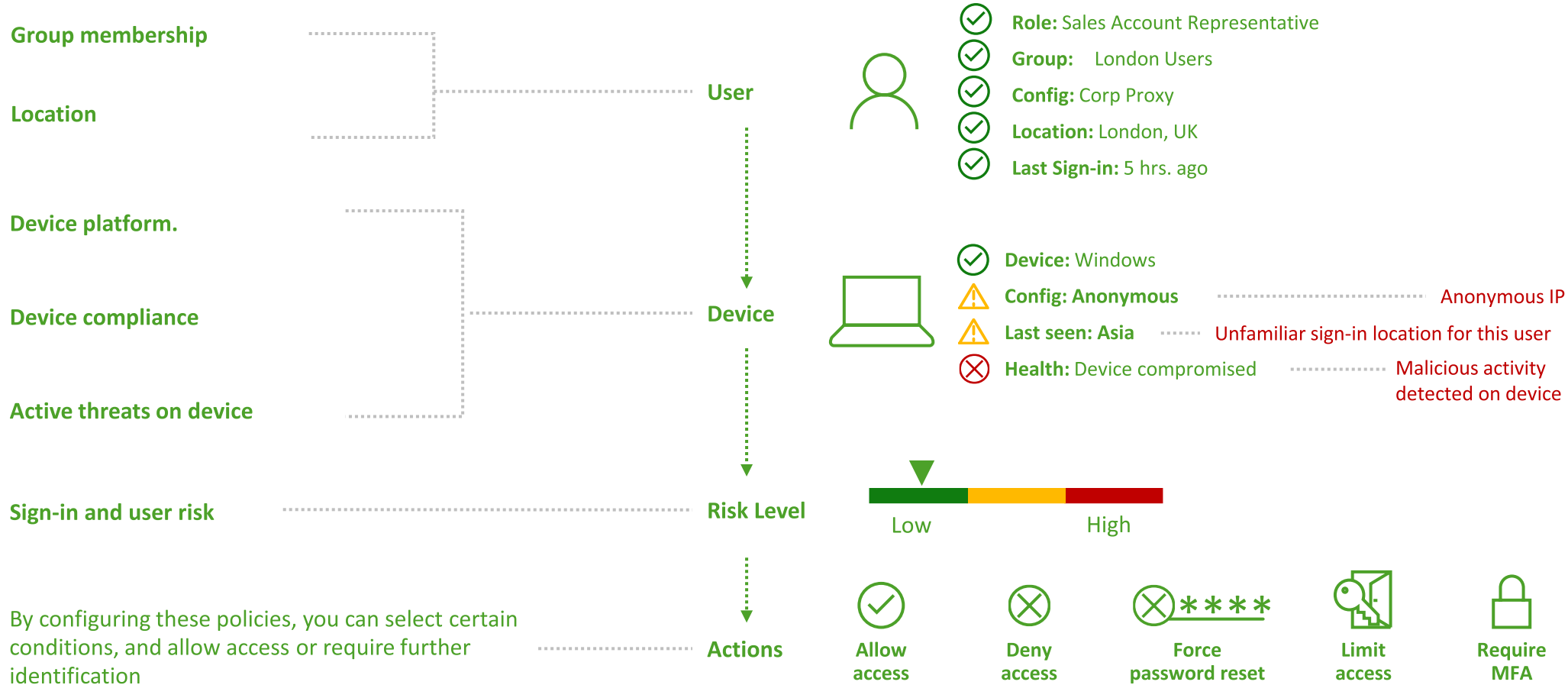
# Windows 11 Client Security



# Conditional Access

Protect at the front door with conditional access

Conditional access policies can be applied based on device state, application sensitivity, location and user rules



# Uff, what options we have and should implemented?

- There are a lot of benchmarks around
- Cyber security have to be in our DNA
- Device Security, Hardening of anything (yes, Servers as well)
- Patching
- Baselines
- Regulations
- Confusing about how to and why
- Order from Company to get Certified (ISO, Audit, etc.)

**At the end, every User in our Company  
has to be able to work and do the Job!**

# Benchmarks today

There are some Benchmark tools, frameworks, compliance examples around, that helps you based on CVE's or Audit relevant settings choosing the right one to get a success and structured environment.



## CIS

The CIS Benchmarks are prescriptive configuration recommendations for more than 25+ vendor product families. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.



## STIGVIEWER

STIGViewer® is for professionals who need access to the Security Technical Implementation Guides (STIGs) and documentation.  
**Unified Compliance Framework®**



## Canonical

Start with Ubuntu and get trusted open source for every part of your stack.



## MS Security baselines

Microsoft is dedicated to providing its customers with secure operating systems, such as Windows and Windows Server, and secure apps, such as Microsoft 365 apps for enterprise and Microsoft Edge.

# Benchmarks today

There are some Benchmark tools, frameworks, compliance examples around, that helps you based on CVE's or Audit relevant settings choosing the right one to get a success and structured environment.



## NCSC Device Security Guidance

While no set of mitigation strategies are guaranteed to protect against all cyber threats, organizations are recommended to implement eight essential mitigation strategies from the Strategies to Mitigate Cyber Security Incidents as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems.



## NIAP

NIAP, through the Cybersecurity Collaboration Center, oversees a national program to evaluate Commercial Off-The-Shelf Information Technology products for conformance to the International Common Criteria.



## ASD's ACSC

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) leads the Australian Government's efforts to improve cyber security. Our role is to help make Australia the most secure place to connect online.



## Additional Audit benchmarks

Some Devices in Production are regulated by the Industry.

For example, they have to be Certified that's not possible to change anything, because it can be impacted to an Application to change the something that will have an impact to the production, like measurement of a high impacted value.

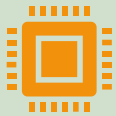
- Pharma industry
  - Medical industry
  - Oil Industry
  - Etc.
- 
- NIST SP 800-53 (Government USA, can be used for Public as well)
  - PCI-DSS (finance / Credit)
  - HIPAA (Healthcare USA)

# Broader scope of Security Baselines - Taxonomy



## Hardware

Security Baselines recommend **hardware** that supports the specified hardware features and specifications, to **support (Windows) security features**



## Policies

Security Baselines recommend **enforcing** the **configuration** of the specified **policies** in the manner described, to **harden Windows** and applications to the designated level of security



## Controls

Security Baselines recommend **enabling** the **security controls** specified in the manner described, to **provide protections** appropriate to the designated level of security.



## Behaviors

Security Baselines recommend **changing** **organizational behaviour** towards the endpoints in the manner described.



# Taxonomy for security configurations - Hardware

- Trusted Platform Module
- UEFI Secure Boot
- Support for Virtualization Based-Security
- Hypervisor Code-Integrity support
- DMA I/O Protection
- Windows Hello for Business supported
- System guard

# Taxonomy for security configurations - Policies

- Advanced Audit policies
- Security Template / Computer Policies
- Disabling legacy protocols and features
- Disabling non-enterprise features

# Taxonomy for security configurations - Controls

- BitLocker Drive Encryption
- Windows Defender Firewall
- Windows Defender Antivirus
  - Network Protection
  - Attack Surface Reduction Rules
  - Cloud Delivered Protection
- Microsoft Defender for Endpoint (EDR / XDR)
- Windows Defender Credential Guard
- Windows Local Administrator Password Solution (LAPS)
- Windows Hello for Business
- Microsoft Defender SmartScreen
  - Phishing Protection (Windows 11)
  - Apps and websites

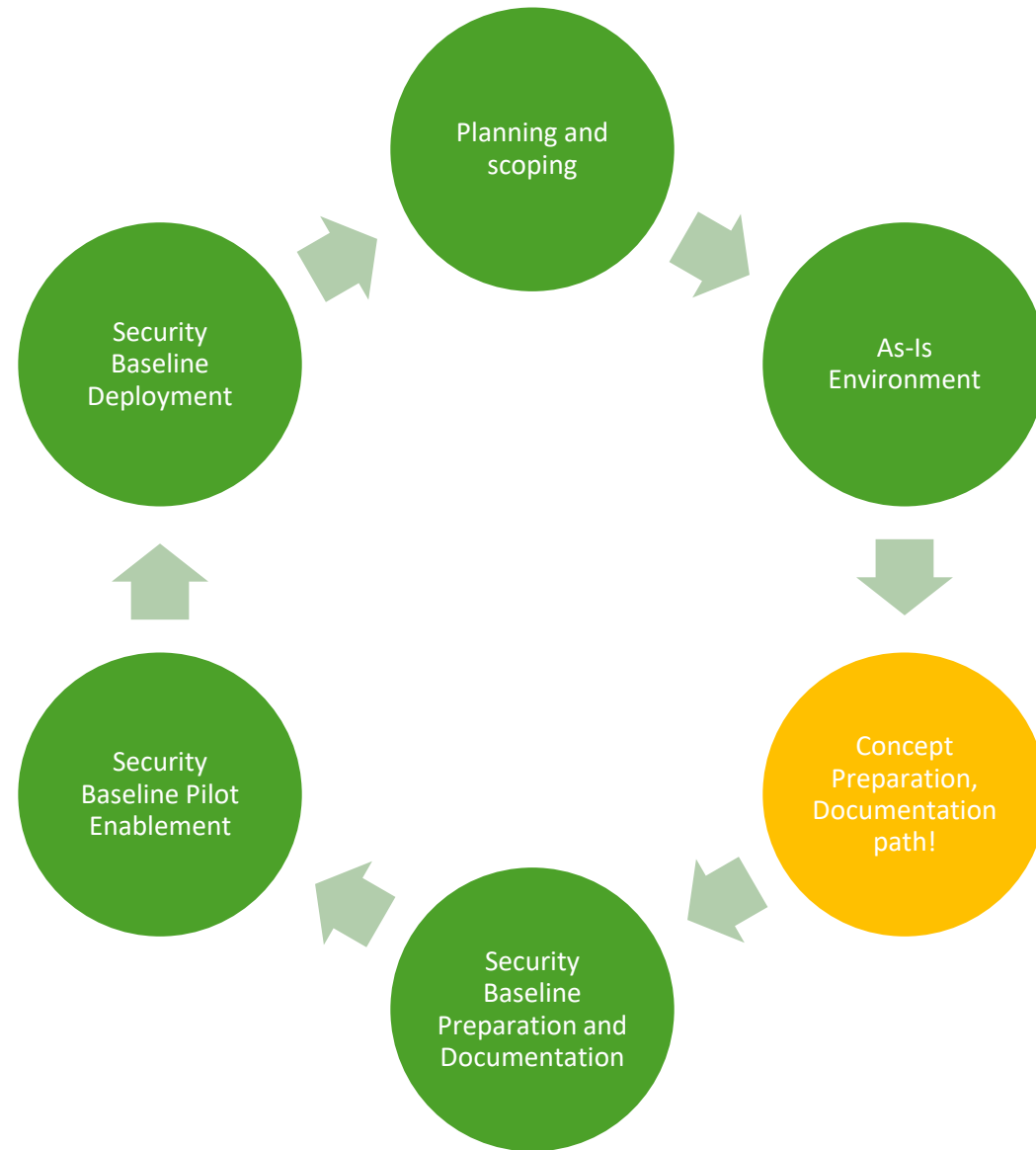
# Taxonomy for security configurations – Controls v2

- Microsoft 365 Apps
  - Add-Ins
  - Macros
  - Legacy File-Types
  - JavaScript
- Edge
  - Extensions
  - Legacy Authentication Schemes
  - SmartScreen

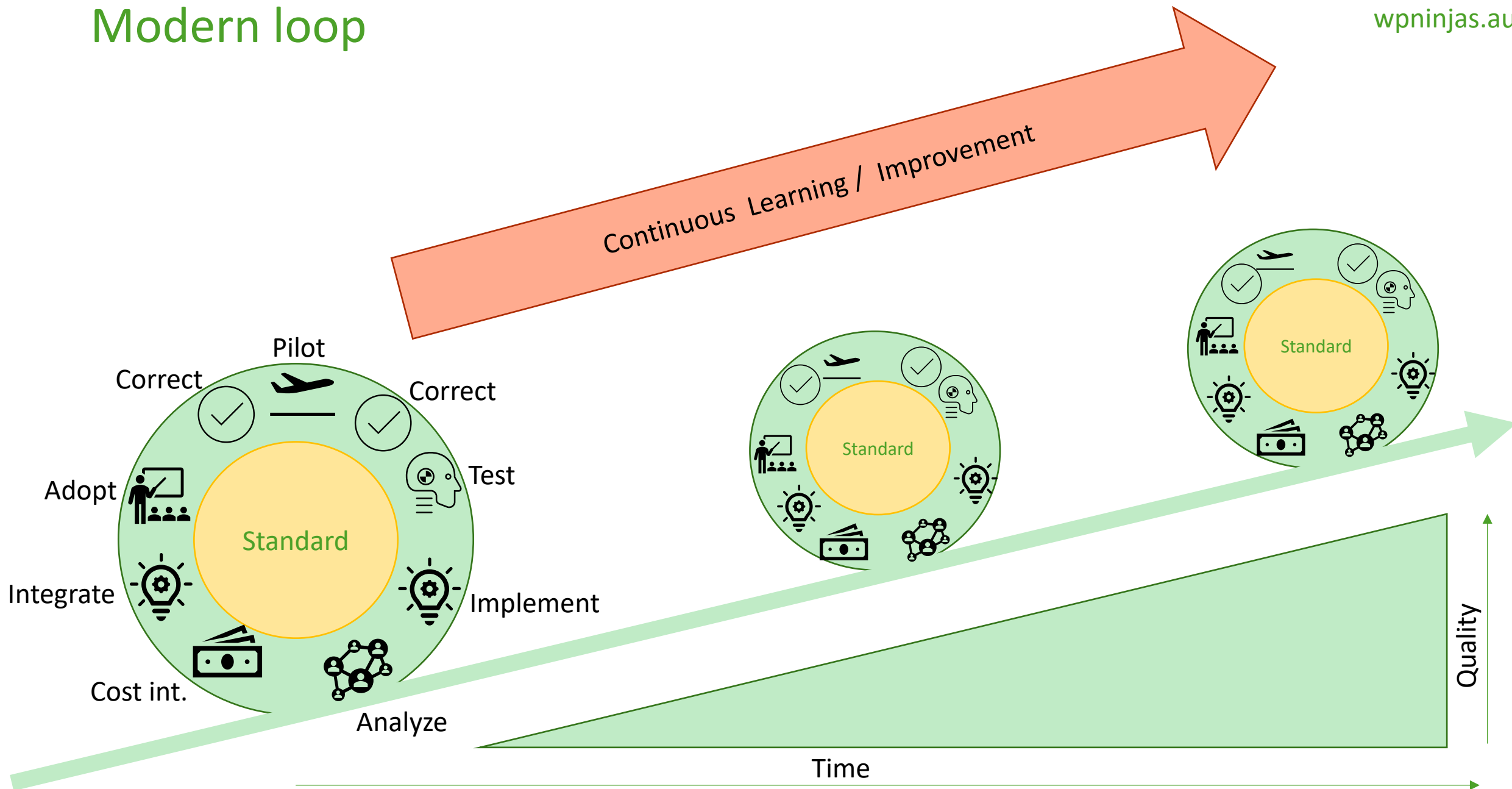
# Taxonomy for security configurations - Behaviors

- Patch Management
  - Operating System
  - AV / EDR
  - Browsers
  - Microsoft 365 Apps
  - 3<sup>rd</sup> Party Apps
- Usage and enforcement of LAPS
- Removal of local admin rights
- Macro Signing
- Adoption of security recommendations

# Recommended Adaption Approach




# Modern loop




# Security Baseline Preparation

Agree and prepare the required documentations including the possibility to document and cover deviations. Security Baselines are a **recommendation** and might vary for your environment

	A	B	C	E	F	G	H	I	J	AA	AB
1	Section #	Recommendation #	Title	Customer Configuration	Justification	Intune Profile / GPO	Description	Rationale Statement	Impact Statement	References	Default Value
4	1.1	1.1.1	(L1) Ensure 'Enforce password history' is set to '24 or more password(s)'				This policy s	The longer a	The major ir	<a href="https://www.cisecurity.org/white-papers/cis-passw">https://www.cisecurity.org/white-papers/cis-passw</a>	24 passwords remembered on domain members. 0 passwords remembered on stand-
5	1.1	1.1.2	(L1) Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'				This policy s	The longer a	If the Maxim	<a href="https://www.cisecurity.org/white-papers/cis-passw">https://www.cisecurity.org/white-papers/cis-passw</a>	42 days.
6	1.1	1.1.3	(L1) Ensure 'Minimum password age' is set to '1 or more day(s)'				This policy s	Users may f	If an admini	<a href="https://www.cisecurity.org/white-papers/cis-passw">https://www.cisecurity.org/white-papers/cis-passw</a>	1 day on domain members; 0 days on stand-
7	1.1	1.1.4	(L1) Ensure 'Minimum password length' is set to '14 or more character(s)'				This policy s	Types of pas	Requiremen	<a href="https://www.cisecurity.org/white-papers/cis-passw">https://www.cisecurity.org/white-papers/cis-passw</a>	7 characters on domain members; 0 characters
8	1.1	1.1.5	(L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'				This policy s	Passwords	If the default	<a href="https://www.cisecurity.org/white-papers/cis-passw">https://www.cisecurity.org/white-papers/cis-passw</a>	Enabled on domain members; Disabled on stand-
9	1.1	1.1.6	(L1) Ensure 'Relax minimum password length limits' is set to 'Enabled'				This policy s	This setting	The _Minim	<a href="https://www.cisecurity.org/white-papers/cis-passw">https://www.cisecurity.org/white-papers/cis-passw</a>	0 (0-14). The _Minimum password length_ may
10	1.1	1.1.7	(L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'				This policy s	Enabling thi	If your organ	<a href="https://www.cisecurity.org/white-papers/cis-passw">https://www.cisecurity.org/white-papers/cis-passw</a>	Disabled.
12	1.2	1.2.1	(L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)'				This policy s	A denial of s	Although it n	<a href="https://www.cisecurity.org/white-papers/cis-passw">https://www.cisecurity.org/white-papers/cis-passw</a>	None, because this policy setting only has
13	1.2	1.2.2	(L1) Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'				This policy s	Setting an a	If this policy	<a href="https://www.cisecurity.org/white-papers/cis-passw">https://www.cisecurity.org/white-papers/cis-passw</a>	0 failed logon attempts.
14	1.2	1.2.3	(L1) Ensure 'Allow Administrator account lockout' is set to 'Enabled'				This policy s	Enabling ac	The built-in /	<a href="https://support.microsoft.com/en-us/topic/kb50202">https://support.microsoft.com/en-us/topic/kb50202</a>	Disabled. (The built-in Administrator account is
15	1.2	1.2.4	(L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'				This policy s	Users can a	If you do not	<a href="https://www.cisecurity.org/white-papers/cis-passw">https://www.cisecurity.org/white-papers/cis-passw</a>	None, because this policy setting only has
19	2.2	2.2.1	(L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'				This security	If an account	None - this i	<a href="https://learn.microsoft.com/en-us/windows/security">https://learn.microsoft.com/en-us/windows/security</a>	No one.
20	2.2	2.2.2	(L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'				This policy s	Users who c	If you remov	<a href="https://learn.microsoft.com/en-us/windows/security">https://learn.microsoft.com/en-us/windows/security</a>	Administrators, backup operators, Everyone, I
21	2.2	2.2.3	(L1) Ensure 'Act as part of the operating system' is set to 'No One'				This policy s	The **Act as	There shoul	<a href="https://learn.microsoft.com/en-us/windows/security">https://learn.microsoft.com/en-us/windows/security</a>	No one.
22	2.2	2.2.4	(L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'				This policy s	A user with t	Organization	<a href="https://learn.microsoft.com/en-us/windows/security">https://learn.microsoft.com/en-us/windows/security</a>	Administrators, LOCAL SERVICE, NETWORK SERVICE


**SecurityBaseLines**
Public

main
1 Branch
0 Tags
Go to file


**mirko colemborg**
updated

.vscode

added files

scripts

del test

Modified MS Security Baseline Windows 11 v2...

rename and update

Modified MSFT Edge version 128.xlsx

updated

Modified Microsoft 365 Apps for enterprise 24...

rename and update

README.md

update

Remediation Sec.-Baseline 24h2.txt

added files

SB\_24H2\_AT\_ST-Data-Protection\_2024-12-16.js...

rename and update



# Security Baselines - Exception handling

**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)
-----------------	---------------------------------

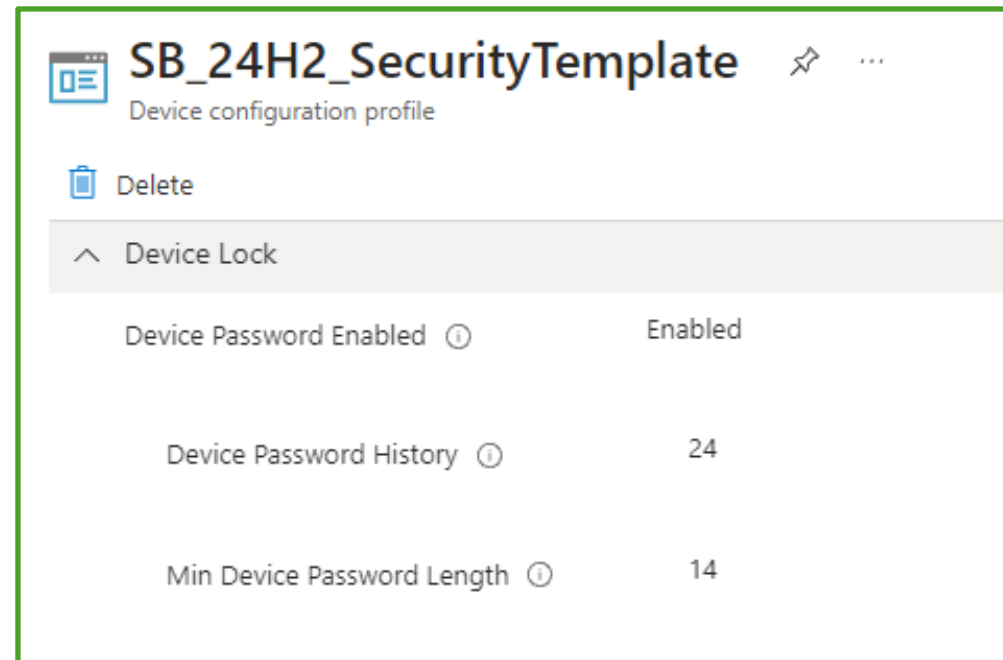
Excluded groups	
-----------------	--

### 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.



# Domain controller GPO assigned to Users in a User Hybrid scenario

- AD DC GPO in place and Hybrid User sync enabled, then be carefully
  - Policy overlapping




# Well-known Security Identifiers (SIDs) Code Definitions

Home > Devices | Configuration >

 **SB\_24H2\_SecurityTemplate**  ...


















Device configuration profile

 Delete

---

^ User Rights

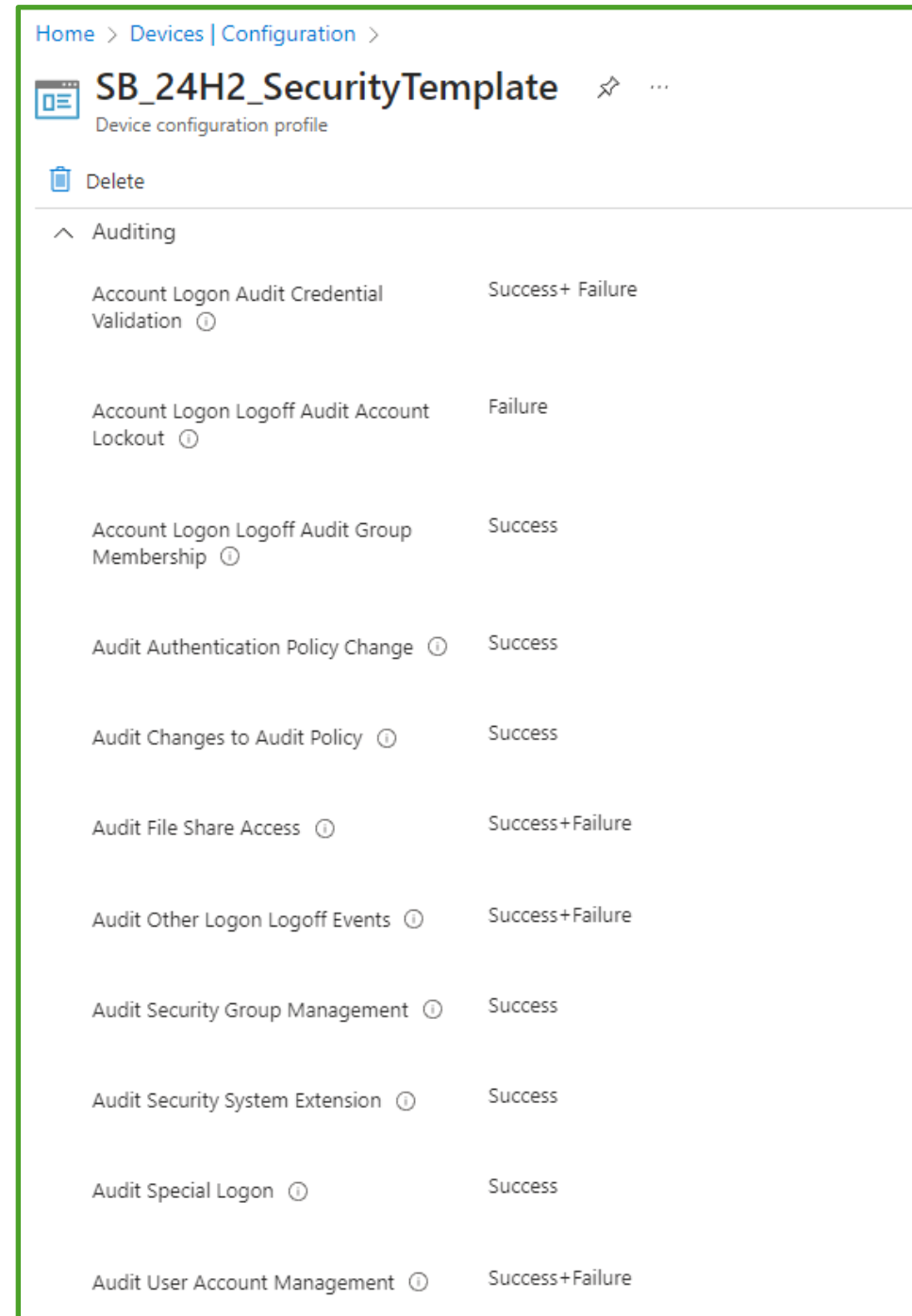
---

Access Credential Manager As Trusted Caller 	*S-1-5-32-544, *S-1-5-32-555
Allow Local Log On 	*S-1-5-32-544, *S-1-5-32-545
Backup Files And Directories 	*S-1-5-32-544
Create Global Objects 	*S-1-5-32-544
Create Page File 	*S-1-5-32-544
Debug Programs 	*S-1-5-32-544
Deny Access From Network 	*S-1-5-113
Deny Remote Desktop Services Log On 	*S-1-5-113
Impersonate Client 	*S-1-5-32-544, *S-1-5-6, *S-1-5-19, *S-1-5-20
Load Unload Device Drivers 	*S-1-5-32-544
Manage Auditing And Security Log 	*S-1-5-32-544
Manage Volume 	*S-1-5-32-544
Modify Firmware Environment 	*S-1-5-32-544
Profile Single Process 	*S-1-5-32-544
Remote Shutdown 	*S-1-5-32-544
Restore Files And Directories 	*S-1-5-32-544
Take Ownership 	*S-1-5-32-544

# Does this make sense?

## Talk to the CISO / SOC

- To collect the right data
- To collect the needed Data
- Forward the Info's
  - Right place
  - Right data
  - Right Information's



The screenshot shows the Windows Security settings for a device configuration profile named 'SB\_24H2\_SecurityTemplate'. The 'Auditing' section is expanded, showing a list of audit events and their configured success and failure actions. Each event name has a help icon (i) next to it.

Home > Devices   Configuration >	
SB_24H2_SecurityTemplate Device configuration profile	
Delete	
Auditing	
Account Logon Audit Credential Validation ⓘ	Success+ Failure
Account Logon Logoff Audit Account Lockout ⓘ	Failure
Account Logon Logoff Audit Group Membership ⓘ	Success
Audit Authentication Policy Change ⓘ	Success
Audit Changes to Audit Policy ⓘ	Success
Audit File Share Access ⓘ	Success+Failure
Audit Other Logon Logoff Events ⓘ	Success+Failure
Audit Security Group Management ⓘ	Success
Audit Security System Extension ⓘ	Success
Audit Special Logon ⓘ	Success
Audit User Account Management ⓘ	Success+Failure

# LANMAN Server / Workstation

This policy setting determines if the SMB client will allow insecure guest logons to an SMB server. If you enable this policy setting or if you do not configure this policy setting, the SMB client will allow insecure guest logons. If you disable this policy setting, the SMB client will reject insecure guest logons. Insecure guest logons are used by file servers to allow unauthenticated access to shared folders. While uncommon in an enterprise environment, insecure guest logons are frequently used by consumer Network Attached Storage (NAS) appliances acting as file servers. Windows file servers require authentication and do not use insecure guest logons by default. Since insecure guest logons are unauthenticated, important security features such as SMB Signing and SMB Encryption are disabled. As a result, clients that allow insecure guest logons are vulnerable to a variety of man-in-the-middle attacks that can result in data loss, data corruption, and exposure to malware. Additionally, any data written to a file server using an insecure guest logon is potentially accessible to anyone on the network. Microsoft recommends disabling insecure guest logons and configuring file servers to require authenticated access.

[Learn more](#)

Enable Insecure Guest Logons  Enabled

Network\lanman server

8 Network\Lanman Server

0 Network\Lanman Workstation

Network\lanman server

Audit insecure guest logon

Enable insecure guest logons

Network\lanman server

Enabled

Disabled

# Confusing, same same

When WDigest authentication is enabled, Lsass.exe retains a copy of the user's plaintext password in memory, where it can be at risk of theft. Microsoft recommends disabling WDigest authentication unless it is needed. If this setting is not configured, WDigest authentication is disabled in Windows 8.1 and in Windows Server 2012 R2; it is enabled by default in earlier versions of Windows and Windows Server. Update KB2871997 must first be installed to disable WDigest authentication using this setting in Windows 7, Windows 8, Windows Server 2008 R2 and Windows Server 2012. Enabled: Enables WDigest authentication. Disabled (recommended): Disables WDigest authentication. For this setting to work on Windows 7, Windows 8, Windows Server 2008 R2 or Windows Server 2012, KB2871997 must first be installed. For more information, see <http://support.microsoft.com/kb/2871997> and <http://blogs.technet.com/b/srd/archive/2014/06/05/an-overview-of-kb2871997.aspx>.

[Learn more](#)

WDigest Authentication (disabling may require KB2871997) ☐ Disabled

Windows Components\Windows Remote Management (WinRM)\Win	Disallow Digest authentication	Enabled
MS Security Guide	WDigest Authentication (disabling may require KB2871997)	Disabled

Home > Devices | Configuration >



## SB\_24H2\_AT\_ST-Defender



Device configuration profile



Delete

Cloud Extended Timeout ⓘ

50

Disable Local Admin Merge ⓘ

Disable Local Admin Merge

Enable File Hash Computation ⓘ

Enable

Enable Network Protection ⓘ

Enabled (block mode)

Home > Devices | Configuration > SB\_24H2\_Computer-Administrative-Template >

## Edit profile - SB\_24H2\_Computer-Administrative-Template

Settings catalog

**Windows Components > Microsoft Defender Antivirus**

[Remove](#)



10 of 12 settings in this subcategory are not configured

Configure local administrator merge  
behavior for lists ⓘ



Disabled

Home > Devices | Configuration >



## SB\_24H2\_AT\_ST-Defender

Device configuration profile



Delete

Enable Network Protection ⓘ	Enabled (block mode)
Hide Exclusions From Local Admins ⓘ	If you enable this setting, local admin exclusion list in Windows Security.
PUA Protection ⓘ	PUA Protection on. Detected items along with other threats.
Real Time Scan Direction ⓘ	Monitor all files (bi-directional).
Submit Samples Consent ⓘ	Send safe samples automatically.

Home > Devices | Configuration > SB\_24H2\_Computer-Administrative-Template >

## Edit profile - SB\_24H2\_Computer-Administrative-Template

Settings catalog

### Windows Components > Microsoft Defender Antivirus > Real-time Protection

[Remove subcategory](#)

**i** 9 of 13 settings in this subcategory are not configured

Scan all downloaded files and attachments ⓘ ☒ Enabled ⓘ

Turn off real-time protection ⓘ ☐ Disabled ⓘ

Turn on behavior monitoring ⓘ ☒ Enabled ⓘ

Turn on process scanning whenever real-time protection is enabled ⓘ ☒ Enabled ⓘ

### Windows Components > Microsoft Defender Antivirus > Scan

[Remove subcategory](#)

**i** 29 of 31 settings in this subcategory are not configured

Scan packed executables ⓘ ☒ Enabled ⓘ

Scan removable drives ⓘ ☒ Enabled ⓘ



## Create Policy ...

Windows Firewall

### Firewall

The Firewall configuration service provider configures the Windows Defender Firewall settings, as well as the desired set of custom rules to be enforced on the device. Using the Firewall CSP the IT admin can now manage non-domain devices, and reduce the risk of network security threats to the corporate network.

Certificate revocation list verification ⓘ	Require
Disable Stateful Ftp ⓘ	True
Enable Packet Queue ⓘ	2 selected
IPsec Exceptions ⓘ	1 selected
Opportunistically Match Auth Set Per KM ⓘ	True
Preshared Key Encoding ⓘ	UTF8 (Default)
Security association idle time ⓘ	<input checked="" type="checkbox"/> Configured 300
Enable Domain Network Firewall ⓘ	Not configured
Enable Private Network Firewall ⓘ	Not configured
Enable Public Network Firewall ⓘ	Not configured



## SB\_24H2\_Firewall

Device configuration profile



Delete

### Configuration settings [Edit](#)

#### ^ Firewall

The Firewall configuration service provider configures the Windows Defender Firewall global settings, per profile settings, as well as the desired set of custom rules to be enforced on the device. Using the Firewall CSP the IT admin can now manage non-domain devices, and reduce the risk of network security threats across all systems connecting to the corporate network.

Enable Domain Network Firewall ⓘ True

Default Inbound Action for Domain Profile ⓘ Block

Default Outbound Action ⓘ Block

Disable Inbound Notifications ⓘ True

Enable Log Dropped Packets ⓘ Enable Logging Of Dropped Packets

Enable Log Success Connections ⓘ Enable Logging Of Successful Connections

Log Max File Size ⓘ 16384

Enable Private Network Firewall ⓘ True

[Home](#) > [Devices | Configuration](#) >



## SB\_24H2\_Computer-Administrative-Template



Device configuration profile



Delete

### Windows Components > File Explorer

Pick one of the following settings:  
(Device)

Warn and prevent bypass

Configure Windows Defender  
SmartScreen ⓘ

Enabled

[Home](#) > [Endpoint security | Security baselines](#) > [Security Baseline for Microsoft Edge | Profiles](#) >

## Create profile



Security Baseline for Microsoft Edge

### SmartScreen settings

Configure Microsoft Defender  
SmartScreen ⓘ

Enabled



# Mixing configs (CSP vs. baselines)

The image shows two side-by-side screenshots of the Microsoft Defender for Endpoint Security Baseline and Windows Configuration settings. The left screenshot shows the 'sec-pol anschau 24H1' baseline, and the right screenshot shows the 'SB Win 24H2 Computer-Administrative-Template' configuration profile. Both screenshots have red boxes highlighting specific settings.

**Left Screenshot: sec-pol anschau 24H1**  
Microsoft Defender for Endpoint Security Baseline

- Delete
- Configure user storage of BitLocker recovery information: Allow 48-digit recovery password
- Deny write access to fixed drives not protected by BitLocker: Enabled
- Enforce drive encryption type on fixed data drives: Enabled
- Select the encryption type: (Device) Used Space Only encryption
- Windows Components > BitLocker Drive Encryption > Operating System Drives**
  - Allow devices compliant with InstantGo or HSTI to opt out of pre-boot PIN: Disabled
  - Allow enhanced PINs for startup: Disabled**

**Right Screenshot: SB Win 24H2 Computer-Administrative-Template**  
Device configuration profile

- Delete
- Enumerate administrator accounts on elevation: Disabled
- Windows Components > BitLocker Drive Encryption > Removable Data Drives**
  - Do not allow write access to devices configured in another organization: False
  - Deny write access to removable drives not protected by BitLocker: Enabled
- Windows Components > BitLocker Drive Encryption > Operating System Drives**
  - Allow enhanced PINs for startup: Enabled**
- Windows Components > AutoPlay Policies**

# Mixing configs (CSP vs. CSP)

## System > Device Installation > Device Installation Restrictions

Prevent installation of devices using drivers that match these device setup classes ⓘ Enabled

Prevented Classes {d48179be-ec20-11d1-b6b8-00c04fa372a7}

Also apply to matching devices that are already installed. False

## System > Device Installation > Device Installation Restrictions

Prevented Classes {d48179be-ec20-11d1-b6b8-00c04fa372a7}

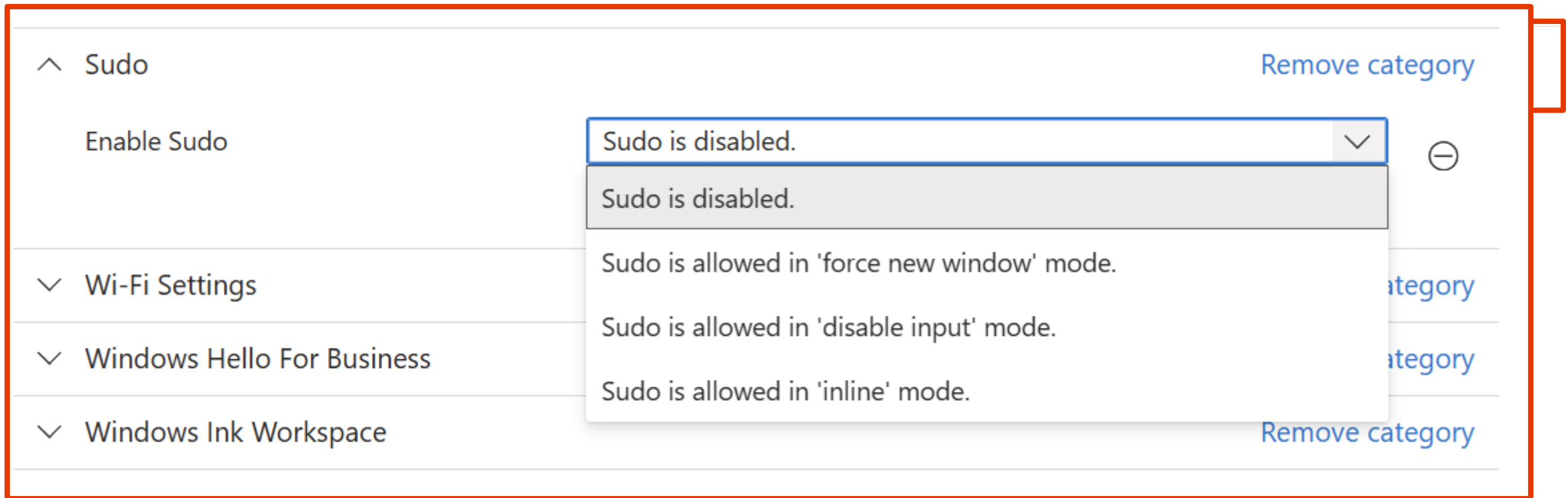
Also apply to matching devices that are already installed. True

Prevent installation of devices using drivers that match these device setup classes ⓘ Enabled

# What's not included

- Some settings from the Security Baseline sheet are no CSP available
- PowerShell best practice
- Intune overall settings
- Entra ID overall settings


# No CSP's for this Settings



- InvalidAuthenticationDelayTimeInMs
- MaxSmb2Dialect
- MinSmb2Dialect

## Settings

- DisableExternalDMAUnderLock

- |                          |   |              |
|--------------------------|---|--------------|
| <input type="checkbox"/> |  w11 23H2 don't touch, only view | Version 23H2 |
| <input type="checkbox"/> | w11 24H2 don't touch, only view   | Version 24H2 |

## What's not included?

---

Although the below settings are configured as a part of the ACSC Windows Hardening Guidelines, they have not been included in this version of the guidelines. It is still recommended to configure each of the settings below as a part of an end to end security strategy.

- AppLocker
  - Organisations have unique Application Whitelisting requirements. Apply your organisations AppLocker policy via the [AppLocker CSP](#). Consider the use of [AaronLocker](#), which aims to make application control using AppLocker and Windows Defender Application Control (WDAC) as easy and practical as possible.
- BitLocker
  - Manage disk encryption with a [Disk Encryption Endpoint Security policy](#).
- Controlled Folder Access
  - The configuration for Controlled Folder Access requires input that is unique to each organisation.
  - [Configure Controlled Folder Access](#) by creating an Attack surface reduction policy in the [Microsoft Intune console](#), under *Endpoint Security > Attack surface reduction*
- Microsoft Defender Application Guard
  - Intune provides the ability to [enable and configure Microsoft Defender Application Guard](#). The configuration of Application Guard requires additional input from the organisation, such as a Windows network isolation policy.
- Windows Update
  - Organisations typically standardise on a management platform that provides patching capabilities. Microsoft's recommendation is to move to [Windows Update for Business](#).
- [Settings that are not available via Settings Catalog, Endpoint Security or device configuration](#).
  - If a setting does not have a corresponding Settings Catalog, Endpoint Security or device configuration setting, it was not configured.
  - A possible way to implement these settings would be with a PowerShell script, deployed via Intune.



## Endpoint Security - PowerShell Constrained Language Mode

Constrained Language mode is designed to allow basic language elements such as loops, conditionals, string expansion, and access to object properties. The restrictions prevent operations that could be abused by a malicious actor.

The Constrained Language mode permits all cmdlets and a subset of PowerShell language elements but limits the object types that can be used.

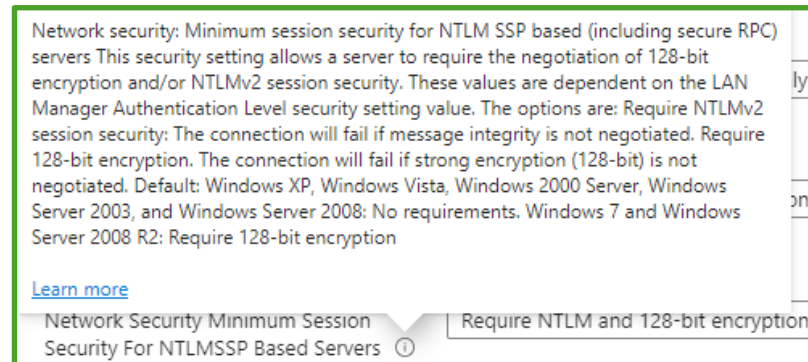
```
"$([Environment]::GetFolderPath("CommonDesktopDirectory"))\*.lnk"
```

## In this case;

- Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'
- Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128\_HMAC\_SHA1, AES256\_HMAC\_SHA1, Future encryption types'

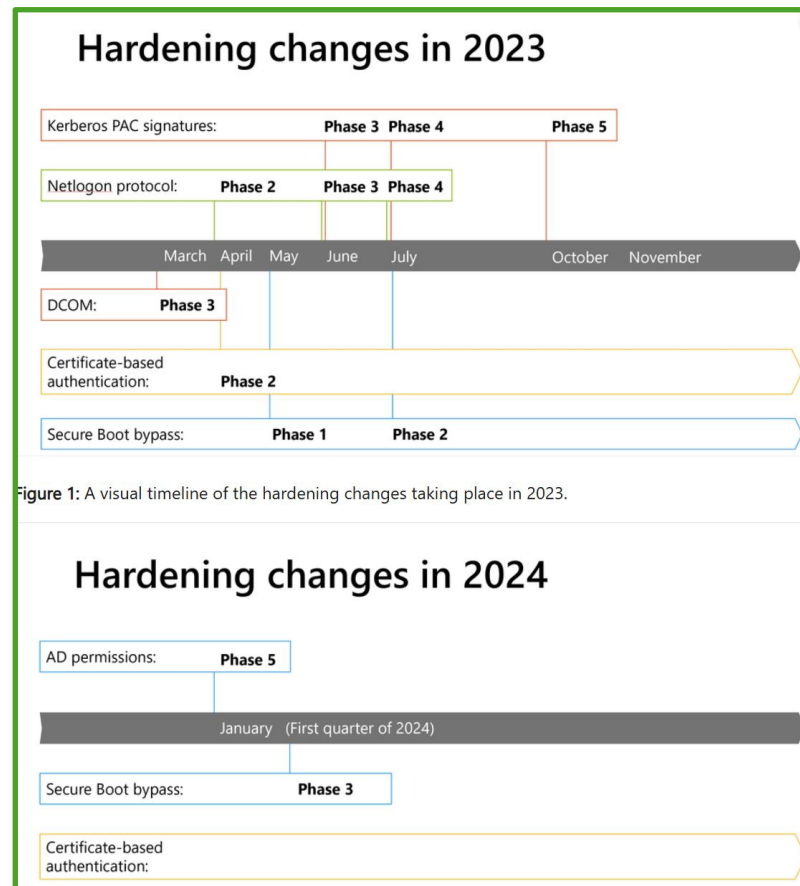
Is this not on Server side?

- SMB Local machine, Client / Server, yes set it for Server (if the Devices shares, it's like a Server)



# Hardening

- Latest Windows hardening guidance and key dates - Microsoft Support



**January 2025**

- PAC Validation changes [KB5037754](#) | Enforcement by default phase

Updates released in or after January 2025 will move all Windows domain controllers and clients in the environment to **Enforced** mode. This mode will enforce secure behavior by default. Existing registry key settings that have been previously set will override this default behavior change.

The default **Enforced** mode settings can be overridden by an Administrator to revert to **Compatibility** mode.

**February 2025 or later**

- Certificate-based authentication [KB5014754](#) | Phase 3

Full Enforcement mode. If a certificate cannot be strongly mapped, authentication will be denied.

**April 2025**

- PAC Validation changes [KB5037754](#) | Enforcement phase



The Windows security updates released in or after April 2025, will remove support for the registry subkeys **PacSignatureValidationLevel** and **CrossDomainFilteringLevel** and enforce the new secure behavior. There will be no support for **Compatibility** mode after installing the April 2025 update.

# Endpoint Security - Non-compliant Devices

Policies Notifications Retire noncompliant devices **Compliance settings** Scripts Monitor

 Save  Discard

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as  Compliant 

# Follow the Principe of zero trust!!!

# Are there some Help around: YES!

Yes, community tools

Documentation FTW!

ACSC MS-Australia

- [SkipToTheEndpoint/OpenIntuneBaseline: Community-driven baseline to accelerate Intune adoption and learning. \(github.com\)](#)
- [ThomasKur/M365Documentation: Automatic Microsoft 365 Documentation to simplify the life of admins and consultants. \(github.com\)](#)
- [alexverboon/IntuneCustomCompliance: Microsoft Intune Custom Compliance \(github.com\)](#)
- [Sander Rozemuller | All about Identity, AVD, Automation, DevOps, Monitoring, Intune and Security](#)
- [Intune-ACSC-Windows-Hardening-Guidelines/docs/ACSC Windows Hardening Guidelines.md at main · microsoft/Intune-ACSC-Windows-Hardening-Guidelines · GitHub](#)



**It's easy to be  
complicated, but very  
complicated to keep it  
easy!**

—— Mirko Colemanberg ——



Thank You



Workplace