



Policy management on a cloudy day

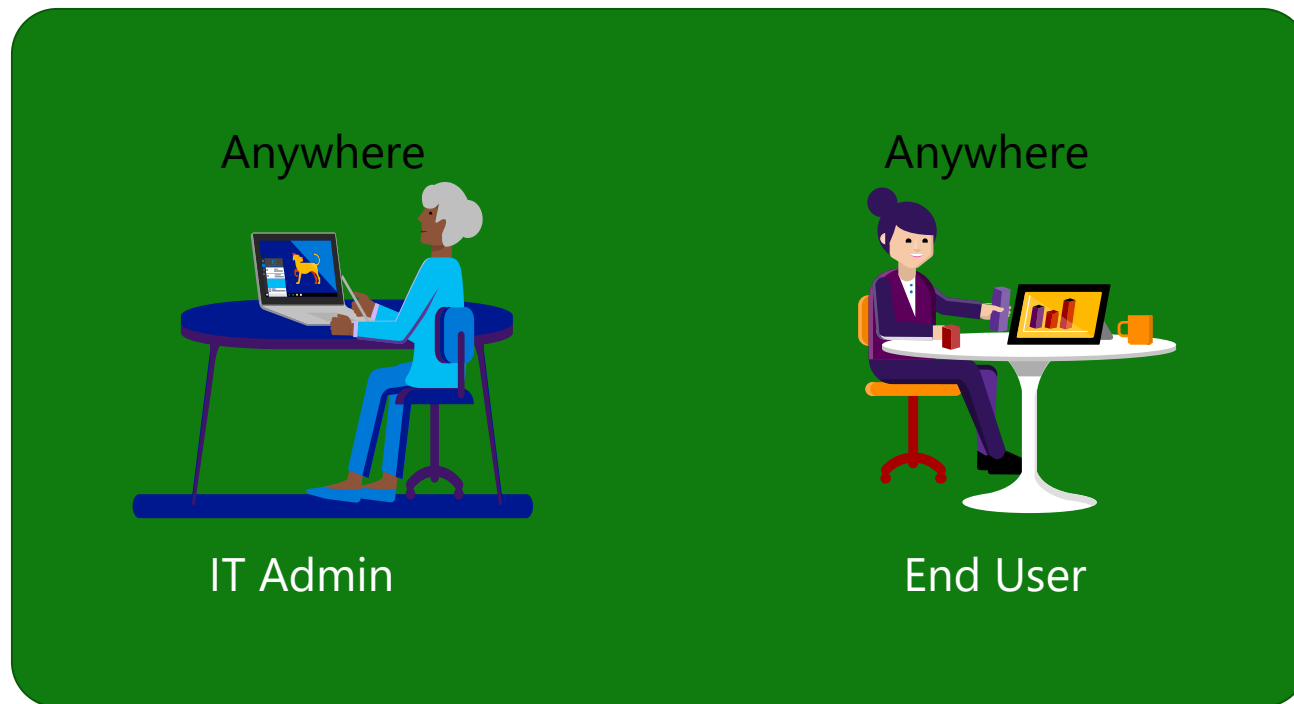
Per Larsen
Senior Product Manager
Microsoft Endpoint Manager
 @PerLarsen1975

Agenda

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

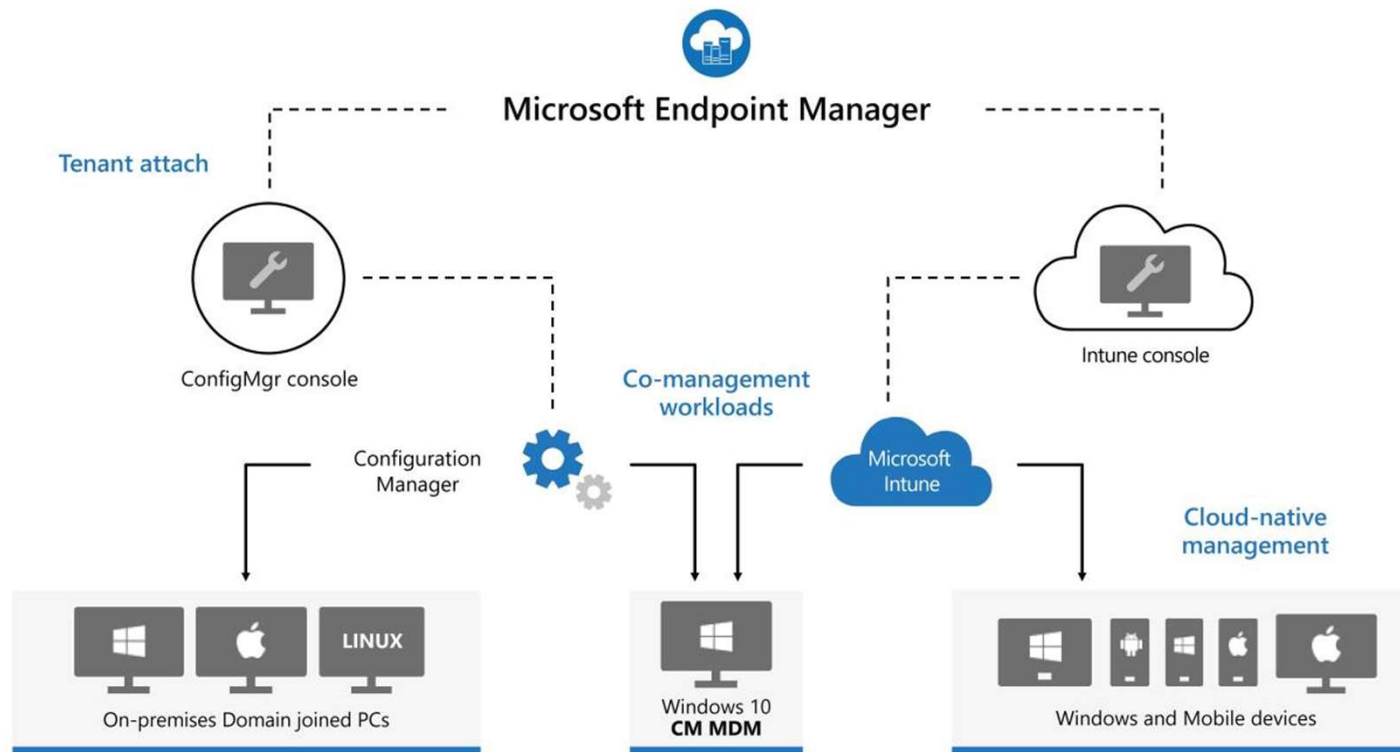
Working from anywhere has changed the landscape for policy management

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



A unified platform including both Configuration Manager and Microsoft Intune

Managing Windows devices



Cloud only devices



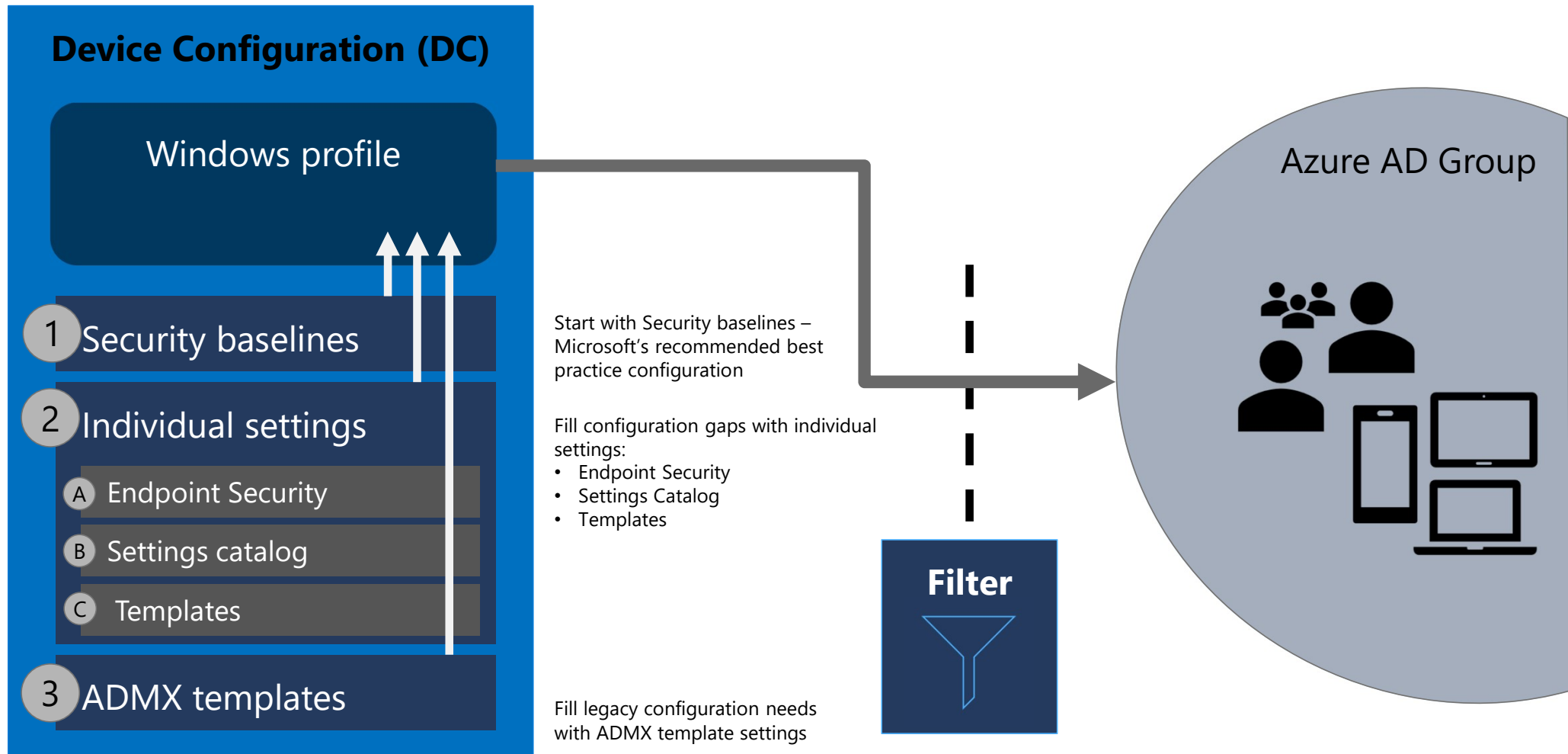
Co-managed devices



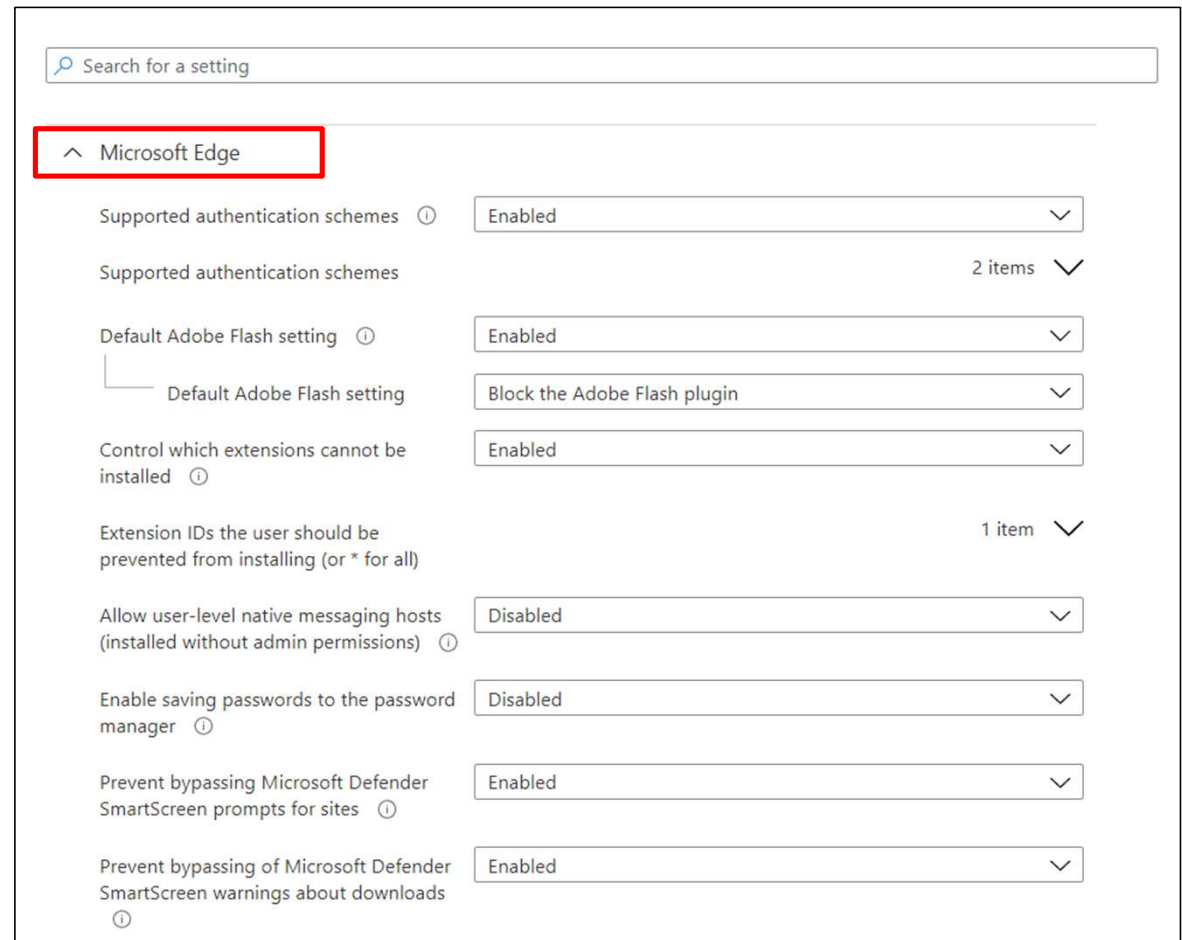
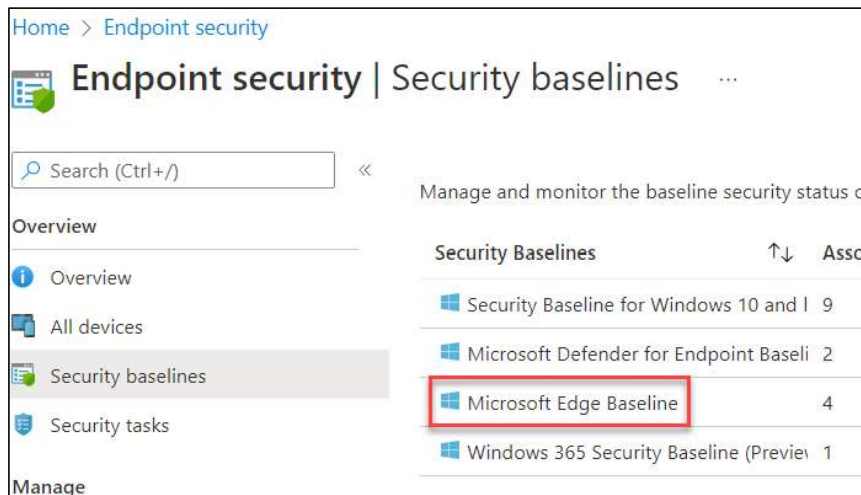
Tenant attached devices

What has changed in policy management

Creating profiles with Microsoft Endpoint Manager



Security Baselines



Settings Catalog

Settings picker

Use commas "," among search terms to lookup settings by their keywords

Search for a setting

+

Add filter

Browse by category

Security

Settings

Smart Screen

Speech

Start

Storage

System

System Services

Task Manager

Task Scheduler

Task Manager

8 settings in "Storage" category

Setting name

☐ Allow Disk Health Model Updates

☐ Allow Storage Sense Global

☐ Allow Storage Sense Temporary Files Cleanup

☐ Config Storage Sense Cloud Content Dehydration Threshold

☐ Config Storage Sense Downloads Cleanup Threshold

☐ Config Storage Sense Global Cadence

☐ Config Storage Sense Recycle Bin Cleanup Threshold

☐ Removable Disk Deny Write Access

+ Add settings

Control Policy Conflict

Remove category

MDM Wins Over GP ⓘ

The MDM policy is used and the GP policy is block... ▾

⊖

Storage

Remove category

Allow Disk Health Model Updates ⓘ

Allow ▾

⊖

Allow Storage Sense Global ⓘ

☐ Block

⊖

Allow Storage Sense Temporary Files Cleanup ⓘ

☒ Allow

⊖

Config Storage Sense Cloud Content Dehydration Threshold * ⓘ

30 ✓

⊖

Config Storage Sense Downloads Cleanup Threshold * ⓘ

60 ✓

⊖

Config Storage Sense Global Cadence * ⓘ

7 ✓

⊖

Config Storage Sense Recycle Bin Cleanup Threshold * ⓘ

3 ✓

⊖

Removable Disk Deny Write Access ⓘ

☐ Disabled

⊖

Settings Catalog

[+ Add settings](#)

^ Control Policy Conflict [Remove category](#)

MDM Wins Over GP ⓘ

The MDM policy is used and the GP policy is block... ▾

 ⊖

^ Storage [Remove category](#)

Allow Disk Health Model Updates ⓘ

Allow ▾

 ⊖

Allow Storage Sense Global ⓘ

☐ Block

 ⊖

Allow Storage Sense Temporary Files Cleanup ⓘ

☒ Allow

 ⊖

Config Storage Sense Cloud Content Dehydration Threshold * ⓘ

30 ✓

 ⊖

Config Storage Sense Downloads Cleanup Threshold * ⓘ

60 ✓

 ⊖

Config Storage Sense Global Cadence * ⓘ

7 ✓

 ⊖

Config Storage Sense Recycle Bin Cleanup Threshold * ⓘ

3 ✓

 ⊖

Removable Disk Deny Write Access ⓘ

☐ Disabled

 ⊖

Settings Catalog

Create device configuration profile

Windows 10 and later - Settings catalog (preview)

^ Authentication

Allow Aad Password Reset ⓘ	<input type="checkbox"/>	Block
Allow EAP Cert SSO (User) ⓘ	<input type="checkbox"/>	Block
Allow Fast Reconnect ⓘ	<input checked="" type="checkbox"/>	Allow
Allow Secondary Authentication Device ⓘ	<input type="checkbox"/>	Block

Remove category



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

Create a profile

Template name

Administrative Templates

Custom ⓘ

Delivery Optimization ⓘ

Device Firmware Configuration Interface ⓘ

Device restrictions ⓘ

Device restrictions (Windows 10 Team) ⓘ

Domain Join ⓘ

Edition upgrade and mode switch ⓘ

Email ⓘ

Endpoint protection ⓘ

Identity protection ⓘ

Kiosk ⓘ

Microsoft Defender for Endpoint (Windows 10 Desktop) ⓘ

Network boundary ⓘ

PKCS certificate ⓘ

PKCS imported certificate ⓘ

SCEP certificate ⓘ

Secure assessment (Education) ⓘ

Shared multi-user device ⓘ

Trusted certificate ⓘ

VPN ⓘ

Wi-Fi ⓘ

Windows health monitoring ⓘ

Device Firmware Configuration Interface

Windows 10 and later

Security Features

Allow local user to change UEFI settings Only not configured settings ▼

CPU and IO virtualization Enabled ▼

Built-in Hardware

DFCI can only manage hardware components built into the device. These settings cannot manage attached peripherals (e.g. USB webcams).

Cameras Enabled ▼

Microphones and speakers Enabled ▼

Radios (Bluetooth, Wi-Fi, NFC, etc..) Enabled ▼

Boot Options

Boot from external media (USB, SD) Disabled ▼

Boot from network adapters Disabled ▼

ADMX based policy



Windows



Office 365



Microsoft Edge



Internet Explorer



Third Party

ADMX based policies - Templates

Administrative Templates

✓ Basics

2 Configuration settings

3 Scope tags

4 Assignments

5 Review + create

All Settings

✓ Computer Configuration

✓ Microsoft Edge

Extensions

User Configuration

Extensions

Computer Configuration/Microsoft Edge/Extensions

Setting Name	↑↓	State	↑↓	Setting type	↑↓	Path	↑↓
Allow specific extensions to be installed		Not configured		Device		\Microsoft Edge\Extensions	
Blocks external extensions from being i...		Not configured		Device		\Microsoft Edge\Extensions	
Configure allowed extension types		Not configured		Device		\Microsoft Edge\Extensions	
Configure extension and user script inst...		Not configured		Device		\Microsoft Edge\Extensions	
Configure extension management settin...		Not configured		Device		\Microsoft Edge\Extensions	
Control which extensions are installed si...		Not configured		Device		\Microsoft Edge\Extensions	
Control which extensions cannot be inst...		Not configured		Device		\Microsoft Edge\Extensions	

ADMX based policies – Settings catalog

Create profile

Windows 10 and later - Settings catalog (preview)

[+ Add settings](#)

Microsoft Edge

Remove category

Extensions

Remove subcategory

Allow specific extensions to be installed

Enabled

Extension IDs to exempt from the block list (Device)

+ Add

Delete

Sort

+ Import

Export

Allow specific extensions to be installed (User)

Disabled

Blocks external extensions from being installed

Enabled

Blocks external extensions from being installed (User)

Disabled

Previous

Next

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

Got feedback?

Group Policy Objects (GPO) and determine your level of modern management support. Click "import" to upload a GPO.

Active Directory Target

MDM Support ↑↓

Page 2 of 4 Next >

Active Directory Target	MDM Support	MDM Support	Last imported
EMW-C-Windows AppLocker Settings - Audit C	100%	No	6/11/2020, 5:00:42 PM
EMW-C-Windows Credential Provider Settings	0%	No	6/11/2020, 5:00:42 PM
EMW-C-Windows Event Forwarding Settings	71%	No	6/11/2020, 5:00:47 PM
EMW-C-Windows MDM Enrollment Settings	No settings in policy	No	6/11/2020, 5:00:43 PM
EMW-C-Windows OS - Configuration Settings	No settings in policy	No	6/11/2020, 5:00:44 PM
EMW-C-Windows OS - Registry Settings	No settings in policy	No	6/11/2020, 5:00:43 PM
EMW-C-Windows OS - Security Settings	75%	No	6/11/2020, 5:00:44 PM
EMW-C-Windows OS - User Account Control Settings	No settings in policy	No	6/11/2020, 5:00:43 PM
EMW-C-Windows Point and Print Restrictions Settings	No settings in policy	No	6/11/2020, 5:00:43 PM
EMW-C-Windows Power Management Settings	No settings in policy	No	6/11/2020, 5:00:43 PM
EMW-C-Windows Remote Assistance Settings	88%	No	6/11/2020, 5:00:43 PM
EMW-C-Windows Remote Desktop Configuration Settings	50%	No	6/11/2020, 5:00:44 PM
EMW-C-Windows Remote Desktop Security Settings	100%	No	6/11/2020, 5:00:44 PM
EMW-C-Windows Remote Desktop Security Settings with I	100%	No	6/11/2020, 5:00:44 PM
EMW-C-Windows Telemetry Settings	57%	No	6/11/2020, 5:00:44 PM
EMW-C-Windows User Profile Settings	0%	No	6/11/2020, 5:00:44 PM
EMW-U-Google Chrome Configuration Settings	0%	No	6/11/2020, 5:00:44 PM
EMW-U-Google Chrome Security Settings	No settings in policy	No	6/11/2020, 5:00:44 PM
EMW-U-Internet Explorer Configuration Settings	100%	No	6/11/2020, 5:00:46 PM
EMW-U-Internet Explorer Security Settings	100%	No	6/11/2020, 5:00:45 PM

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

review) >

Security Settings

ot feedback? < Back

Group Policy Setting Category	MDM Support ↑↓	Min OS Version ↑↓	Sc
I with... Microsoft Edge/Native Messag	✓ Yes	15063	De
page Microsoft Edge	⚠ No	0	De
Microsoft Edge/SmartScreen se	✓ Yes	15063	De
ck po... Microsoft Edge/SmartScreen set	✓ Yes	15063	De
Microsoft Edge/Extensions	✓ Yes	15063	De
ension... Microsoft Edge/Extensions	✓ Yes	15063	De
Microsoft Edge/Content settings	✓ Yes	15063	De
setting Microsoft Edge/Content settings	✓ Yes	15063	De
er Microsoft Edge/Password manager and protection	✓ Yes	15063	De
Microsoft Edge	✓ Yes	15063	De
Microsoft Edge	⚠ No	0	De
ion e... Microsoft Edge	⚠ No	0	De
en pr... Microsoft Edge/SmartScreen settings	✓ Yes	15063	De
reen ... Microsoft Edge/SmartScreen settings	✓ Yes	15063	De
Microsoft Edge/HTTP authentication	✓ Yes	15063	De
rthenti... Microsoft Edge/HTTP authentication	✓ Yes	15063	De

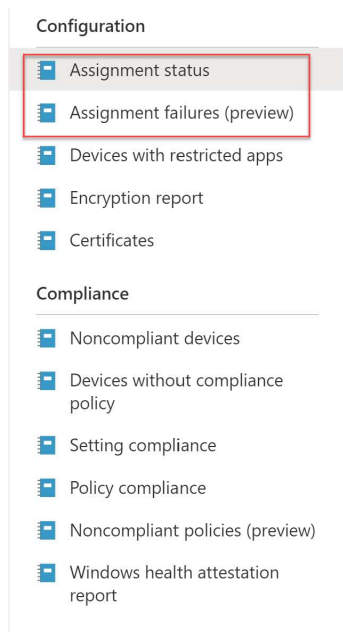
Monitoring

The 4 Report Types:



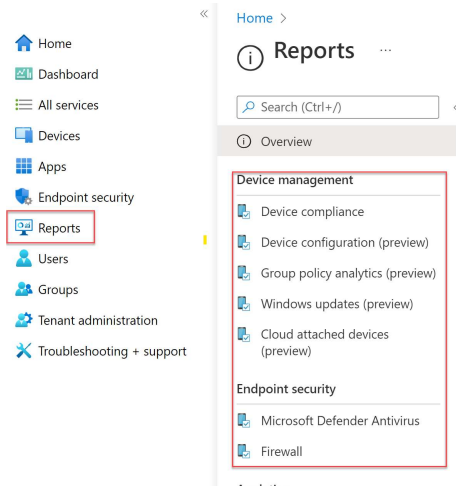
Operational

"Non-compliant devices"



Organizational

"Corporate vs personal devices"



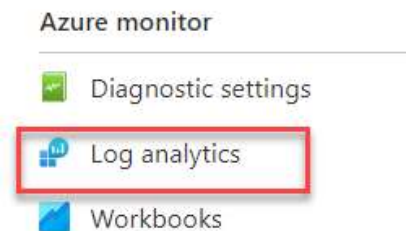
Historical

"Platform enrollment trends"



Specialist

"What about joining with AAD?"



Devices – Configuration profiles

Microsoft Endpoint Manager admin center

Home > Devices

Devices | Configuration profiles

Search (Ctrl+/)

+ Create profile Columns Refresh Export Filter

Search by name

Profile name	Platform	Profile type	Assigned	Last modified	
1111 - 3-30	Windows 10 and later	Custom	No	3/30/21, 12:23 AM	...
Policy 1	Android device adm...	Custom	No	4/30/21, 3:02 PM	...
Policy 2	Android device adm...	Device restrictions	No	4/30/21, 3:02 PM	...
Test Policy	Windows 10 and later	Endpoint protection	Yes	4/27/21, 3:22 AM	...
Intune data collection policy	Windows 10 and later	Windows health monitoring	Yes	4/19/21, 11:47 PM	...
Custom policy			No	4/09/21, 8:40 AM	...
wifi			No	3/09/21, 1:49 AM	...
ADMX policy			No	3/08/21, 7:40 PM	...
Bitlocker policy			No	4/15/21, 9:30 PM	...
Updates policy			No	5/12/21, 4:21 PM	...
Wifi	Windows 10 and later	Settings Catalog	Yes	3/19/21, 11:43 AM	...
sample policy	Windows 10 and later	Settings Catalog	No	3/15/21, 11:21 AM	...
laura's policy	Windows 10 and later	Settings Catalog	No	3/23/21, 3:57 PM	...
Policy for group 1	Windows 10 and later	Settings Catalog	Yes	3/15/21, 1:31 PM	...
policy group 3	Windows 10 and later	Settings Catalog	Yes	3/19/21, 3:49 PM	...
abc	Windows 10 and later	Settings Catalog	No	4/15/21, 2:36 PM	...
adm_x_Logon	Windows 10 and later	Settings Catalog	Yes	4/08/21, 8:51 PM	...

Navigate to Configuration profiles list and select individual policy

Devices – Configuration profiles

Microsoft Endpoint Manager admin center

Home > Devices > Test Policy

Device configuration profile

Delete

Device and user check-in status

Succeeded 0 Error 0 Conflict 6 Not Applicable 1

View Report

Device assignment status

This report shows all the devices that are targeted by the policy, including devices in a pending policy assignment state.

Per setting status

View the configuration status of each setting for this policy across all devices and users.

Properties

Basics Edit

Name Test Policy

Description --

Platform Windows 10 and later

Profile type Device restrictions

Assignments Edit

Included groups

Updated view of policy summary. Chart shows accurate count of devices and users in each state. Report automatically updates subject to devices checking in.

Click down to view list report.

Ability to click down to device assignment status report and per-setting status report

Demo

Questions ???



© Copyright Microsoft Corporation. All rights reserved.