

Stop Trusting Defaults: Master Intune and Entra ID Security Before It's Too Late!



Speakers



Jörgen Nilsson

Trusted Advisor



jorgenccmexec



in/ccmexec



Jan Ketil Skanke

Principal Cloud Architect



jankeskanke



in/JankeSkanke

Can't see our slides? Can't hear? Need to repeat the question? Call us out!

Takeaways

- ◆ Default settings in a new tenant must be configured so we are in control, both from security and functionality perspective.
- ◆ We will focus on defaults in Intune and Entra as they are tightly integrated
- ◆ We will clearly show when Intune Admin is not enough and additional permissions is needed.
- ◆ New settings are introduced all the time with new default values

Did you check your default values lately?

DEMO

Intune defaults

Tenant



Tenant admin | Customization | Branding

- ◆ Configure branding
- ◆ Corporate information
- ◆ Support information

Home > Tenant admin | Customization > Default | Properties >

Edit customization policy ...

1 Settings 2 Review + save


Branding


Organization name *


Color

Theme color ⓘ Text color: Black

Show in header ⓘ

Upload logo for theme color background ⓘ 
Recommended image height: Greater than 72 px. Max file size: 750 KB. File type: PNG, JPG, or JPEG.
[Remove](#)



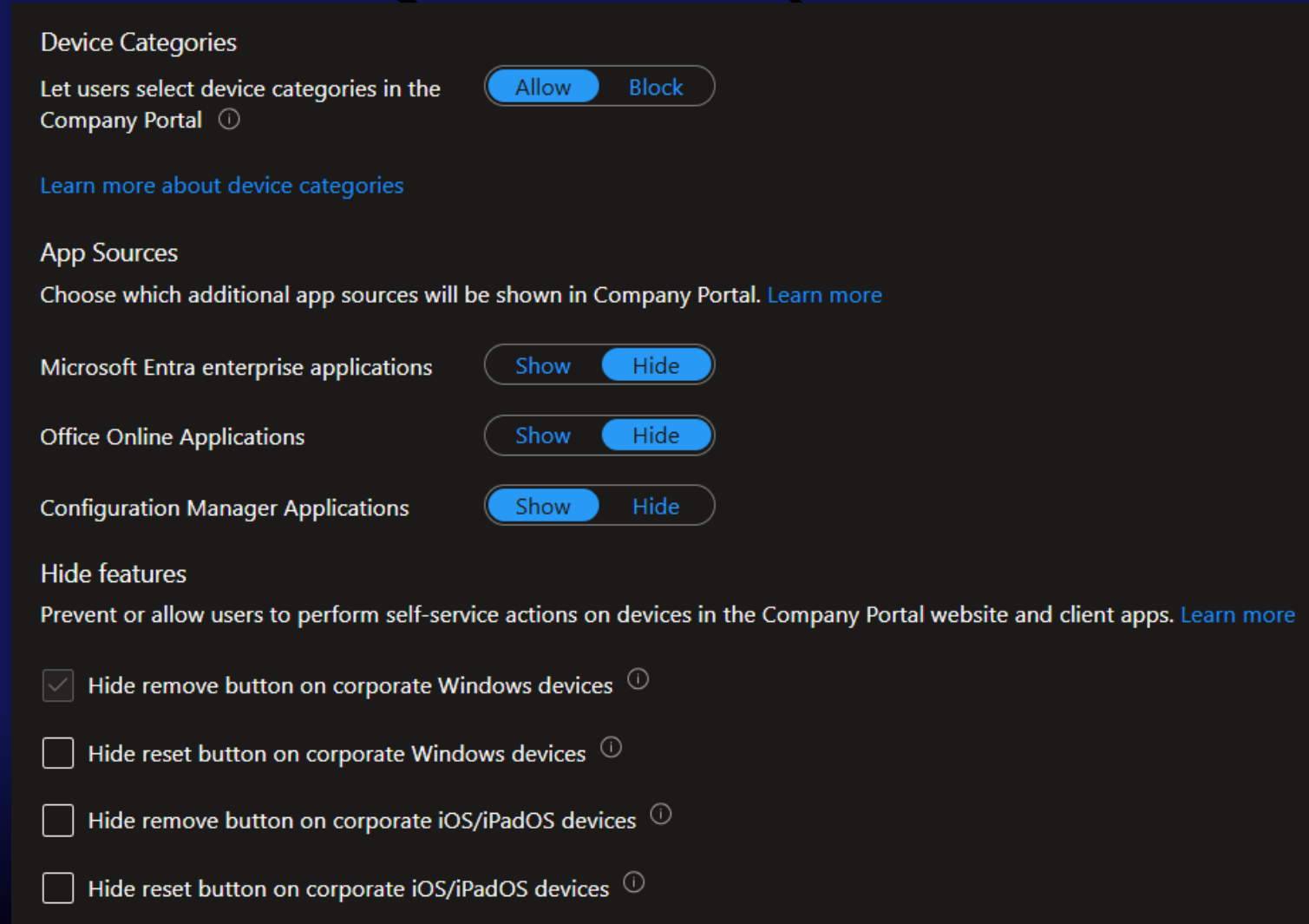
Upload logo for white or light background ⓘ 
Recommended image height: Greater than 72 px. Max file size: 750 KB. File type: PNG, JPG, or JPEG.
[Remove](#)

[Tenant admin - Microsoft Intune admin center](#)

Tenant admin | Customization

- ◆ Configure what users are allowed to do (Reset/Remove)
- ◆ Which apps to show
- ◆ Device Categories

[Tenant admin - Microsoft Intune admin center](#)



The screenshot displays the 'Customization' settings in the Microsoft Intune admin center. It is divided into several sections:

- Device Categories:** A toggle switch labeled 'Let users select device categories in the Company Portal' is currently set to 'Allow'.
- App Sources:** A section titled 'Choose which additional app sources will be shown in Company Portal' with a 'Learn more' link.
- App Source Toggles:** Three rows of toggle switches for 'Microsoft Entra enterprise applications', 'Office Online Applications', and 'Configuration Manager Applications'. All three are currently set to 'Hide'.
- Hide features:** A section titled 'Prevent or allow users to perform self-service actions on devices in the Company Portal website and client apps' with a 'Learn more' link. It contains four checkboxes:
 - Hide remove button on corporate Windows devices
 - Hide reset button on corporate Windows devices
 - Hide remove button on corporate iOS/iPadOS devices
 - Hide reset button on corporate iOS/iPadOS devices

Tenant admin | Diagnostics setting

- ◆ Intune Audit Logs are saved for 2 year in Intune
- ◆ Regulatory requirement to save them longer?
- ◆ We can ship the following logs:
 - AuditLogs
 - OperationalLogs
 - DeviceComplianceOrg
 - Devices
 - Windows365AuditLogs
- ◆ Why ship them to log analytics?

Answer: More information is shown!

Destination details

- Send to Log Analytics workspace
- Archive to a storage account
- Stream to an event hub
- Send to partner solution

Tenant admin | Device diagnostics

- ◆ Additional diagnostics to collect on Autopilot failure
- ◆ Additional information to collect

Device diagnostics are available for corporate-managed devices running Windows 10, version 1909 and later, or Windows 11. Diagnostics may include user identifiable information such as user or device name. ⓘ

Enabled

Automatically capture diagnostics when devices experience a failure during the Autopilot process on Windows 10 version 1909 or later and Windows 11. Diagnostics may include user identifiable information such as user or device name. ⓘ

Enabled

Diagnostic data is available only for devices managed by Intune app protection policy. The data could include user-identifiable information, such as user or device name. The data is stored in Microsoft support systems and isn't subject to Intune data management policies or protections. Some applications might collect and store data using systems other than Intune. For more info, check privacy documentation for each app. ⓘ

Enabled

Intune roles / Scope tags

- ◆ Build your own roles! The helpdesk role has way to much permissions.

Help Desk Operator
Microsoft Intune

Search

Overview

Manage

- Properties
- Assignments

Roles

In this section you can:

- Assign administrators to Endpoint Manager Roles
- Create and configure custom Endpoint Manager Roles

Tenant Admin: Scoped permissions

- ◆ Preview in 2026-04
- ◆ Separate resource permissions instead of merge
- ◆ Important to be able to have different permissions for managing VIP devices for example.

Unlicensed administrators
Allow admins without an Intune license to access Intune. Their scope of access is determined by the Intune roles you've assigned them.

Enabled

All unlicensed admins have access to Intune. To revoke access from an unlicensed admin, remove them as a member from their Microsoft 365 group and remove them from their Microsoft 365 group to Intune roles.

Scoped permissions
Separate resource permissions associated with scope tags (recommended).

[Learn more about separating permissions](#)

Enabled

Resource permissions associated with scope tags are separated for this tenant.

Permissions Assessment Report

Generate Report

↓ Export Columns ▾

Search ⓘ

Device Enrollment | Enrollment Restrictions

- ◆ Control which types of devices can enroll in intune
- ◆ Personal/Corporate

Enrollment restrictions ...

Device enrollment with Company Portal

Windows restrictions Android restrictions macOS restrictions iOS restrictions

+ Create restriction Refresh Columns ▾

A device must comply with the highest priority enrollment restrictions assigned to its user. You can drag and drop restrictions to change their priority. Default restrictions may be edited, but not deleted. [Learn more.](#)

Device type restrictions

Define which platforms, versions, and management types can enroll.

Priority	Name
Default	All Users

Tenant admin | Autopatch groups

- ◆ Enroll in Autopatch!
- ◆ How many Autopatch groups do I need?
- ◆ What updates to cover?

Dynamic group distribution ⓘ

Deployment ring	Assigned group ⓘ	Dynamic group distribution ⓘ
Windows Autopatch - Test	None	Not applicable
Windows Autopatch - Ring1	None	<input checked="" type="checkbox"/> 1 %
Windows Autopatch - Ring2	None	<input checked="" type="checkbox"/> 9 %
Windows Autopatch - Ring3	None	<input checked="" type="checkbox"/> 90 %
Windows Autopatch - Last	None	Not applicable

Tenant admin | Tenant management

- ◆ Deploys the Autopatch client broker
- ◆ Autopatch device readiness
- ◆ Support log collection

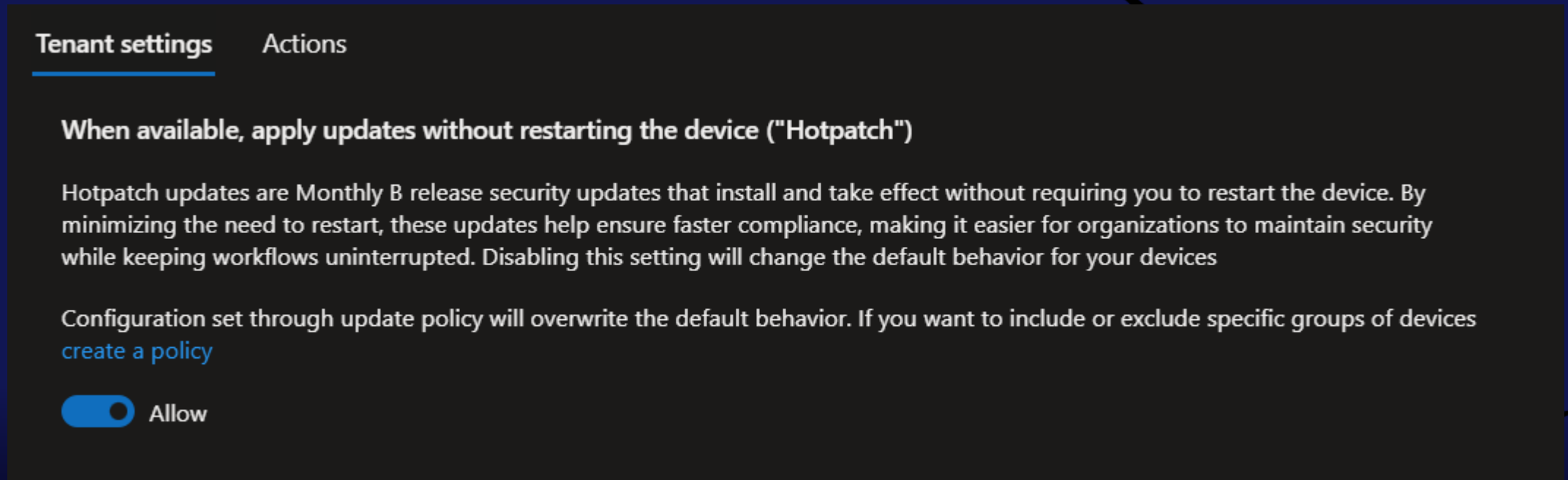
The screenshot displays the 'Actions' tab in the Microsoft Intune tenant management interface. At the top, there are tabs for 'Tenant settings' and 'Actions'. Below the tabs, a message states: 'Your tenant configuration has changed. Complete these actions to keep the service working well.' There are two buttons: 'Refresh' (with a circular arrow icon) and 'Export' (with a downward arrow icon). Below this is a search bar with a magnifying glass icon and a help icon (i). A table lists the actions:

Name ↑↓	Description	Severity ↑↓	Status ↑↓
Manage client broker	Install Windows Autopatch client agent to devices for	i Informational	⊖ Not started

A modal dialog is open with the title 'Install client broker?'. The text inside reads: 'The Windows Autopatch client broker allows Autopatch registered devices to communicate update readiness data and log collection information to the Autopatch service.' At the bottom of the dialog are two buttons: 'Install' (highlighted in blue) and 'Cancel'.

Tenant admin | Tenant management

- ◆ Hotpatch enabled by default for **ALL** autopatch customers. (2026-04)
- ◆ Default Allow – even in existing tenants



Tenant settings Actions

When available, apply updates without restarting the device ("Hotpatch")

Hotpatch updates are Monthly B release security updates that install and take effect without requiring you to restart the device. By minimizing the need to restart, these updates help ensure faster compliance, making it easier for organizations to maintain security while keeping workflows uninterrupted. Disabling this setting will change the default behavior for your devices

Configuration set through update policy will overwrite the default behavior. If you want to include or exclude specific groups of devices [create a policy](#)

Allow

Devices | Device clean-up rules

- ◆ Establish a clean-up rule in Intune, note that this will not delete the devices in Entra.
- ◆ Soft-delete is used

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 ⓘ

Devices | Compliance

- ◆ Default compliance policies should be configured

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Co

Mark devices with no compliance policy assigned as ⓘ

Not compliant

Compliance status validity period (days) ⓘ

45 *

Connectors and tokens | Windows data

- ◆ Windows diagnostics data
 - ◆ Windows Update reports
- ◆ Windows license verification
 - ◆ Enables remediation scripts
 - ◆ Upgrade readiness report

Use the settings below to enable Intune features that use Windows diagnostic data.[Learn more about Windows diagnostic data](#)

Windows data

Some Intune features, including Windows update reports, require sharing Windows diagnostic data with Intune.[Learn more about features that require Windows diagnostic data](#)

Enable features that require Windows diagnostic data in processor configuration ⓘ

Off

Windows license verification

Some Intune features require specific Windows licensing to use them. Features including the Windows 11 Upgrade Readiness report and Remediations require Windows license verification.

If you want to use these features, confirm your tenant has one of the following licenses:

- Windows 10 or later Enterprise E3 or E5; or Microsoft 365 F3, E3, or E5
- Windows 10 or later Education A3 or A5; or Microsoft 365 A3 or A5
- Windows Virtual Desktop Access E3 or E5

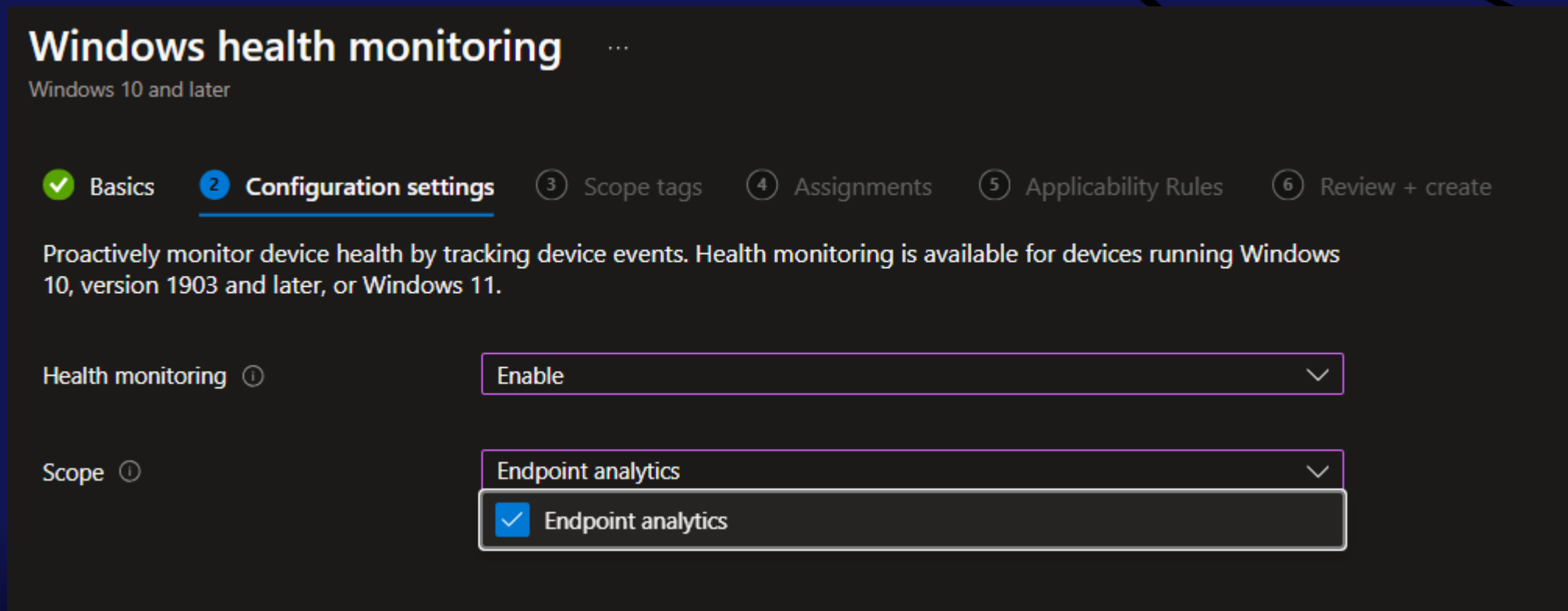
You must be a Global Administrator or Intune Service Administrator to confirm licenses.[Learn more about Roles in Intune](#)

I confirm that my tenant owns one of these licenses. Off

[Connectors and tokens - Microsoft Intune admin center](#)

Windows Health Monitoring

- ◆ Enables Endpoint analytics



The screenshot shows the 'Windows health monitoring' configuration page in the Microsoft Management Console. The page is titled 'Windows health monitoring' with a subtitle 'Windows 10 and later'. It features a progress bar with six steps: 1. Basics (checked), 2. Configuration settings (active), 3. Scope tags, 4. Assignments, 5. Applicability Rules, and 6. Review + create. Below the progress bar, there is a descriptive text: 'Proactively monitor device health by tracking device events. Health monitoring is available for devices running Windows 10, version 1903 and later, or Windows 11.' The main configuration area has two dropdown menus. The first is labeled 'Health monitoring' and is set to 'Enable'. The second is labeled 'Scope' and is set to 'Endpoint analytics'. A dropdown menu is open for the 'Scope' setting, showing 'Endpoint analytics' selected with a blue checkmark.

Windows health monitoring ...
Windows 10 and later

✓ Basics 2 **Configuration settings** 3 Scope tags 4 Assignments 5 Applicability Rules 6 Review + create

Proactively monitor device health by tracking device events. Health monitoring is available for devices running Windows 10, version 1903 and later, or Windows 11.

Health monitoring ⓘ Enable

Scope ⓘ Endpoint analytics

✓ Endpoint analytics



Endpoint analytics

Proactively optimize your end user experience and track your progress. [Learn more](#)



Analyze device performance to eliminate productivity killers.




Get personalized recommendations for improving the user experience.



Proactively detect top support issues before users call help desk.

Collect device data from

All cloud-managed devices

We anonymize and aggregate the scores from all enrolled organizations to keep the All organizations (median) baseline up-to-date. You can stop gathering data at any time. [Learn more](#) 

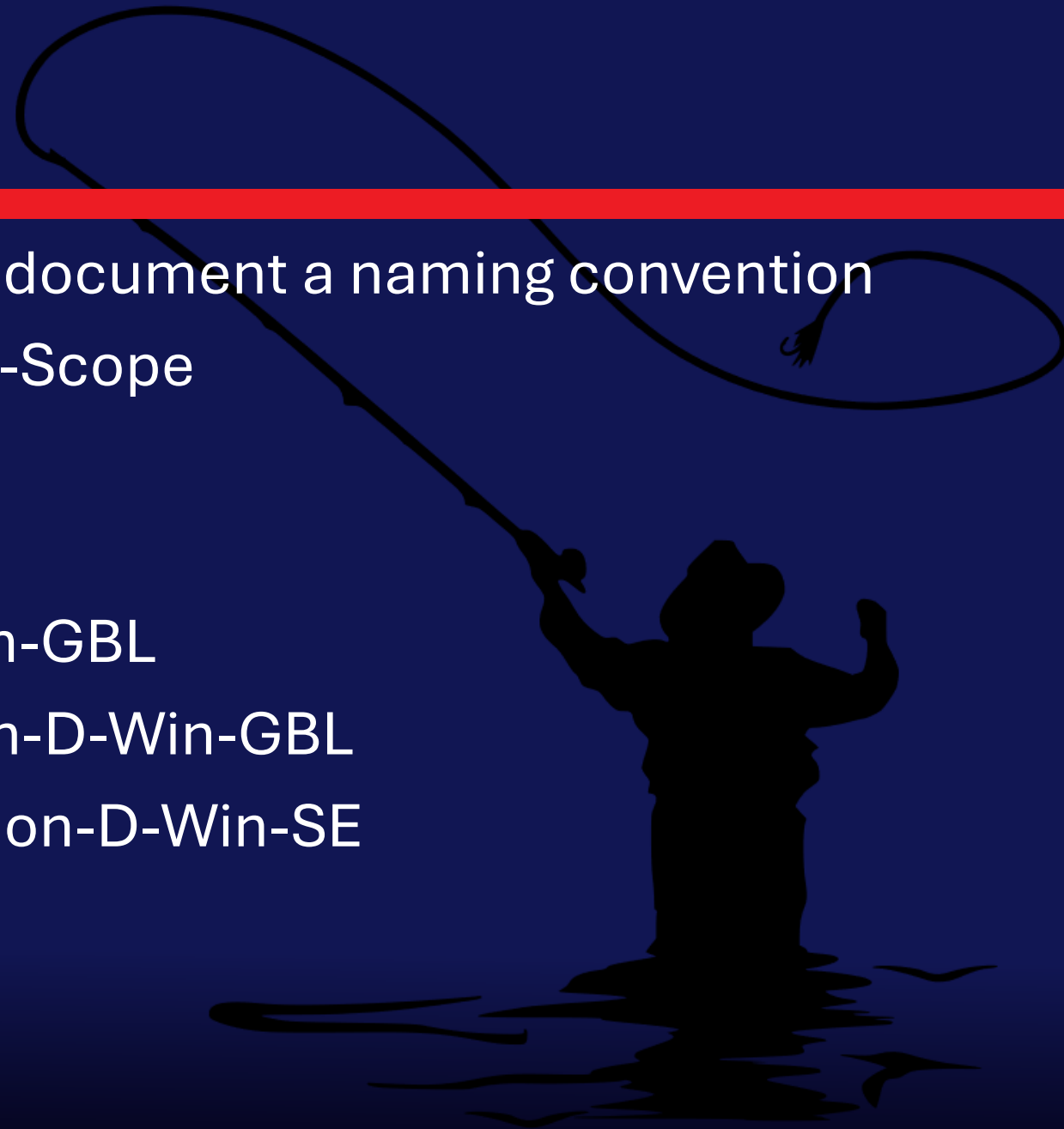
Start



Naming Convention

- ◆ Before starting to create objects, document a naming convention
- ◆ CPxx1-Description-D/U-Platform-Scope

- ◆ Example:
- ◆ CP001-Edge Configuration-D-Win-GBL
- ◆ EP001-Defender AV Configuration-D-Win-GBL
- ◆ EP001.1-Defender AV Configuration-D-Win-SE



Devices | Enrollment – Windows Hello for business

- ◆ Default not configured tenant-wide
- ◆ Windows Hello for Business is enabled by default for devices that are Microsoft Entra joined

Configure Windows Hello for Business: ⓘ

Not configured

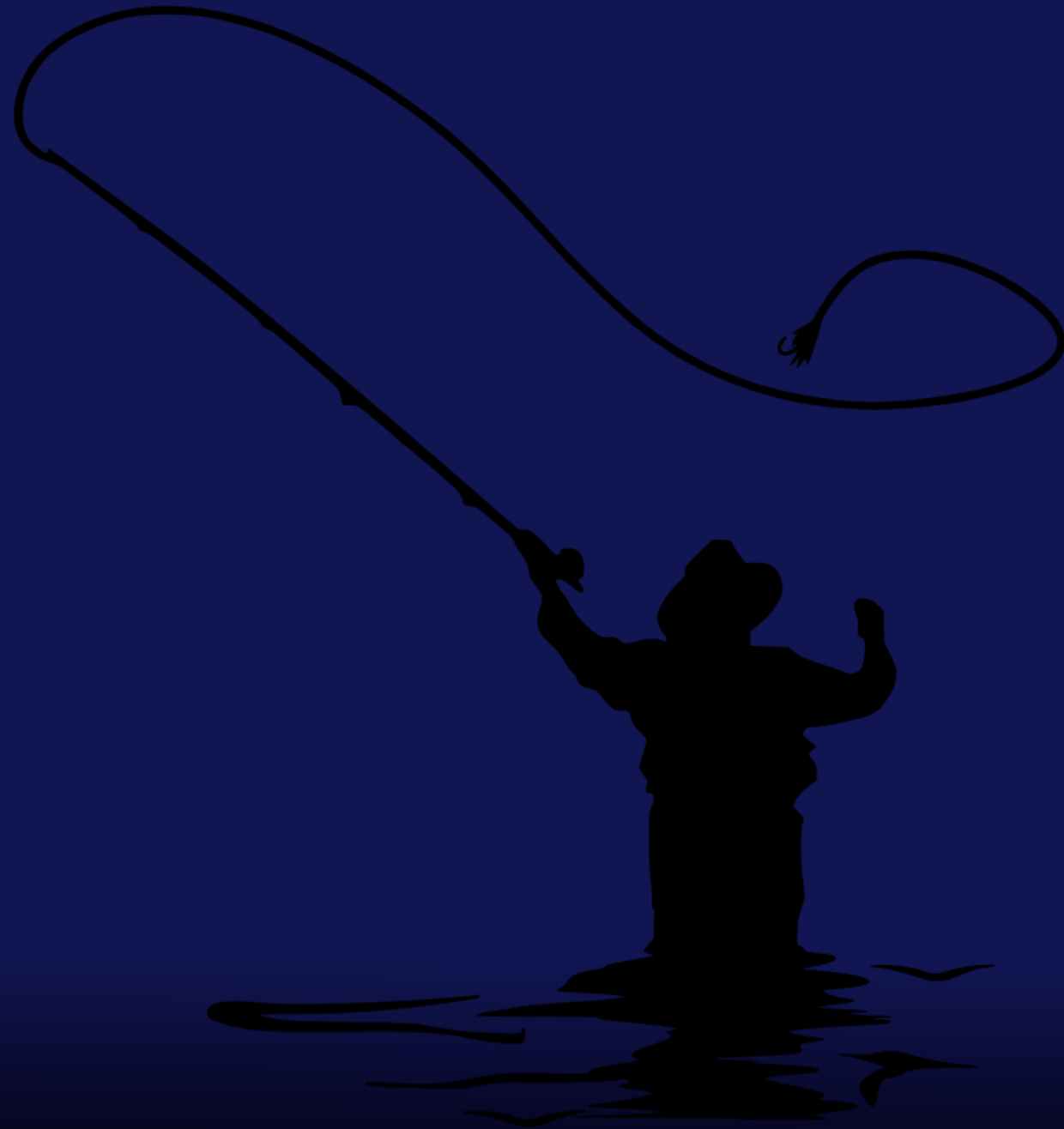


Use security keys for sign-in: ⓘ

Not configured



Entra ID



Entra ID Tenant Settings



Default Tenant Security – Security Defaults

- ◆ Security Defaults are a catch all approach to identity management
- ◆ Requiring all users to register for multifactor authentication
- ◆ Requiring administrators to do multifactor authentication
- ◆ Blocking legacy authentication protocols
- ◆ Protecting privileged activities like access to the Entra portal
- ◆ This seems like a good place to start?

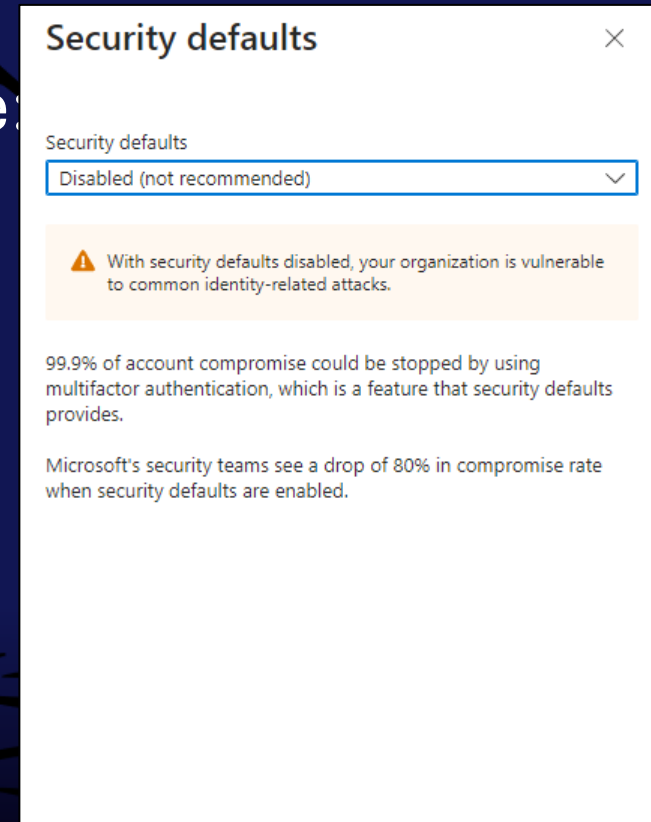


But..

- ◆ The configuration does not provide flexibility, so what do we do?
We disable it..

- ◆ That means we need to also configure and manage:

- ◆ Conditional Access
- ◆ Authentication Methods
- ◆ Enterprise Applications



Top things to take control of in Entra

- ◆ Apply Tenant Branding
- ◆ Entra ID Portal Access
- ◆ Security Group Creation
- ◆ Microsoft 365 Group Creation
- ◆ Create New Tenant Setting
- ◆ Guest / User Invite Settings
- ◆ Enterprise Application / Application Consent Settings
- ◆ And all the Device / Intune Related settings ..





Consent and permissions | User consent settings



Save



Discard



Got feedback?

Manage



User consent settings



Admin consent settings



Permission classifications

Control when end users and group owners are allowed to grant consent to applications and agent identities, and when they will be required to request administrator review and approval. Allowing users to grant apps and agent identities access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)



Do not allow user consent

An administrator will be required for all apps and agent identities.



Allow user consent for apps from verified publishers, for selected permissions

All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.



Let Microsoft manage your consent settings (Recommended)

Automatically update your organization to Microsoft's current user consent guidelines. [Learn more](#)



Enable user consent for popular Mail clients

Users can consent to popular applications for specific Mail permissions. List of applications and permissions allowed for user consent are located [here](#).

Microsoft recommended user consent policy

The setting labeled "Let Microsoft manage your consent settings," the Microsoft managed policy, will update with Microsoft's latest recommended default consent settings. This is also the default for a new tenant. The setting's rules are currently: End users can consent for any user consentable delegated permissions EXCEPT:

- For Microsoft Graph: `Files.Read.All`, `Files.ReadWrite.All`, `Sites.Read.All`, `Sites.ReadWrite.All`, `Mail.Read`, `Mail.ReadWrite`, `Mail.ReadBasic`, `Mail.Read.Shared`, `Mail.ReadBasic.Shared`, `Mail.ReadWrite.Shared`, `MailboxItem.Read`, `Calendars.Read`, `Calendars.ReadBasic`, `Calendars.ReadWrite`, `Calendars.Read.Shared`, `Calendars.ReadWrite.Shared`, `Chat.Read`, `Chat.ReadWrite`, `OnlineMeetings.Read`, `OnlineMeetings.ReadWrite`, `MailBoxFolder.Read`, `MailBoxFolder.ReadWrite`, `MailBoxSettings.Read`, `MailBoxSettings.ReadWrite`, `EAS.AccessAsUser.All`, `EWS.AccessAsUser.All`, `IMAP.AccessAsUser.All`, `POP.AccessAsUser.All`.
- For Office 365 Exchange Online: `EAS.AccessAsUser.All`, `EWS.AccessAsUser.All`, `IMAP.AccessAsUser.All`, `POP.AccessAsUser.All`.

Mail client policy

An additional policy is enabled by default is the **microsoft-user-allow-default-consent-apps** policy. This policy allows end-users in your organization to consent for popular mail applications for mail permissions. When this policy is enabled, end users will be able to consent for specific delegated mail permissions (Microsoft Graph and Office 365 Exchange Online permissions: EAS.AccessAsUser.All, EWS.AccessAsUser.All, IMAP.AccessAsUser.All, POP.AccessAsUser.All) for the following applications:

- Apple Mail (application ID: f8d98a96-0999-43f5-8af3-69971c7bb423)
- Spark Email (application ID:b50c1dbd-1855-4e54-b07c-d3c3029e93d3)
- eM Client (application ID:e9a7fea1-1cc0-4cd9-a31b-9137ca5deedd)
- Android-Samsung (application ID:8acd33ea-7197-4a96-bc33-d7cc7101262f)
- Android-Mail (application ID:2cee05de-2b8f-45a2-8289-2a06ca32c4c8)
- Thunderbird (application ID:9e5f94bc-e8a4-4e73-b8be-63364c29d753)

DEMO

Entra ID defaults

Tenant



Entra ID Device Settings



Entra Defaults

Device Settings

- ◆ Entra configurations
- ◆ Entra Join settings
- ◆ Local Administrator settings
- ◆ Enterprise State Roaming
- ◆ Other settings



MDM User Scope

MDM user scope ⓘ

None Some All

MDM terms of use URL ⓘ

MDM discovery URL ⓘ

Disable MDM enrollment when adding work or school account on Windows ⓘ

No

MDM compliance URL ⓘ

[Restore default MDM URLs](#)

Entra Join Settings

- ◆ How can we join device to Entra?
- ◆ Require MFA?
- ◆ Number of devices

Microsoft Entra join and registration settings

Users may join devices to Microsoft Entra ⓘ

All Selected None

Selected
No member selected


Users may register their devices with Microsoft Entra ⓘ

All None

[Learn more on how this setting works](#)

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

Yes No

 We recommend that you require Multifactor Authentication to register or join devices with Microsoft Entra using [Conditional Access](#). Set this device setting to No if you require Multifactor Authentication using Conditional Access.

Maximum number of devices per user ⓘ

Unlimited

Local Admin settings


Local administrator settings

Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)



Yes

No

Registering user is added as local administrator on the device during Microsoft Entra join (Preview) 

All

Selected

None

LAPS + Bitlocker

Enable Microsoft Entra Local Administrator Password Solution (LAPS) ⓘ

Yes

No

Other settings

Restrict users from recovering the BitLocker key(s) for their owned devices ⓘ

Yes

No

ESR | Windows Backup

i Starting May 2026, Enterprise State Roaming (ESR) management is moving to Windows Backup for Organizations. [Learn more](#)

Users may sync settings and app data across devices ⓘ

All

Selected

None

Selected

No member selected

DEMO

Entra Device defaults

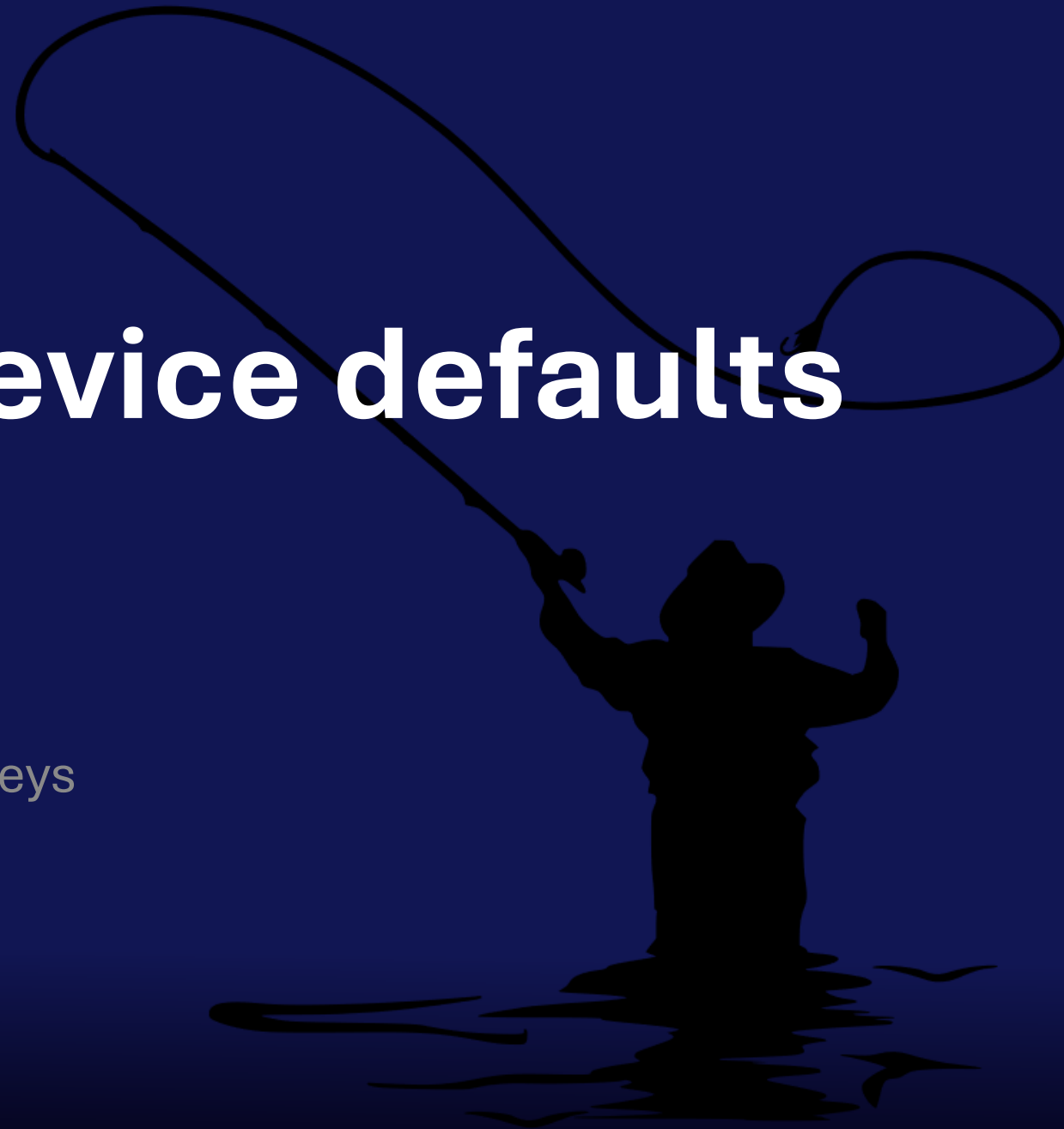
Entra Join

Windows LAPS

Device Local Admin

Bitlocker Recovery Keys

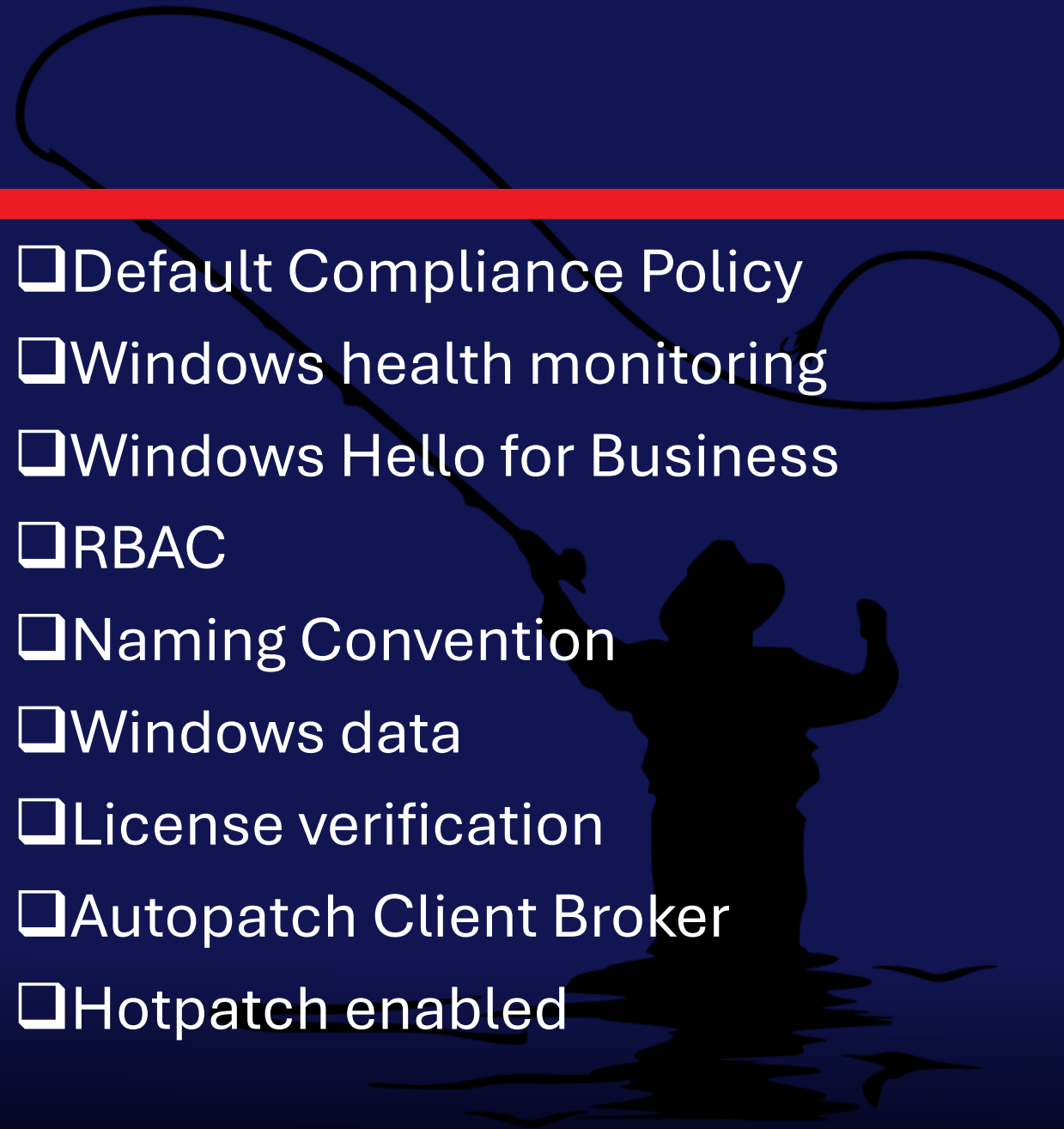
AutoEnrollment



Intune Checklist

- Configure branding – Corporate information
- Customization – what can the users do, what settings?
- Diagnostics setting
- Device diagnostics
- Scope tags
- Enrollment restrictions
- Device clean-up rules

- Default Compliance Policy
- Windows health monitoring
- Windows Hello for Business
- RBAC
- Naming Convention
- Windows data
- License verification
- Autopatch Client Broker
- Hotpatch enabled



Entra ID Device checklist

- Entra ID Defaults (Security)
- Apply Tenant Branding
- Entra ID Portal Access
- Security Group Creation
- Microsoft 365 Group Creation
- Create New Tenant Setting
- Guest / User Invite Settings
- Enterprise Application / Application Consent Settings



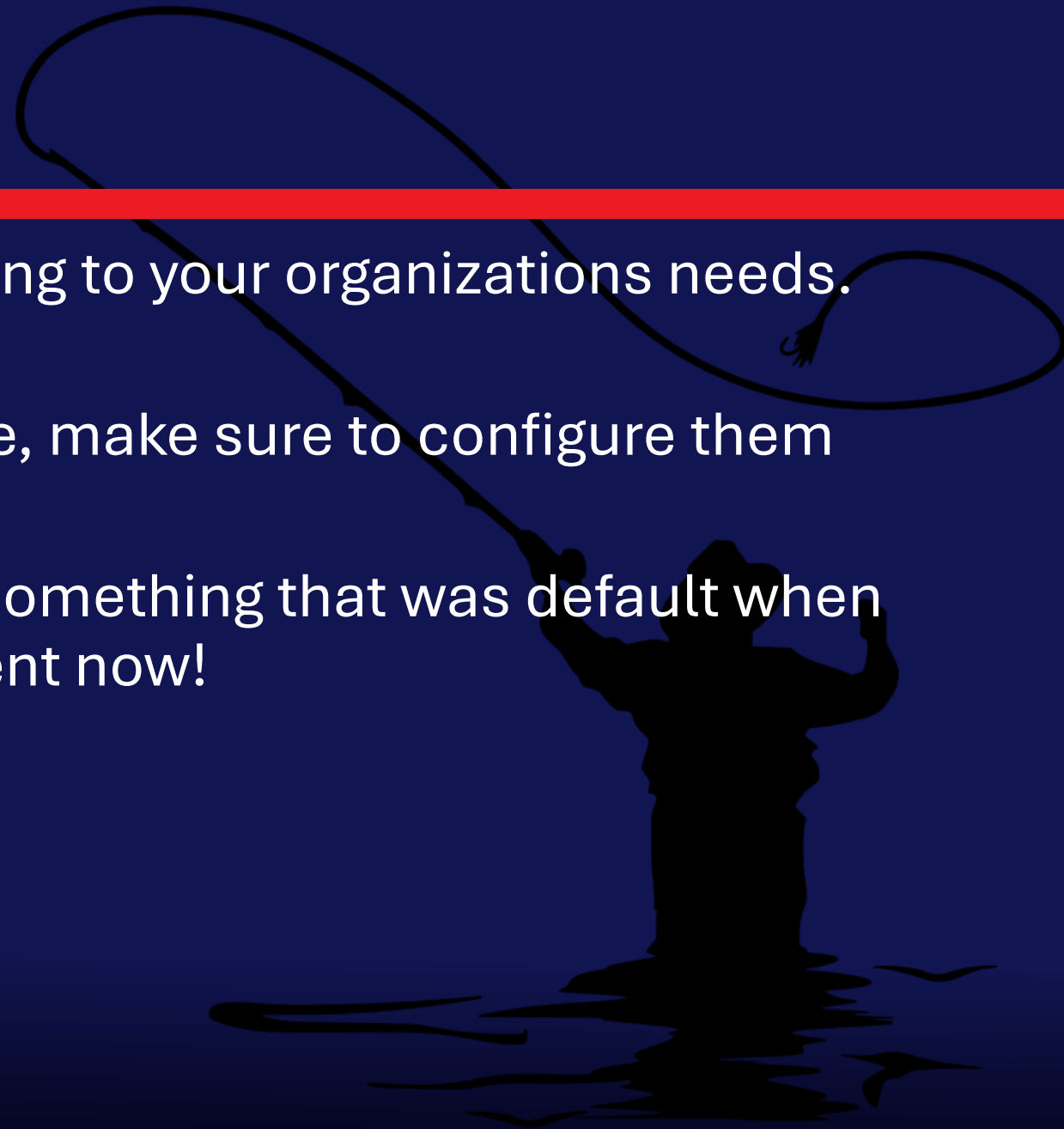
Entra ID Device checklist

- Entra Join Settings
- Windows LAPS
- Device Local Administrators
- Tenant Branding
- Bitlocker Recovery Keys
- Autoenrollment



Summary

- ◆ Configure all the settings according to your organizations needs. Do NOT rely on the defaults.
- ◆ New features are added over time, make sure to configure them and make a choice.
- ◆ Defaults also change over time, something that was default when your tenant was created is different now!



SAVE THE DATES

Oct 25-28, 2026



May 2-6, 2027



Oct 10-13, 2027



Extended Q&A



2Pint

Recast

robopack
empowered by SOFTWARE
CENTRAL

SquaredUp

CODETWO

baramundi

ninjaOne

Rimo3



TeamViewer

numecent

aiden