

How to Protect your Business from the Threat of Unmanaged Devices

Myron Helgering
Tech Lead Security
Pink Elephant

Level: Intermediate

Session Survey

- Your feedback is very important to us
- Please take a moment to complete the session survey found in the mobile app
- Use the QR code or search for “Converge360 Events” in your app store
- Find this session on the Agenda tab
- Click “Session Evaluation”
- Thank you!



Agenda

- Introduction on unmanaged devices
- Customer landscape and solution requirements
- Options
 - Block access
 - App-enforced restrictions
 - MAM for Windows and MTD Connector
 - Session policies and In-browser protection
- Takeaways & Q&A



About me

- Technology Lead Security
- Microsoft Security MVP
- Blogger and Speaker
- Huge fantasy geek



Myron Helgering



in/myronhelgering



myronhelgering.com

TECHMENTOR
IN-DEPTH TRAINING FOR IT PROS

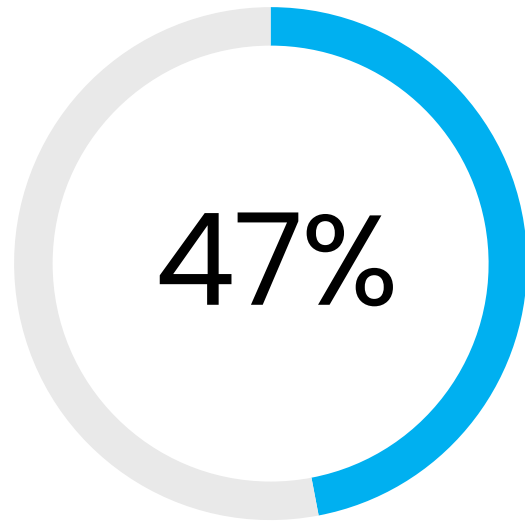
× **Cybersecurity** **LIVE!**
(DEFENDING AGAINST RANSOMWARE AND OTHER ATTACKS)

What is an unmanaged device?

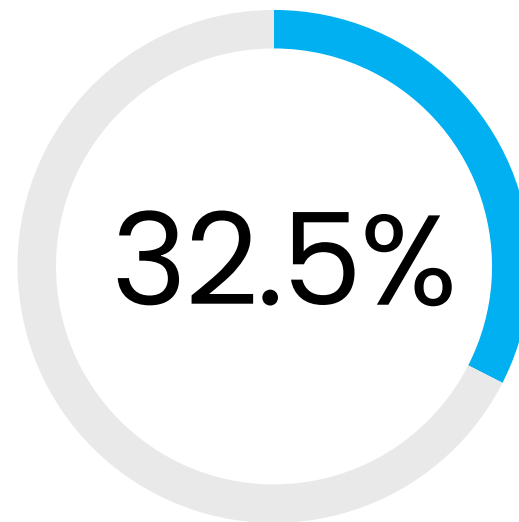
“A device that accesses company apps and data while not being (MDM) managed by the company.”

- Personal device
- Bring-your-own-device
- Managed by another company
- Unmanaged company device

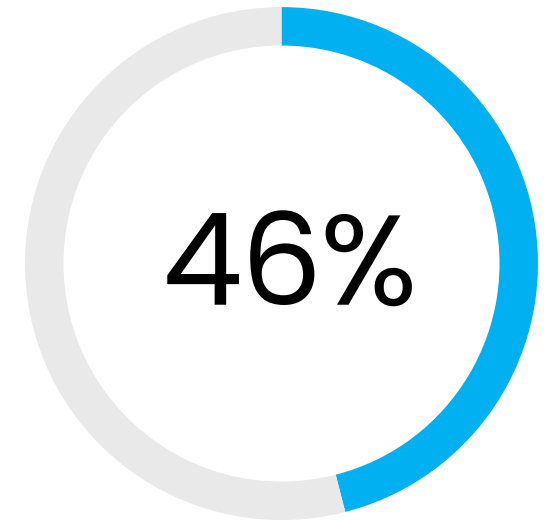
Numbers on unmanaged devices



of companies allow access to company resources from unmanaged devices ¹



of corporate devices in enterprise organizations are unmanaged ²



of compromised systems via stolen credentials were unmanaged devices ³

¹ Kolide Shadow IT Report 2023

² Palo Alto Device Security Threat Report 2025

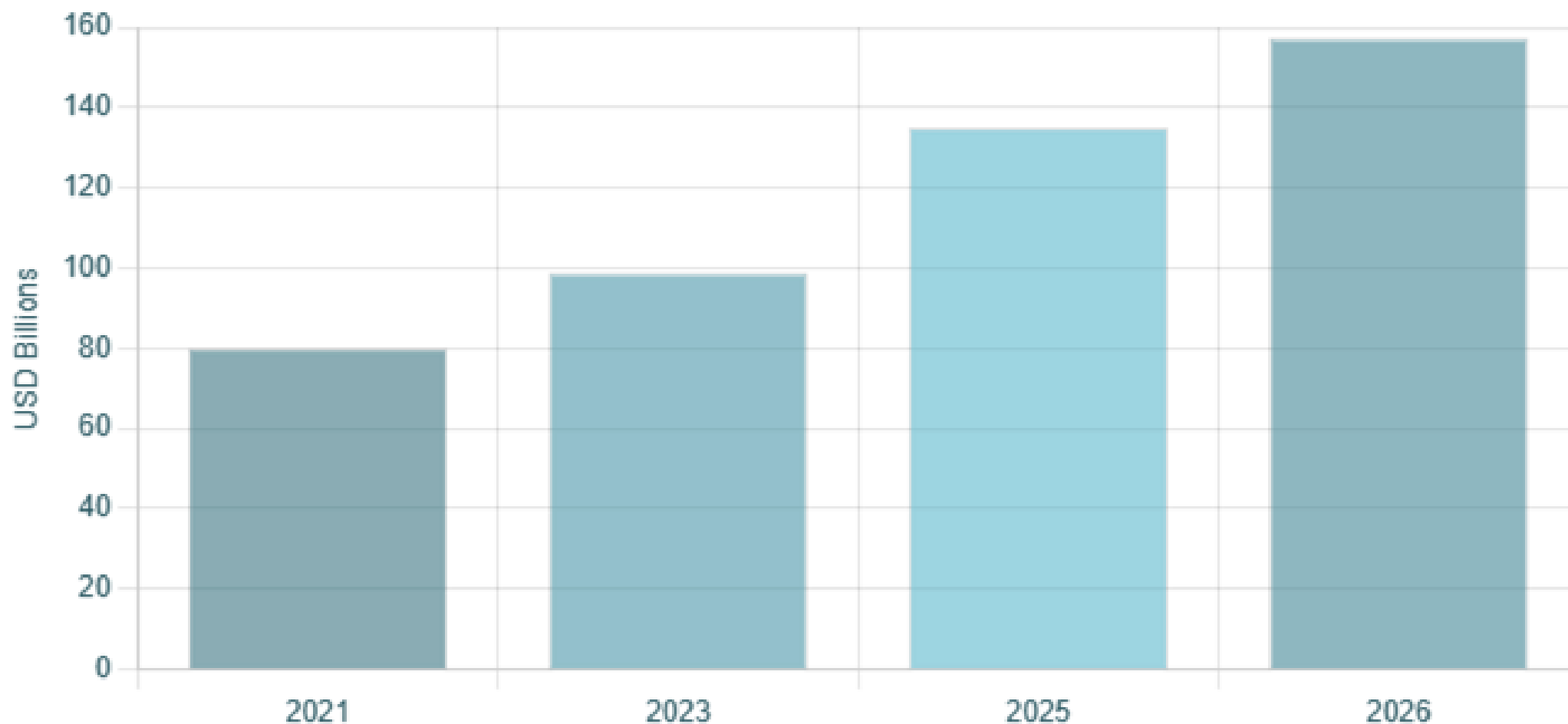
³ Verizon DBIR Data Breach Investigations Report 2025

Numbers on unmanaged devices

3.5x

more likely to be
infected on an
unmanaged device ¹

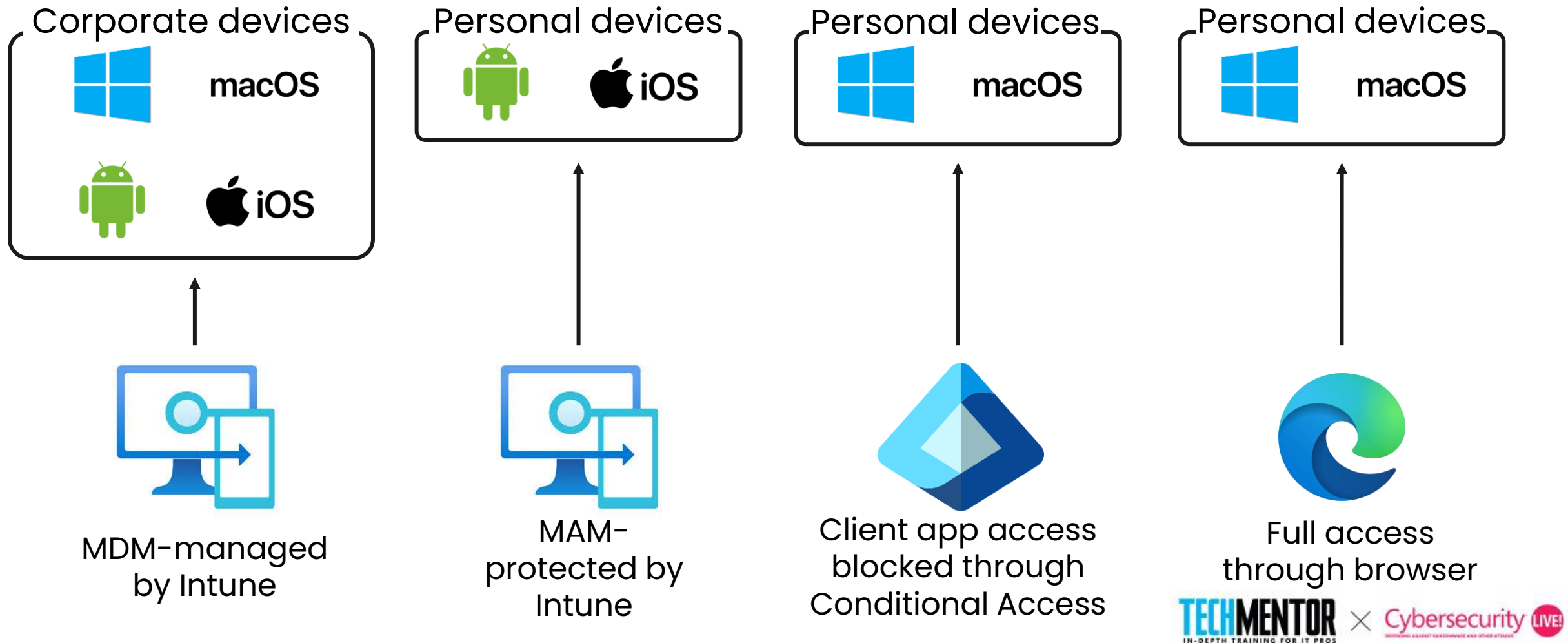
BYOD market size and growth



Next section

➔ Customer landscape and solution requirements

Customer landscape



Solution requirements

- Employees are **allowed** to access corporate data from **personal** devices.
- The solution **supports** both **Windows** and **macOS** devices.
- The solution must **prevent data from leaking** to unmanaged locations, such as devices and cloud apps.
- The solution **verifies** that the device is **up to date and secure**.

Next section

- ✓ Customer landscape and solution requirements
- ➔ Block access

Block access for unmanaged devices

Name *

Block access for unmanaged devices

Assignments

Users ⓘ

All users included and specific users excluded

Target resources ⓘ

All cloud apps

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

2 controls selected

- ☒ Require device to be marked as compliant
- ☒ Require Microsoft Entra hybrid joined device



 Microsoft

albus.dumbledore@myronhelgering.com

You can't get there from here

This application contains sensitive information and can only be accessed from:

- Helgering domain joined devices. Access from personal devices is not allowed.

[More details](#)

Solution requirements

- Employees are **allowed** to access corporate data from **personal** devices. 
- The solution **supports** both **Windows** and **macOS** devices. 
- The solution must **prevent data from leaking** to unmanaged locations, such as devices and third-party cloud apps. 
- The solution **verifies** that the device is **up to date and secure**. 

Next section

- ✓ Customer landscape and solution requirements
- ✓ Block access
- ➔ App enforced restrictions

- 
- Home
- Sites

Active sites

Deleted sites
- SharePoint Embedded
- Backup
- Policies
- Advanced

Script sources

More features
- Advanced management

PRO
- Customize navigation
- 

Access control

Use these settings to restrict how users are allowed to access content in SharePoint and OneDrive.

Unmanaged devices

Restrict access from devices that aren't compliant or joined to a domain.

Idle session sign-out

Unmanaged devices

The setting you select here will apply to all users in your organization.

[Learn more about controlling access from unmanaged devices.](#)

If you don't want to limit or block access organization-wide, you can do so for specific sites.

[Learn how to control access to specific sites by using Microsoft PowerShell](#)

☐ Allow full access from desktop apps, mobile apps, and the web

☒ Allow limited, web-only access

Policy name

Created by

State ↓

[SharePoint admin center]Block access from apps on unmanaged devices - 2026/07/31

USER

On

[SharePoint admin center]Use app-enforced Restrictions for browser access - 2026/07/31

USER

On

OneDrive access restriction

Restrict access to OneDrive content by security group.

Save

SPO Admin Center
Enable app-enforced
restrictions for
SharePoint Online

Policy 1: Block access from apps on unmanaged devices

- Block access from desktop apps on unmanaged devices
- Applies to SharePoint Online by default, but more apps can be added



albus.dumbledore@myronhelgering.com

You cannot access this right now

Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.

[Sign out and sign in with a different account](#)

[More details](#)

Policy 2: Use app-enforced restrictions for browser access

- Enforces limited web access on unmanaged devices
- Blocks download, print, or syncing
- Can only apply to SharePoint Online and **Exchange Online**

 Your organization doesn't allow you to download, print, or sync using this device. To use these actions, use a device that's joined to a domain or marked compliant by Intune. For help, contact your IT department. [More info.](#)

Enable app-enforced restrictions for Exchange Online

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Connect-ExchangeOnline
PS C:\WINDOWS\system32> Set-OwaMailBoxPolicy -Identity OwaMailboxPolicy-Default -ConditionalAccessPolicy ReadOnly
PS C:\WINDOWS\system32> Get-OwaMailBoxPolicy | select-object ConditionalAccess*

ConditionalAccessPolicy ConditionalAccessFeatures
-----
ReadOnly                {Offline, AttachmentDirectFileAccessOnPrivateComputersEnabled, AttachmentDirectFileAccess0..
.
```

Set-OwaMailBoxPolicy -Identity OwaMailboxPolicy-Default -ConditionalAccessPolicy ReadOnly

Edit sensitivity label

- ✓ Label details
- ✓ Scope
- ✓ Items
- Groups & sites**
- ✓ Privacy & external user access
- External sharing & conditional access
- Finish

Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

- ☐ **Control external sharing from labeled SharePoint sites**
When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.
- ☒ **Use Microsoft Entra Conditional Access to protect labeled SharePoint sites**
You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.
 - ☒ Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't [Microsoft Entra hybrid joined](#) or enrolled in Intune).

i For this setting to work, you must also configure the SharePoint feature that blocks or limits access to SharePoint files from unmanaged devices. [Learn more](#)

☐ Allow full access from desktop apps, mobile apps, and the web

☒ Allow limited, web-only access *i*

☐ Block access *i*- ☐ Choose an existing authentication context. Each context has an Microsoft Entra Conditional Access policy applied to enforce restrictions. [Learn more about authentication context](#)

Compliant Device - *v*

Solution requirements

- Employees are **allowed** to access corporate data from **personal** devices. ✓
- The solution **supports** both **Windows** and **macOS** devices. ✓
- The solution must **prevent data from leaking** to unmanaged locations, such as devices and third-party cloud apps. ✗
- The solution **verifies** that the device is **up to date and secure**. ✗

Next section

- ✓ Customer landscape and solution requirements
- ✓ Block access
- ✓ App enforced restrictions
- ➔ MAM for Windows and MTD Connector

- Home
- Dashboard
- All services
- Explorer
- Devices
- Apps
- Endpoint security
- Agents
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Connectors and tokens | Mobile Threat Defense

Search

+ Create Refresh Columns

Add filters

- Windows 365 partner connectors
- Windows data
- Apple
 - Apple VPP Tokens
- Android and ChromeOS
 - Managed Google Play
 - Chrome Enterprise
 - Firmware over-the-air update
- Cross platform
 - Microsoft Defender for Endpoint
 - Mobile Threat Defense**
 - Partner device management
 - Partner compliance management
 - TeamViewer connector
 - ServiceNow connector
 - Certificate connectors
 - Derived Credentials

MTD connector	Status	Enabled platforms	Last successful sync
No results found			

Microsoft Intune
Create new Mobile
Threat Defense (MTD)
connector

- Home
- Dashboard
- All services
- Explorer
- Devices
- Apps
- Endpoint security
- Agents
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Tenant admin | Connectors and tokens > Connectors

Connectors and tokens | Mobile Threat Defense

Search

+ Create

Add filter

- Windows 365 partner connectors
- Windows data
- Apple
 - Apple VPP Tokens
- Android and ChromeOS
 - Managed Google Play
 - Chrome Enterprise
 - Firmware over-the-air update
- Cross platform
 - Microsoft Defender for Endpoint
 - Mobile Threat Defense**
 - Partner device management
 - Partner compliance management
 - TeamViewer connector
 - ServiceNow connector
 - Certificate connectors
 - Derived Credentials

Add Connector

Mobile Threat Defense

Connection status

Last synchronized

Not set up

--

Select the Mobile Threat Defense connector to setup *

Windows Security Center

Create

Microsoft Intune
Select Windows
Security Center

Microsoft Intune
Connector
is ready to use

- Home
- Dashboard
- All services
- Explorer
- Devices
- Apps
- Endpoint security
- Agents
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Tenant admin | Connectors and tokens > Connectors and tokens

Connectors and tokens | Mobile Threat Defense

Search

- Windows 365 partner connectors
- Windows data
- Apple
 - Apple VPP Tokens
- Android and ChromeOS
 - Managed Google Play
 - Chrome Enterprise
 - Firmware over-the-air update
- Cross platform
 - Microsoft Defender for Endpoint
 - Mobile Threat Defense**
 - Partner device management
 - Partner compliance management
 - TeamViewer connector
 - ServiceNow connector
 - Certificate connectors
 - Derived Credentials

Create Refresh Columns

Add filters

MTD connector	Status	Enabled platforms	Last successful sync
Windows Security Center	Not set up	None	-

Microsoft Intune
Create
app protection policy
for Windows

[Home](#) > [Apps](#)

Apps | Protection

[+ Create](#)[Refresh](#)[Export](#)[Columns](#)[App protection report: V](#)

iOS/iPadOS

Android

Windows

Windows Information Protection

[?](#)[Add filters](#)

Deployed

Last modified

Platform

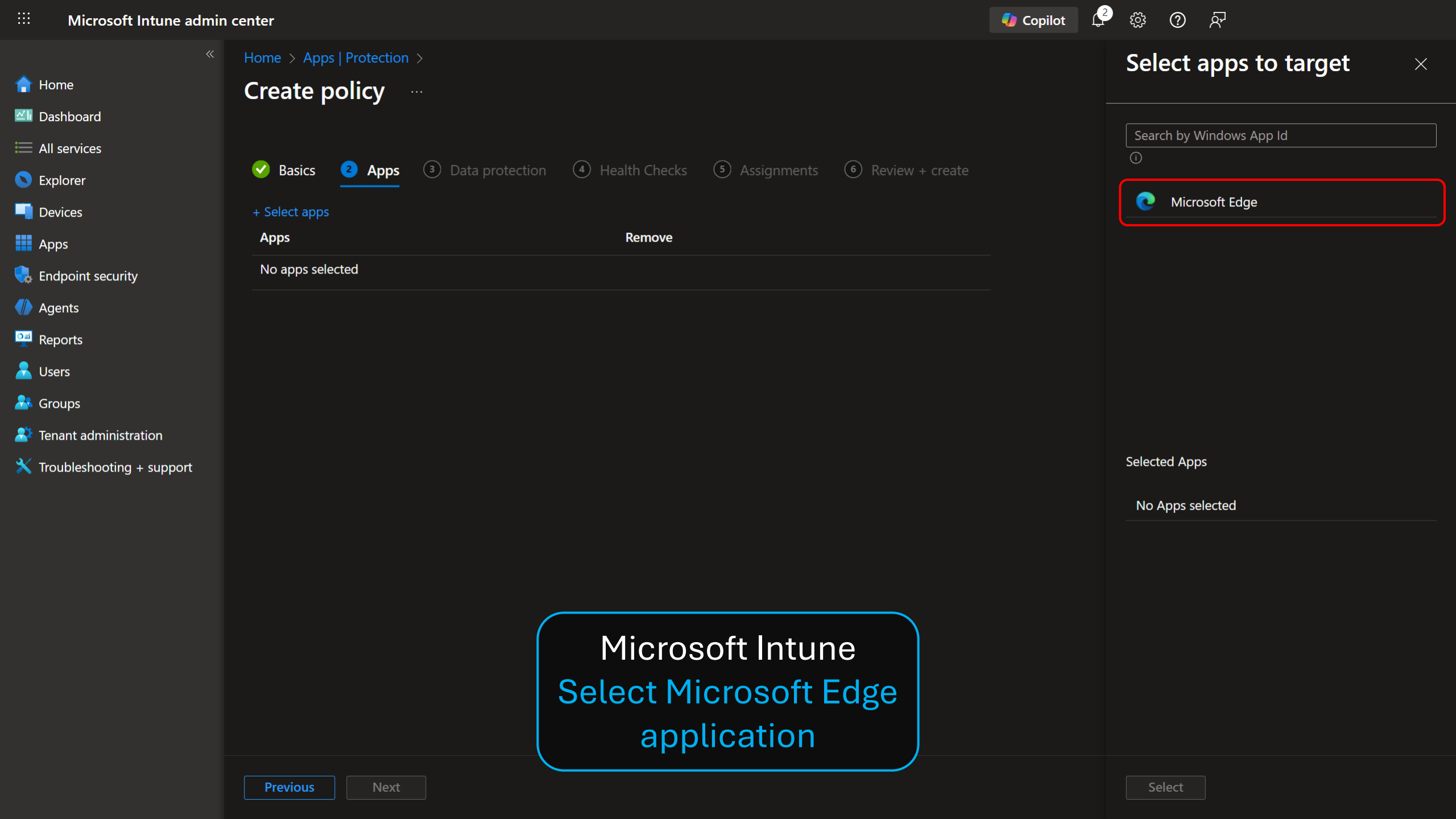
Management type



You have no policies.

[Overview](#)[All Apps](#)[Monitor](#)[Platforms](#)[Windows](#)[iOS/iPadOS](#)[macOS](#)[Android](#)[Manage apps](#)[Configuration](#)**[Protection](#)**[iOS app provisioning profiles](#)[S mode supplemental policies](#)[Policies for Microsoft 365 apps](#)[App selective wipe](#)[Quiet time](#)[Policy sets](#)[Organize apps](#)

Add or remove favorites by pressing Ctrl+Shift+F



Home > Apps | Protection >

Create policy ...

- ✓ Basics
- 2 Apps**
- 3 Data protection
- 4 Health Checks
- 5 Assignments
- 6 Review + create

+ Select apps

Apps

Remove

No apps selected

Select apps to target



Search by Windows App Id



Microsoft Edge

Selected Apps

No Apps selected

Previous

Next

Select

Microsoft Intune
Select Microsoft Edge
application

Microsoft Intune

Configure Data Protection settings

- Home
- Dashboard
- All services
- Explorer
- Devices
- Apps
- Endpoint security
- Agents
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Apps | Protection >

Create policy ...

- ✓ Basics
- ✓ Apps
- 3 Data protection
- 4 Health Checks
- 5 Assignments
- 6 Review + create

This group includes the Data Loss Prevention (DLP) controls, like cut, copy, paste, and save-as restrictions. These settings determine how users interact with data in the apps.

Data Transfer

Receive data from ⓘ

All sources

Send org data to ⓘ

No destinations

Allow cut, copy, and paste for ⓘ

Org data destinations and any source

NEW

Functionality

Print org data ⓘ

Block

Previous

Next

- Home
- Dashboard
- All services
- Explorer
- Devices
- Apps
- Endpoint security
- Agents
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Create policy

- Basics
- Apps
- Data protection
- Health Checks
- Assignments
- Review + create

Set the health check conditions for your app protection policy. Select a **Setting** and enter the **Value** that users must meet to access your org data. Then select the **Action** you want to take if users do not meet your conditionals. In some cases, multiple actions can be configured for a single setting. [Learn more about health check actions.](#)

App conditions

Configure the following health check settings to verify the application configuration before allowing access to org accounts and data.

Setting	Value	Action	
Offline grace period	1440	Block access (minutes)	...
Offline grace period	90	Wipe data (days)	...
Select one			

Device conditions

Configure the following health check settings to verify the device configuration before allowing access to org accounts and data.

Similar device based settings can be configured for enrolled devices. [Learn more about configuring device compliance settings for enrolled devices.](#)

Important! Make sure your Mobile Threat Defense (MTD) connector is set up in order to properly secure your organization's data based on threat evaluations from the connected Mobile Threat Defense services.

If your tenant has a connection set up with both Microsoft Defender for Endpoint and a MTD service (non-Microsoft) and do not configure a primary MTD service or there is a conflict when targeting a user, the default will be Microsoft Defender for Endpoint.

[Learn more about Mobile Threat Defense for unenrolled devices.](#)

Setting	Value	Action	
Min OS version	10.0.22621	Block access	...
Max allowed device threat level	Medium	Block access	...

Microsoft Intune
Configure Health
Checks settings

Offline grace period

90

Wipe data (days)

Select one



Microsoft Intune Configure Health Checks settings

Device conditions

Configure the following health check settings to verify the device configuration before allowing access to org accounts and data.

Similar device based settings can be configured for enrolled devices. [Learn more about configuring device compliance settings for enrolled devices.](#)



Important! Make sure your Mobile Threat Defense (MTD) connector is set up in order to properly secure your organization's data based on threat evaluations from the connected Mobile Threat Defense services.

If your tenant has a connection set up with both Microsoft Defender for Endpoint and a MTD service (non-Microsoft) and do not configure a primary MTD service or there is a conflict when targeting a user, the default will be Microsoft Defender for Endpoint.

[Learn more about Mobile Threat Defense for unenrolled devices.](#)

Setting	Value	Action
Min OS version	10.0.22621	Block access ...
Max allowed device threat level	Medium	Block access ...

Previous

Next

Microsoft Entra admin center

Home

Entra agents

Favorites

Entra ID

Overview

Users

Groups

Devices

Agent ID (Preview)

Enterprise apps

App registrations

Roles & admins

Delegated admin partners

Domain services

Conditional Access

Multifactor authentication

Identity Secure Score

Authentication methods

Search resources, services, and docs (G+/)

Copilot

Home > Conditional Access

Conditional Access | Policies

Microsoft Entra ID

Overview

Policies

Deleted Policies

Insights and reporting

Diagnose and solve problems

Manage

Named locations

Custom controls (Preview)

Terms of use

VPN connectivity

Authentication contexts

Authentication strengths

Classic policies

Monitoring

Sign-in logs

Audit logs

Troubleshooting + Support

New support request

New policy

New policy from template

Upload policy file

What if

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. [Learn more](#)

Microsoft-managed policies

Policies created 3

User created policies

Policies created 33

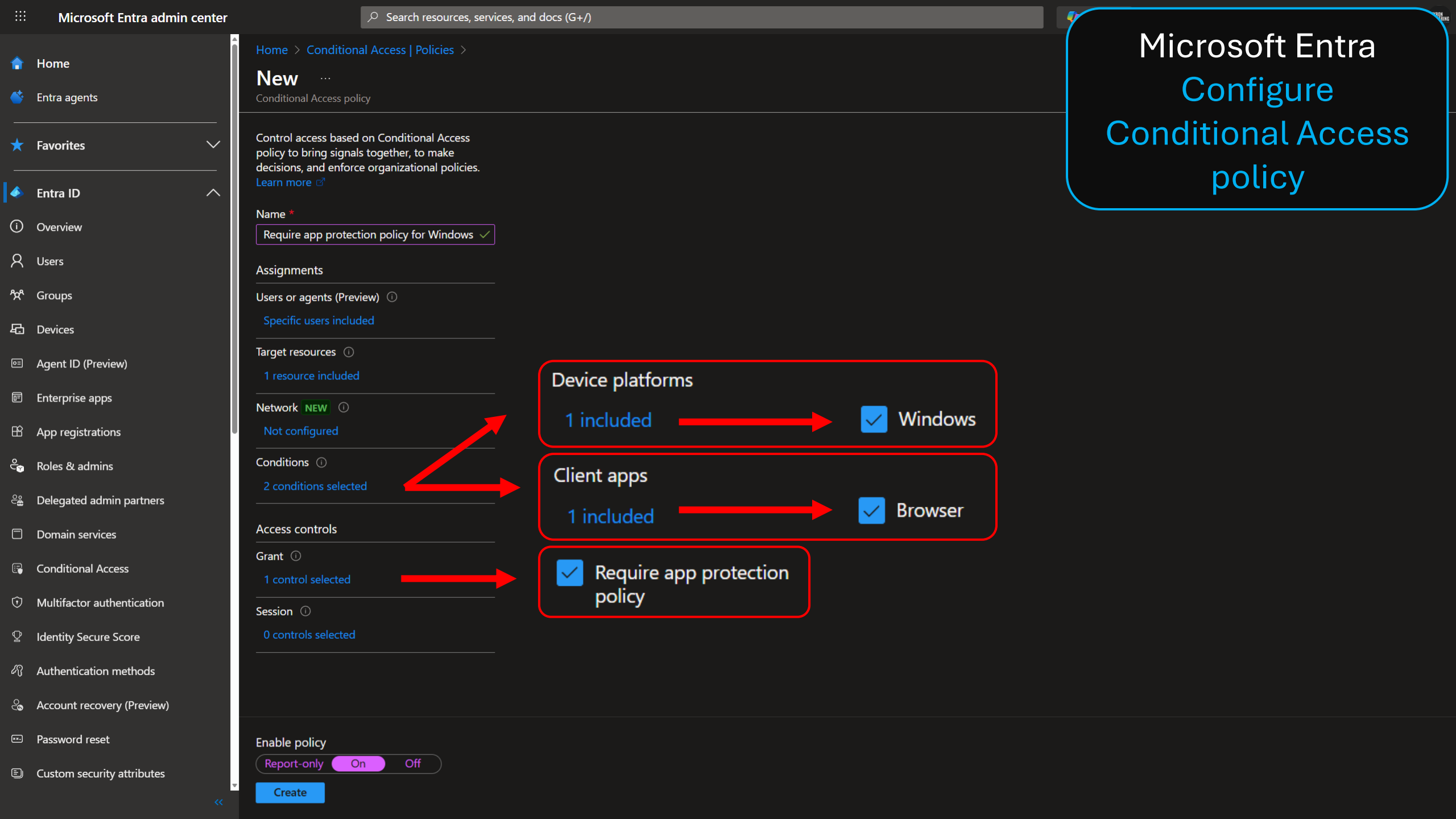
Search

Add filter

36 out of 36 policies found

Policy name	Created by	State	Alert
Block legacy authentication	MICROSOFT	Off	
Multifactor authentication for admins accessing Microsoft Admin Portal	MICROSOFT	Off	
Phishing-resistant multifactor authentication for admins	MICROSOFT	Off	
Block access for unknown or unsupported device platforms	USER	Off	
Block access for unmanaged devices	USER	Off	
Block access from desktop apps on unmanaged devices	USER	Off	
Block all personal devices (device filters)	USER	Off	
Block legacy authentication	USER	On	
CA11 - Block access for all locations except Netherlands	USER	Off	

Microsoft Entra
Create Conditional
Access policy



Microsoft Entra Configure Conditional Access policy

Home > Conditional Access | Policies >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
[Learn more](#)

Name *

Require app protection policy for Windows ✓

Assignments

Users or agents (Preview) ⓘ

[Specific users included](#)

Target resources ⓘ

[1 resource included](#)

Network **NEW** ⓘ

[Not configured](#)

Conditions ⓘ

[2 conditions selected](#)

Access controls

Grant ⓘ

[1 control selected](#)

Session ⓘ

[0 controls selected](#)

Device platforms

1 included



Windows

Client apps

1 included



Browser



Require app protection
policy

Enable policy

Report-only

On

Off

Create

Demo: MAM for Windows

1. MTD Connector
2. App Protection Policy
3. Conditional Access Policy

15:17

Saturday, 31 January



Old user experience

Stay signed in

Windows will remember your preferences and websites on this device.

☒ Allow my organization to manage this device

No, sign in to this device

1 Platform settings

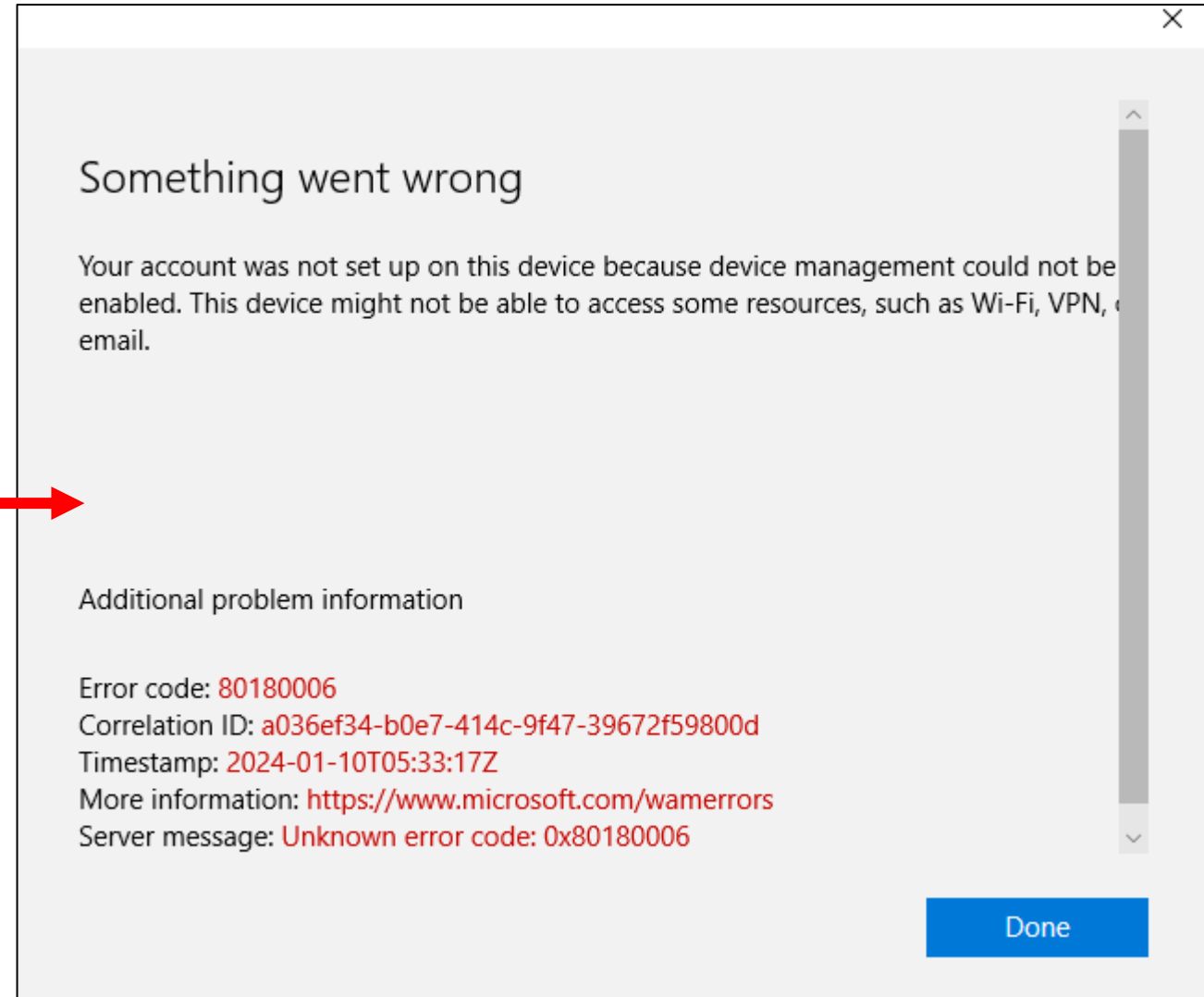
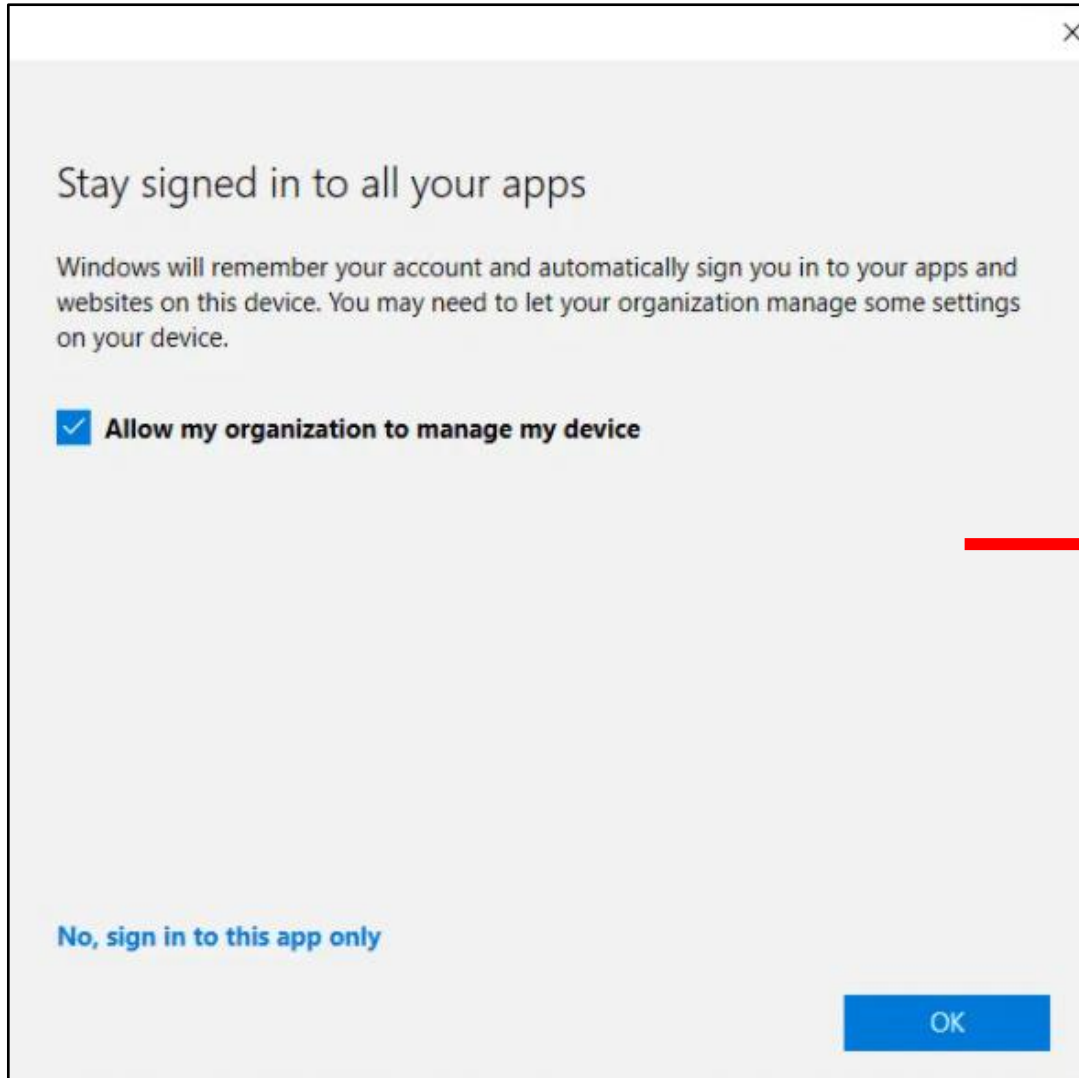
2 Review + save

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. [Learn more](#)

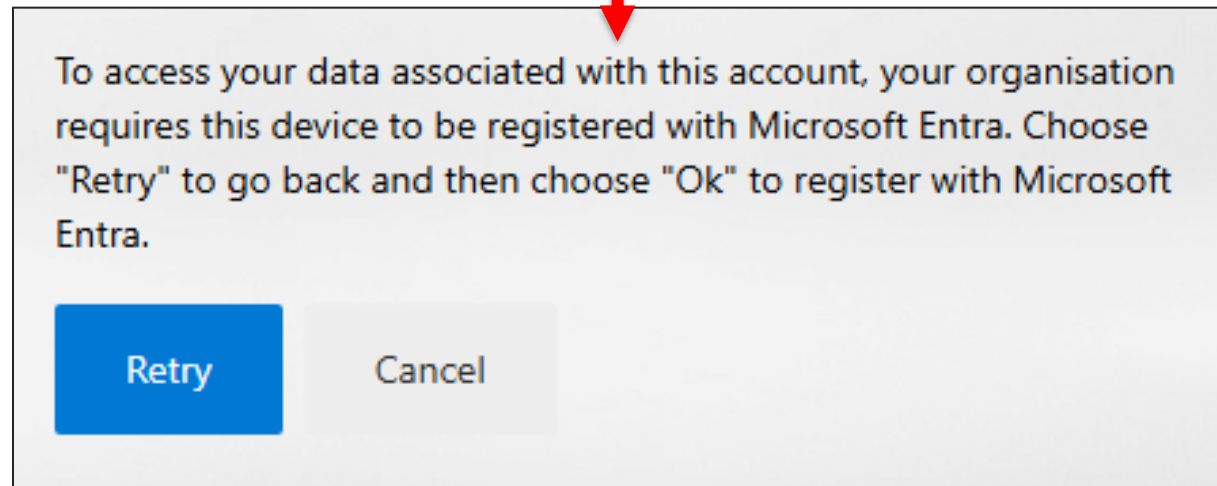
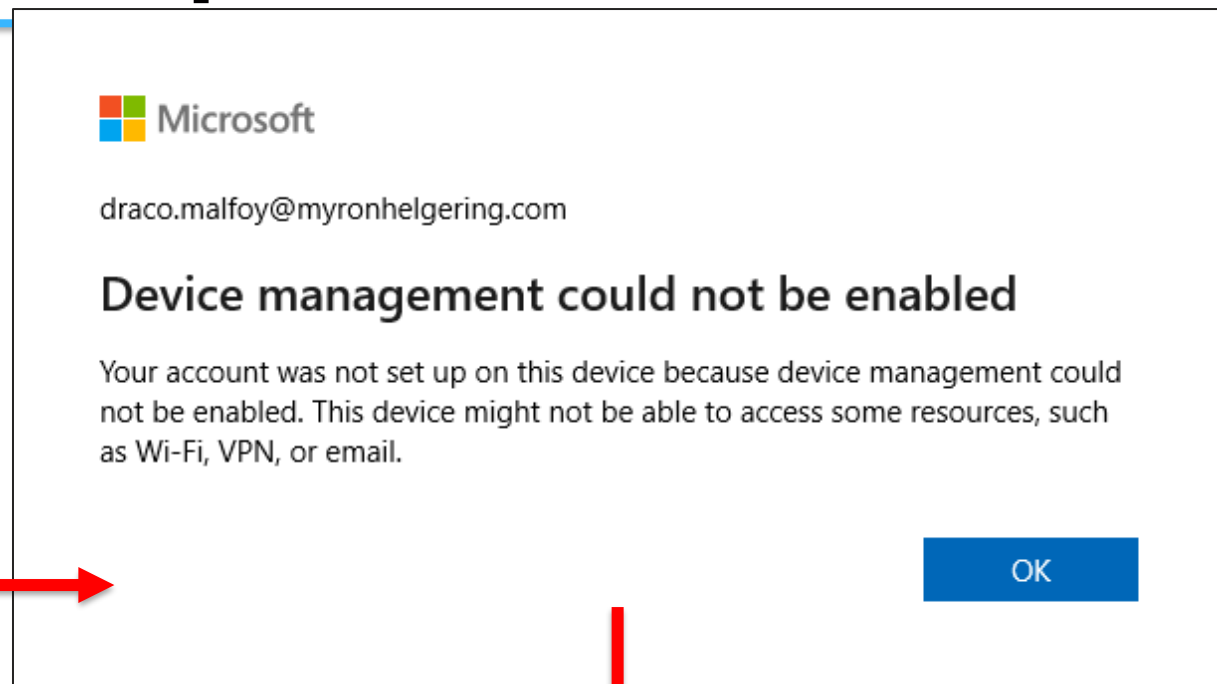
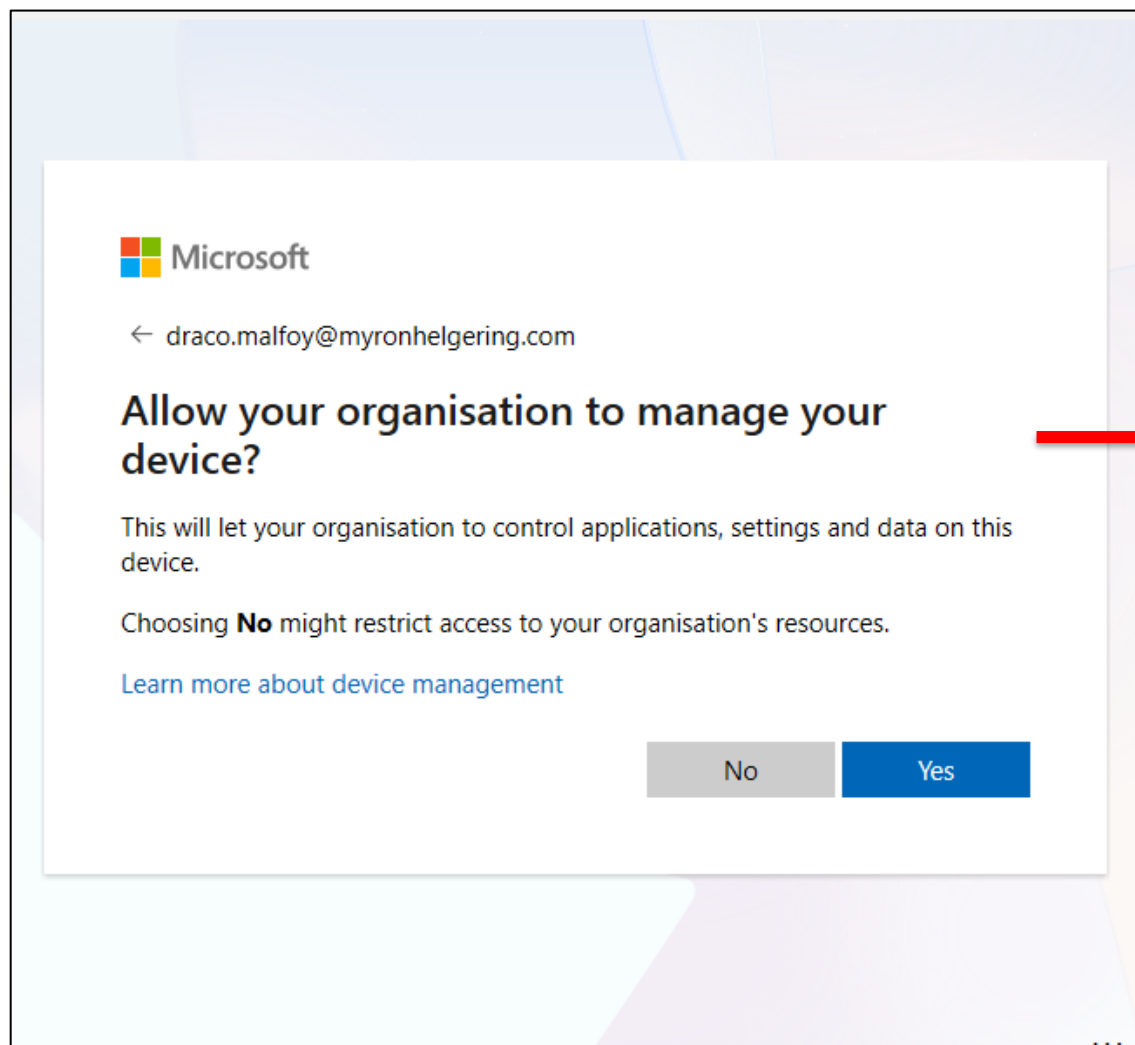
Type	Platform	versions	Personally owned	Device manufacturer
Android Enterprise (work profile)	AllowBlock	Allow min/max range: MinMax	AllowBlock	Manufacturer name
Android device administrator	AllowBlock	Allow min/max range: MinMax	AllowBlock	Manufacturer name
iOS/iPadOS	AllowBlock	Allow min/max range: MinMax	AllowBlock	Restriction not supported
macOS	AllowBlock	Restriction not supported	AllowBlock	Restriction not supported
Windows (MDM) ⓘ	AllowBlock	Allow min/max range: MinMax	AllowBlock	Restriction not supported

OK

Old user experience



New user experience





Microsoft Intune
Disable MDM
enrollment during
device registration

- Home
- Dashboard
- All services
- Explorer
- Devices
- Apps
- Endpoint security
- Agents
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Devices | Enrollment

Microsoft Intune

MDM user scope ⓘ

☐ None ☐ Some ☒ All

MDM terms of use URL ⓘ

<https://portal.manage.microsoft.com/TermsOfUse.aspx>

MDM discovery URL ⓘ

<https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc>

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

☒ Yes



MDM compliance URL ⓘ

<https://portal.manage.microsoft.com/?portalAction=Compliance>

[Restore default MDM URLs](#)

Windows Information Protection (WIP) user scope ⓘ

☐ None ☐ Some ☒ All

WIP terms of use URL ⓘ

WIP discovery URL ⓘ

<https://wip.manage.microsoft.com/Enroll>

Save

Discard

Delete

Sign in to your account

https://login

Chat

 Microsoft

← draco.malfoy@myronhelgering.com

Allow your organisation to manage your device?

This will let your organisation to control applications, settings and data on this device.

Choosing **No** might restrict access to your organisation's resources.

[Learn more about device management](#)

No

Yes

...

Terms of use

Privacy & cookies

...

M365 admin center

Enable Protected Downloads for MAM-registered devices

☒ Windows ☒ macOS

☐ Enforce secure enterprise browser access ⓘ

When enabled, Microsoft Edge for Business becomes the only browser allowed on managed devices, ensuring your content protections stay active and

☐ Block use of cloud apps in browsers where Purview in-browser protections don't apply ⓘ

When enabled, this setting prevents users from accessing specific LLM cloud applications in non-compliant browsers. It blocks these apps in Chrome and restricting the use of other non-compliant browsers.

Enable watermarking protection Preview

When enabled, sensitive-labeled content will display a visible watermark overlay to help prevent unauthorized sharing or data leakage

Enabled ▾

Policy applies to *

☒ Windows ☒ macOS

Enable browser-based tenant restrictions Preview

Block sign-ins to personal or external Microsoft accounts using policy-based header injections

Not configured ▾

Protected Clipboard ⓘ Preview

Restrict copy/paste actions between managed web apps based on session policies to prevent unauthorized data transfer across web boundaries.

Shared Boundary ▾

Policy applies to *

☒ Windows ☒ macOS

Screen capture protection Preview

Restricts screenshots and recordings of protected content.

Enabled ▾

Policy applies to *

☒ Windows ☒ macOS

Protected Downloads Preview

Restrict downloads of protected content based on session policies to prevent unauthorized data transfer.

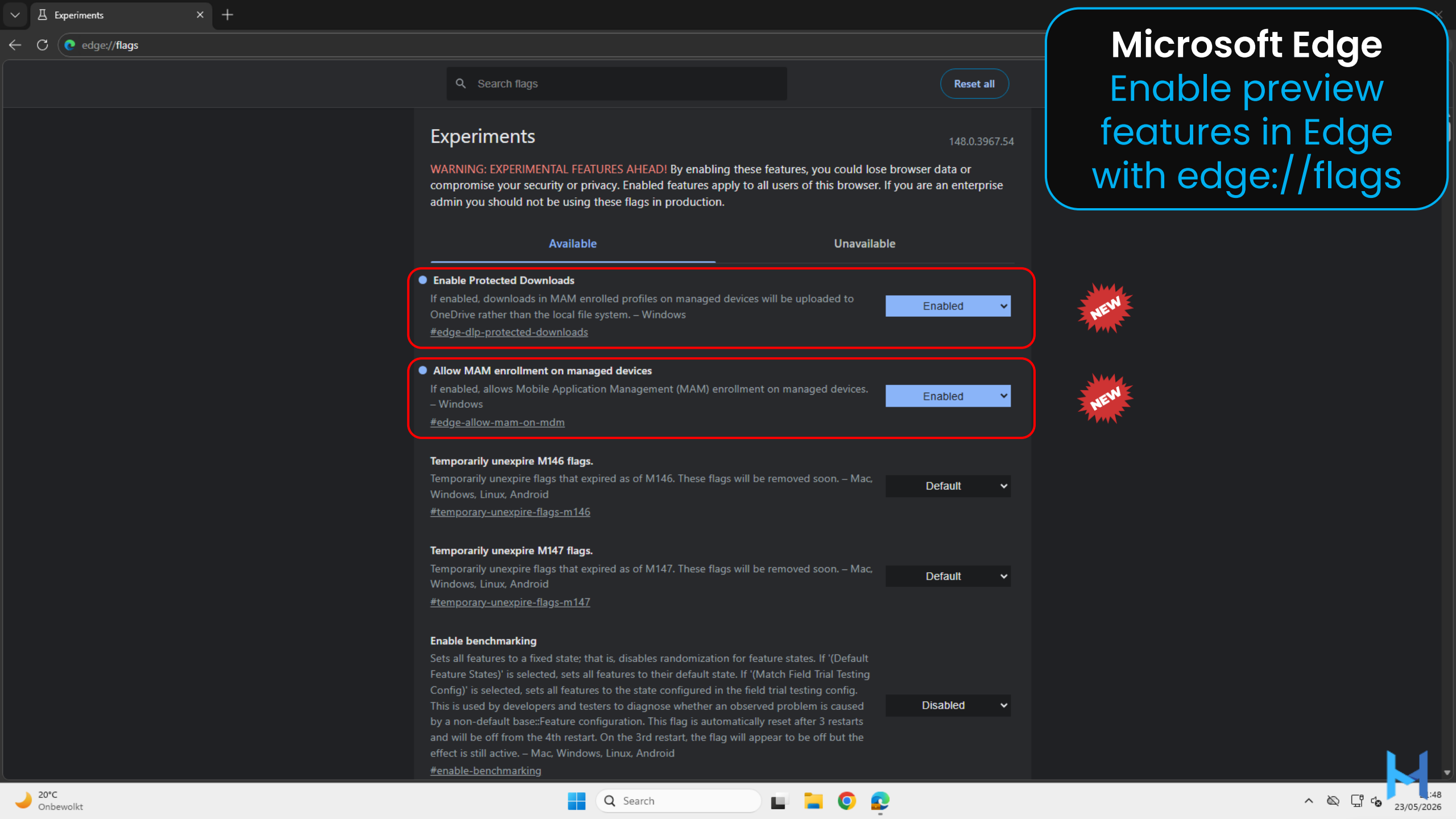
Enabled ▾

Policy applies to *

☒ Windows

NEW





Microsoft Edge
Enable preview
features in Edge
with edge://flags

NEW

NEW

Experiments

148.0.3967.54

WARNING: EXPERIMENTAL FEATURES AHEAD! By enabling these features, you could lose browser data or compromise your security or privacy. Enabled features apply to all users of this browser. If you are an enterprise admin you should not be using these flags in production.

Available

Unavailable

● Enable Protected Downloads

If enabled, downloads in MAM enrolled profiles on managed devices will be uploaded to OneDrive rather than the local file system. – Windows

[#edge-dlp-protected-downloads](#)

Enabled

● Allow MAM enrollment on managed devices

If enabled, allows Mobile Application Management (MAM) enrollment on managed devices. – Windows

[#edge-allow-mam-on-mdm](#)

Enabled

Temporarily unexpire M146 flags.

Temporarily unexpire flags that expired as of M146. These flags will be removed soon. – Mac, Windows, Linux, Android

[#temporary-unexpire-flags-m146](#)

Default

Temporarily unexpire M147 flags.

Temporarily unexpire flags that expired as of M147. These flags will be removed soon. – Mac, Windows, Linux, Android

[#temporary-unexpire-flags-m147](#)

Default

Enable benchmarking

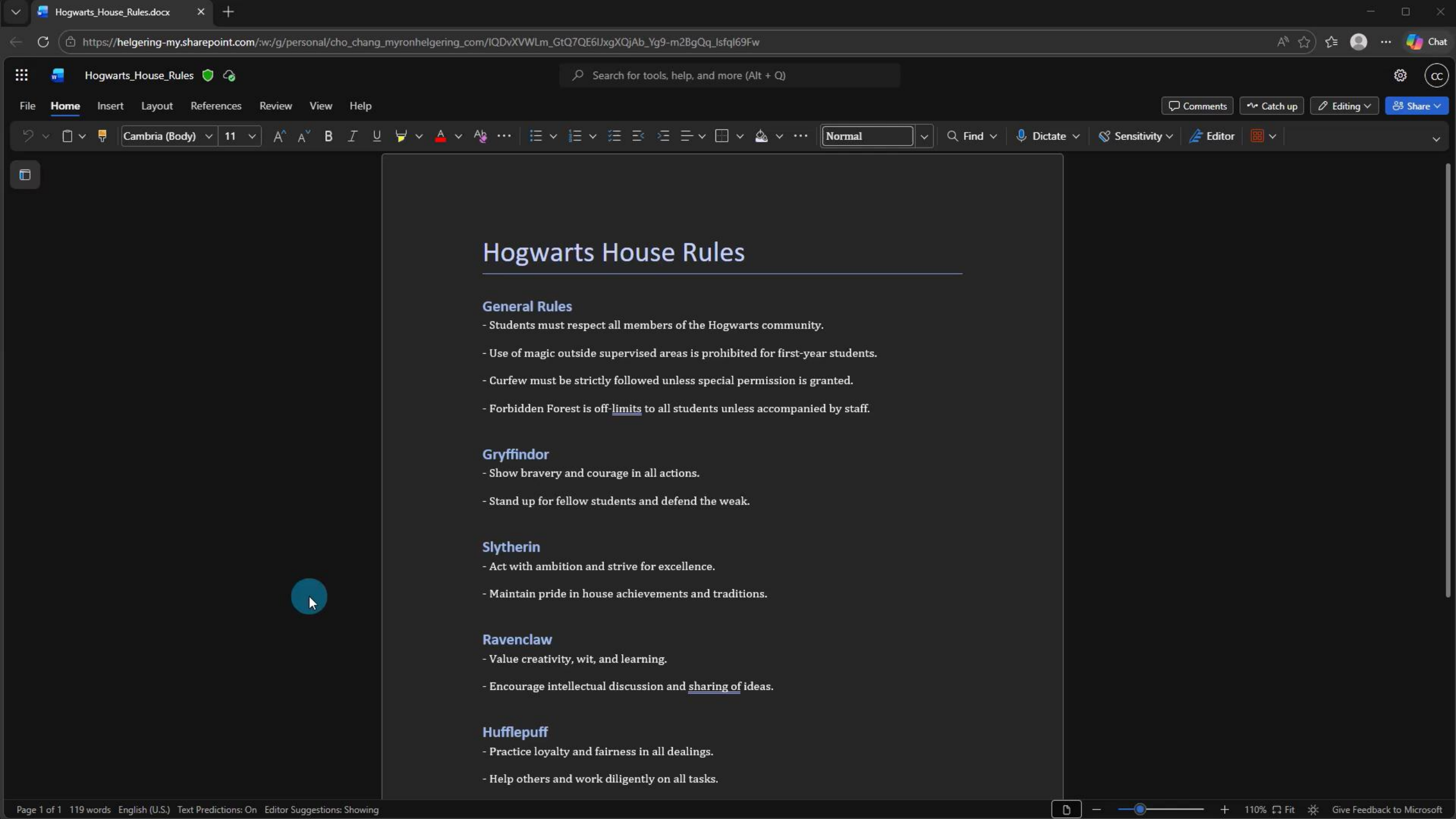
Sets all features to a fixed state; that is, disables randomization for feature states. If '(Default Feature States)' is selected, sets all features to their default state. If '(Match Field Trial Testing Config)' is selected, sets all features to the state configured in the field trial testing config. This is used by developers and testers to diagnose whether an observed problem is caused by a non-default base::Feature configuration. This flag is automatically reset after 3 restarts and will be off from the 4th restart. On the 3rd restart, the flag will appear to be off but the effect is still active. – Mac, Windows, Linux, Android

[#enable-benchmarking](#)

Disabled

Demo: Protected Downloads for MAM-registered devices

1. App protection policy (MAM)
2. Conditional access policy
3. Edge for Business policy
4. Enable preview flags in Edge



Hogwarts House Rules

General Rules

- Students must respect all members of the Hogwarts community.
- Use of magic outside supervised areas is prohibited for first-year students.
- Curfew must be strictly followed unless special permission is granted.
- Forbidden Forest is off-limits to all students unless accompanied by staff.

Gryffindor

- Show bravery and courage in all actions.
- Stand up for fellow students and defend the weak.

Slytherin

- Act with ambition and strive for excellence.
- Maintain pride in house achievements and traditions.

Ravenclaw

- Value creativity, wit, and learning.
- Encourage intellectual discussion and sharing of ideas.

Hufflepuff

- Practice loyalty and fairness in all dealings.
- Help others and work diligently on all tasks.

Solution requirements

- Employees are **allowed** to access corporate data from **personal** devices. ✓
- The solution **supports** both **Windows** and **macOS** devices. ✗
- The solution must **prevent data from leaking** to unmanaged locations, such as devices and third-party cloud apps. ✓
- The solution **verifies** that the device is **up to date and secure**. ✓

What to expect in the future?



Next section

- ✓ Customer landscape and solution requirements
- ✓ Block access
- ✓ App enforced restrictions
- ✓ MAM for Windows and MTD Connector
- ➔ Session policies and in-browser protection

Microsoft Entra admin center

Home

Entra agents

Favorites

Entra ID

Overview

Users

Groups

Devices

Agent ID (Preview)

Enterprise apps

App registrations

Roles & admins

Delegated admin partners

Domain services

Conditional Access

Multifactor authentication

Identity Secure Score

Authentication methods

Search resources, services, and docs (G+/)

Copilot

Home > Conditional Access

Conditional Access | Policies

Microsoft Entra ID

Overview

Policies

Deleted Policies

Insights and reporting

Diagnose and solve problems

Manage

Named locations

Custom controls (Preview)

Terms of use

VPN connectivity

Authentication contexts

Authentication strengths

Classic policies

Monitoring

Sign-in logs

Audit logs

Troubleshooting + Support

New support request

New policy

New policy from template

Upload policy file

What if

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. [Learn more](#)

Microsoft-managed policies

Policies created 3

User created policies

Policies created 33

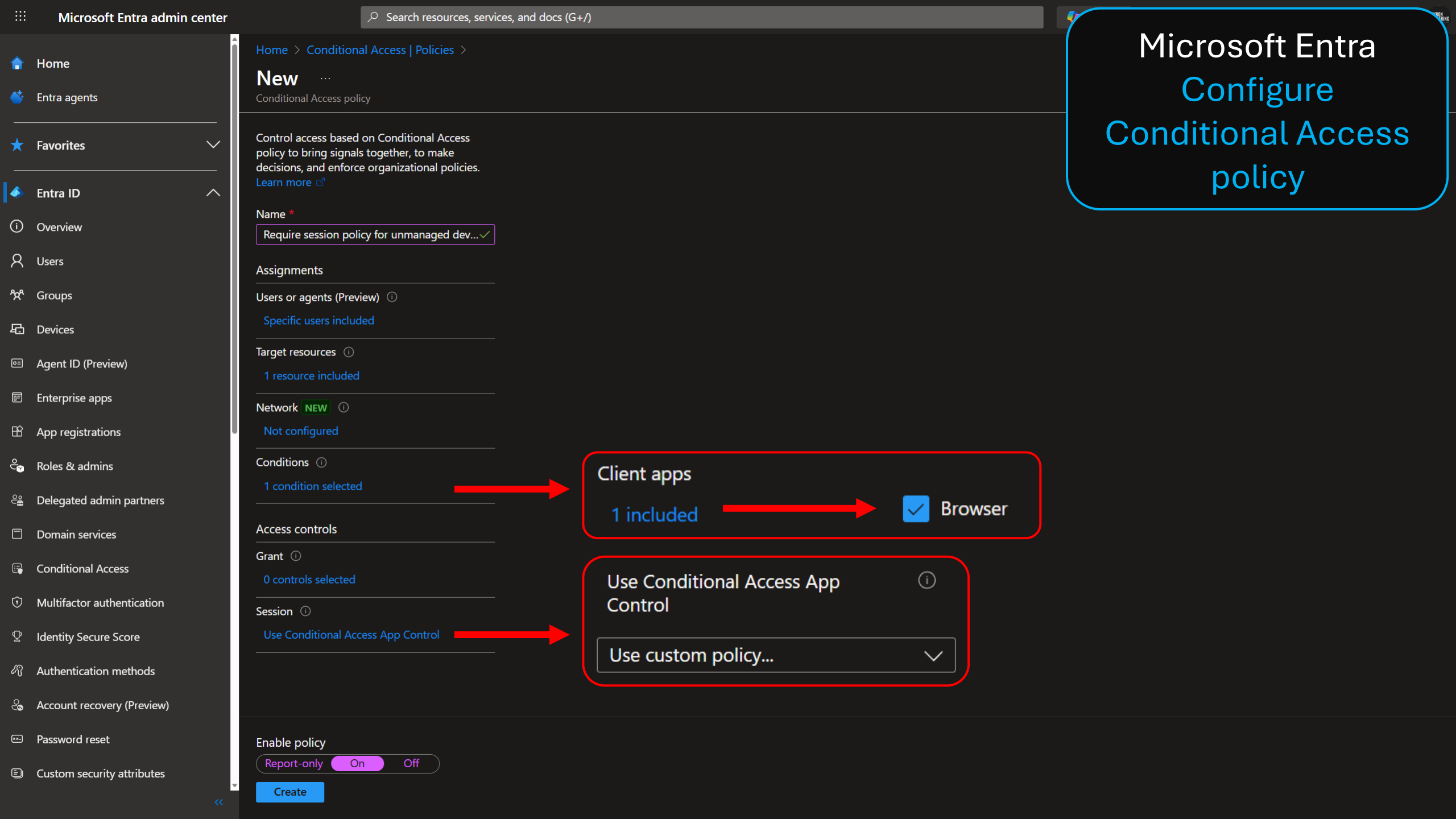
Search

Add filter

36 out of 36 policies found

Policy name	Created by	State	Alert
Block legacy authentication	MICROSOFT	Off	
Multifactor authentication for admins accessing Microsoft Admin Portal	MICROSOFT	Off	
Phishing-resistant multifactor authentication for admins	MICROSOFT	Off	
Block access for unknown or unsupported device platforms	USER	Off	
Block access for unmanaged devices	USER	Off	
Block access from desktop apps on unmanaged devices	USER	Off	
Block all personal devices (device filters)	USER	Off	
Block legacy authentication	USER	On	
CA11 - Block access for all locations except Netherlands	USER	Off	

Microsoft Entra
Create Conditional
Access policy



Microsoft Entra Configure Conditional Access policy

Client apps

1 included

☒ Browser

Use Conditional Access App Control

Use custom policy...

Policy name *

MDA - Block file downloads on unmanaged devices

Policy severity *

Category *

DLP

Description

Session control type *

Select the type of control

Control file download (1)

Actions

Select an action to be applied when user activity matches the policy.

☐ Audit

Monitor activities

☒ Block

A default block message is displayed when possible

☐

Customize block message ⓘ

Activity source

Add activity filters to the policy

Activities matching all of the following

[Edit and preview results](#)

×

App

Manual onboarding

equals

Microsoft 365

×

Device

Tag

does not equal

Intune compliant, Microsoft Entra Hybrid joined ⓘ

+ Add a filter

Search

Policy name *

MDA - Block cut/copy and print actions on unmanage

Policy severity *

Category *

DLP

Description

Session control type *

Select the type of control you want to enable:

Block activities

Activity source

Add activity filters to the policy

Activities matching all of the following

Edit and preview results

×

App

Manual onboarding

equals

Microsoft 365

×

Activity type

equals

Print, Cut/Copy item

×

Device

Tag

does not equal

Intune compliant, Microsoft Entra Hybrid joined

Two ways of protection with session policies

Reverse proxy

General available

All browsers and operating systems

No user interaction required

Slower user experience

N/A

In-browser protection

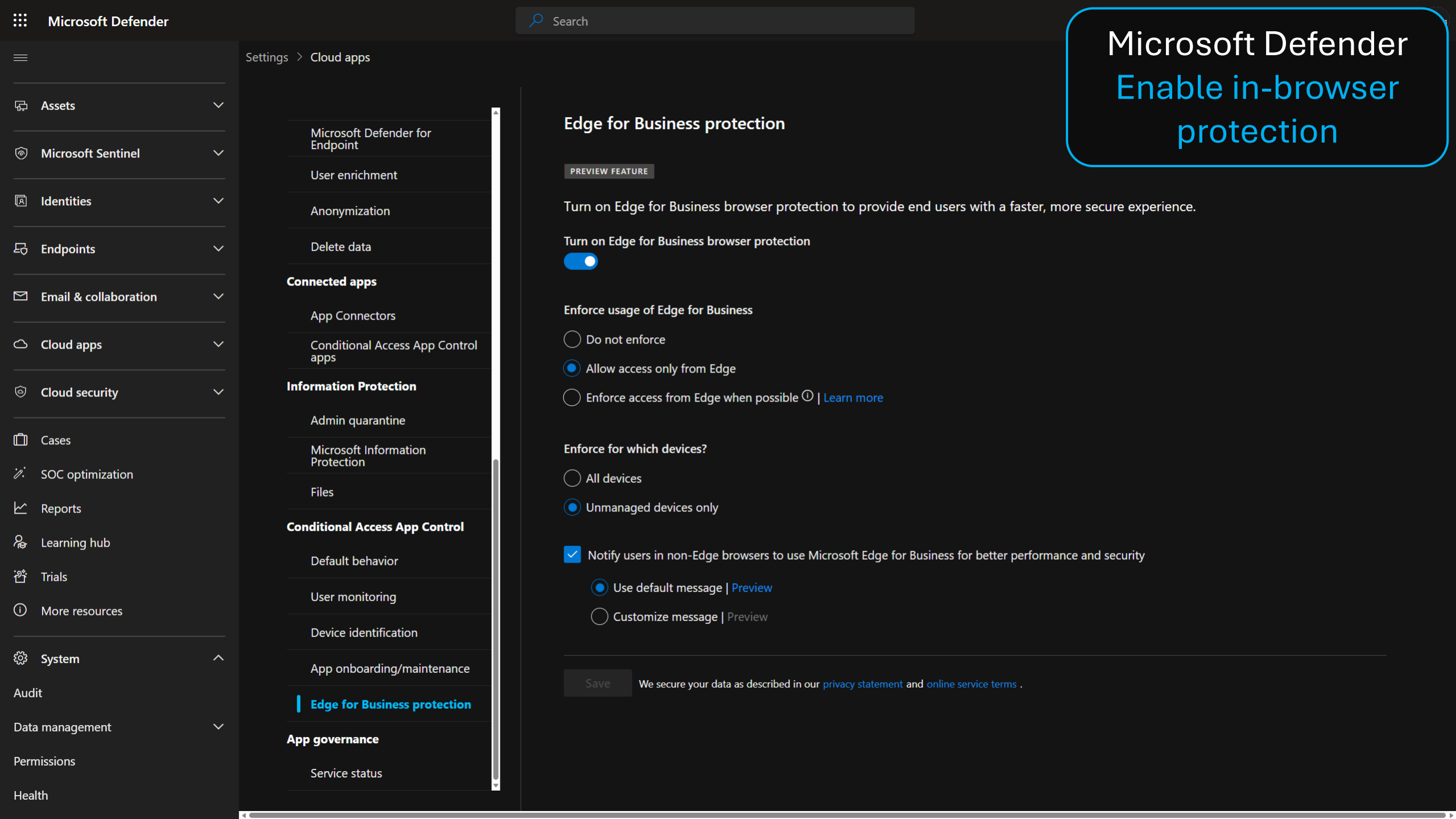
Still in preview (after 2+ years)

Edge with Windows 10/11 or MacOS

Requires Edge profile sign in

Faster user experience

Supports MAM & DLP restrictions



Microsoft Defender
Enable in-browser
protection

Edge for Business protection

PREVIEW FEATURE

Turn on Edge for Business browser protection to provide end users with a faster, more secure experience.

Turn on Edge for Business browser protection

☒

Enforce usage of Edge for Business

- ☐ Do not enforce
- ☒ Allow access only from Edge
- ☐ Enforce access from Edge when possible ⓘ | [Learn more](#)

Enforce for which devices?

- ☐ All devices
- ☒ Unmanaged devices only

☒ Notify users in non-Edge browsers to use Microsoft Edge for Business for better performance and security

- ☒ Use default message | [Preview](#)
- ☐ Customize message | [Preview](#)

[Save](#) We secure your data as described in our [privacy statement](#) and [online service terms](#) .

Edge for Business protection

PREVIEW FEATURE

Turn on Edge for Business browser protection to provide end users with a faster, more secure experience.

Turn on Edge for Business browser protection



Enforce usage of Edge for Business

- ☐ Do not enforce
- ☒ Allow access only from Edge
- ☐ Enforce access from Edge when possible ⓘ | [Learn more](#)

Enforce for which devices?

- ☐ All devices
- ☒ Unmanaged devices only

☒ Notify users in non-Edge browsers to use Microsoft Edge for Business for better performance and security

- ☒ Use default message | [Preview](#)
- ☐ Customize message | [Preview](#)

Microsoft Defender
Enable in-browser
protection

Demo: Session policies

1. Conditional access policy
2. 2x session policies
3. In-browser protection



Draco Malfoy



Enter your PIN

A dark grey rectangular input field for the PIN. The text "PIN" is visible on the left side of the field. A blue circular cursor is positioned at the start of the input field.

[I forgot my PIN](#)

- Microsoft Defender
-
- Endpoints
- Email & collaboration
- Cloud apps
- Cloud discovery
- Cloud app catalog
- OAuth apps
- App governance
- Activity log
- Governance log
- Policies
- Policy management
- Policy templates
- Cloud security
- Cases
- SOC optimization

Search

Files matching all of the following

Filters:

×

Sensitivity label

▼

equals

▼

Confidential-Internal only

▼

+

Add a filter

Inspection method

Data Classification Service

▼

Match if

Any

▼

of the following occur:

🛡️

Credit Card Number

✕

⌵

Advanced settings

[Choose another inspection type](#)

☐

Unmask the last 4 characters of a match ⓘ

Actions

Select an action to be applied when user activity matches the policy.

☐

Audit

Monitor activities

☒

Block

A default block message is displayed when possible

Microsoft Defender
Block “sensitive” file
downloads with
session policy

Solution requirements

- Employees are **allowed** to access corporate data from **personal** devices. ✓
- The solution **supports** both **Windows** and **macOS** devices. ✓
- The solution must **prevent data from leaking** to unmanaged locations, such as devices and third-party cloud apps. ✓
- The solution **verifies** that the device is **up to date and secure**. ✗

MAM for Windows vs Session policies

MAM for Windows

Intune license (M365 E3 or BP)

Device health checks

Remote selective wipe

Data protection restrictions

Allow copy/paste within Edge

N/A

Unmanaged devices only

App level targeting (Edge only)

N/A

Session policies

M365 E5 license

N/A

N/A

Data protection restrictions

N/A

macOS support

Support for any device

Granular cloud-app targeting

Protection based on sensitive files

Next section

- ✓ Customer landscape and solution requirements
- ✓ Block access
- ✓ App enforced restrictions
- ✓ MAM for Windows and MTD Connector
- ✓ Session policies and in-browser protection
- ➔ BONUS OPTION!

Microsoft Purview

Create DLP policy
for Managed Cloud
Apps

Location	Scope
 Exchange email	Turn on location to scope
 SharePoint sites	Turn on location to scope
 OneDrive accounts	Turn on location to scope
 Teams chat and channel messages	Turn on location to scope
 Devices	Turn on location to scope
 Instances	Turn on location to scope
 On-premises repositories	Turn on location to scope
 Fabric and Power BI workspaces	Turn on location to scope
 Microsoft 365 Copilot and Copilot Chat	Turn on location to scope
 ☒  Managed cloud apps	All users, groups, managed apps Edit

Back

Next

Cancel

Microsoft Defender
DLP rule becomes a
Session Policy

Policies

Threat detection Information protection **Conditional access** Shadow IT All policies

Starting June 15th, 2025, Microsoft Defender for Cloud Apps will adopt a dynamic threat detection model to enhance accuracy and responsiveness, policies that migrated will be disabled - For more information, visit our documentation.

Filters: Advanced filters

Name: Type: **Select type** Status: **ACTIVE** **DISABLED** Severity:

Category: **Select risk category**

+ Create policy Export Hide filters Table settings

	Policy	Count	S..	A...	Mo...	
	MDA - Block cut/copy and print actions on unmanaged devices	0 active in...	 Low	⚡	Jan 24, 2...	
	MDA - Block file downloads on unmanaged devices [Disabled]	0 active in...	 Low	⚡	Jan 26, 2...	
	Purview - Block cut/copy and print actions on unmanaged devic	1 active in...	 Low	🔔 ⚡	Jan 26, 2...	
	Purview - Block sensitive file downloads on unmanaged devices	0 active in...	 Low	🔔 ⚡	Jan 26, 2...	
	Purview - Block cut/copy and print actions on unmanaged devic	2 active in...	 Low	🔔 ⚡	Jan 26, 2...	



Edit session policy

Microsoft Defender
Policies are read-only from Defender

 This policy has been configured in Purview. Click [here](#) to view and manage it.

 To ensure that this policy runs as expected, we recommend checking the conditional access policies created in Entra ID.

Policy name *

Purview - Block sensitive file downloads on unmanage

Policy severity *

☒ ☐ ☐ ☒ ☐ ☒ ☒

Category *

DLP

Description





Configure enhanced security mode



Additional settings

Protect labeled content in Microsoft 365 online ⓘ

Keeps Microsoft Information Protection safeguards active for labeled content in Office online apps, preventing actions like print or screenshot where restricted.

Not configured



Enforce secure enterprise browser access ⓘ

When enabled, Microsoft Edge for Business becomes the only browser allowed on managed devices, ensuring your content protections stay active and cannot be bypassed.



Block use of cloud apps in browsers where Purview in-browser protections don't apply ⓘ

When enabled, this setting prevents users from accessing specific LLM cloud applications in non-compliant browsers. It blocks these apps in Chrome and Edge, while completely restricting the use of other non-compliant browsers.

NEW

Enable watermarking protection Preview

When enabled, sensitive-labeled content will display a visible watermark overlay to help prevent unauthorized sharing or data leakage

Enabled ▾

Policy applies to *



Windows



macOS

Enable browser-based tenant restrictions

Block sign-ins to personal or external Microsoft accounts using policy-based header injections

Not configured ▾

NEW

Protected Clipboard ⓘ Preview

Restrict copy/paste actions between managed web apps based on session policies to prevent unauthorized data transfer across web boundaries.

Shared Boundary ▾

Policy applies to *



Windows



macOS

NEW

Screen capture protection Preview

Restricts screenshots and recordings of protected content.

Enabled ▾

Policy applies to *



Windows



macOS



Takeaways

- **Block unmanaged devices:** Do it whenever possible.
- **App-enforced restrictions:** Avoid them; better options are available.
- **MAM for Windows + Session Policies:** The best solution available today.
- **DLP for Managed Cloud Apps:** Keep an eye on it; it may replace Session Policies in the future.

Time for questions!

Session Survey

- Your feedback is very important to us
- Please take a moment to complete the session survey found in the mobile app
- Use the QR code or search for “Converge360 Events” in your app store
- Find this session on the Agenda tab
- Click “Session Evaluation”
- Thank you!

