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

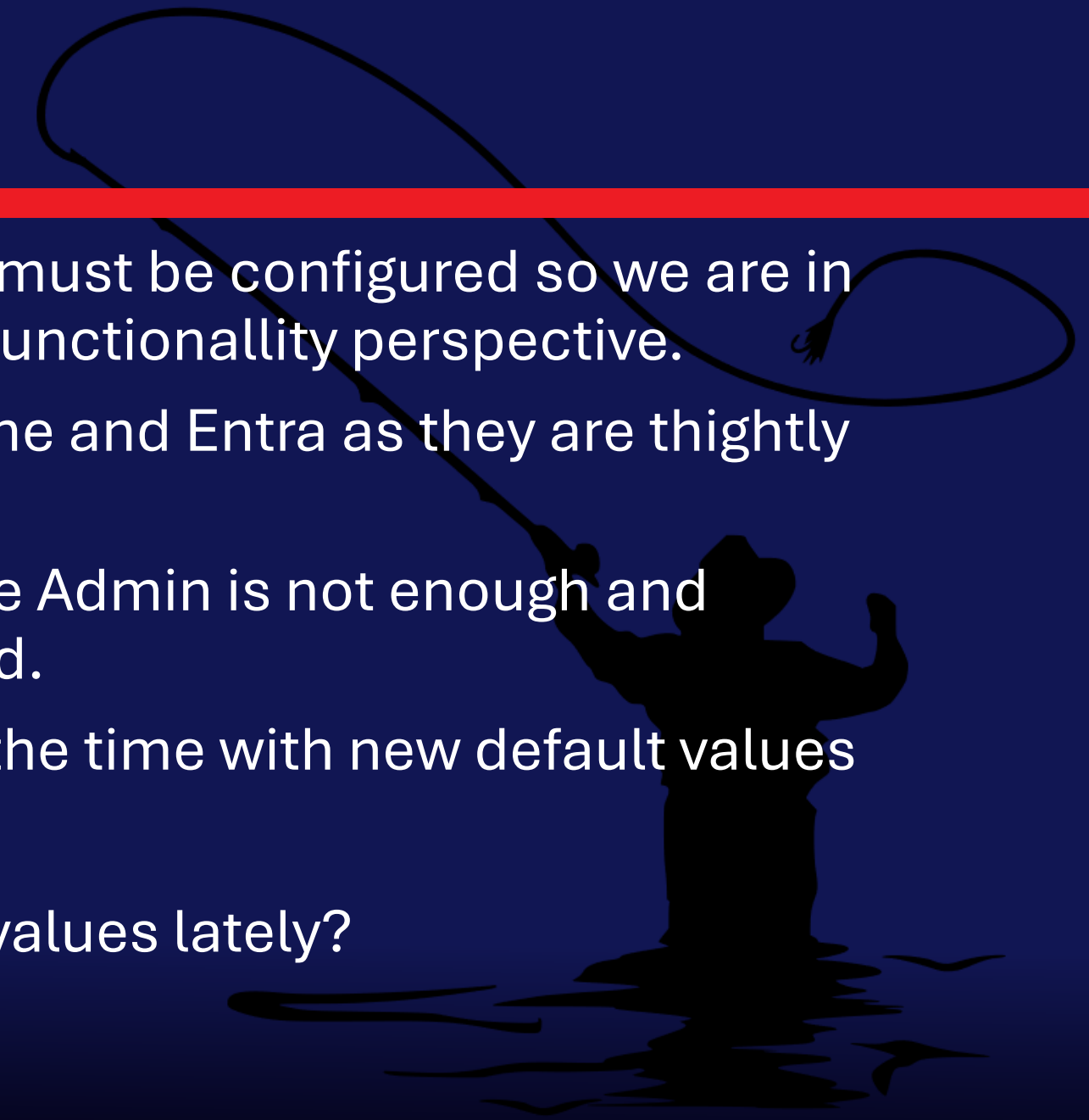
in/JankeSkanke

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

Takeways

- Default settings in a new tenant must be configured so we are in control, both from security and functionallity perspective.
- We will focus on defaults in Intune and Entra as they are thightly 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?



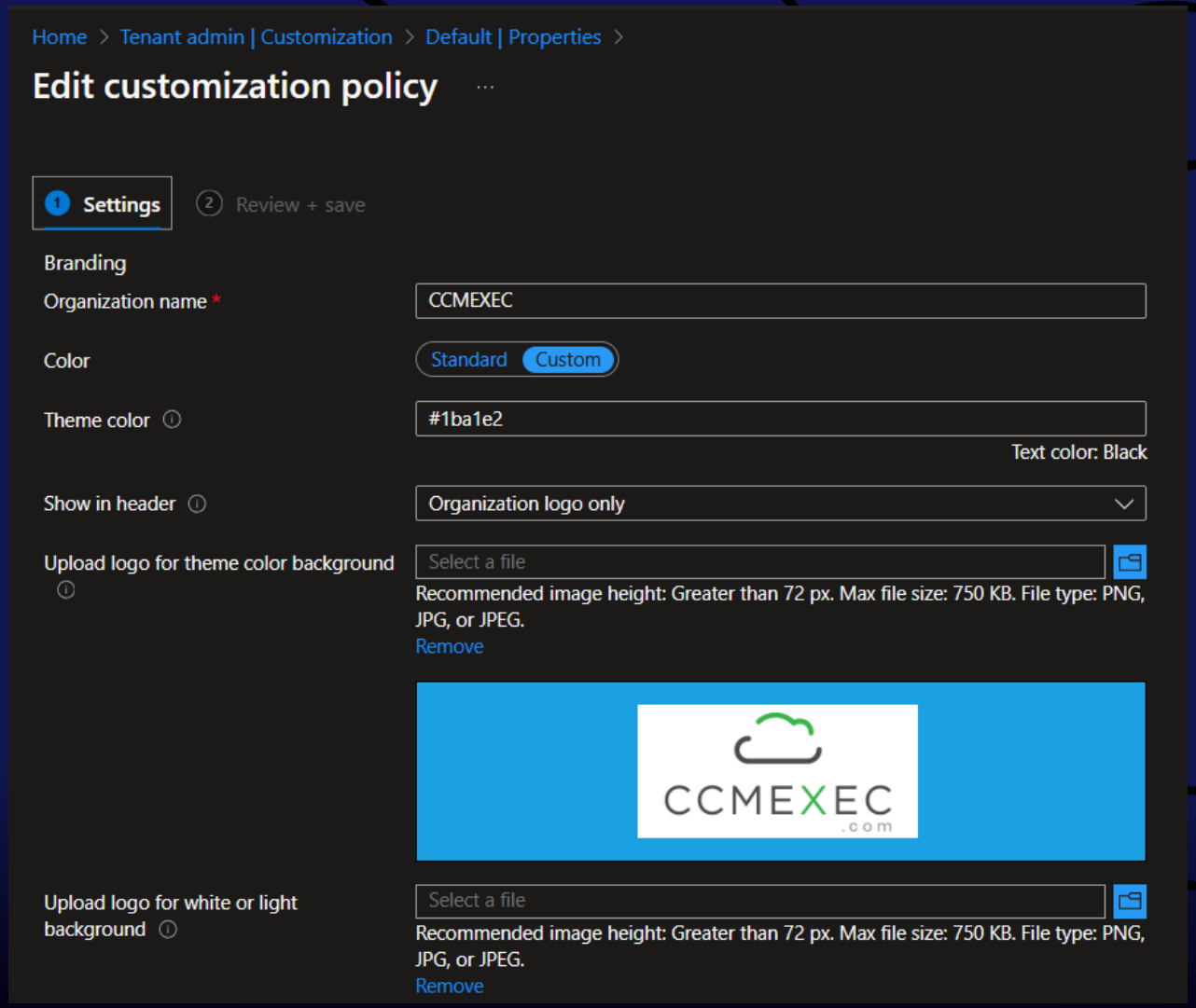
DEMO

Intune defaults

Tenant

Tenant admin | Customization | Branding

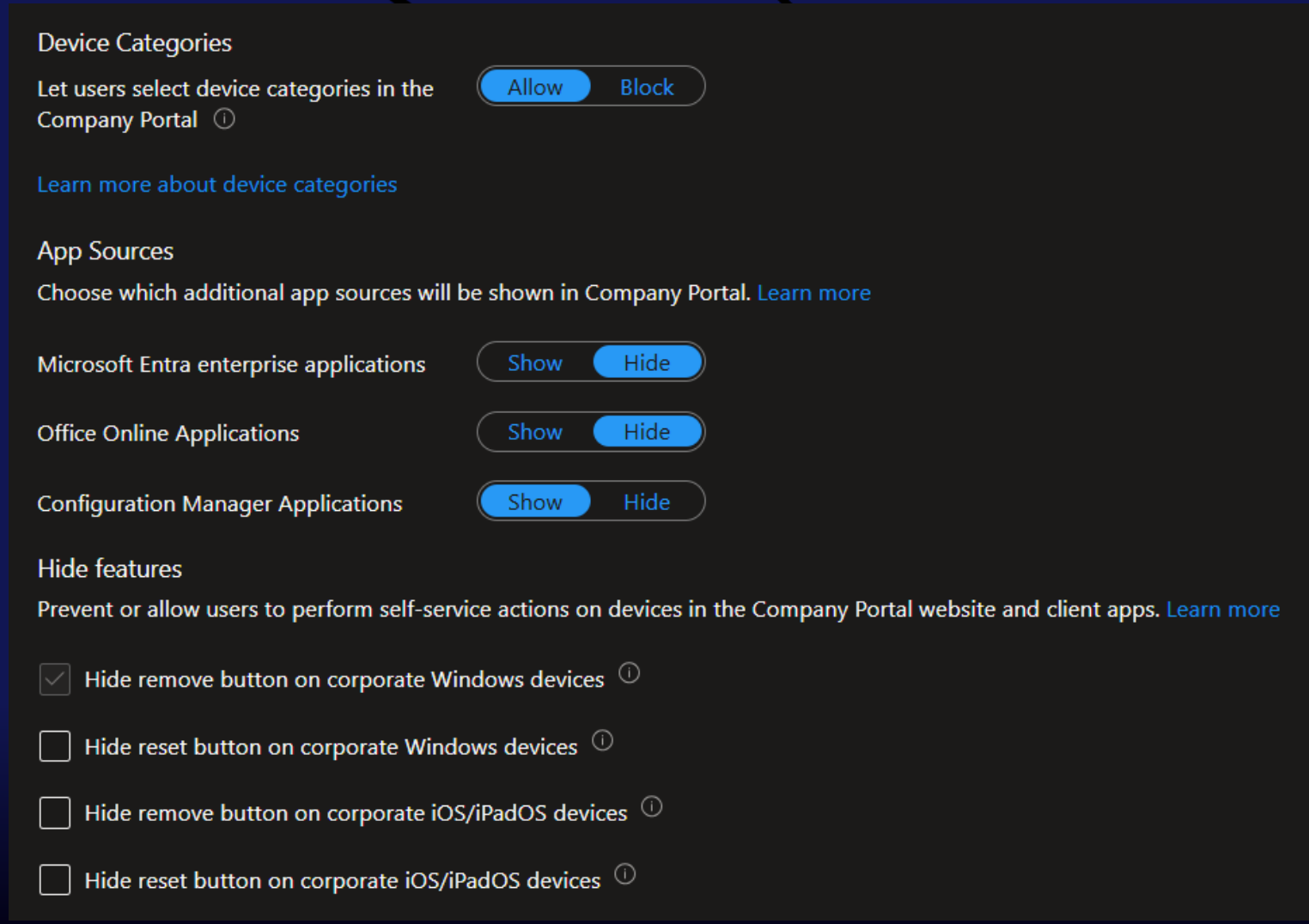
- Configure branding
- Corporate information
- Support information



Tenant admin - Microsoft Intune admin center

Tenant admin | Customization

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

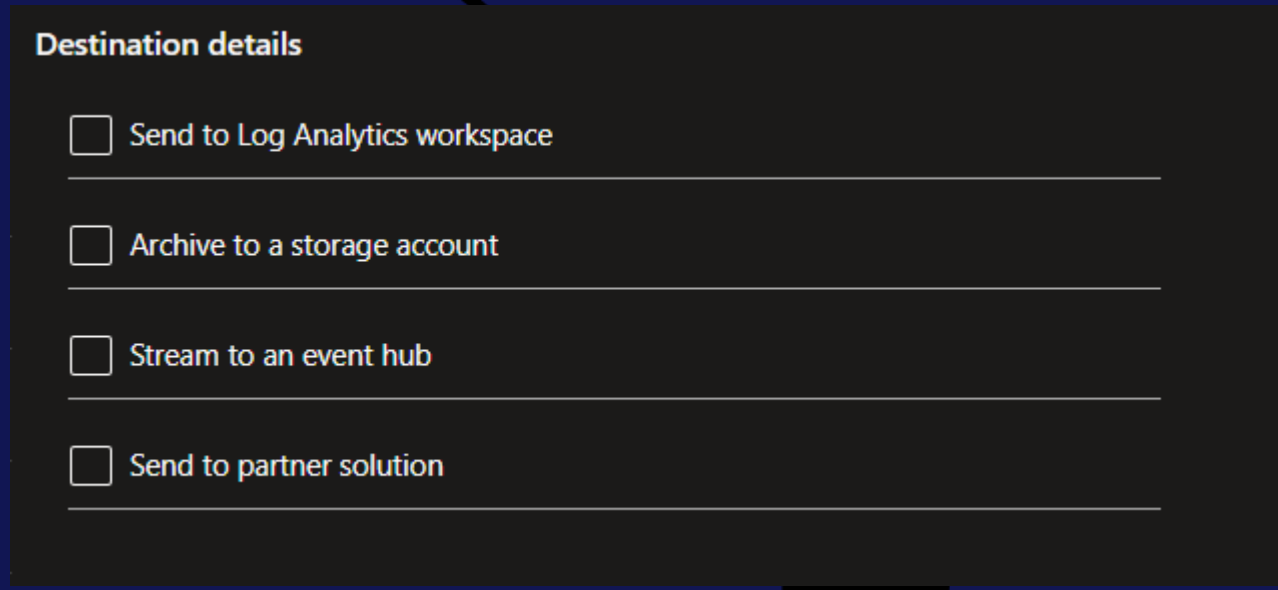


Tenant admin - Microsoft Intune admin center

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?

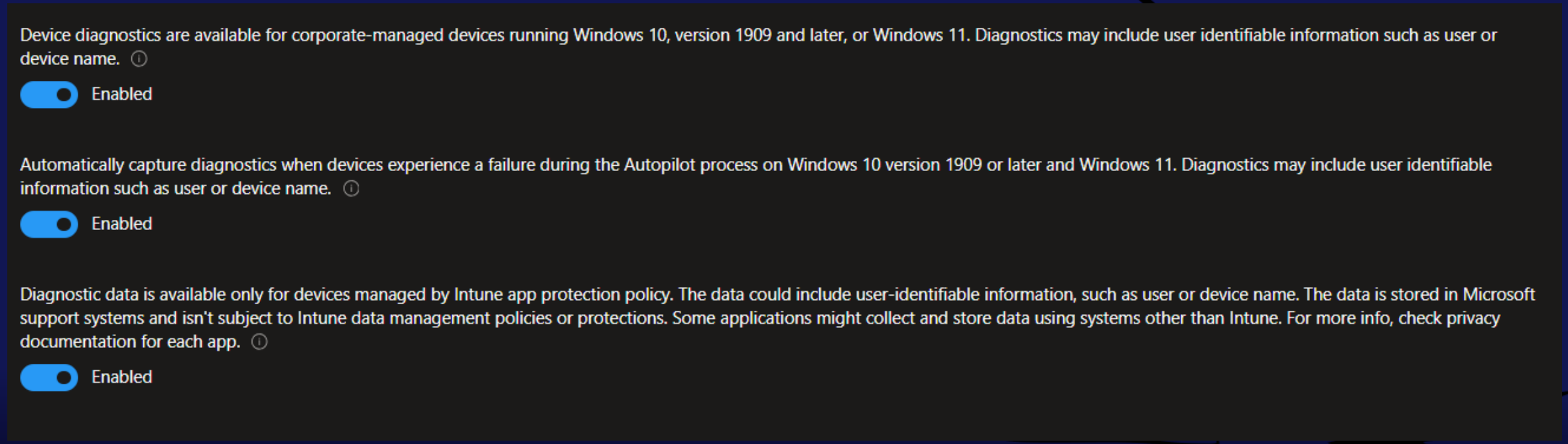
Answer: More information is shown!



Tenant admin - Microsoft Intune admin center

Tenant admin | Device diagnostics

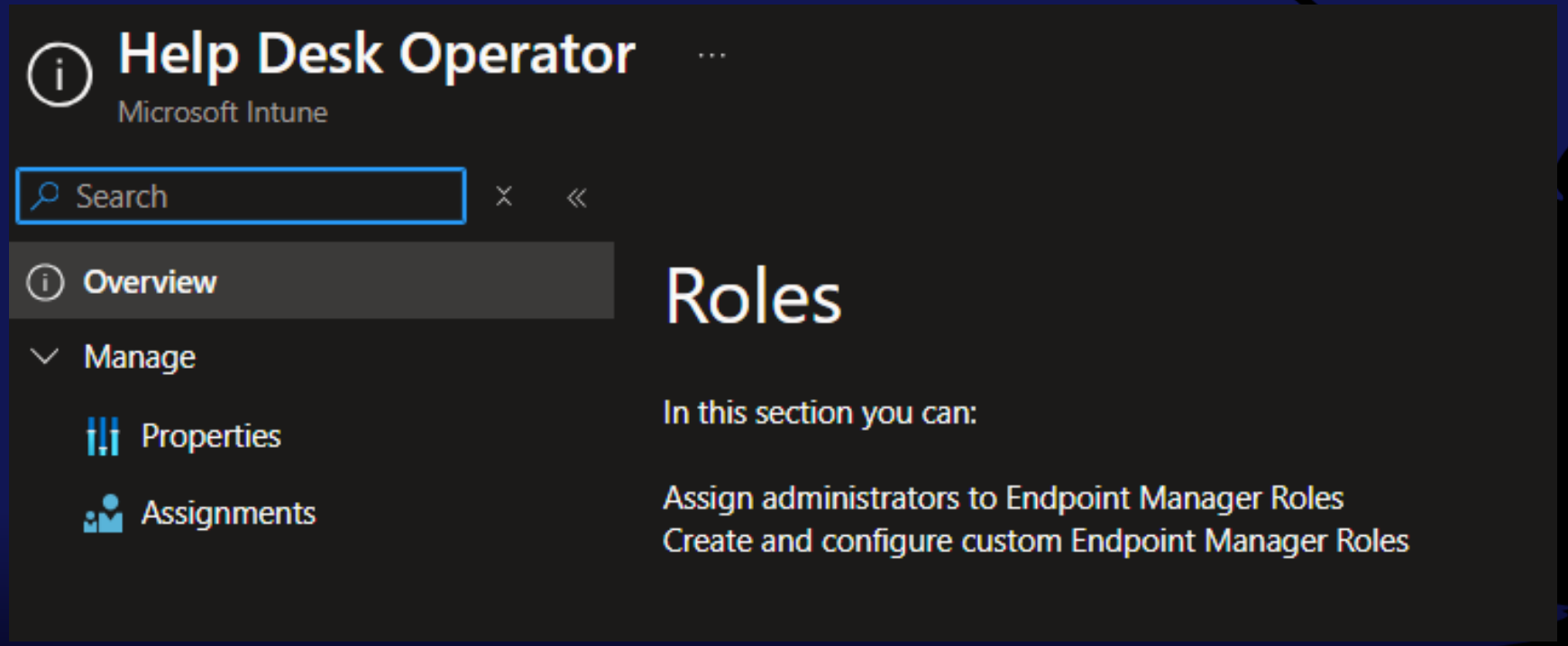
- Additional diagnostics to collect on Autopilot failure
- Additional information to collect



Tenant admin - Microsoft Intune admin center

Intune roles / Scope tags

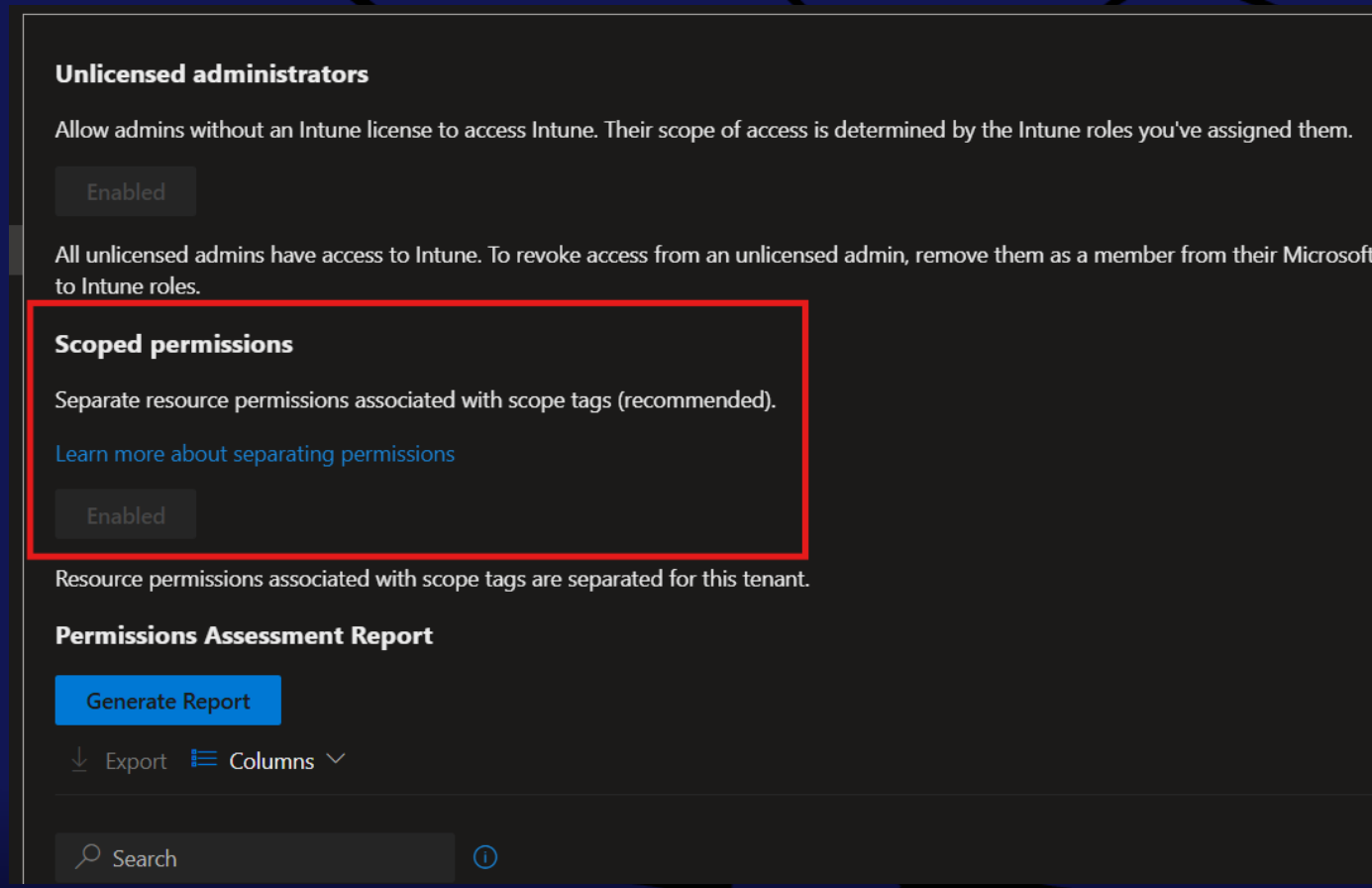
- Build your own roles! The helpdesk role has way to much permissions.



Intune roles - Microsoft Intune admin center

Tenant Admin: Scoped permissions

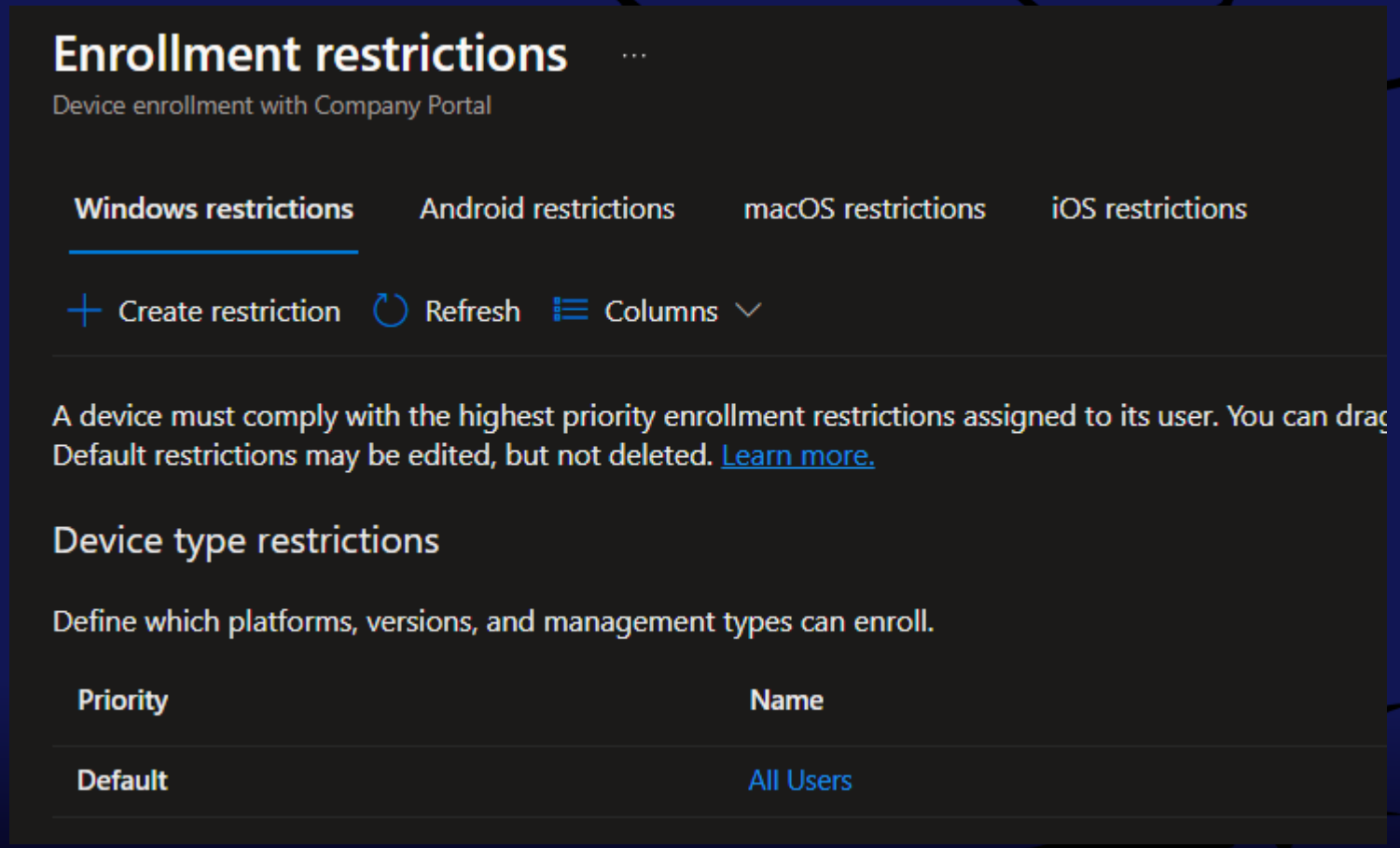
- Preview in 2026-04
- Separate resource permissions instead of merge
- Important to be able to have different permissions for managing VIP devices for example.



[Intune roles - Microsoft Intune admin center]

Device Enrollment | Enrollment Restrictions

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



Enrollment restrictions - Microsoft Intune admin center

Tenant admin | Autopatch groups

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

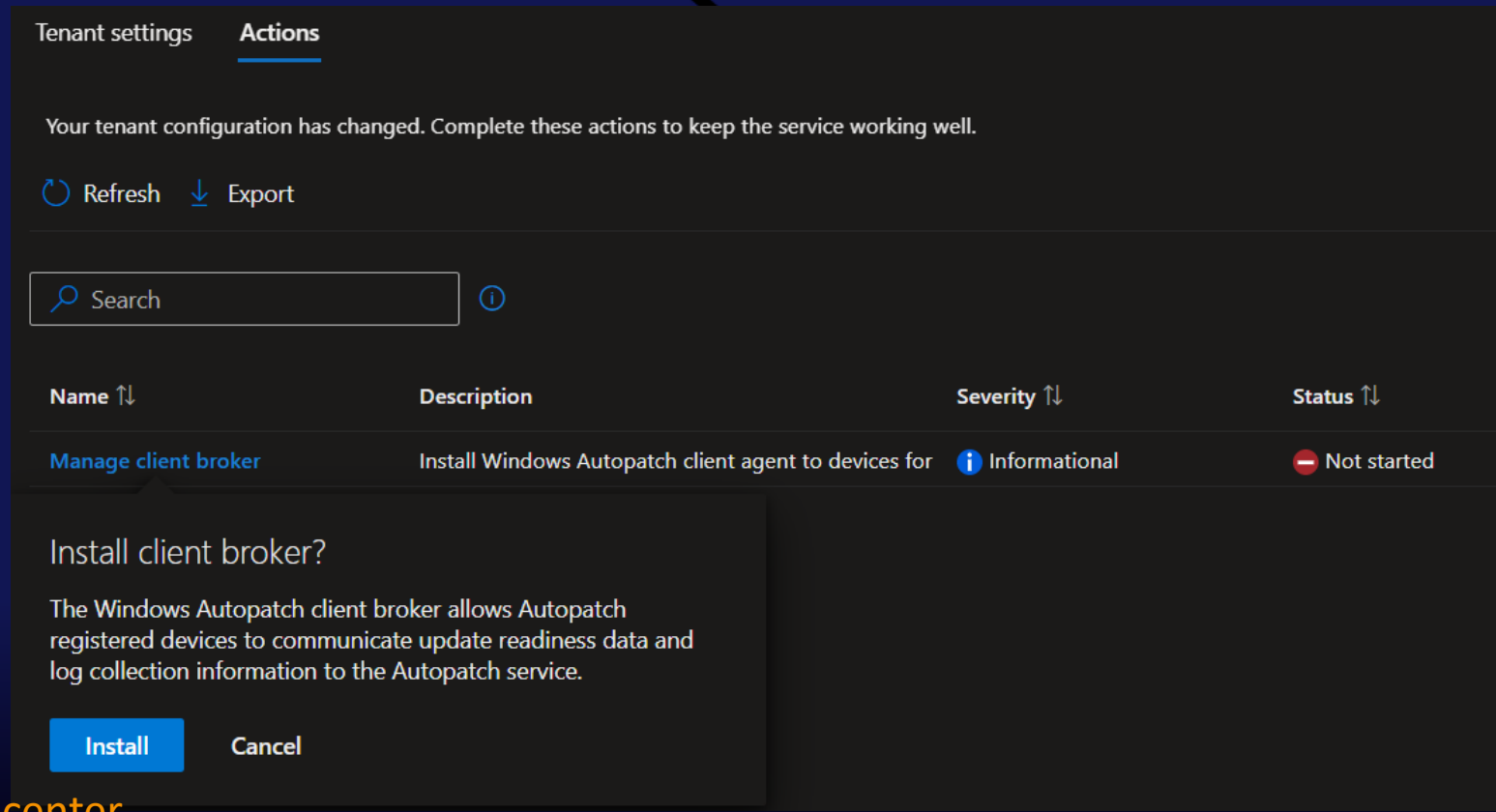
Dynamic group distribution ⓘ

Deployment ring	Assigned group ⓘ	Dynamic group distribution ⓘ
Windows Autopatch - Test	None	Not applicable
Windows Autopatch - Ring1	None	☑ 1 %
Windows Autopatch - Ring2	None	☑ 9 %
Windows Autopatch - Ring3	None	☑ 90 %
Windows Autopatch - Last	None	Not applicable

Tenant admin - Microsoft Intune admin center

Tenant admin | Tenant management

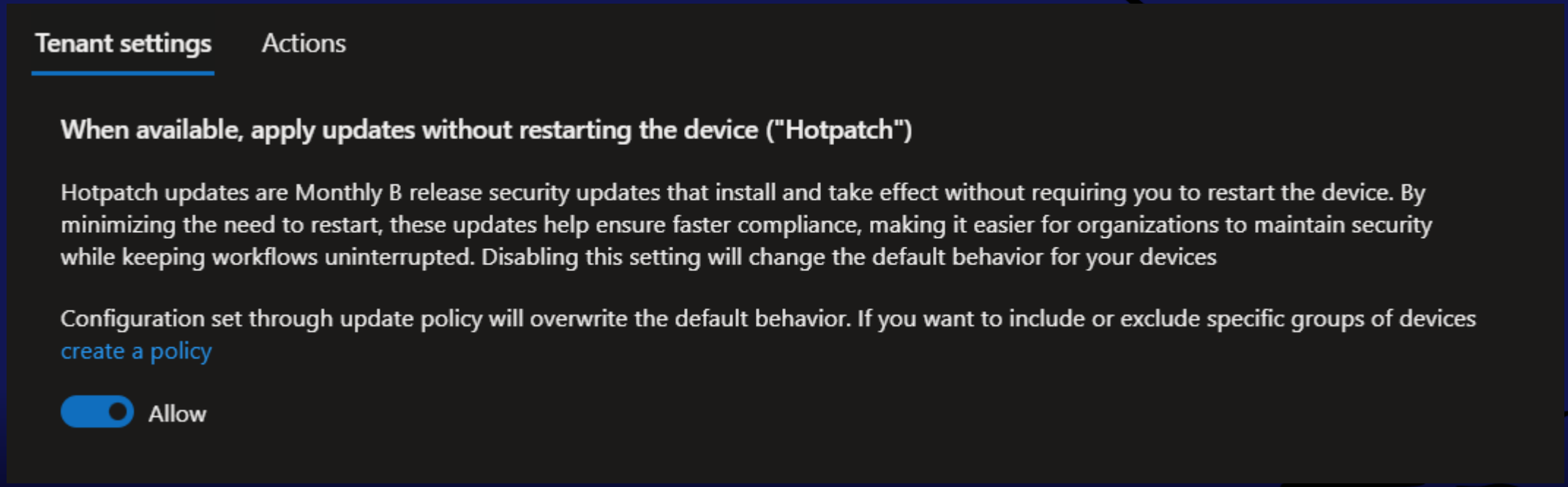
- Deploys the Autopatch client broker
- Autopatch device readiness
- Support log collection



Tenant admin - Microsoft Intune admin center

Tenant admin | Tenant management

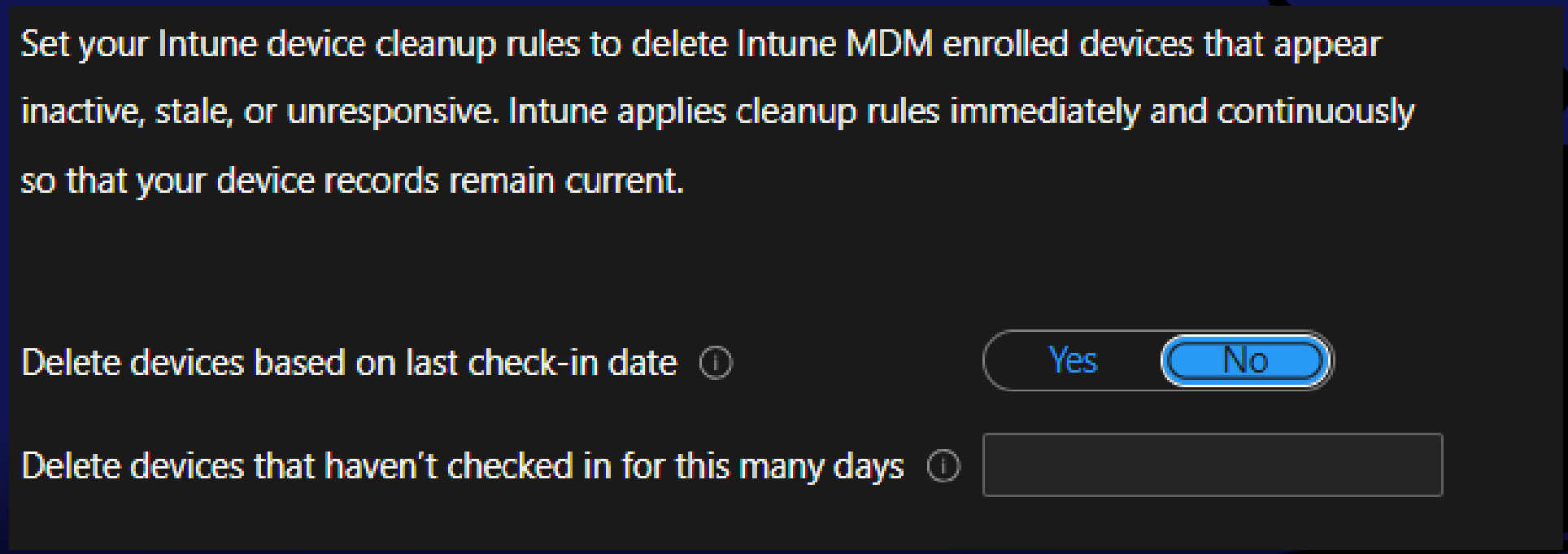
- Hotpatch enabled by default for **ALL** autopatch customers. (2026-04)
- Default Allow – even in existing tenants



Tenant admin - Microsoft Intune admin center

Devices | Device clean-up rules

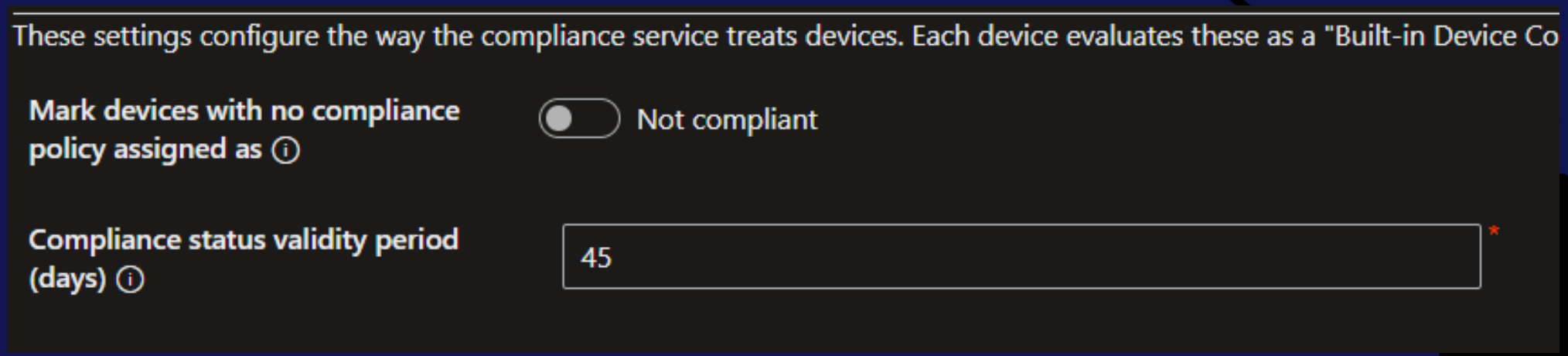
- Establish a clean-up rule in Intune, note that this will not delete the devices in Entra.
- Soft-delete is used



Devices - Microsoft Intune admin center

Devices | Compliance

- Default compliance policies should be configured

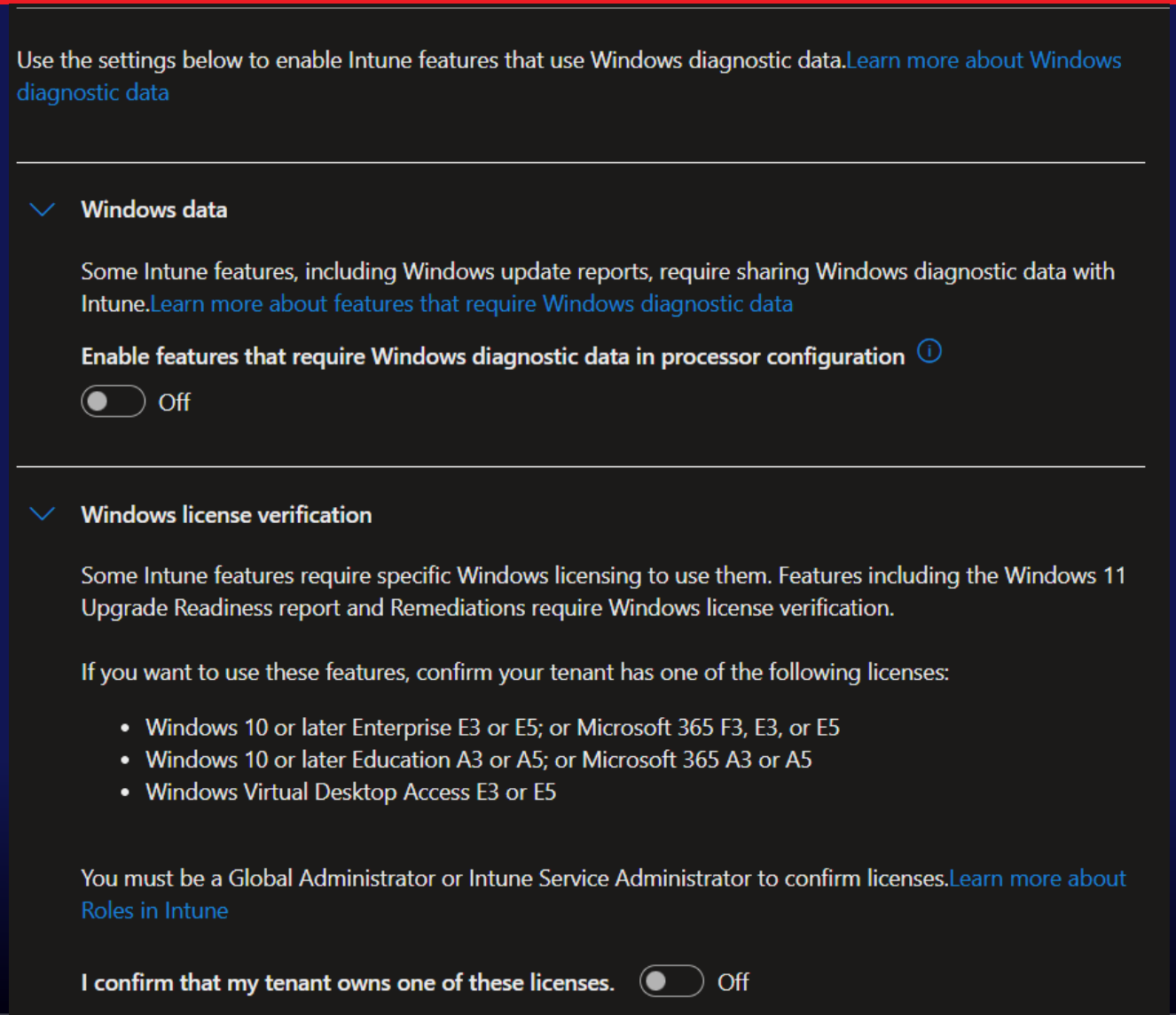


Devices - Microsoft Intune admin center

Connectors and tokens | Windows data

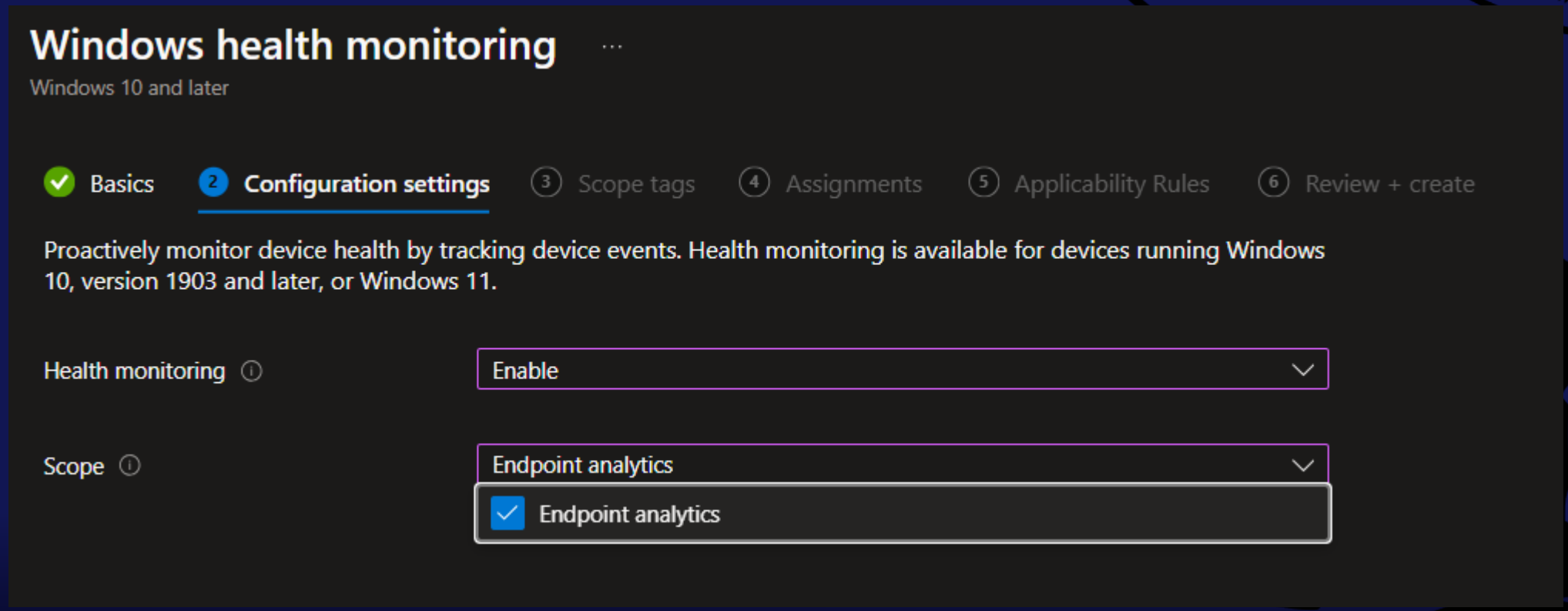
- Windows diagnostics data
  - Windows Update reports
- Windows license verification
  - Enables remediation scripts
  - Upgrade readiness report

Connectors and tokens - Microsoft Intune admin center



Windows Health Monitoring

- Enables 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

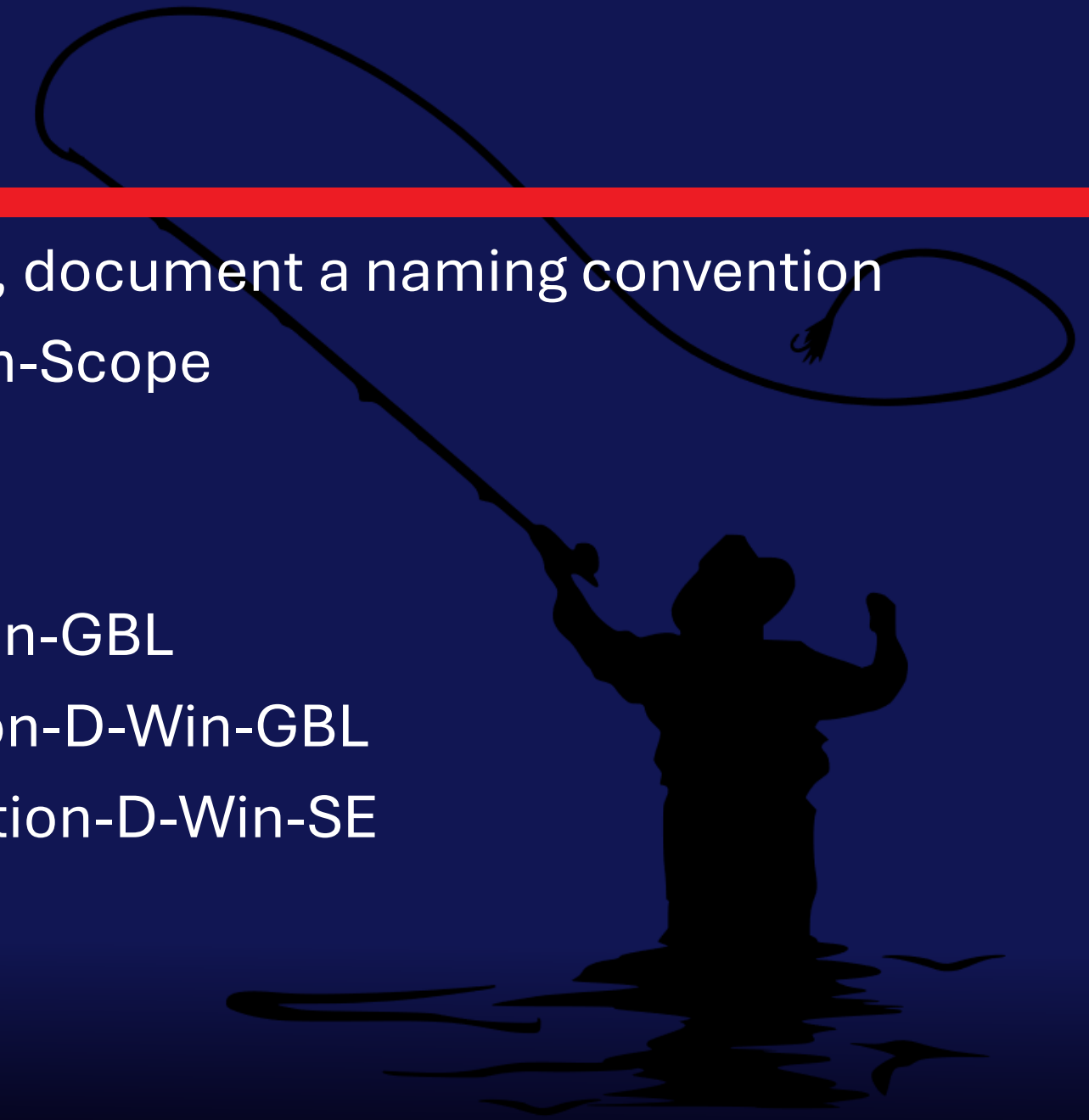
We anonymize and aggregate the scores from all enrolled organizations to keep the All organizations (median) baseline up-to-date. You can stop gathering data at any time. Learn more

Start

Naming Convention

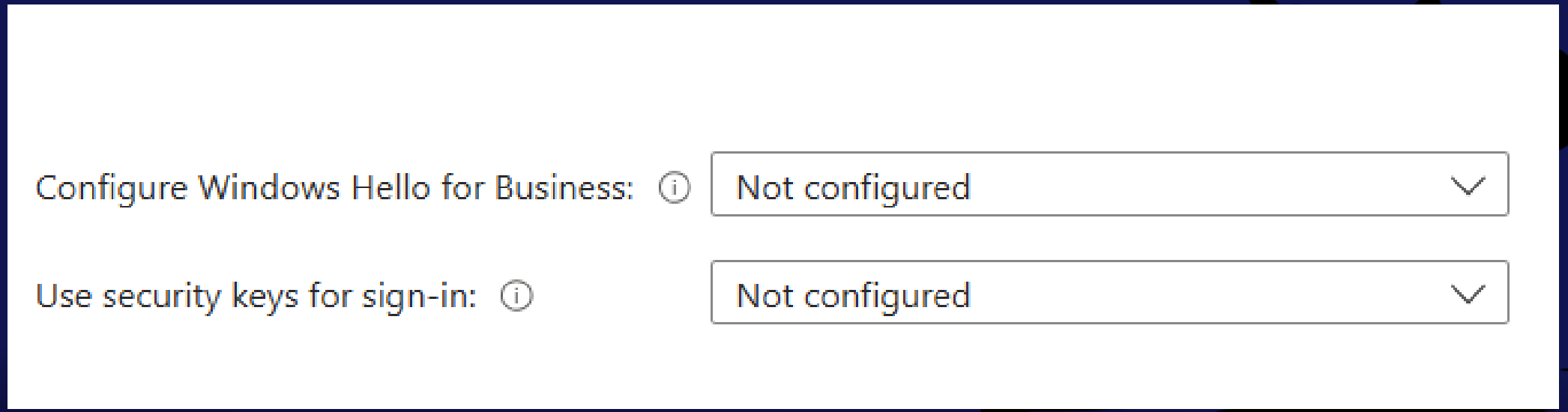
- Before starting to create objects, document a naming convention
- CPxx1-Description-D/U-Platform-Scope

- 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



Windows Hello for Business - Microsoft Intune admin center

Entra ID

Entra ID Tenant Settings

Default Tenant Security – Security Defaults

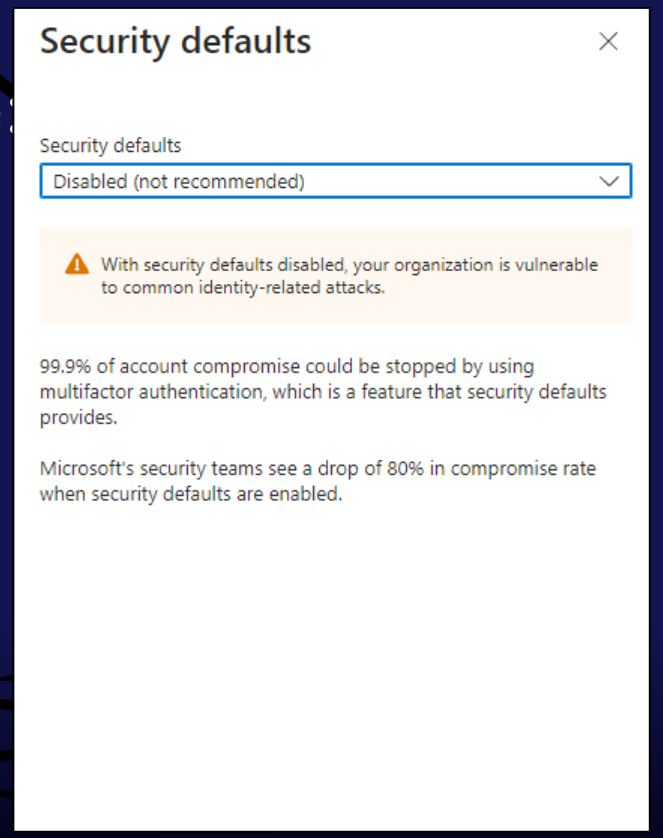
- Security Defaults are a catch all approach to identity management
- Requiring all users to register for multifactor authentication
- Requiring administrators to do multifactor authentication
- Blocking legacy authentication protocols
- Protecting privileged activities like access to the Entra portal

- 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?

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

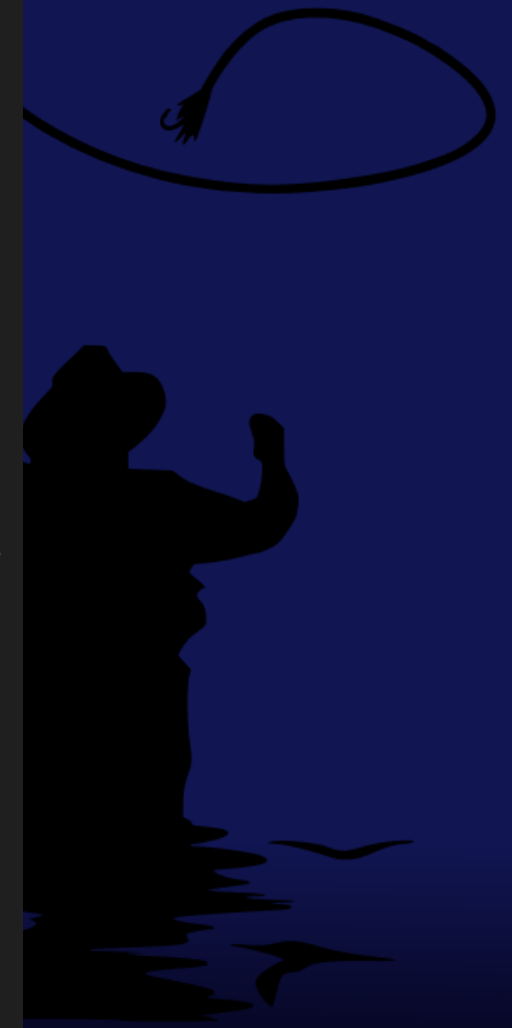
Configure whether users are allowed to consent for applications to access your organization's data. Learn more

- 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
  - [x] 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

MMS

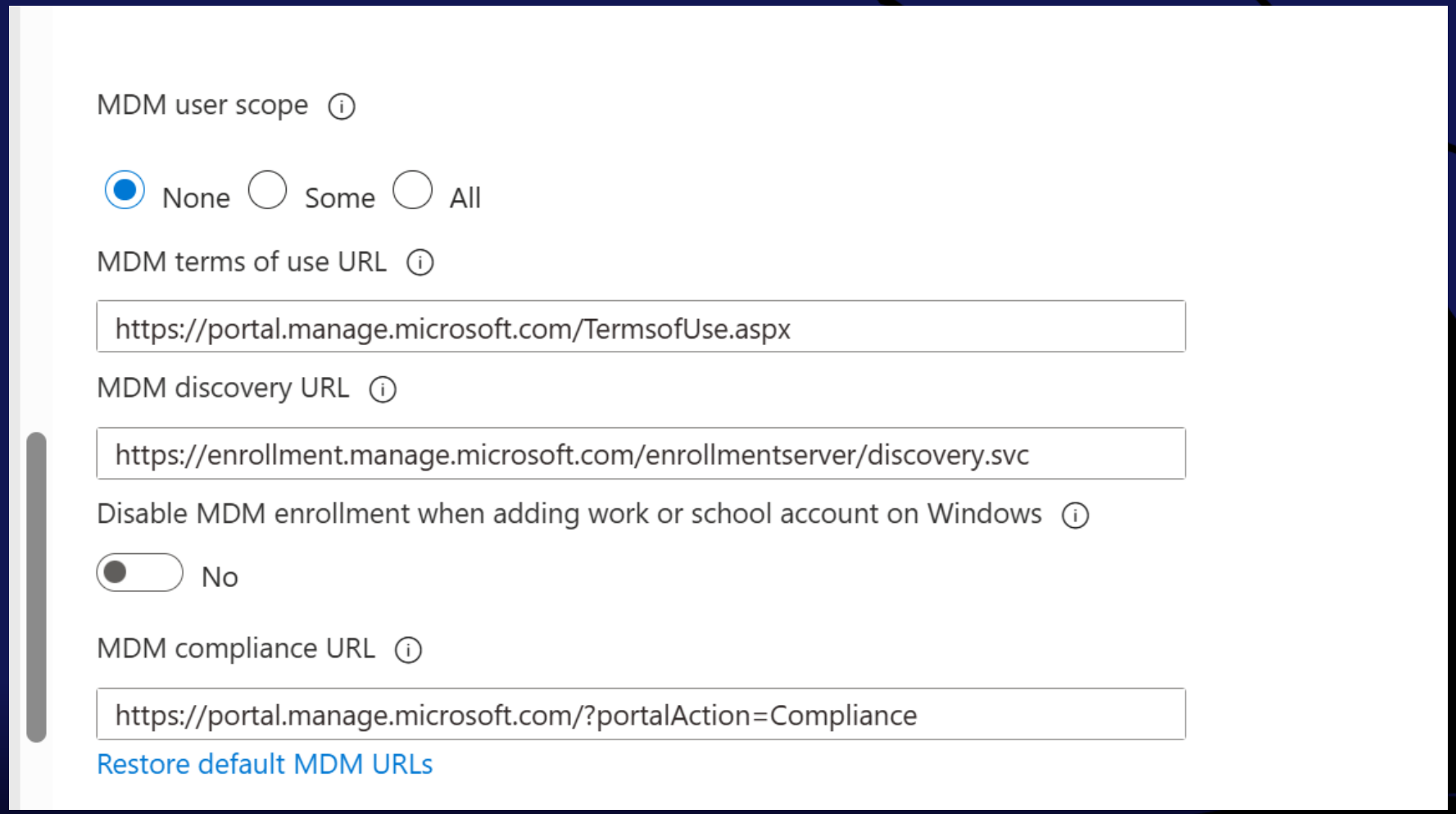
Entra ID Device Settings

Entra Defaults

Device Settings

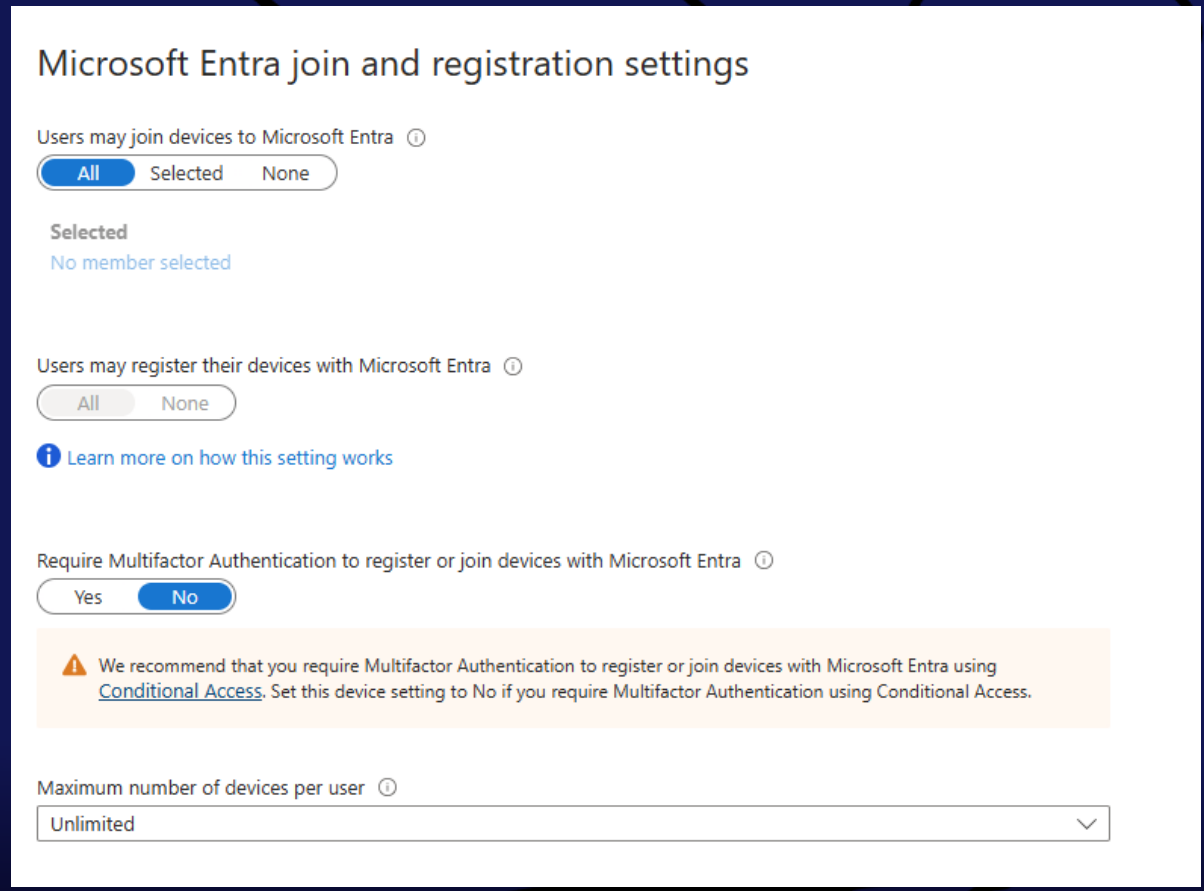
- Entra configurations
- Entra Join settings
- Local Administrator settings
- Enterprise State Roaming
- Other settings

MDM User Scope

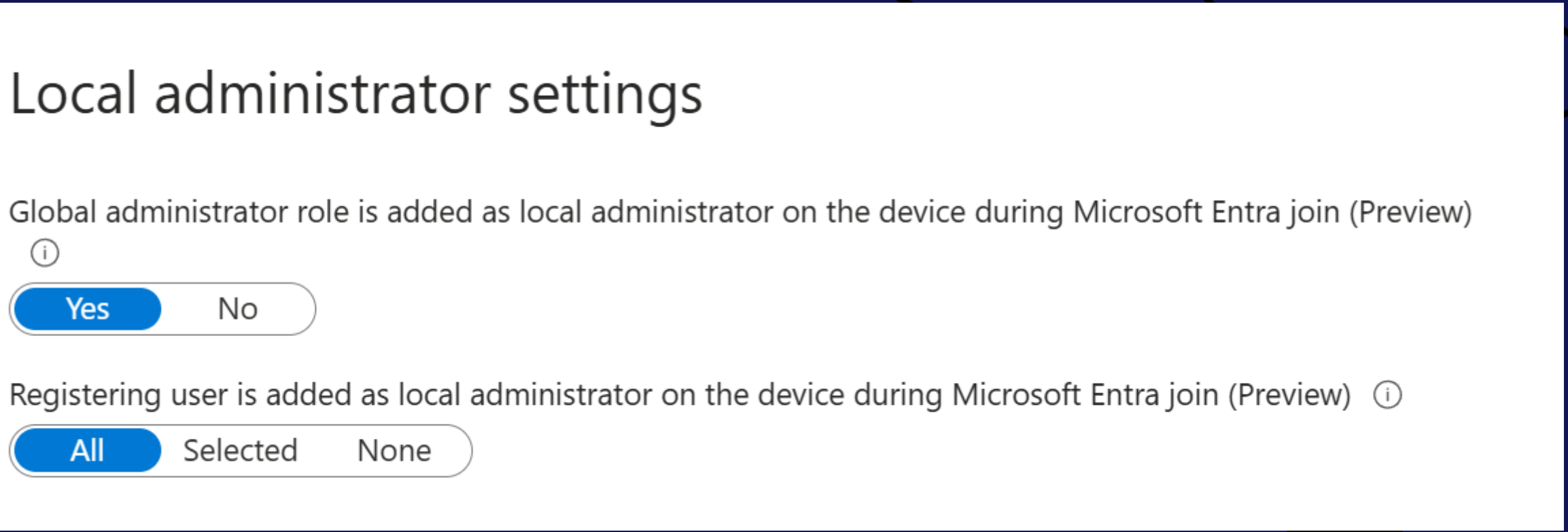


Entra Join Settings

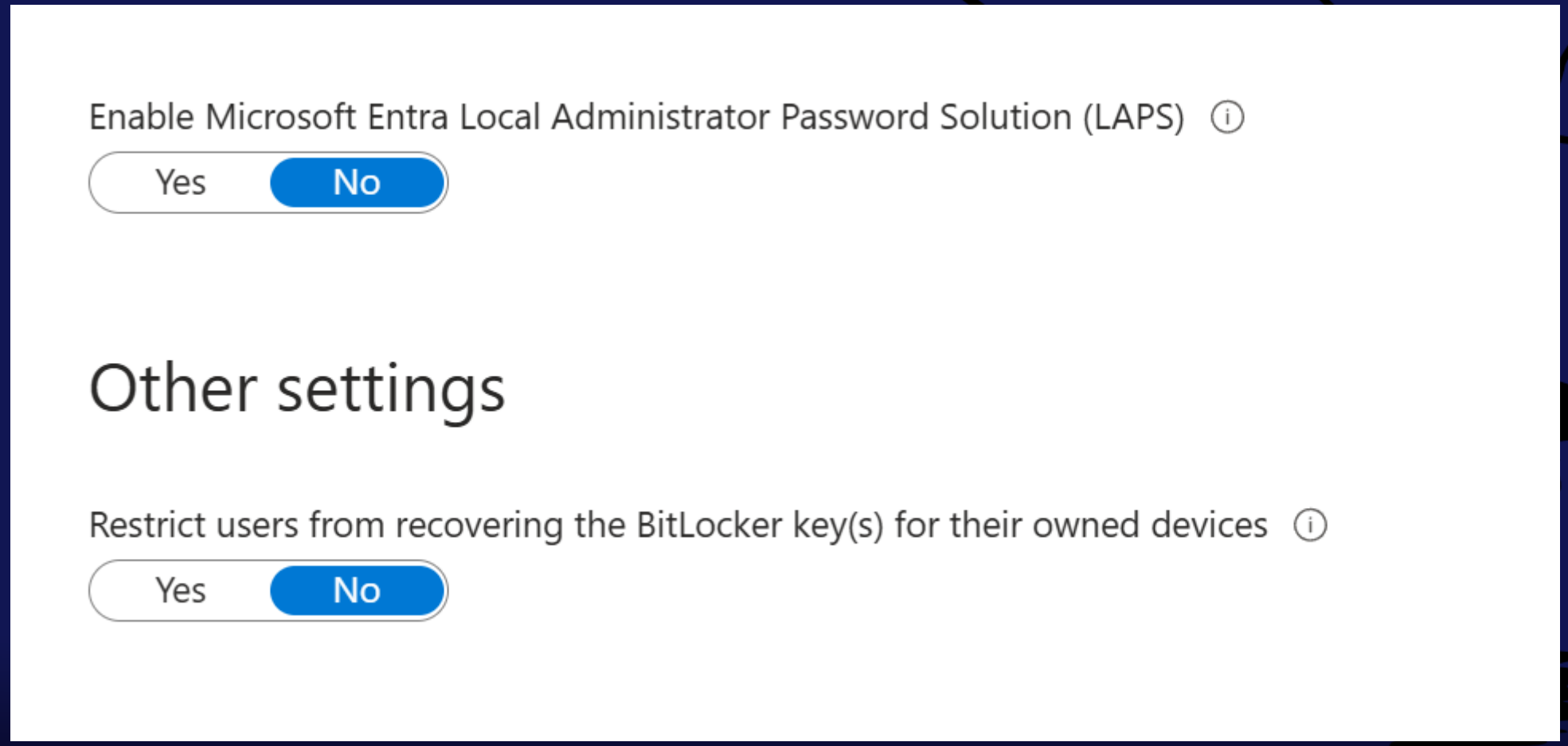
- How can we join device to Entra?
- Require MFA?
- Number of devices



Local Admin settings



LAPS + Bitlocker



ESR | Windows Backup

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

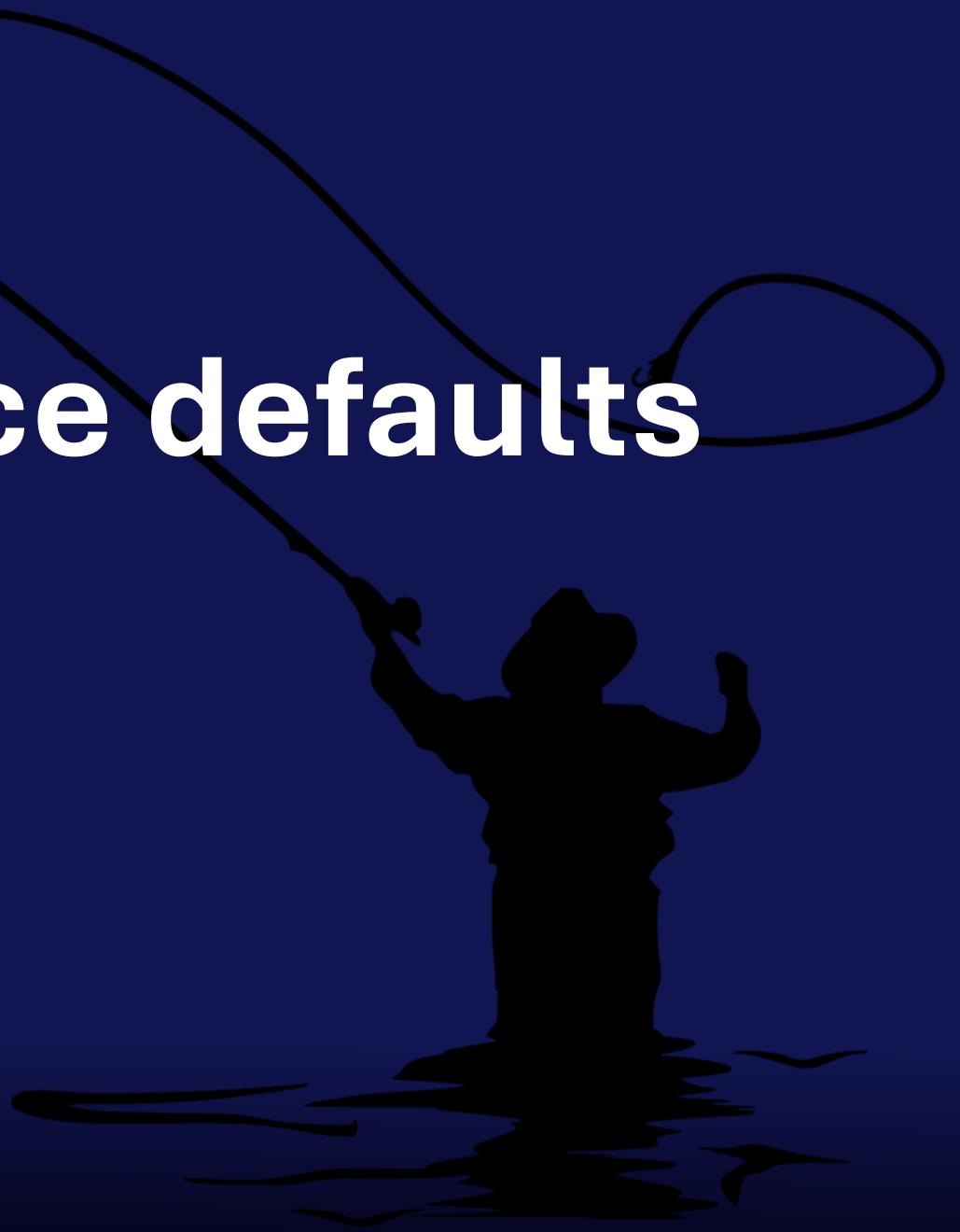
Entra Join

Windows LAPS

Device Local Admin

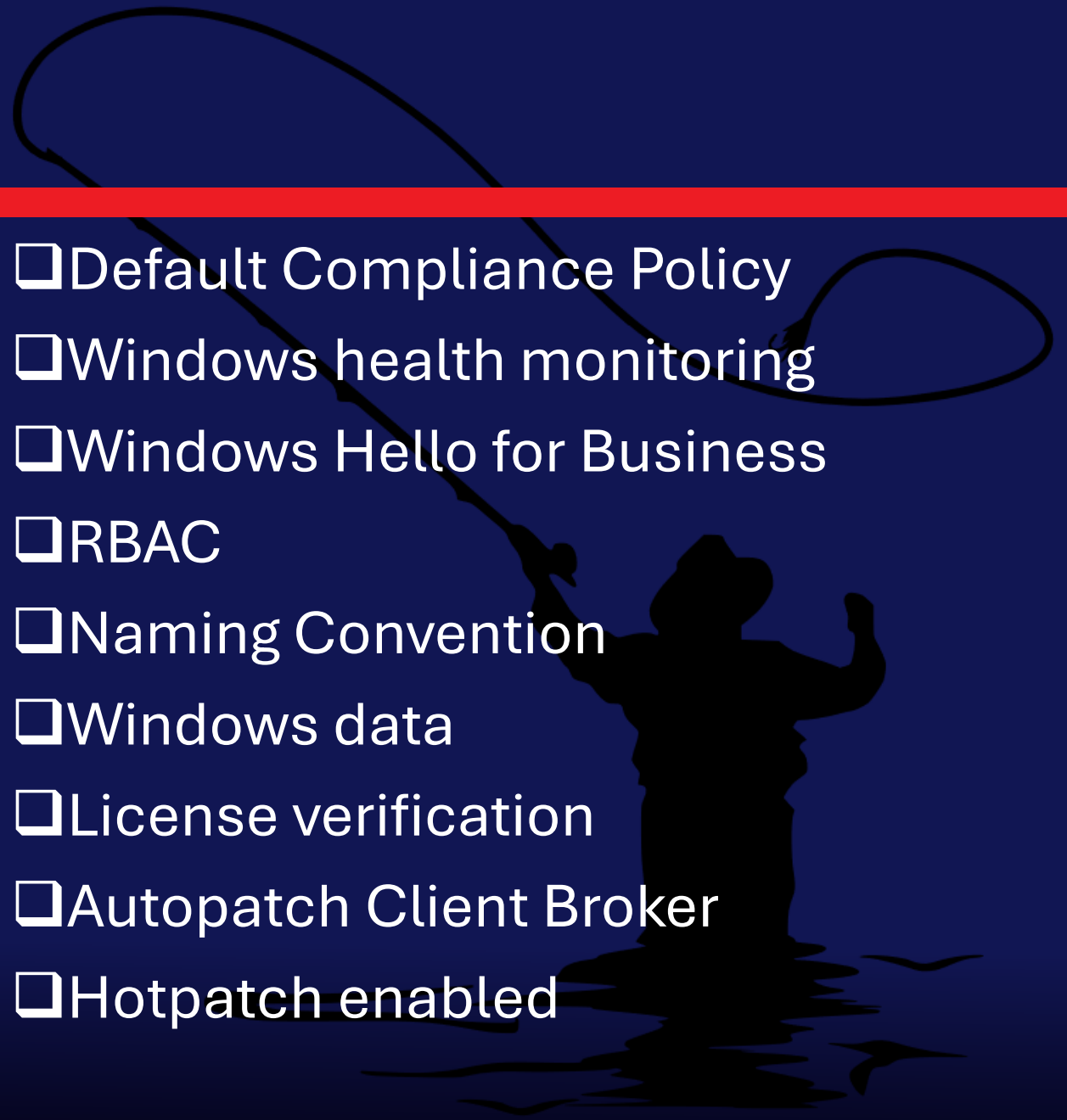
Bitlocker Recovery Keys

AutoEnrollment



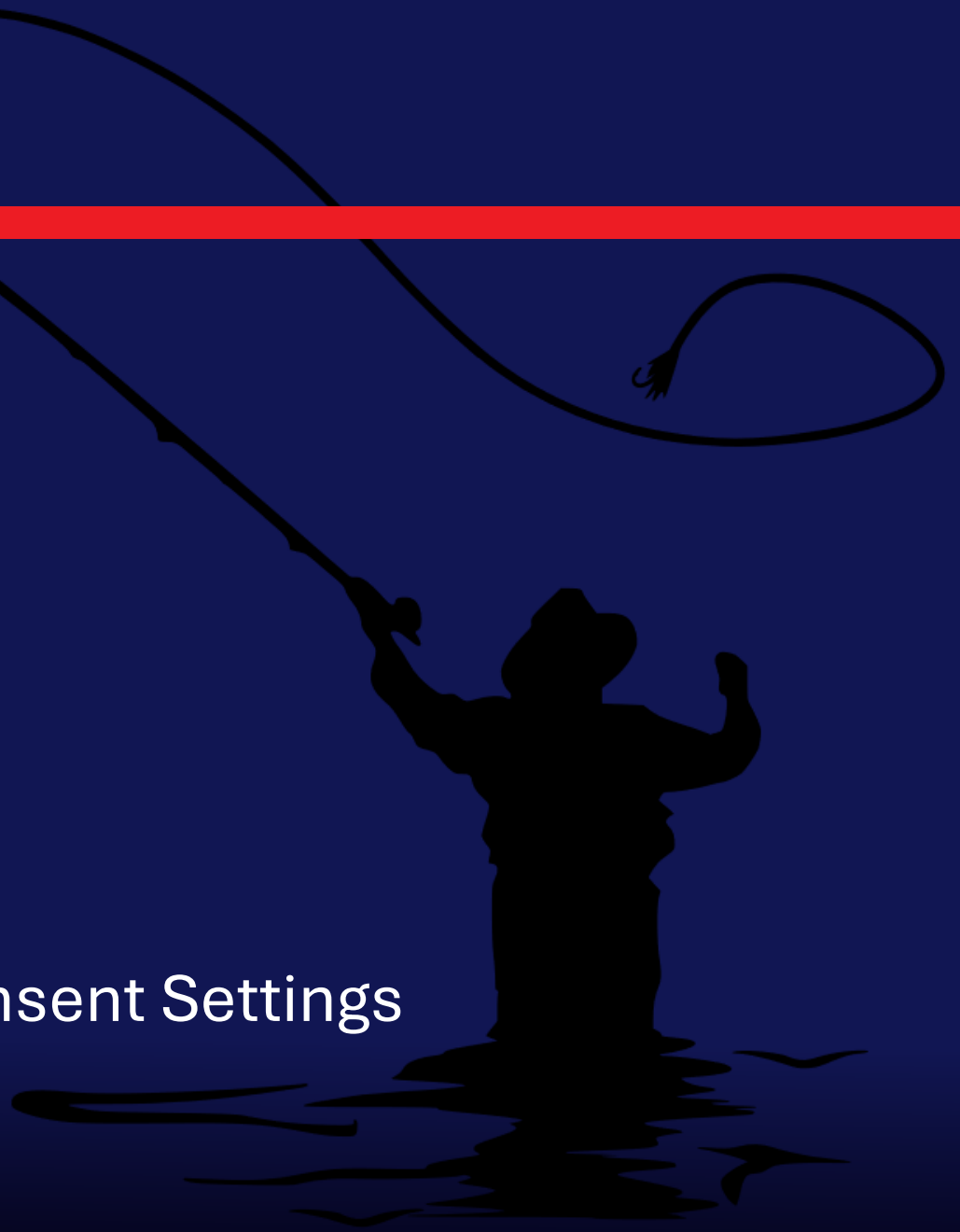
Intune Checklist

- ❑ 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

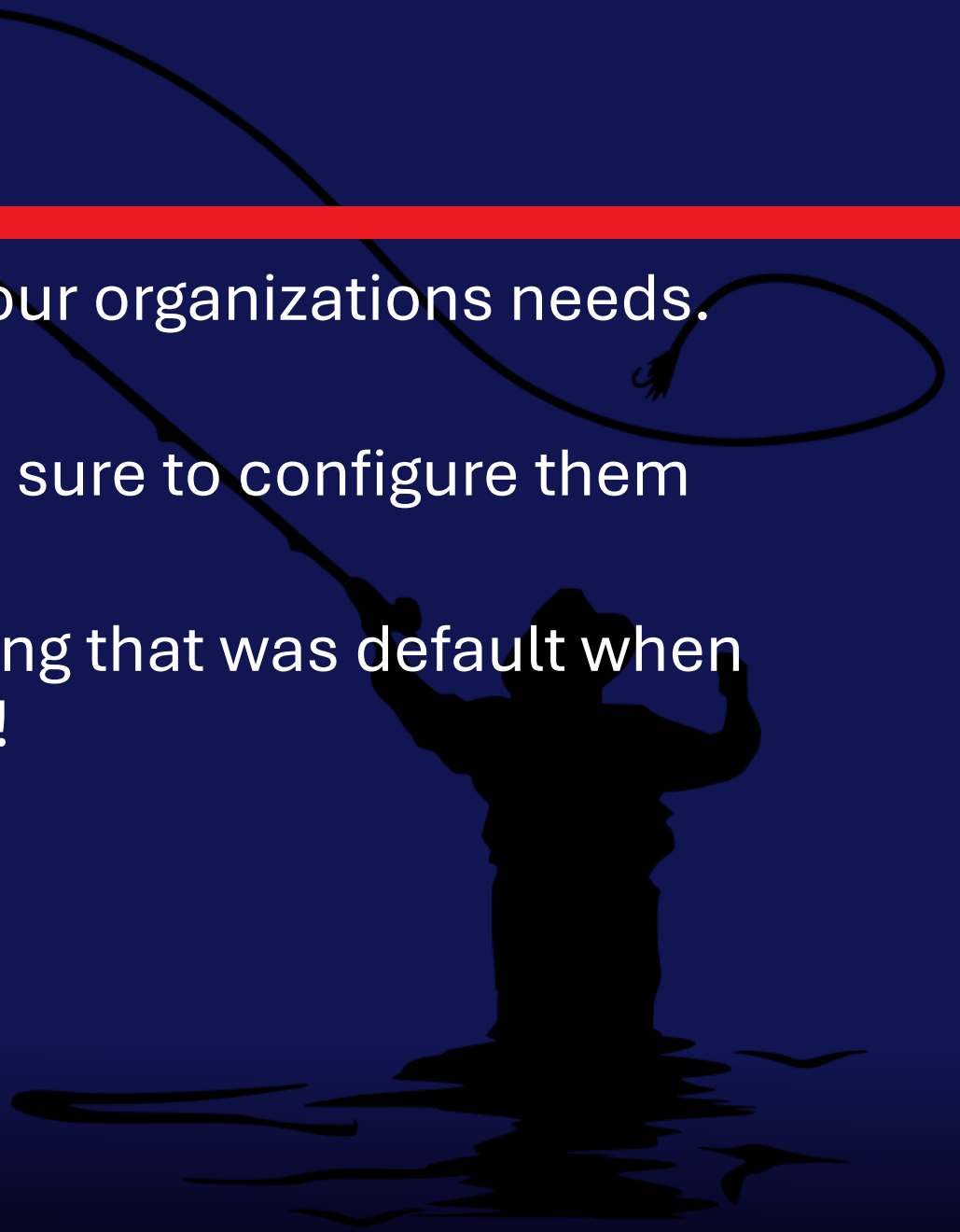


Entra ID Device checklist

- ❑ 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!



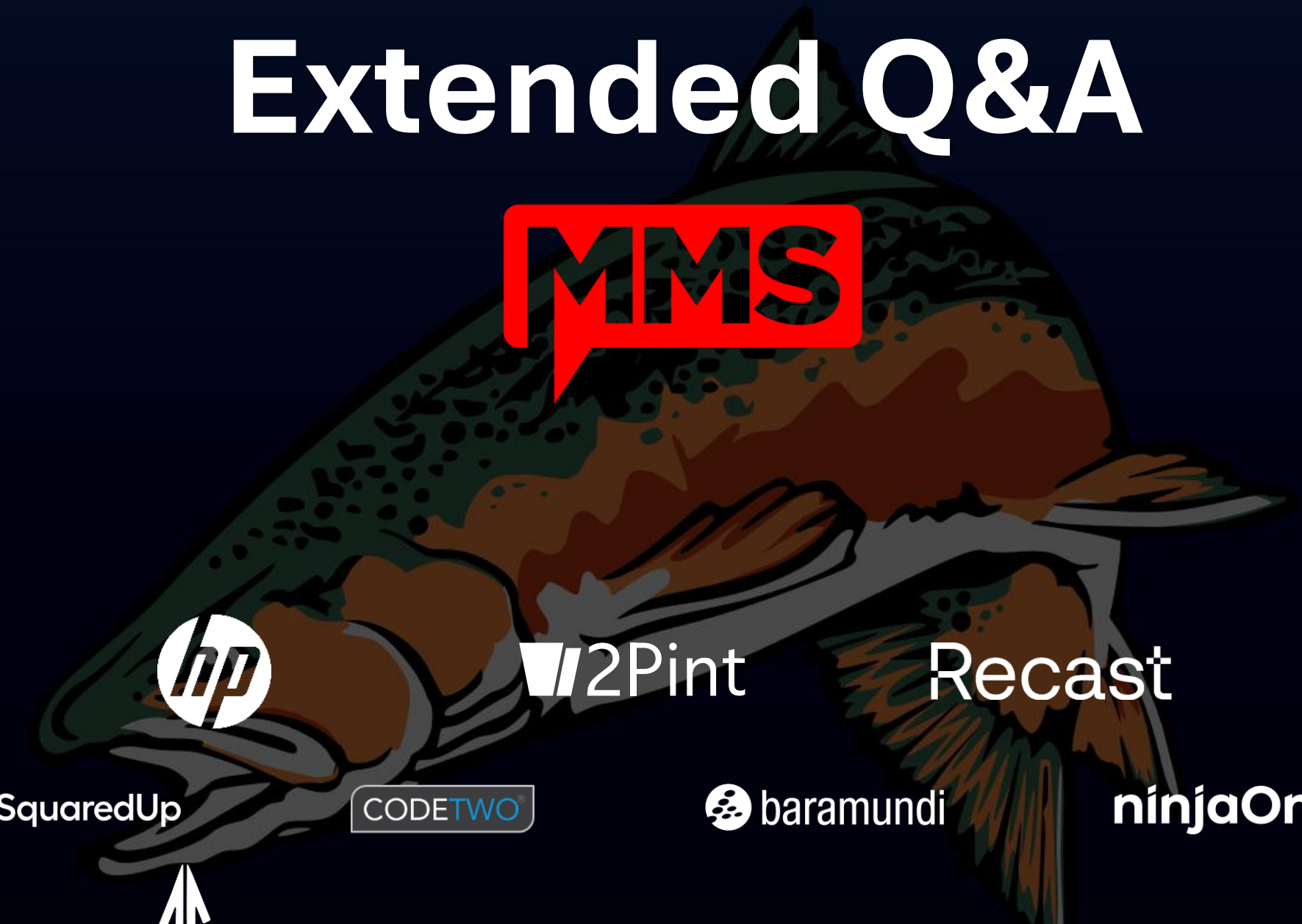
SAVE THE DATES

Oct 25-28, 2026

May 2-6, 2027

Oct 10-13, 2027

Extended Q&A



MMS

PATCH MY PC

hp

2Pint

Recast

robopack
empowered by SOFTWARE CENTRAL

SquaredUp

CODETWO

baramundi

ninjaOne

Rimo3

App Control

TeamViewer

numecent

aiden