Microsoft

Policy management on a cloudy day

Per Larsen
Senior Product Manager
Microsoft Endpoint Manager
@PerLarsen1975

Agenda

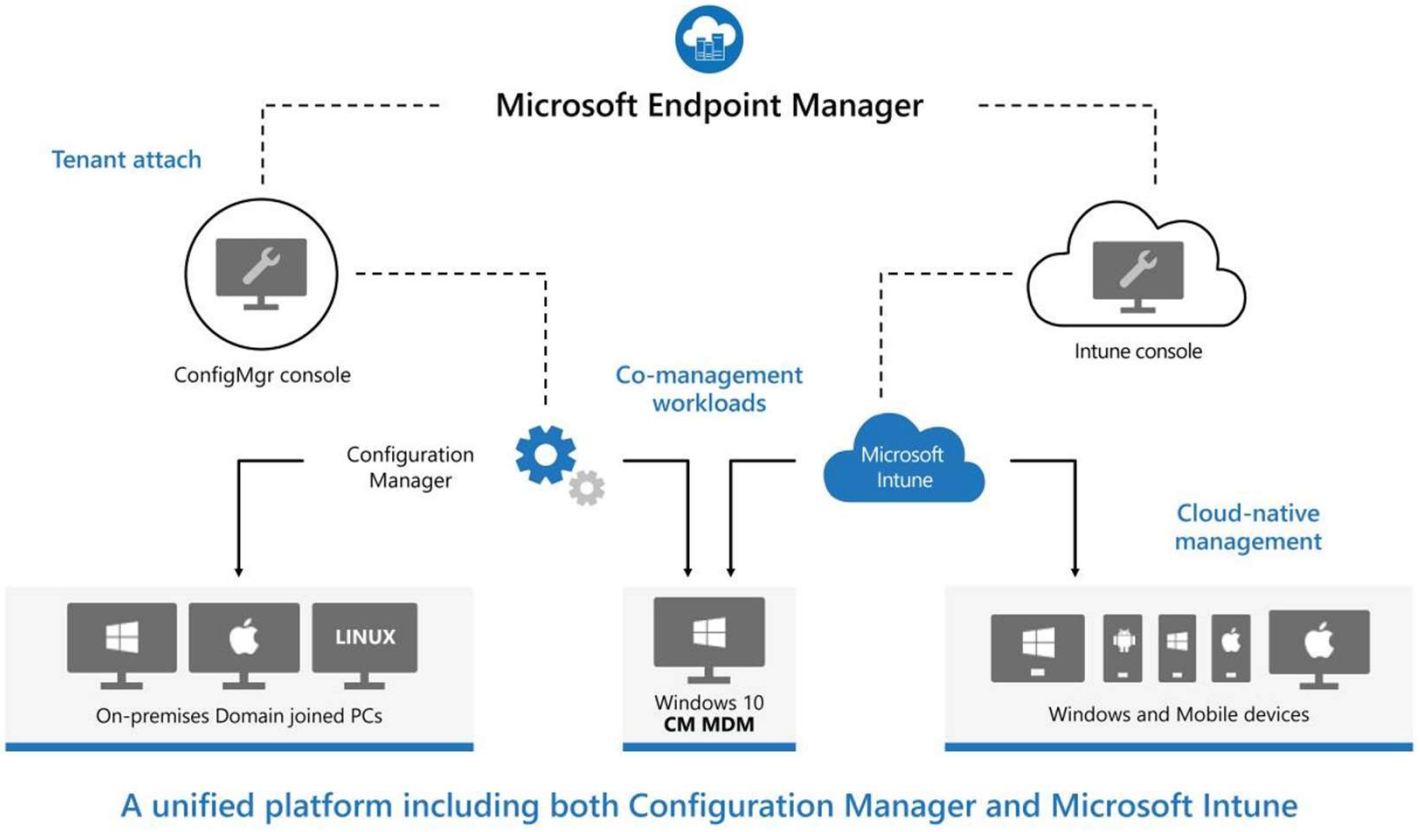
- Working from anywhere
- What has changed in policy management
- How do I get started
- Monitoring

Working from anywhere has changed the landscape for policy management

Work from anywhere changed Policy Management

Users no longer reliably connect to the corporate network that is forcing administrators to change the way they manage their organization's devices.

Microsoft Endpoint Manager



Managing Windows devices

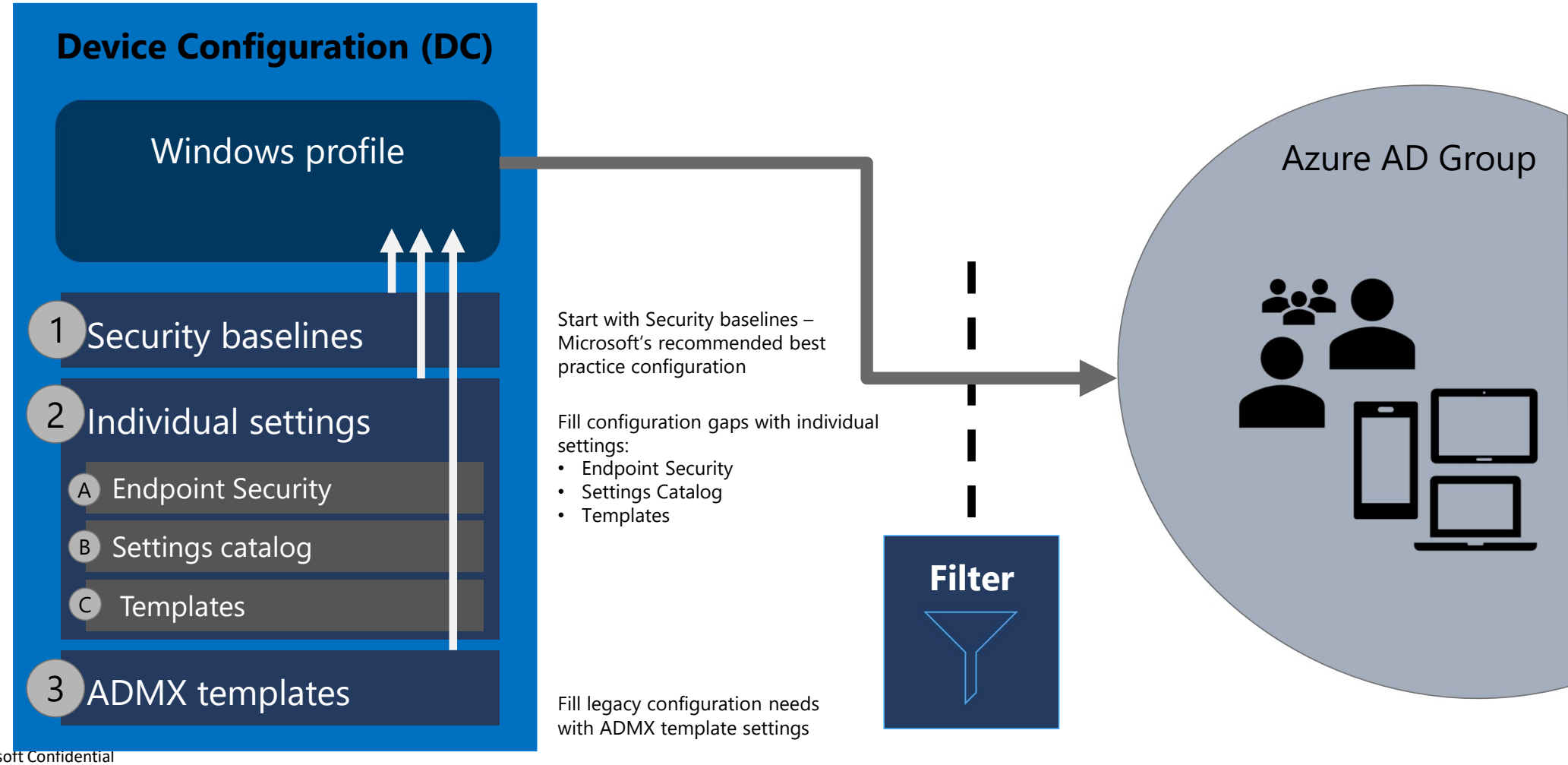
Cloud only devices

Co-managed devices

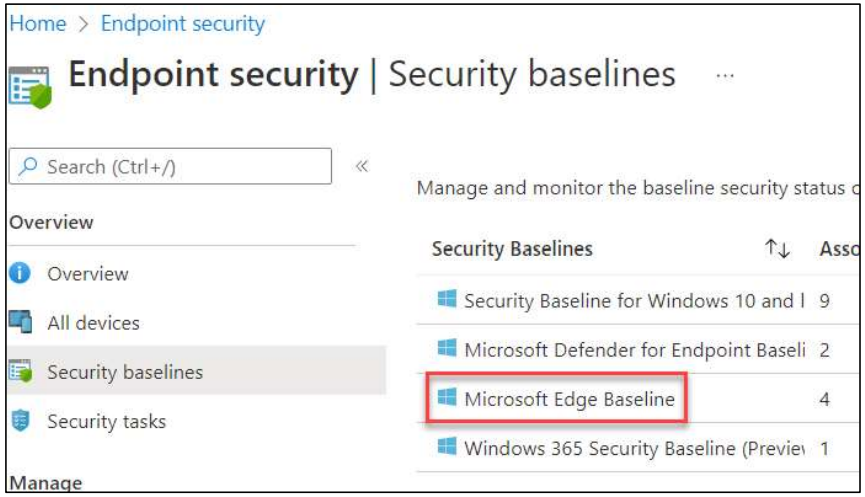
Tenant attached devices

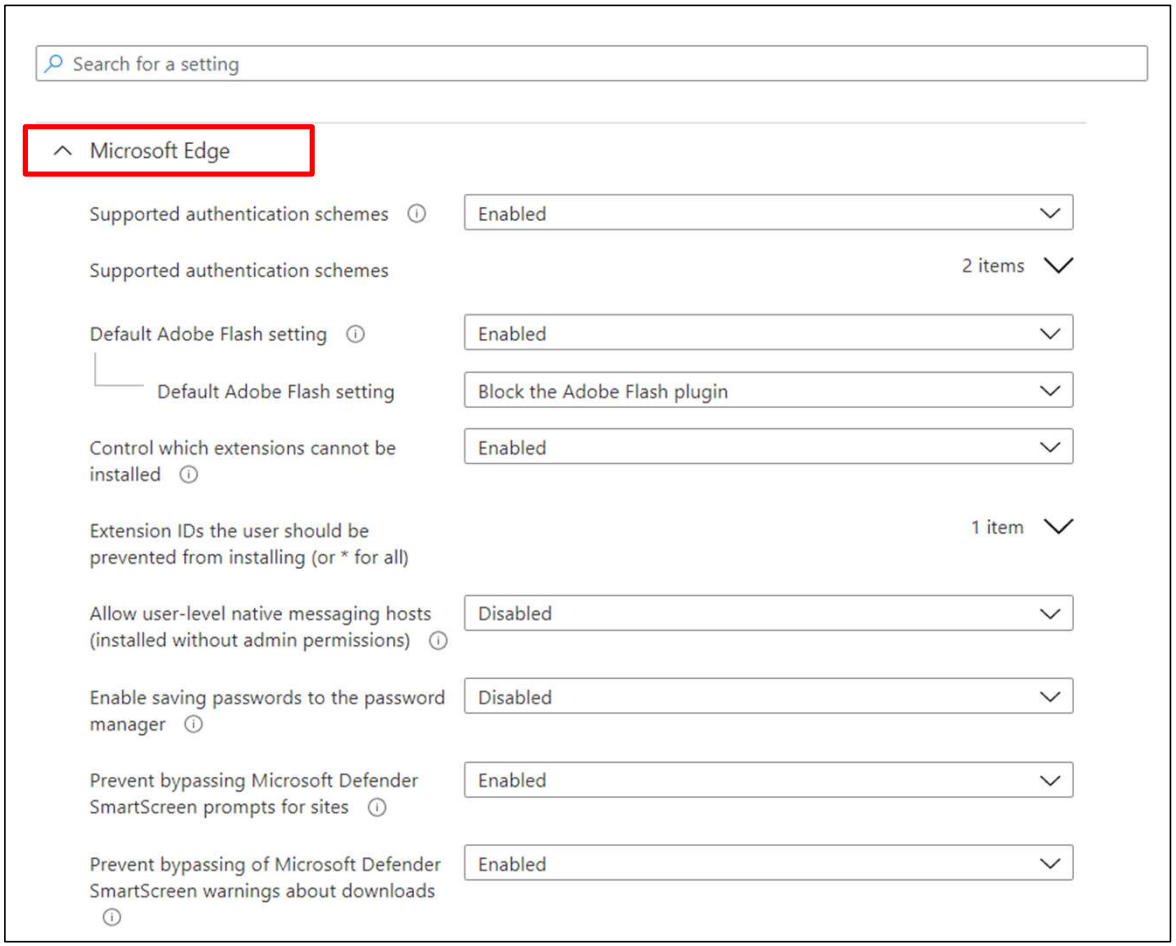
What has changed in policy management

Creating profiles with Microsoft Endpoint Manager

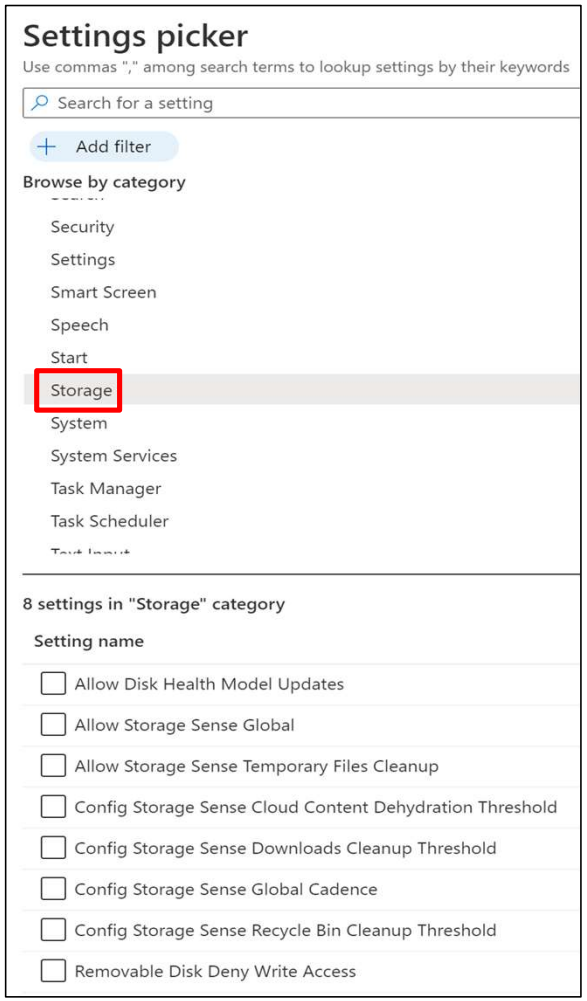


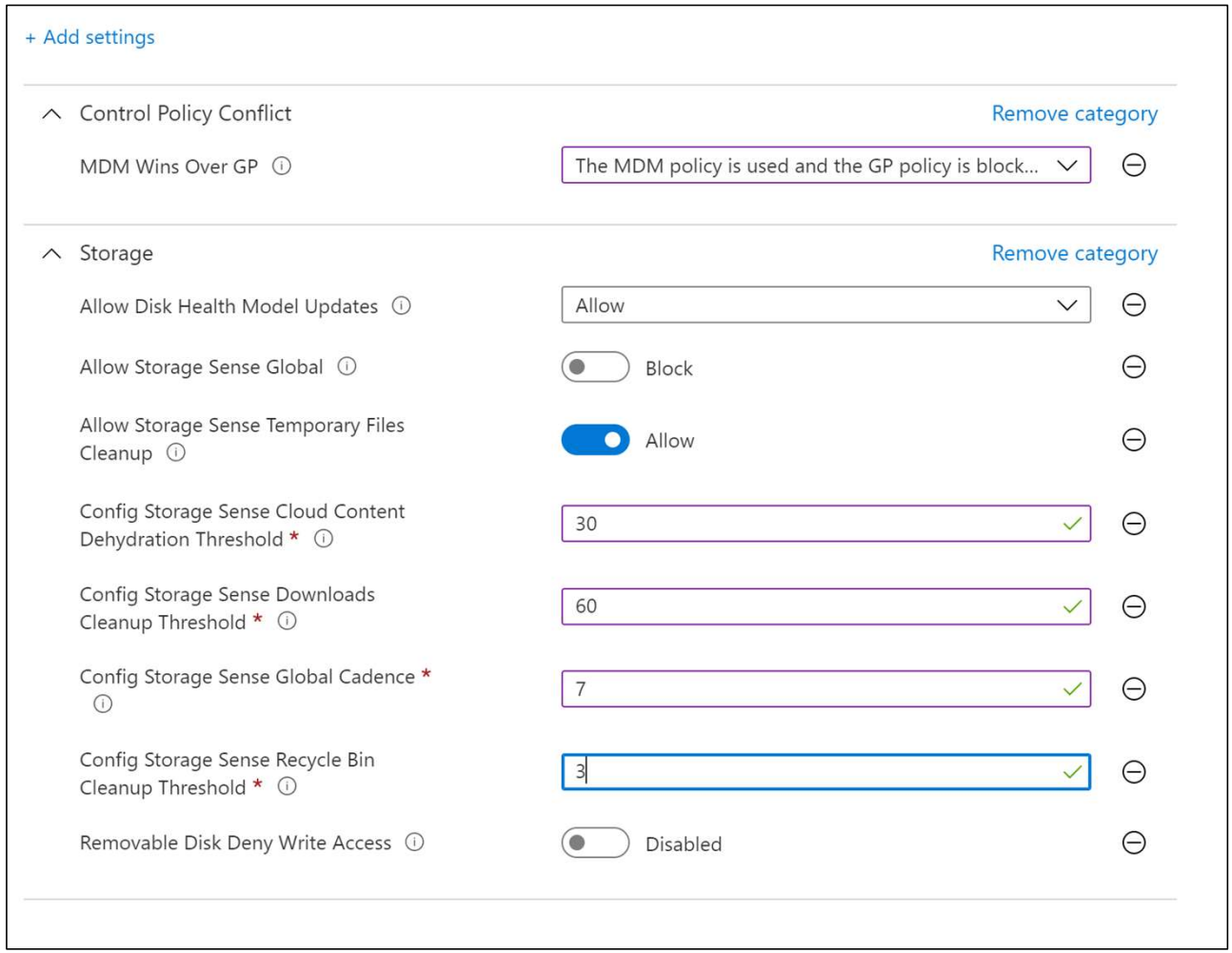
Security Baselines



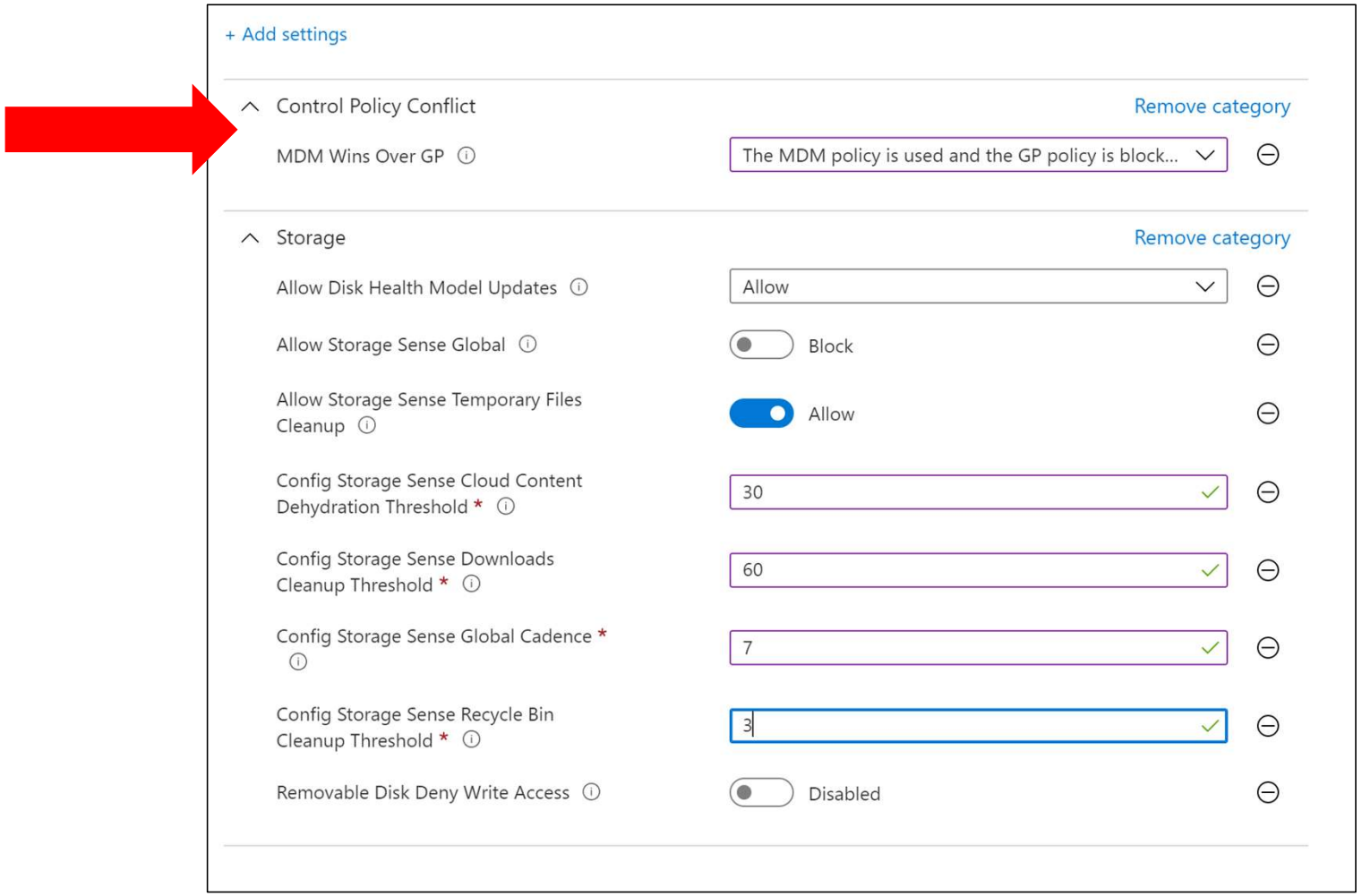


Settings Catalog

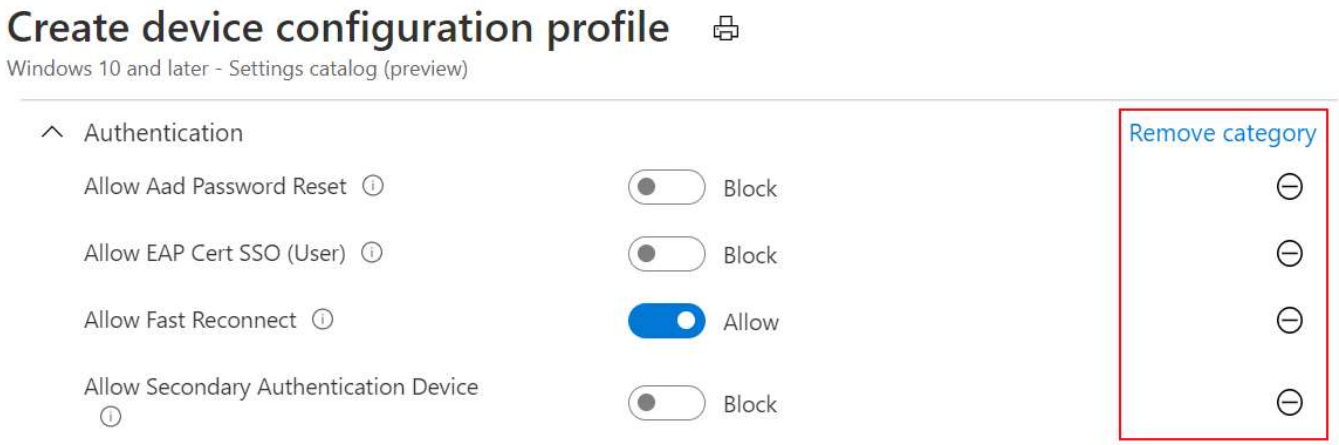




Settings Catalog



Settings Catalog



When you select the minus:

- Intune doesn't change or update this setting. The minus is the same as **Not configured**. When set to **Not configured**, the setting is no longer managed.
- The setting is **removed** from the policy. The next time you open your policy, the setting isn't **shown**. You can **add** it again.
- The next time devices **check in**, the setting is no longer **locked**.

Device scope vs user scope settings

- **User scoped** policy writes to HKEY_CURRENT_USER (HKCU).
- **Device scoped** policy writes to HKEY_LOCAL_MACHINE (HKLM).

- When a device checks-in to Intune, the device always presents a **deviceID**. The device may or may not present a **userID**, depending on the check-in timing and if a user is signed in.

Device scope vs user scope settings

- If a **device scope** policy is assigned to a **device**, then **all users** on that device have that setting applied.

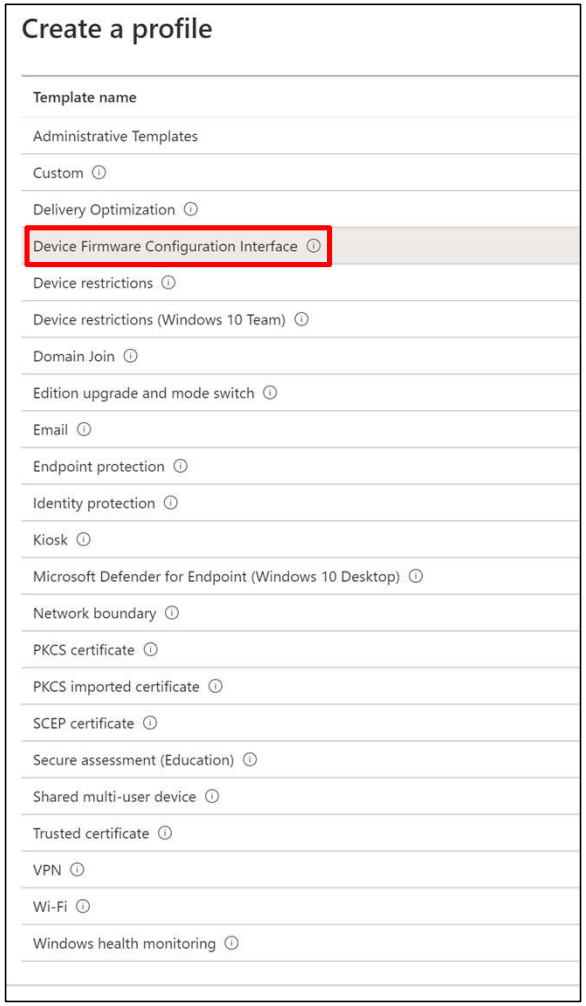
- If a **user scope** policy is assigned to a **device**, then **all users** on that device have that setting applied. This behavior is like a loopback set to merge.

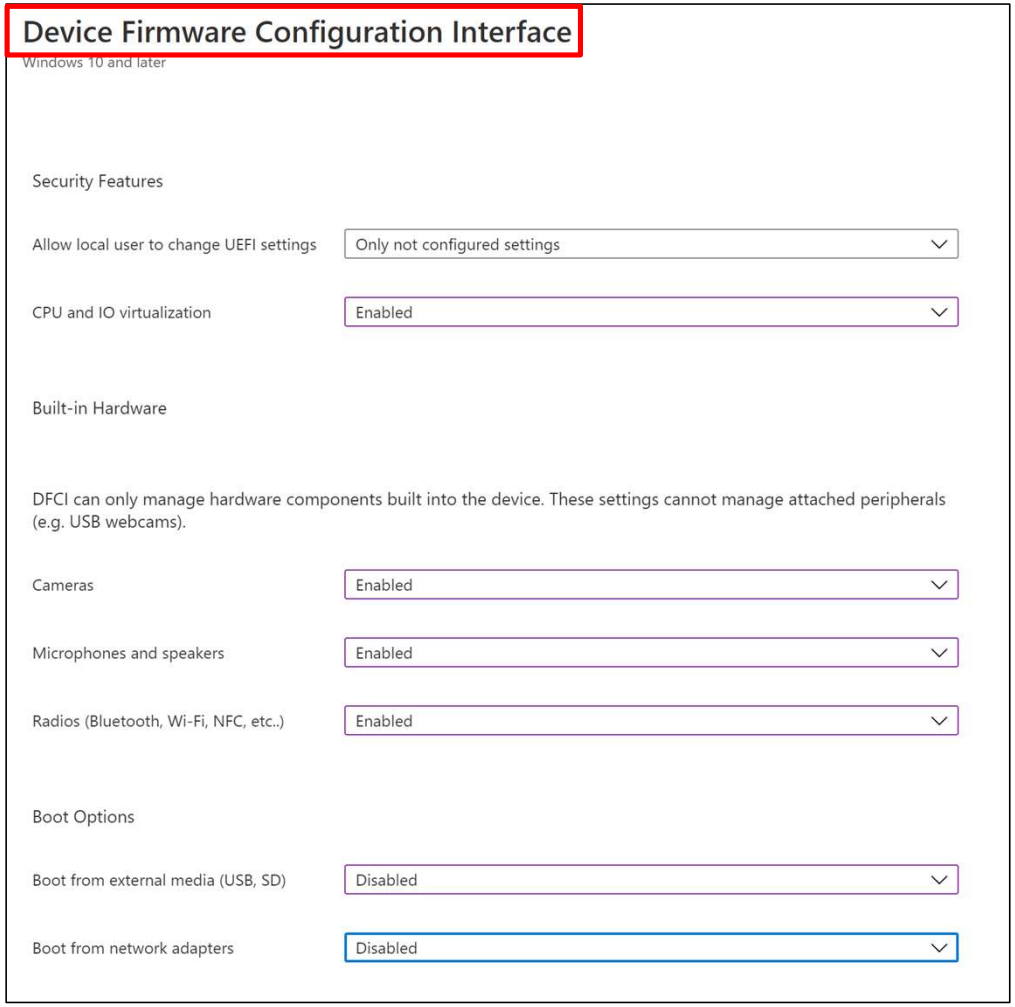
Device scope vs user scope settings

- If a **user scoped** policy is assigned to a **user**, then only **that user** has that setting applied.

- If a **device scoped** policy is assigned to a **user**, once that user signs in and an Intune sync occurs, then the **device scope** settings apply to **all users** on the device.

Templates





ADMX based policy

Windows

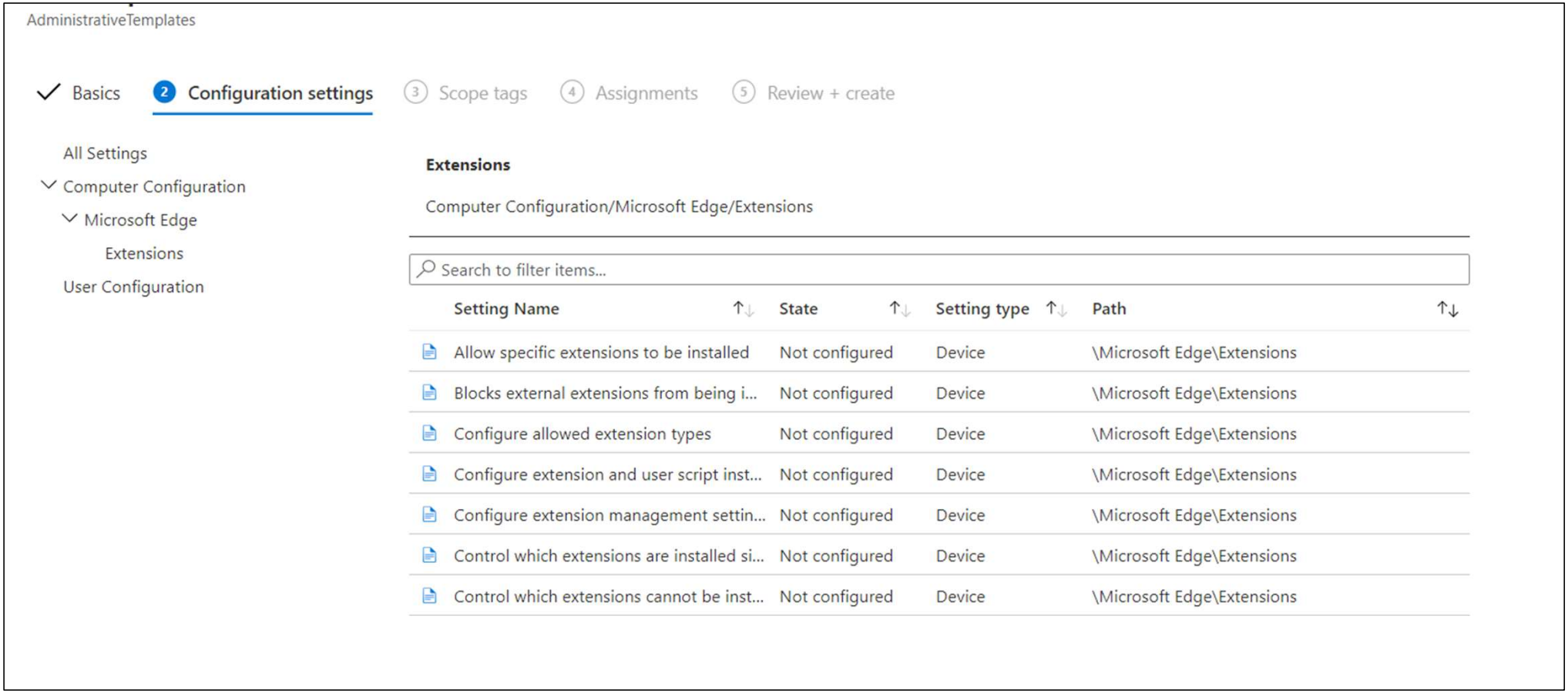
Office 365

Microsoft Edge

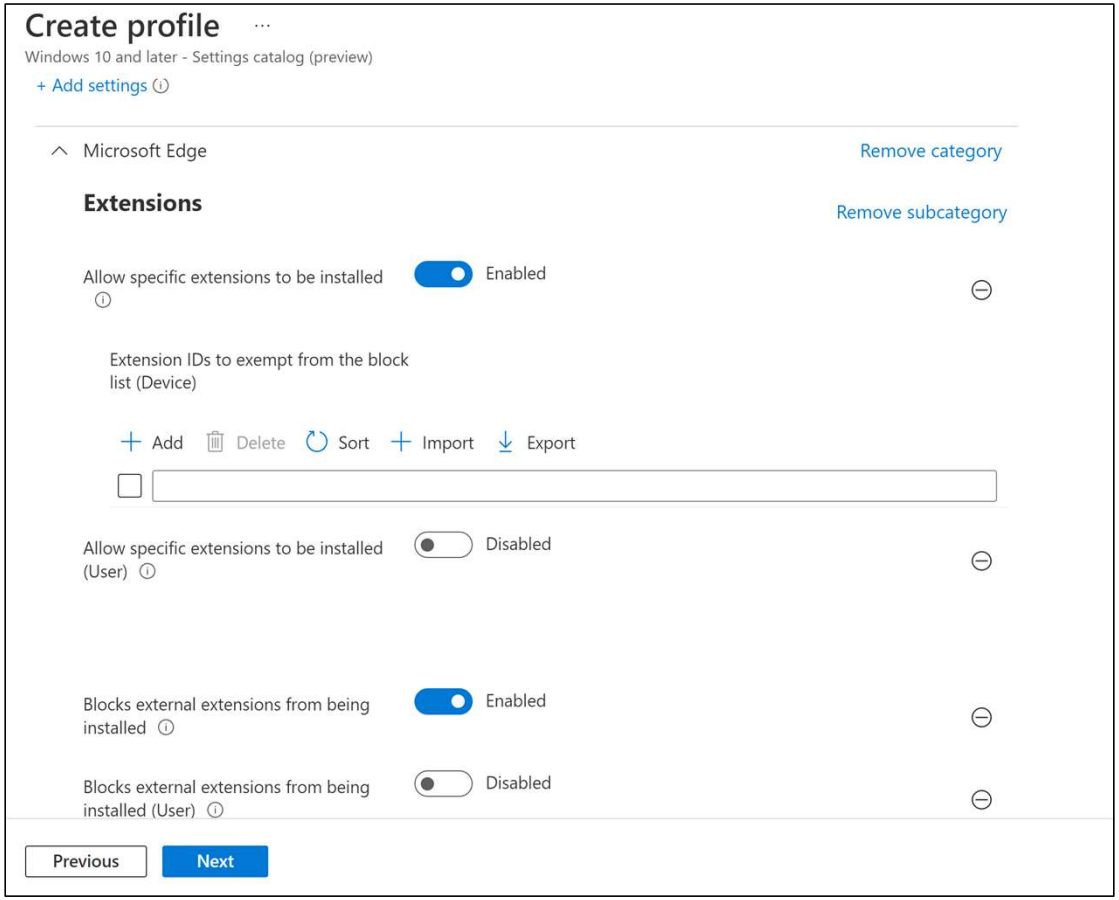
Internet Explorer

Third Party

ADMX based policies - Templates



ADMX based policies – Settings catalog



Demo

How do I get started

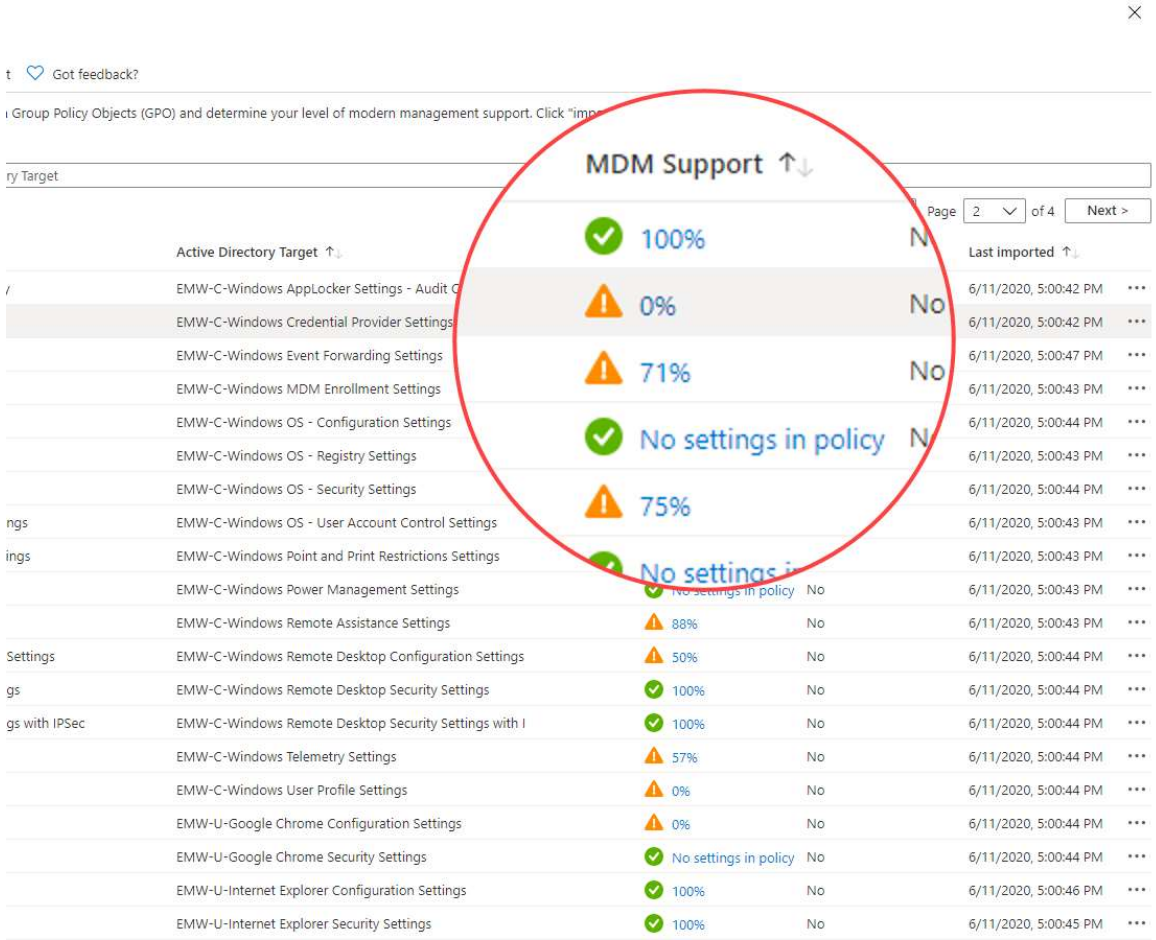
How to get started

START FRESH

GROUP POLICY ANALYTICS

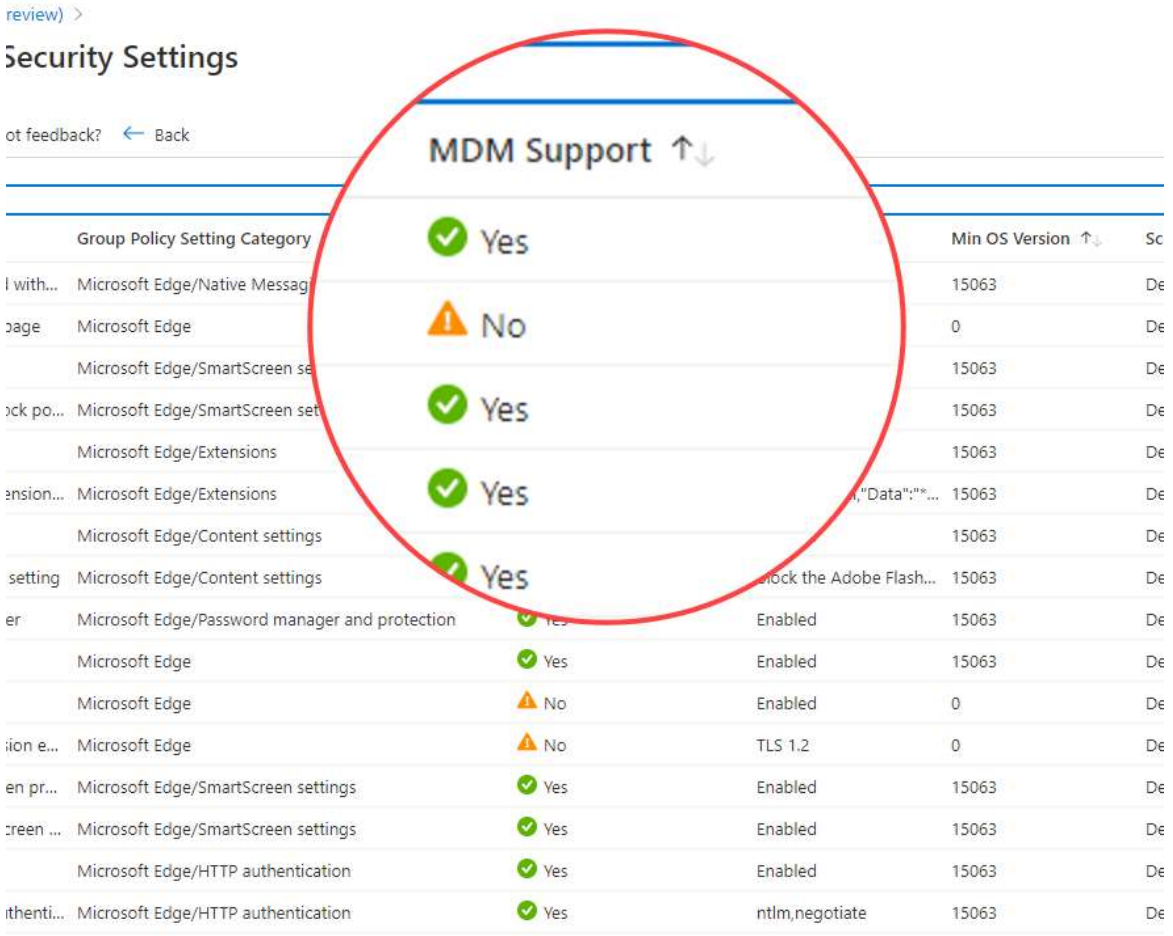
Group Policy Analytics (Preview)

- Upload existent policy
- Validate MDM support



Group Policy Analytics (Preview)

- Get detailed information
- Settings name
- Group Policy Settings Category
- MDM Support
- Value
- Min OS version
- Scope (User/Device)
- CSP Name
- CSP Mapping

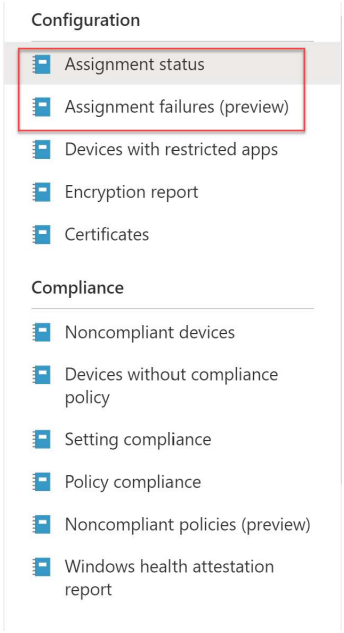


Monitoring

The 4 Report Types:

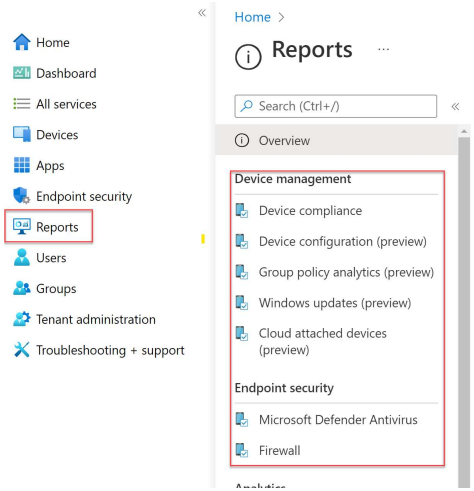
Operational

"Non-compliant devices"



Organizational

"Corporate vs personal devices"

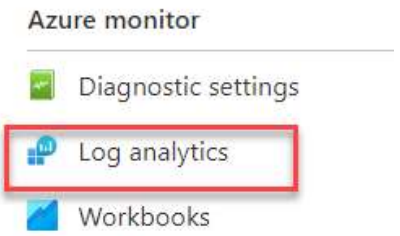


Historical

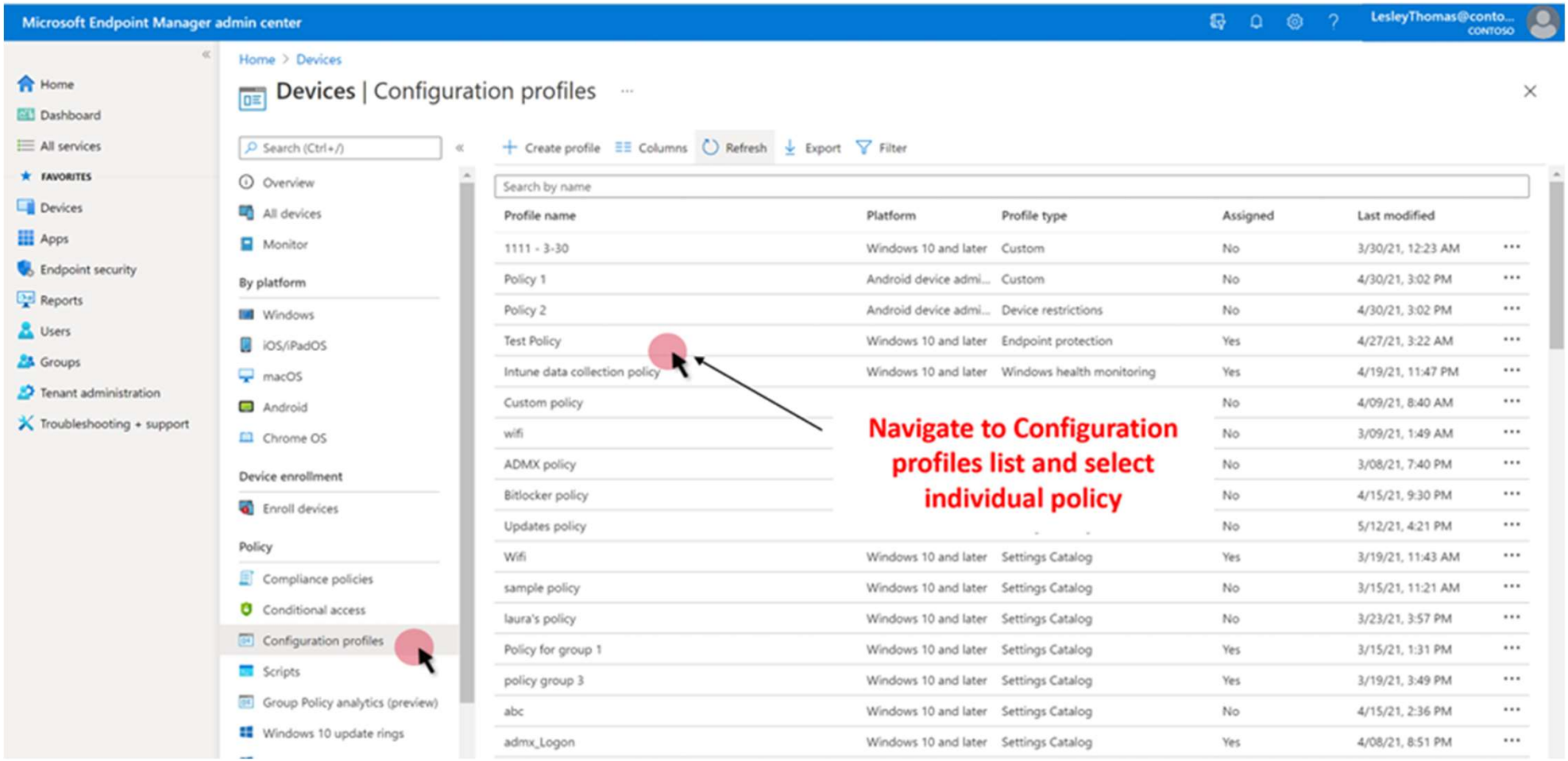
"Platform enrollment trends"

Specialist

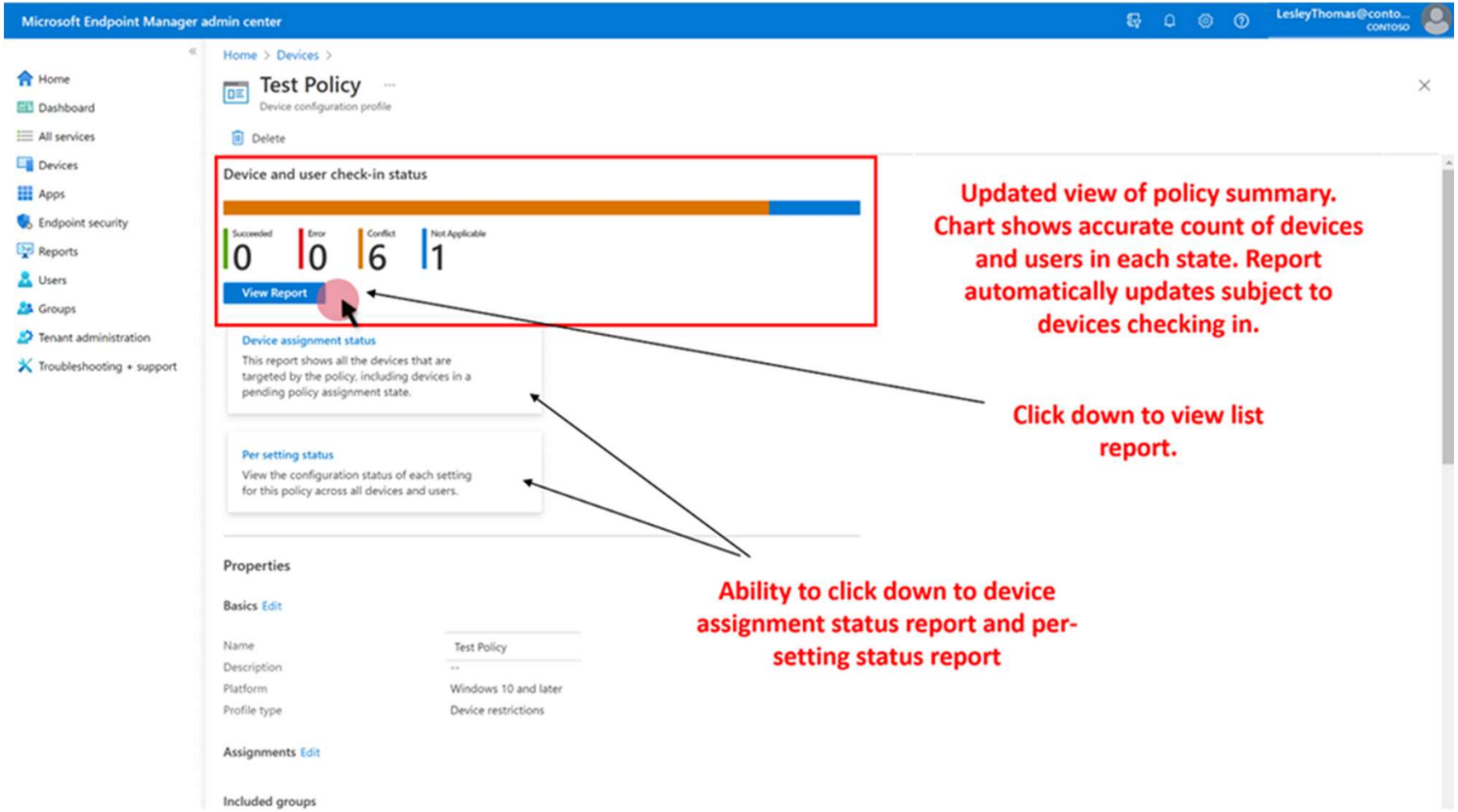
"What about joining with AAD?"



Devices – Configuration profiles



Devices – Configuration profiles



Demo

Questions ???