ORLANDO LIVE! 360 TECH CON 2025 FLORIDA

TECH EVENTS WITH PERSPECTIVE

# Six Methods to Protect Your Business from the Threat of Unmanaged Devices

**Myron Helgering**

Level: Intermediate

Visual Studio LIVE! EXPERT SOLUTIONS FOR ENTERPRISE DEVELOPERS

Data Platform LIVE! INSIGHTS FOR MANAGING YOUR DATA ESTATE

TECHMENTOR IN-DEPTH TRAINING FOR IT PROS

Artificial Intelligence LIVE! AI FOR DEVELOPERS AND DATA SCIENTISTS

Cloud & Containers LIVE! CLOUD-NATIVE, PAAS & SERVERLESS COMPUTING

Cybersecurity & Ransomware LIVE! DEFENDING AGAINST RANSOMWARE AND OTHER ATTACKS

# 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!

# About me

- Solution Lead @ Pink Elephant
- Microsoft Security MVP
- Blogger and Speaker
- Fantasy geek

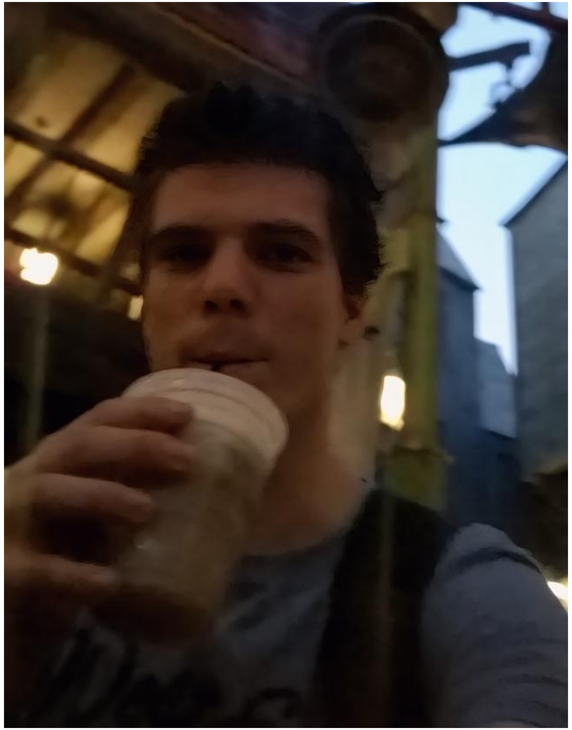
Myron Helgering

in/myronhelgering myronhelgering.com

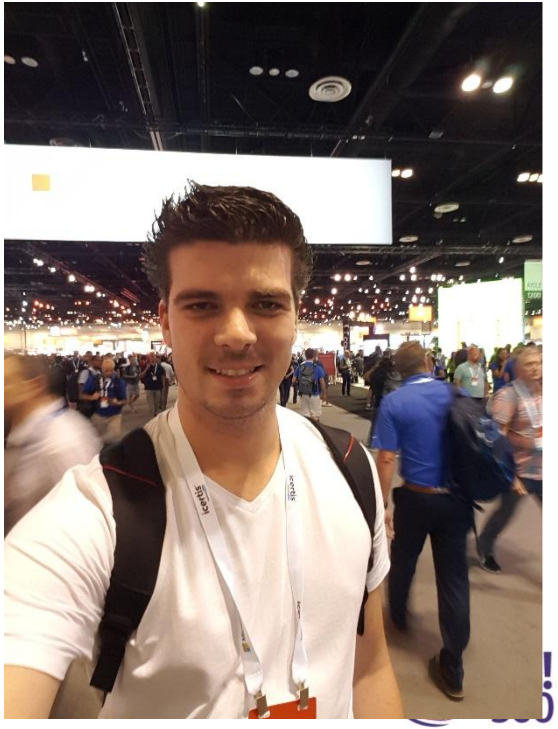
# I 💘 Orlando

2007

2016



2018

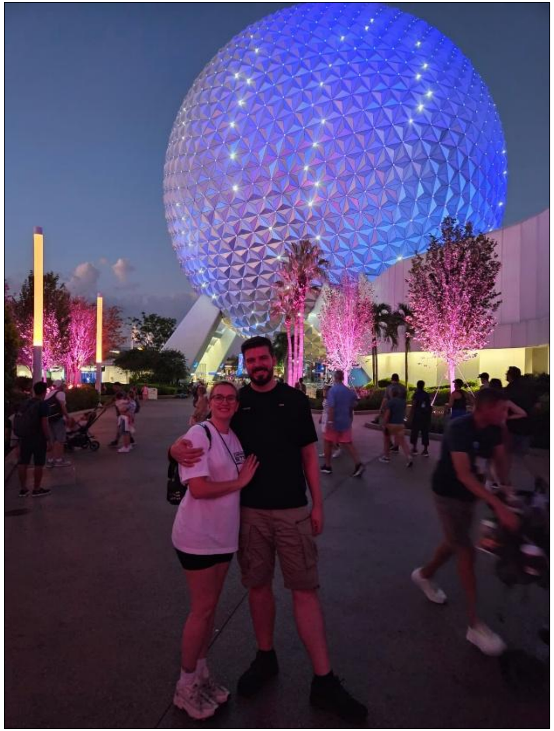


TECH EVENTS WITH PERSPECTIVE

# I 💘 Orlando

2019

2024



2025

LIVE! 360
TECH CON 2025
ORLANDO
FLORIDA
Cybersecurity & Ransomware LIVE!
Banda Sea 2
Cybersecurity & Ransomware Live! Pre-Con Hands-On Lab: Sunday, Nov 16
9:00 AM - 6:00 PM CRHOL01 Hands-On Lab: Protect, Detect, Respond with Microsoft Defender XDR - Stefan Schörling & Mattias Borg
Cybersecurity & Ransomware Live! Pre-Con Workshops: Monday, Nov 17
8:30 AM - 5:30 PM CRM01 Workshop: Designing a Privileged Access Management Solution - Sami Laiho
Cybersecurity & Ransomware Live! Day 1: Tuesday, November 18
8:00 AM - 9:00 AM Cybersecurity & Ransomware Live! Keynote: 2026 Ransomware State of the Union - Sami Laiho, Chief Research Officer, Adminize
9:15 AM - 10:30 AM CRT02 Using Security Copilot and Defender XDR to Streamline Your SOC - John O'Neill Sr.
1:30 PM - 1:50 PM CRT04 Fast Focus: Connect Securely to Your Home Network Without a Single Firewall Port Open - Sami Laiho
2:00 PM - 2:20 PM CRT06 Fast Focus: Elevate to Admin on Demand - Sami Laiho
2:45 PM - 4:00 PM CRT08 When Hackers Collide – Unleashing Sticky Data Protection - Andy Malone
4:15 PM - 5:30 PM CRT10 Unlocking Next-Gen Cloud Security: What's New in Microsoft Defender for Cloud - Markus Lintuala
Cybersecurity & Ransomware Live! Day 2: Wednesday, November 19
8:00 AM - 9:15 AM CRW02 What Security Engineers and Developers Must Know About Azure AI Solutions - Markus Lintuala
9:30 AM - 10:45 AM CRW04 Automated Data Security: Identifying Sensitive Data with Microsoft Purview - Myron Helgering
2:00 PM - 3:15 PM CRW06 Improve Your Resilience with Cybersecurity Table-top Exercises - Stefan Schörling & Mattias Borg
4:00 PM - 5:15 PM CRW08 BYOAI: Bring Your Own AI to the Cybersecurity Fight - Michael Van Horenbeeck
Cybersecurity & Ransomware Live! Day 3: Thursday, November 20
8:00 AM - 9:15 AM CRH01 Securing, Managing and Hacking Microsoft Copilot - Stephen L. Rose
9:30 AM - 10:45 AM CRH03 Building a Resilient Incident Response Team: Beyond Playbooks and Tools - John O'Neill Sr.
11:00 AM - 12:00 PM Cybersecurity & Ransomware Live! Panel Discussion: How to Not Get Hacked in 2026 - Sami Laiho (moderator) Erica Burgess, Michael Niehaus, Stefan Schörling, & Michael Van Horenbeeck
1:00 PM - 2:15 PM CRH05 Six Methods to Protect Your Business From the Threat of Unmanaged Devices - Myron Helgering
2:30 PM - 3:45 PM CRH07 Why Domain Tiering is Critical to Prevent Ransomware - Sami Laiho

# Agenda

01 Unmanaged Devices

02 Method 1, 2 & 3

03 App Enforced Restrictions

04 Session Policies

05 App Protection Policies

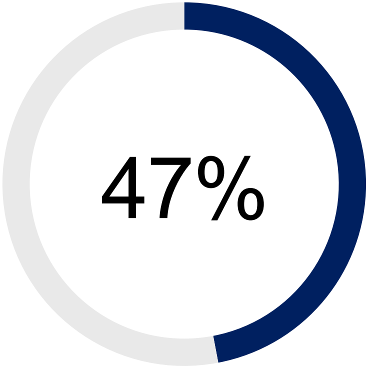
06 Takeaways & Q&A

# What is an unmanaged device?

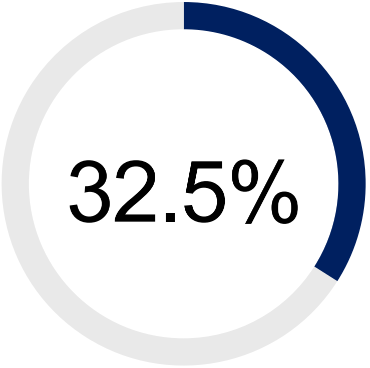
*“A device that accesses company apps and data while not being (MDM) managed by the company.”*

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

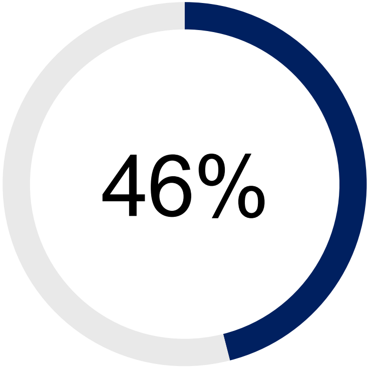
# Numbers on unmanaged devices



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

TECH EVENTS WITH PERSPECTIVE

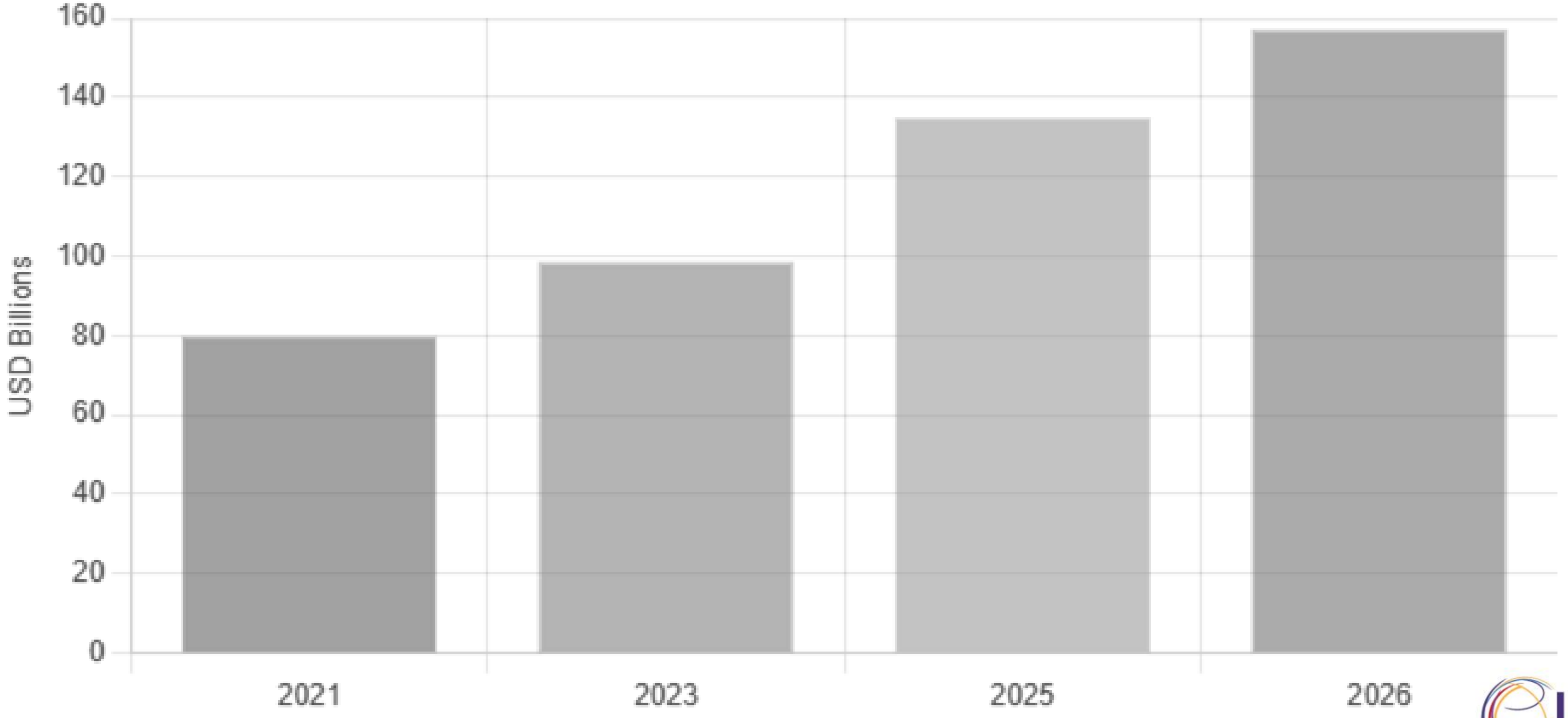
# Numbers on unmanaged devices

# 3.5x

more likely to be infected on
an unmanaged device [1]

[1] Palo Alto Device Security Threat Report 2025

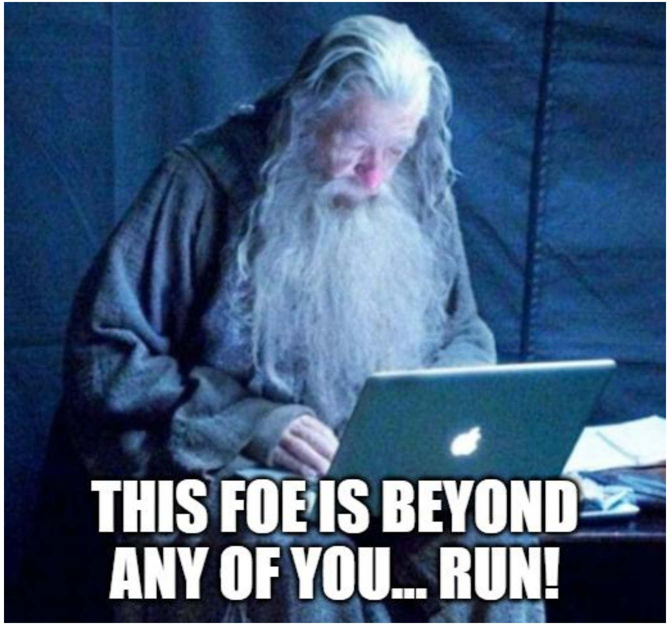
# BYOD market size and growth



1 Market Analysis Report on Bring Your Own Devices by GrandViewResearch 2022

# Challenges with unmanaged devices

- No insight in vulnerabilities or device compliance
- Users are local administrator on their device
- Can’t update or patch OS and software
- Can’t enforce security configurations and policies
- Can’t encrypt hard drive
- Can’t remotely wipe device
- Can’t prevent data leakage



# Method 1: Do nothing…

- Let employees be productive on any device
- Easy to implement
- Accept the security risks

✗ I would not recommend this method as the risks are just too high.

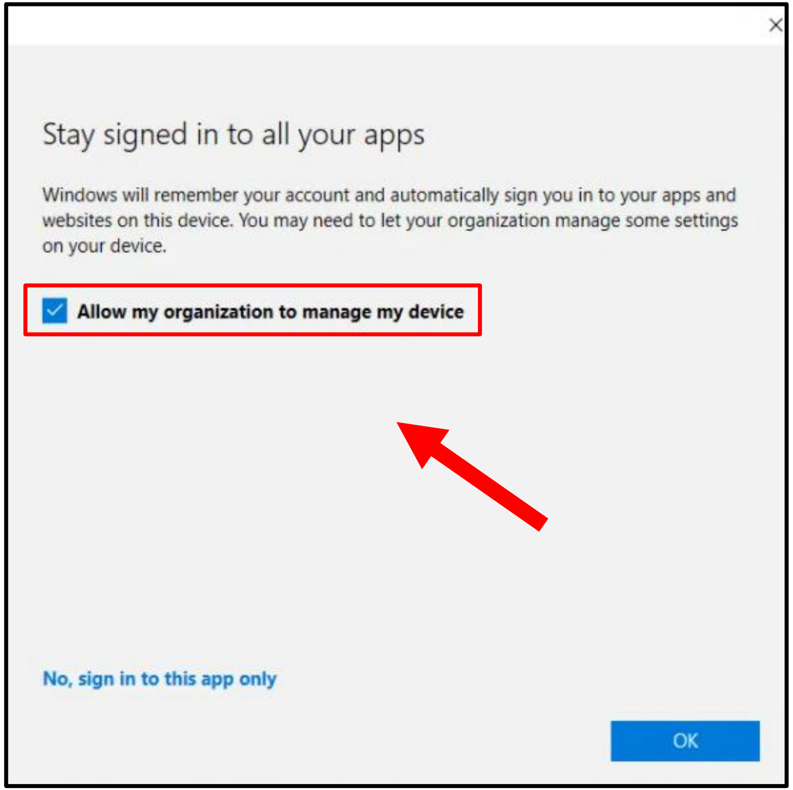
# Example of doing nothing

# Method 2: Manage personal devices

- Require device enrollment
- Reduces security risks
- Complete control over devices

! I would **not** recommend this method unless there is no other way.

# Enrollment during Office sign-in

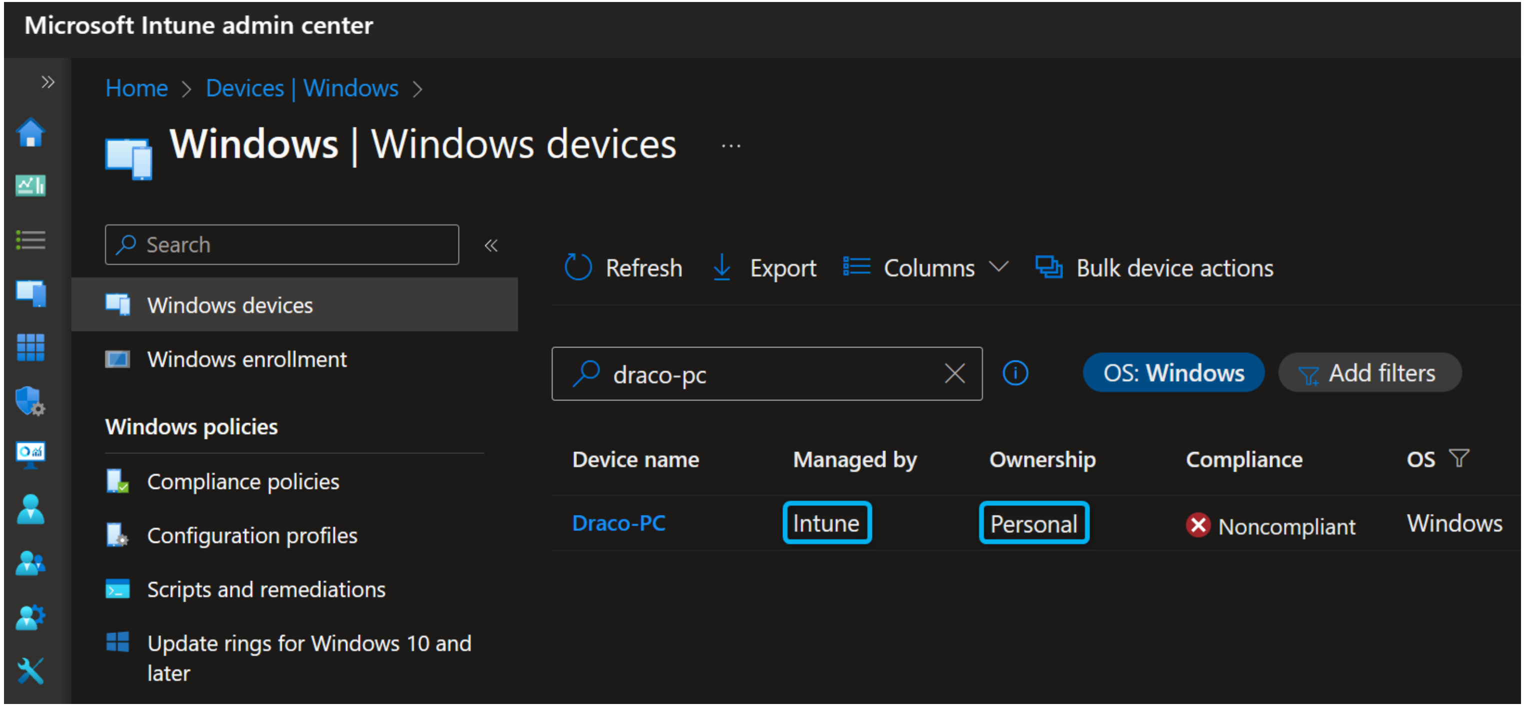


Stay signed in to all your apps

Windows will remember your account and automatically sign you in to your apps and websites on this device. You may need to let your organization manage some settings on your device.

☑ **Allow my organization to manage my device**

# Personal devices managed by Intune



Microsoft Intune admin center

Home > Devices | Windows >

## Windows | Windows devices ...

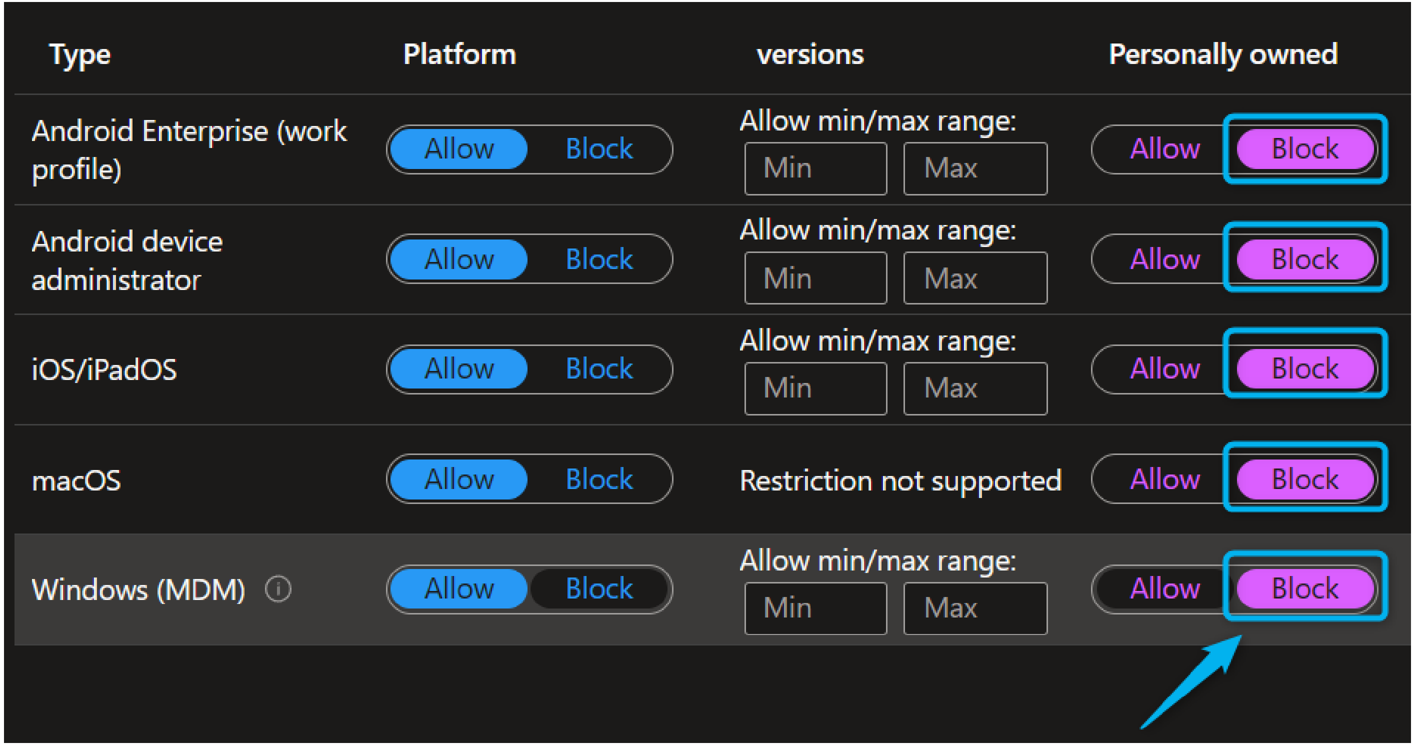
draco-pc

OS: Windows

Add filters

| Device name | Managed by | Ownership | Compliance | OS |
|---|---|---|---|---|
| Draco-PC | Intune | Personal | ✕ Noncompliant | Windows |

# Enrollment Restrictions

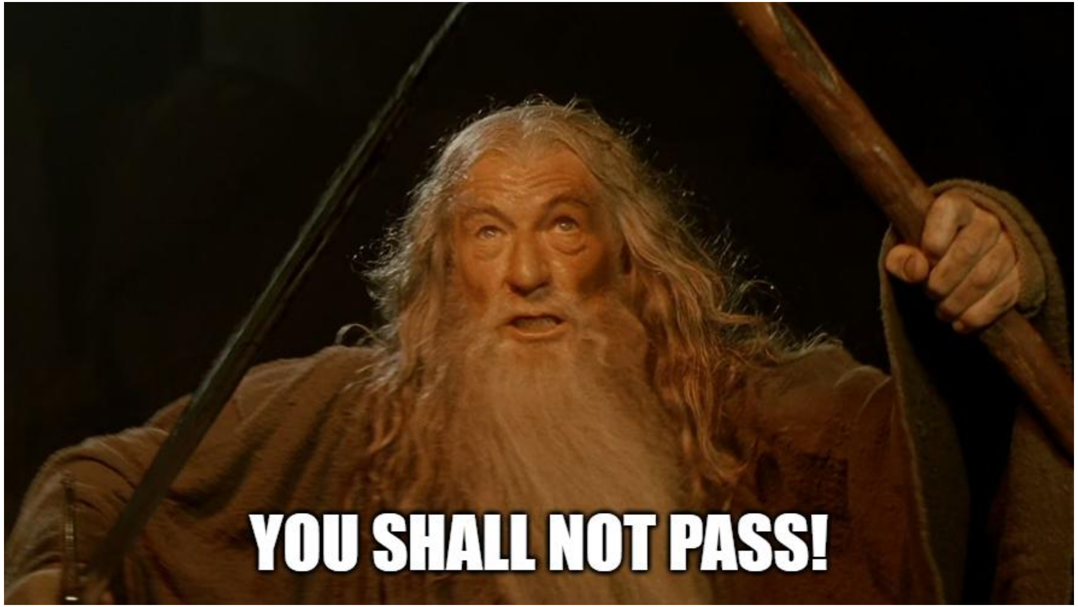


| Type | Platform | versions | Personally owned |
|---|---|---|---|
| Android Enterprise (work profile) | [✓ Allow] Block | Allow min/max range:<br>Min Max | Allow [✓ Block] |
| Android device administrator | [✓ Allow] Block | Allow min/max range:<br>Min Max | Allow [✓ Block] |
| iOS/iPadOS | [✓ Allow] Block | Allow min/max range:<br>Min Max | Allow [✓ Block] |
| macOS | [✓ Allow] Block | Restriction not supported | Allow [✓ Block] |
| Windows (MDM) ⓘ | [✓ Allow] Block | Allow min/max range:<br>Min Max | Allow [✓ Block] |

# Example of managing personal devices

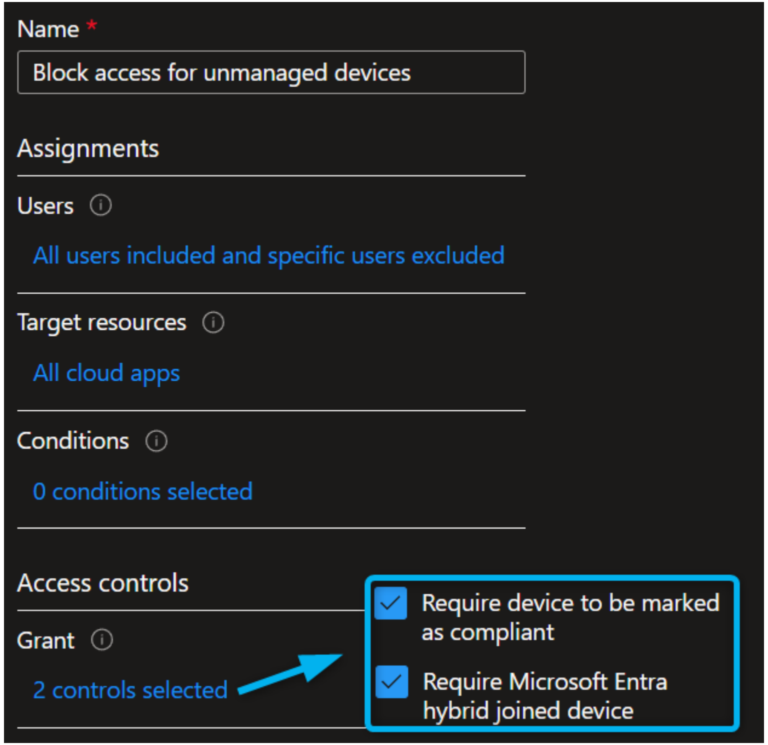
# Method 3: Block access

- Block access
- Reduces security risks
- Reduces user productivity



! High-security method but only suitable for some situations and organizations.

# Block Access with Conditional Access policy



Name *

Block access for unmanaged devices

Assignments

Users ⓘ

All users included and specific users excluded

Target resources ⓘ

All cloud apps

Conditions ⓘ

0 conditions selected

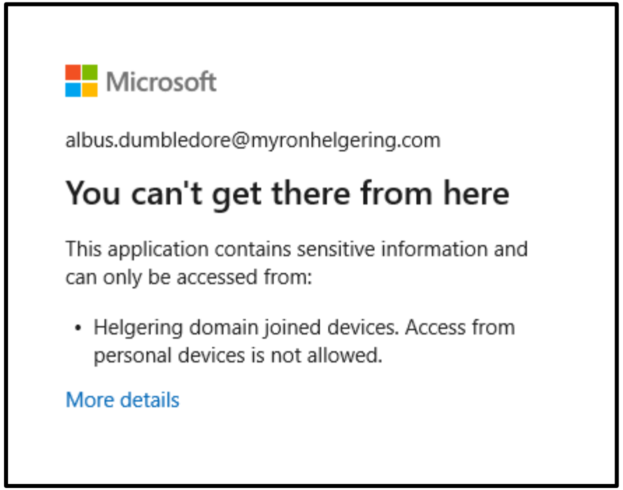
Access controls

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

# Some recommendations

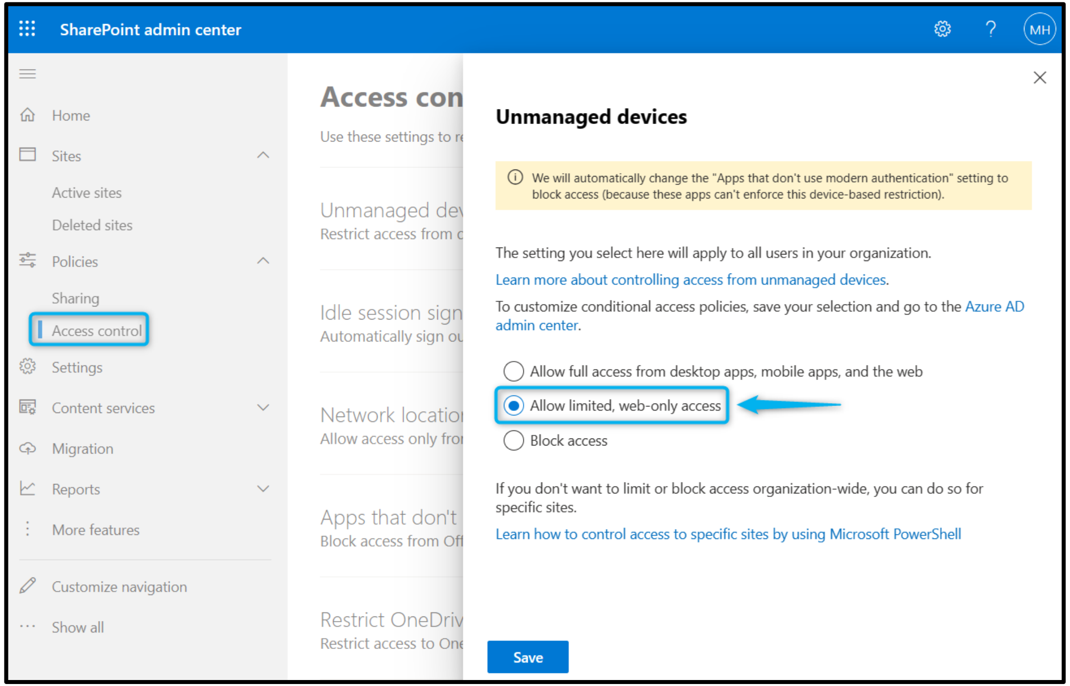
- Identify user groups working from unmanaged devices or locations such as VDI/RDS
- Exclude service and guest accounts?
- Decide which apps you want to target
- Enable Single Sign On (SSO) for third party browsers
- Always deploy your policies in pilot and/or report-only first

# Method 4: App Enforced Restrictions

- Enforces web-only access
- Restricts download, print & sync
- Supports SharePoint & Exchange Online
- Can target specific locations
- Troublesome configuration

✓ Balanced method with minimal features, but suitable for any company.

Enable in SharePoint Admin Center (or PowerShell)



## Unmanaged devices

ⓘ We will automatically change the "Apps that don't use modern authentication" setting to block access (because these apps can't enforce this device-based restriction).

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

Learn more about controlling access from unmanaged devices.

To customize conditional access policies, save your selection and go to the Azure AD admin center.

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

● Allow limited, web-only access

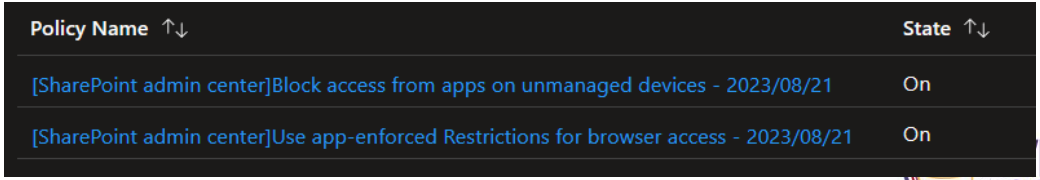
○ Block access

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

Save

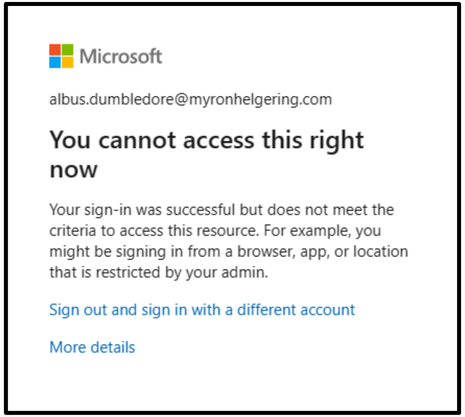
Conditional Access policies are created



| Policy Name ↑↓ | State ↑↓ |
|---|---|
| [SharePoint admin center]Block access from apps on unmanaged devices - 2023/08/21 | On |
| [SharePoint admin center]Use app-enforced Restrictions for browser access - 2023/08/21 | On |

## 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



Microsoft

albus.dumbledore@myronhelgering.com

You cannot access this right now

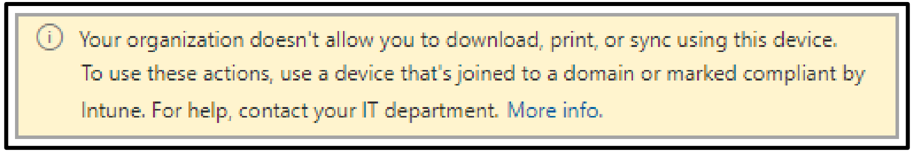
Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.

Sign out and sign in with a different account

More details

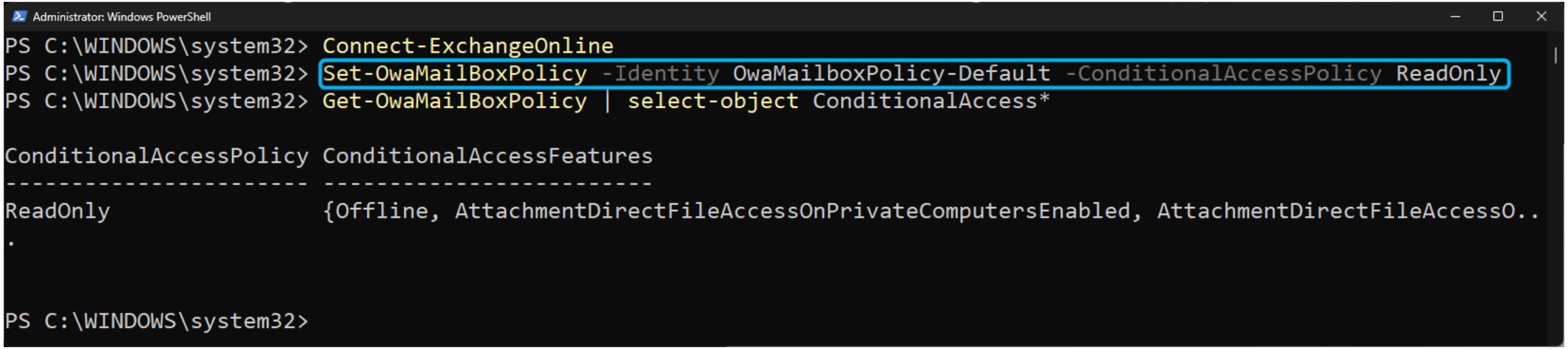
## Policy 2: Use app-enforced restrictions for browser access

- 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 with Powershell

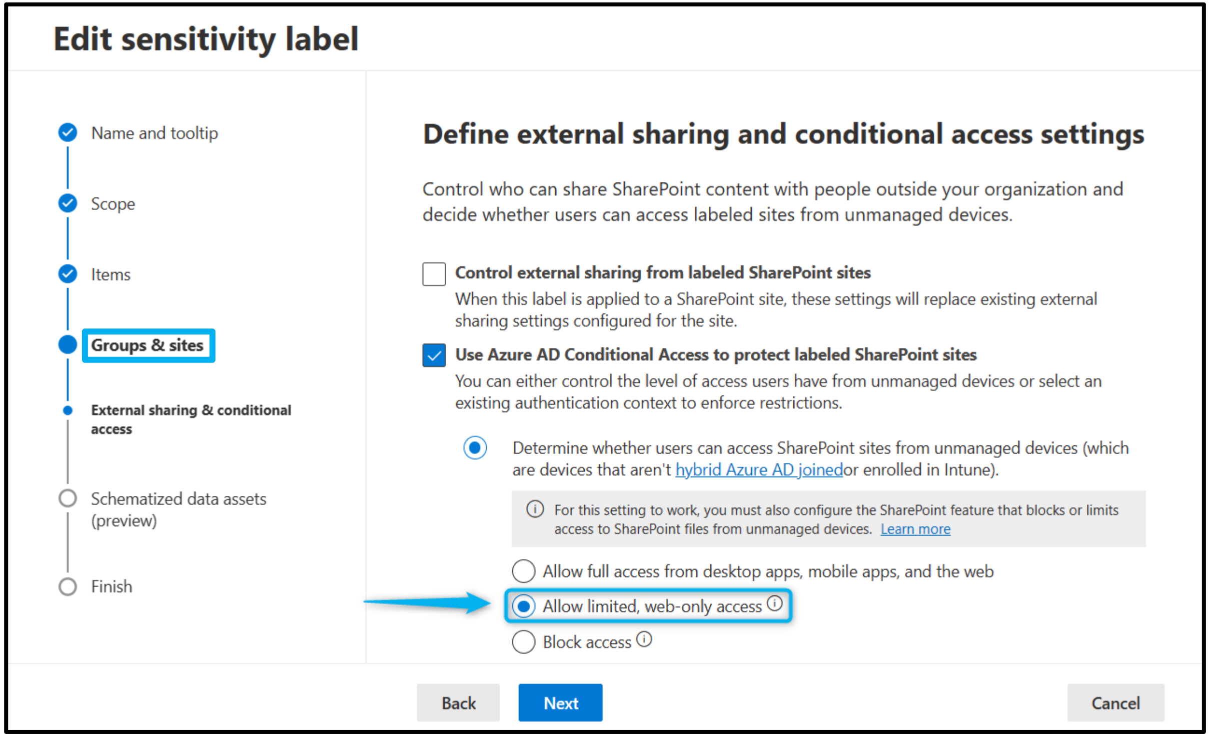


```
PS C:\WINDOWS\system32> Connect-ExchangeOnline
PS C:\WINDOWS\system32> Set-OwaMailBoxPolicy -Identity OwaMailboxPolicy-Default -ConditionalAccessPolicy ReadOnly
PS C:\WINDOWS\system32> Get-OwaMailBoxPolicy | select-object ConditionalAccess*

ConditionalAccessPolicy ConditionalAccessFeatures
----------------------- -------------------------
ReadOnly                {Offline, AttachmentDirectFileAccessOnPrivateComputersEnabled, AttachmentDirectFileAccessO..
.


PS C:\WINDOWS\system32>
```

Set-OwaMailBoxPolicy -Identity OwaMailboxPolicy-Default -ConditionalAccessPolicy ReadOnly

# Sensitivity Labels

- Target locations with sensitive data only
- Applies to M365 Groups, SharePoint Sites, and Teams



## Edit sensitivity label

✓ Name and tooltip
✓ Scope
✓ Items
● Groups & sites
● External sharing & conditional access
○ Schematized data assets (preview)
○ 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 Azure AD 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 hybrid Azure AD joinedor enrolled in Intune).

ⓘ 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 ⓘ

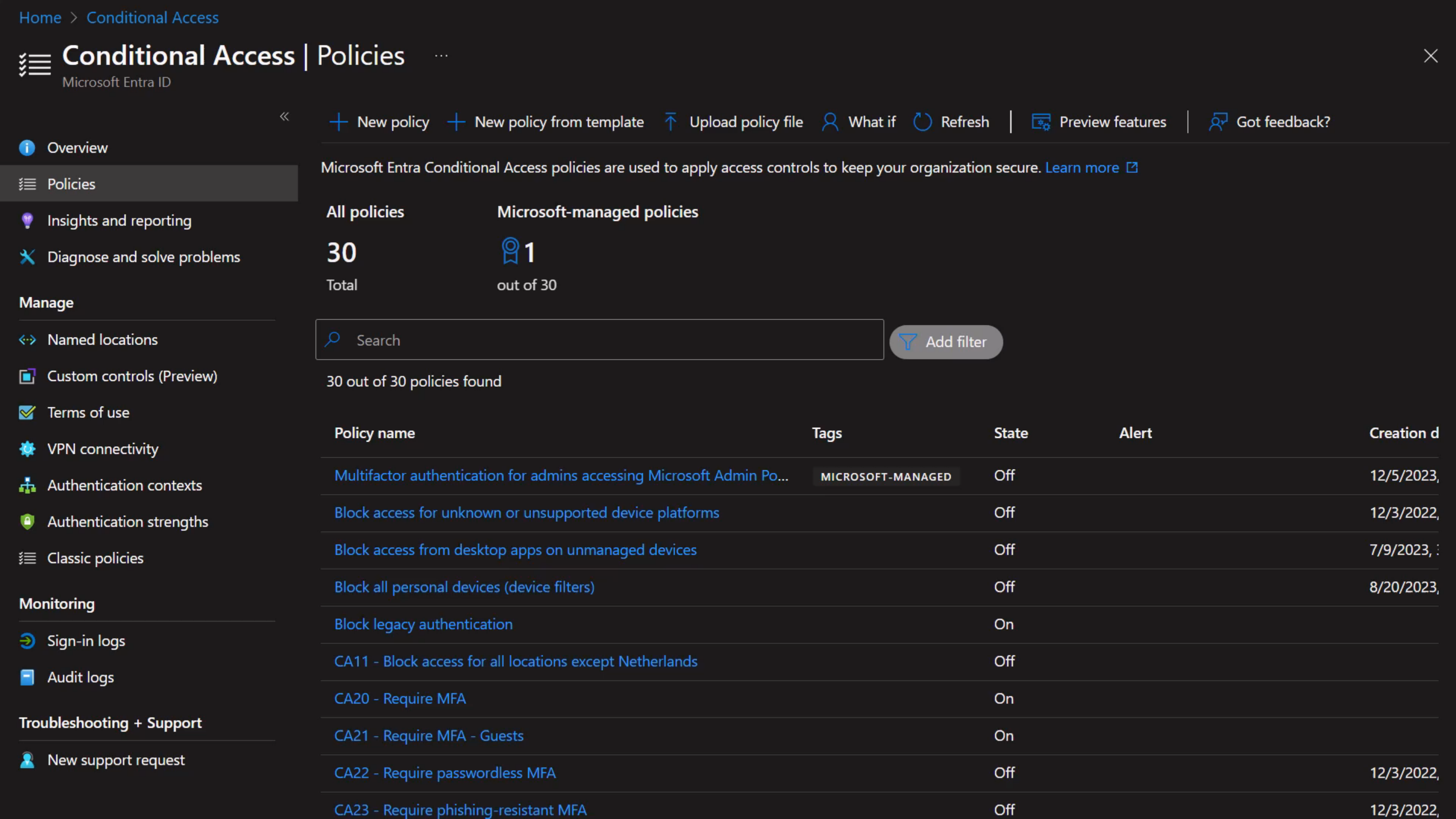
○ Block access ⓘ

# Method 5: Session Policies

- Applies web restrictions through a reverse proxy
- Restricts download, upload, print, cut/copy, paste, and more!
- Supports Microsoft 365 and third-party cloud apps

✓ Great method for many different scenarios but comes with a price tag.

# Demo: Session Policies with Microsoft Defender for Cloud Apps



Conditional Access | Policies

Microsoft Entra ID

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more

All policies

30

Total

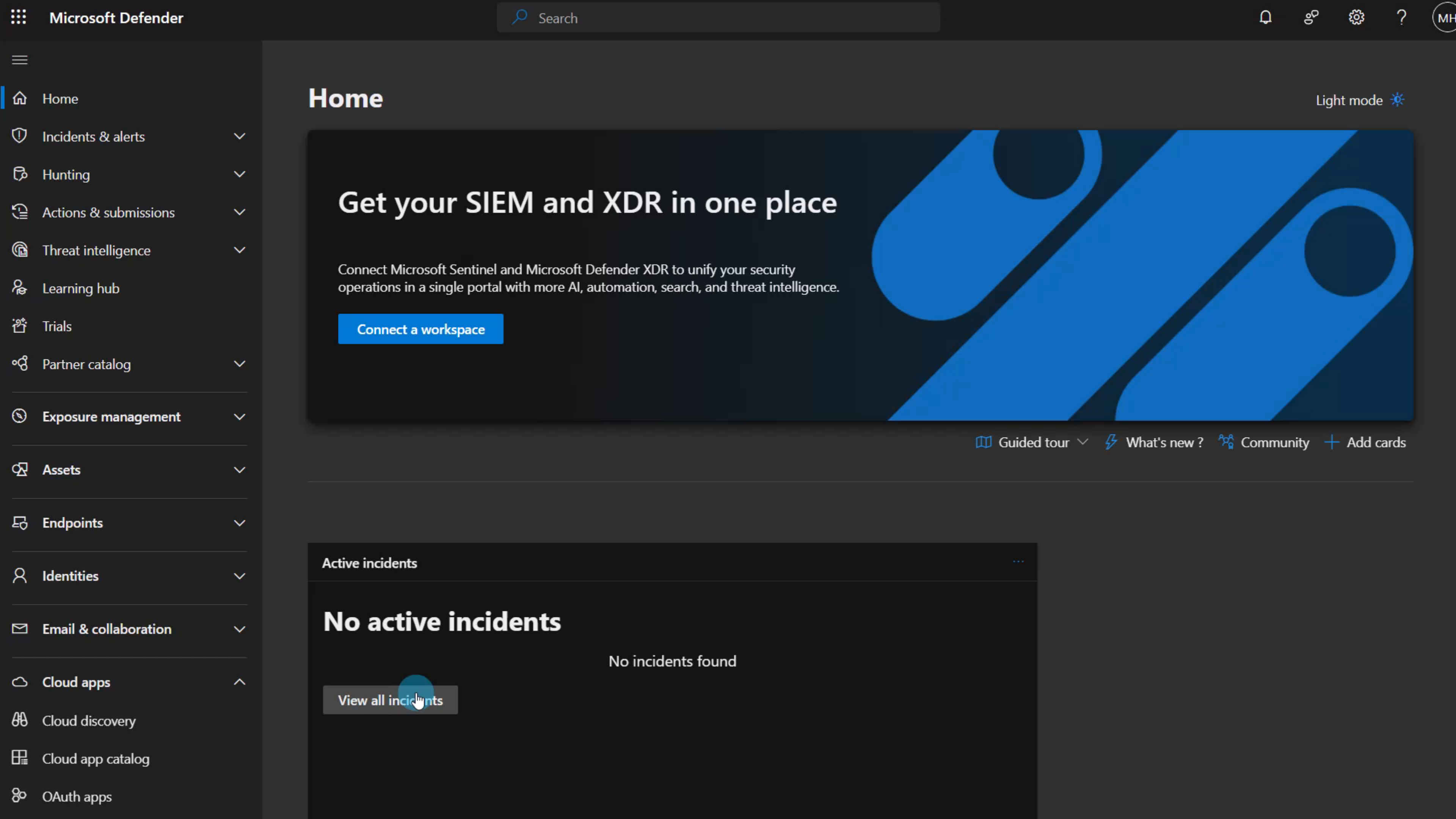
Microsoft-managed policies

1

out of 30

30 out of 30 policies found

| Policy name | Tags | State | Alert | Creation d |
|---|---|---|---|---|
| Multifactor authentication for admins accessing Microsoft Admin Po... | MICROSOFT-MANAGED | Off | | 12/5/2023, |
| Block access for unknown or unsupported device platforms | | Off | | 12/3/2022, |
| Block access from desktop apps on unmanaged devices | | Off | | 7/9/2023, |
| Block all personal devices (device filters) | | Off | | 8/20/2023, |
| Block legacy authentication | | On | | |
| CA11 - Block access for all locations except Netherlands | | Off | | |
| CA20 - Require MFA | | On | | |
| CA21 - Require MFA - Guests | | On | | |
| CA22 - Require passwordless MFA | | Off | | 12/3/2022, |
| CA23 - Require phishing-resistant MFA | | Off | | 12/3/2022, |



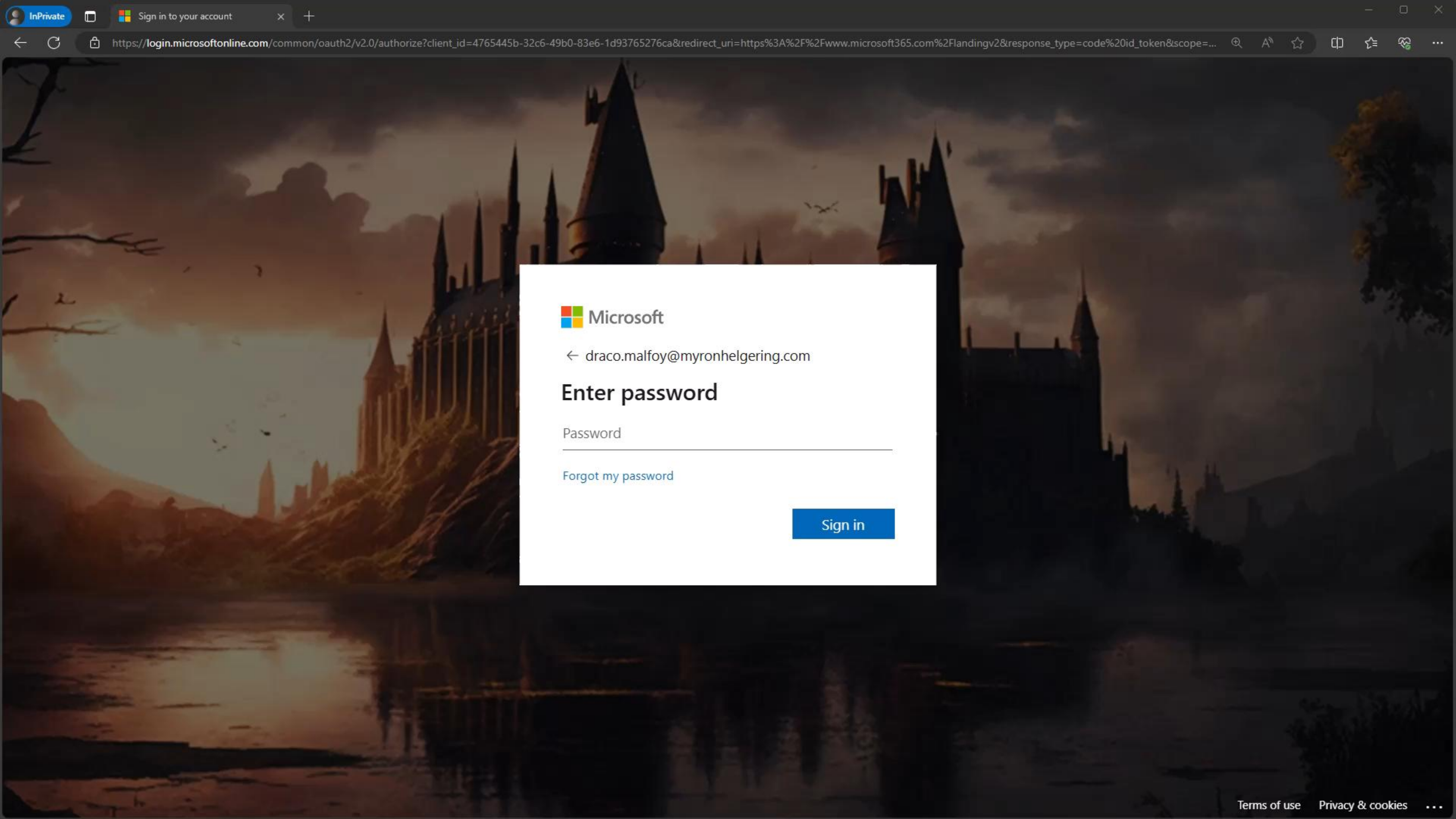
Home

Get your SIEM and XDR in one place

Connect Microsoft Sentinel and Microsoft Defender XDR to unify your security operations in a single portal with more AI, automation, search, and threat intelligence.

No active incidents

No incidents found



https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A%2F%2Fwww.microsoft365.com%2Flandingv2&response_type=code%20id_token&scope=...

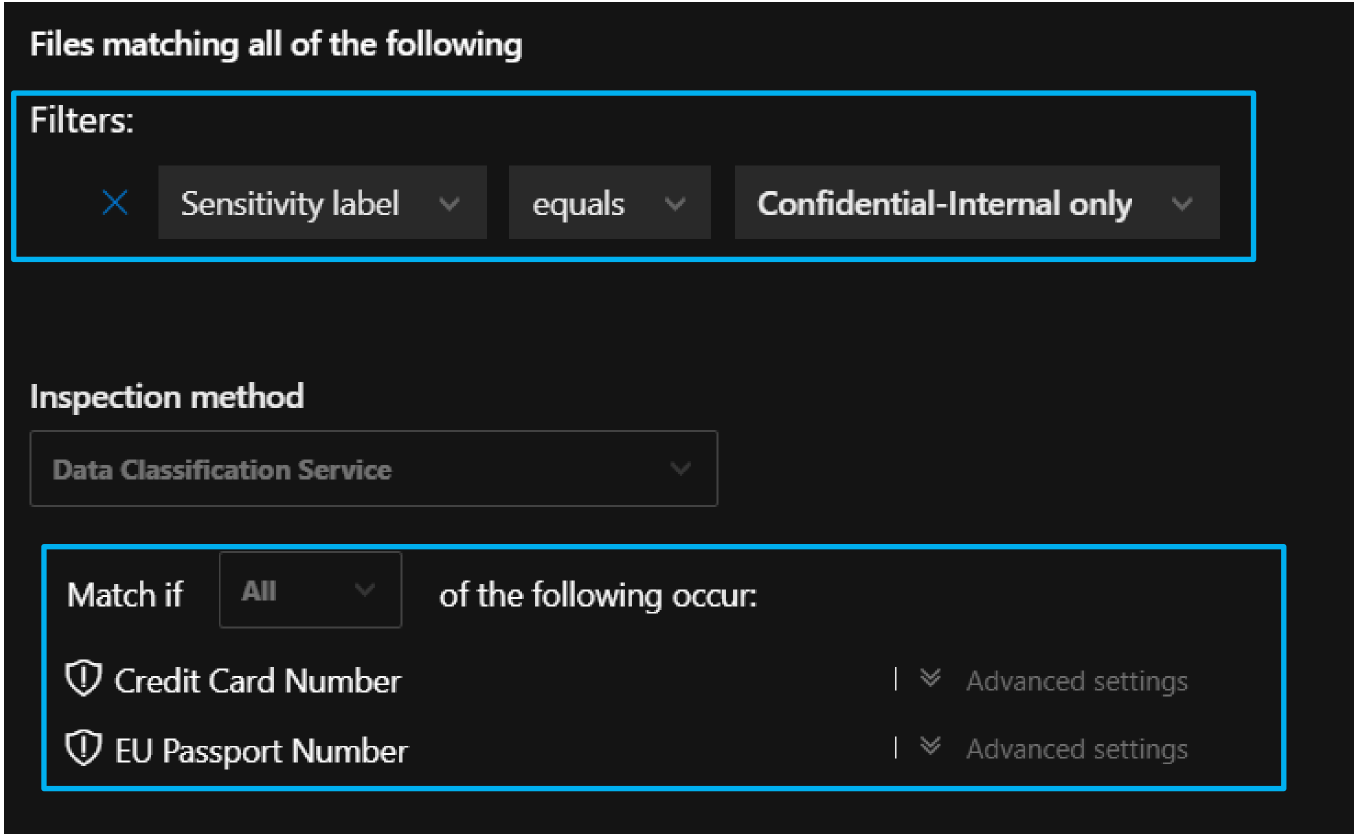
Microsoft

← draco.malfoy@myronhelgering.com

Enter password

Password

# Block only if data is sensitive



Files matching all of the following

Filters:

Sensitivity label equals Confidential-Internal only

Inspection method

Data Classification Service

Match if All of the following occur:

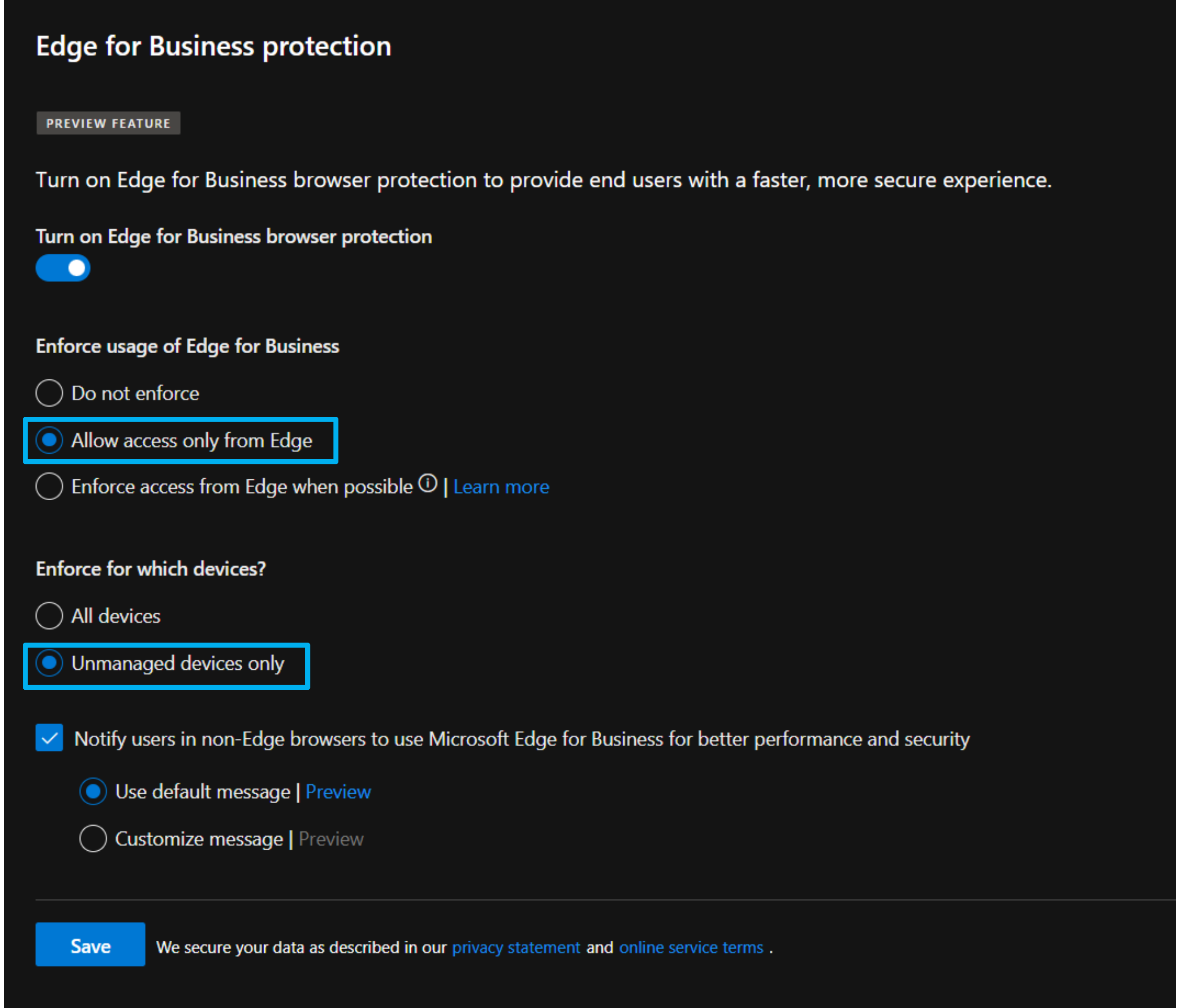
- Credit Card Number — Advanced settings
- EU Passport Number — Advanced settings

TECH EVENTS WITH PERSPECTIVE

General

# Two ways of protection with session policies

| Reverse proxy (Default) | In-browser protection (Preview) |
|---|---|
| All browsers and operating systems | Edge with Windows 10/11 or MacOS |
| No user interaction needed | Requires Edge profile sign in |
| Slower user experience | Faster user experience |
| Easier to bypass controls (dev tools) | Harder to bypass controls (dev tools) |
| Less secure (doesn’t support MAM) | More secure (supports MAM) |
| Supports all restrictions | Doesn’t support all restrictions yet |



## 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

We secure your data as described in our privacy statement and online service terms .

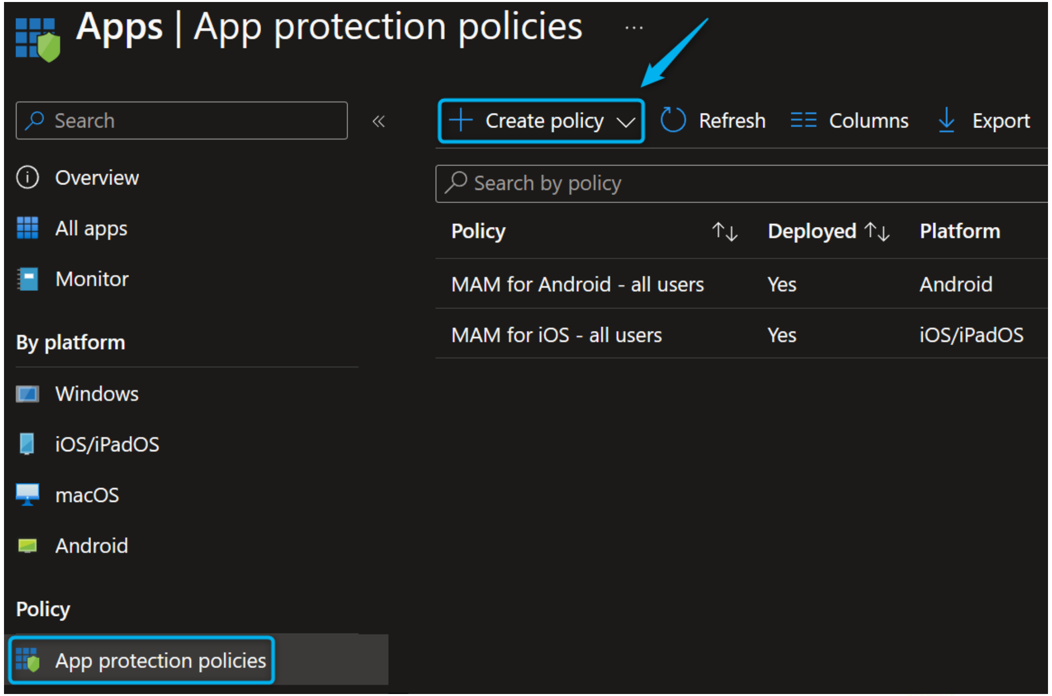
# Method 6: App protection policies

- Manage and wipe corporate data through managed apps
- Apply data protection controls
- Enforce secure authentication
- Ensure device compliance
- Android, iOS & Windows only

✓ Great method with many security features, especially for Android and iOS devices.

# App protection policies for Android & iOS

- No copy/paste between apps
- No printing or downloading
- No screenshots
- Encrypt app data
- Secure authentication (PIN/biometric)
- Set device conditions such as minimum OS or app version

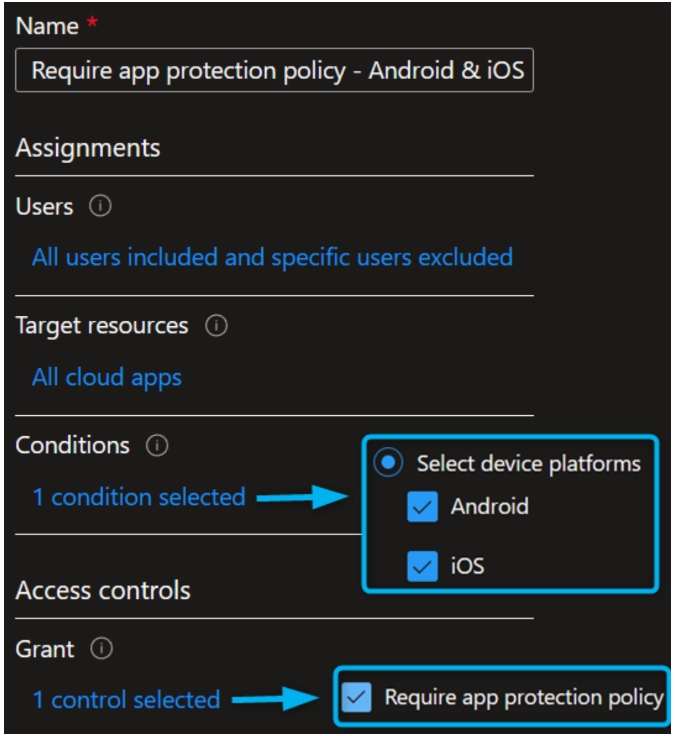


Apps | App protection policies

| Policy | Deployed | Platform |
|---|---|---|
| MAM for Android - all users | Yes | Android |
| MAM for iOS - all users | Yes | iOS/iPadOS |

# Require app protection policy with Conditional Access

- Authenticator app for iOS
- Company Portal app for Android



Name *

Require app protection policy - Android & iOS

Assignments

Users ⓘ

All users included and specific users excluded

Target resources ⓘ

All cloud apps

Conditions ⓘ

1 condition selected →

● Select device platforms

☑ Android

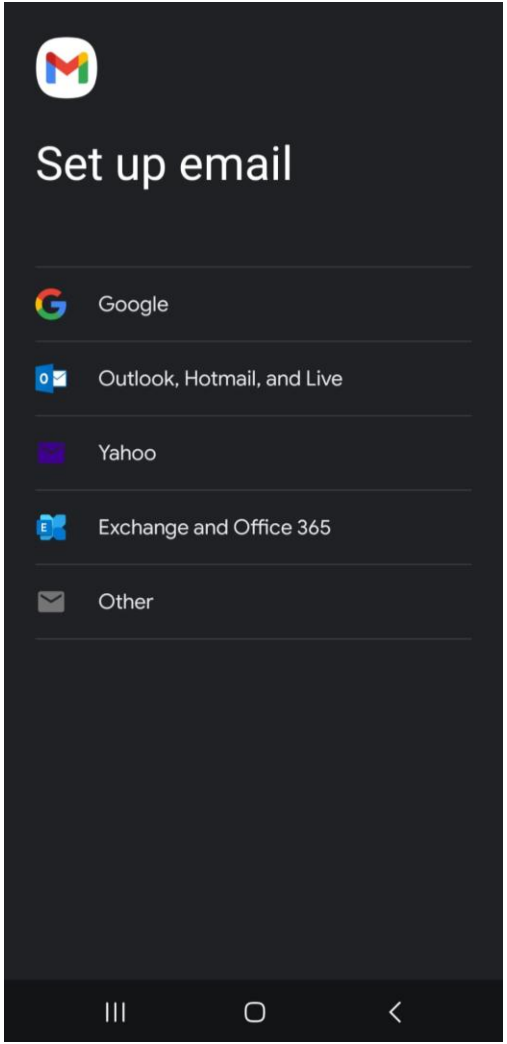
☑ iOS

Access controls

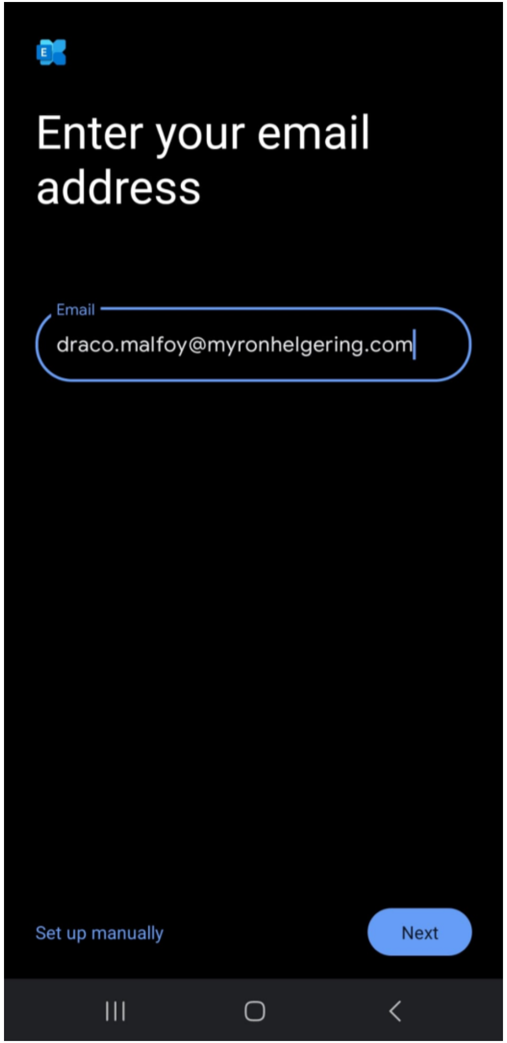
Grant ⓘ

1 control selected →

☑ Require app protection policy

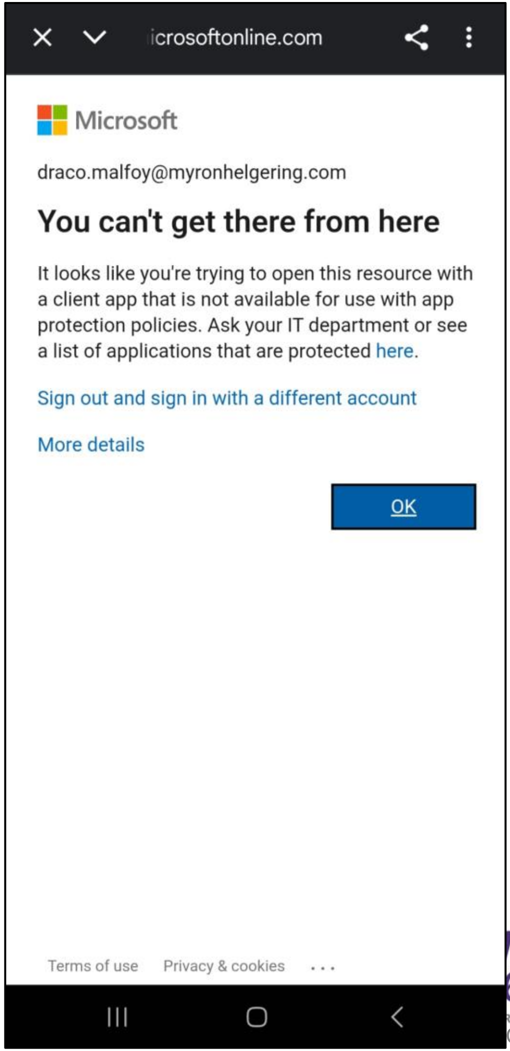


Set up email



Enter your email address

Email: draco.malfoy@myronhelgering.com



icrosoftonline.com

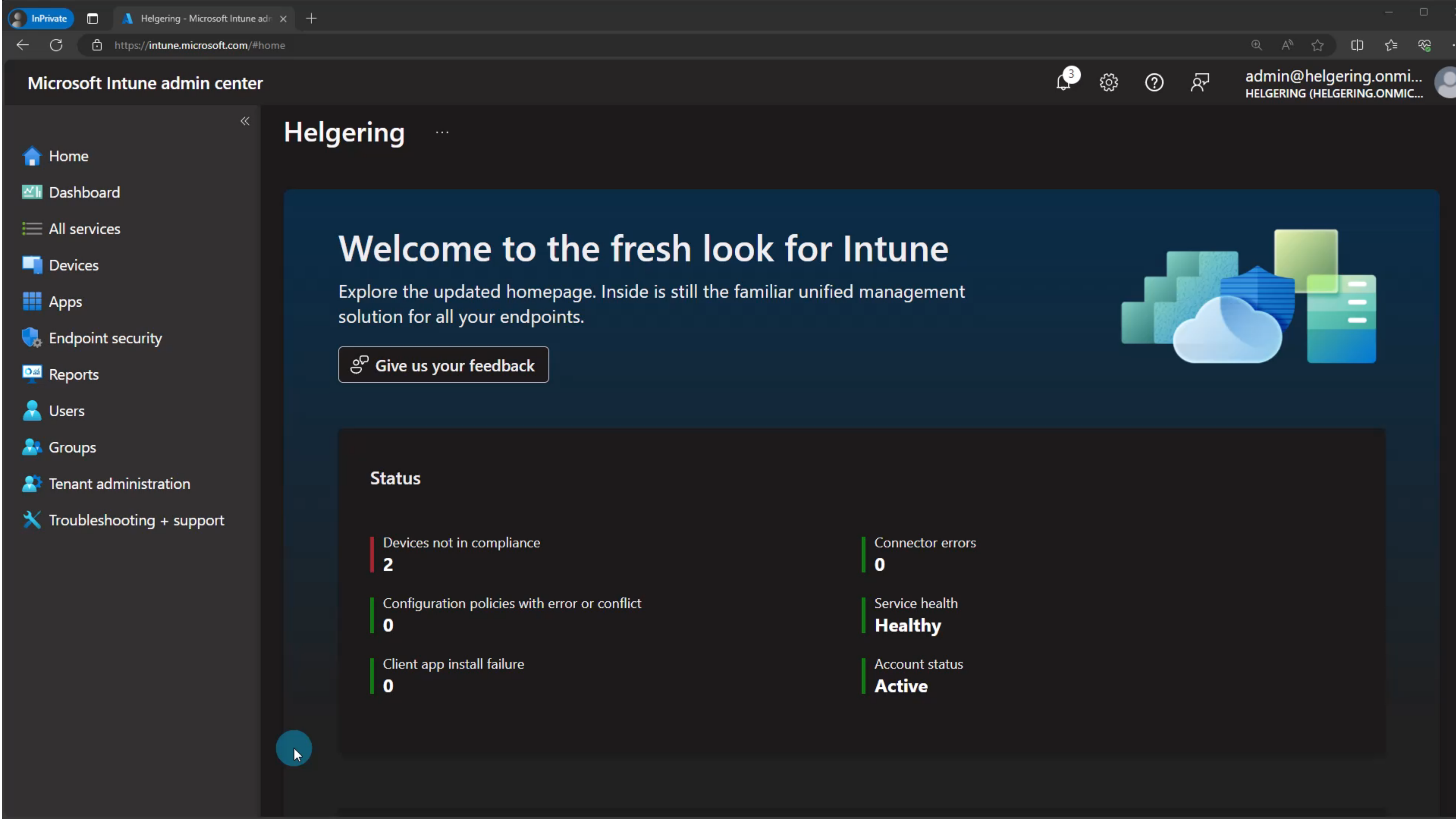
Microsoft

draco.malfoy@myronhelgering.com

You can't get there from here

It looks like you're trying to open this resource with a client app that is not available for use with app protection policies. Ask your IT department or see a list of applications that are protected here.

# Demo: Mobile Application Management (MAM) for Windows


InPrivate
Helgering - Microsoft Intune adr
https://intune.microsoft.com/#home
Microsoft Intune admin center
3
admin@helgering.onmi...
HELGERING (HELGERING.ONMIC...
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

# Helgering

## Welcome to the fresh look for Intune

Explore the updated homepage. Inside is still the familiar unified management solution for all your endpoints.

### Status

Devices not in compliance
**2**

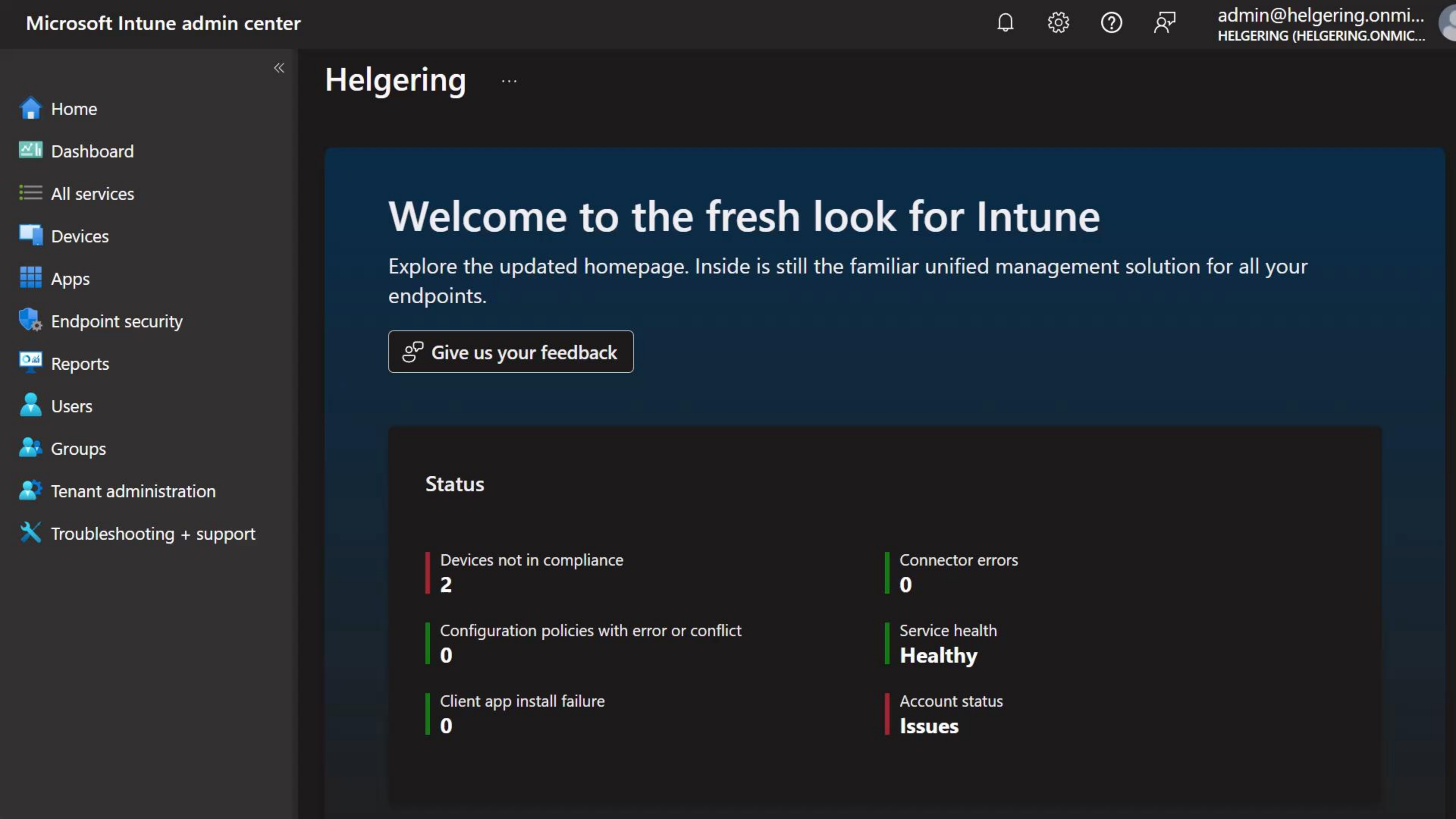
Connector errors
**0**

Configuration policies with error or conflict
**0**

Service health
**Healthy**

Client app install failure
**0**

Account status
**Active**



Welcome to the fresh look for Intune

Explore the updated homepage. Inside is still the familiar unified management solution for all your endpoints.

Status

Devices not in compliance
2

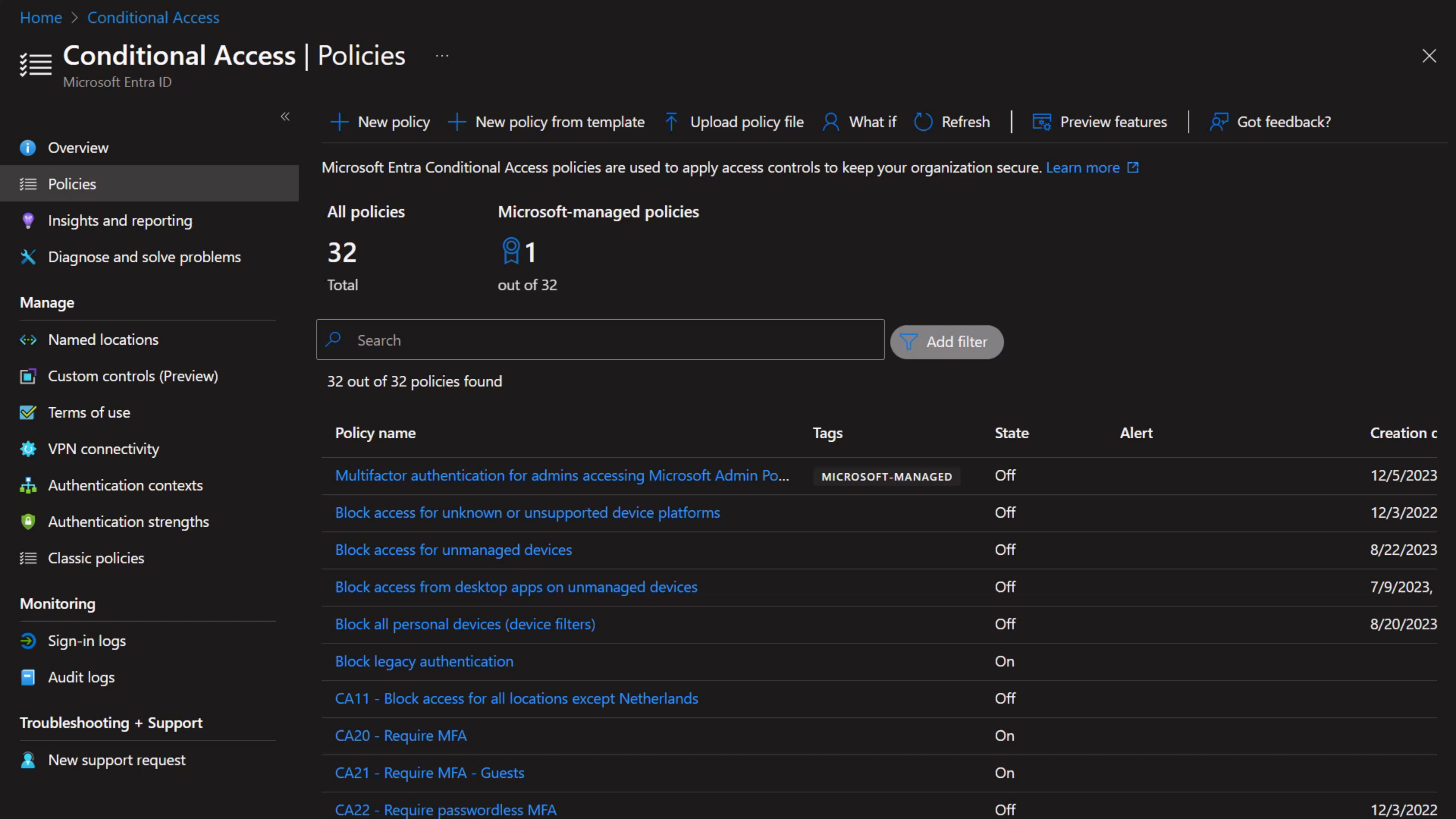
Configuration policies with error or conflict
0

Client app install failure
0

Connector errors
0

Service health
Healthy

Account status
Issues



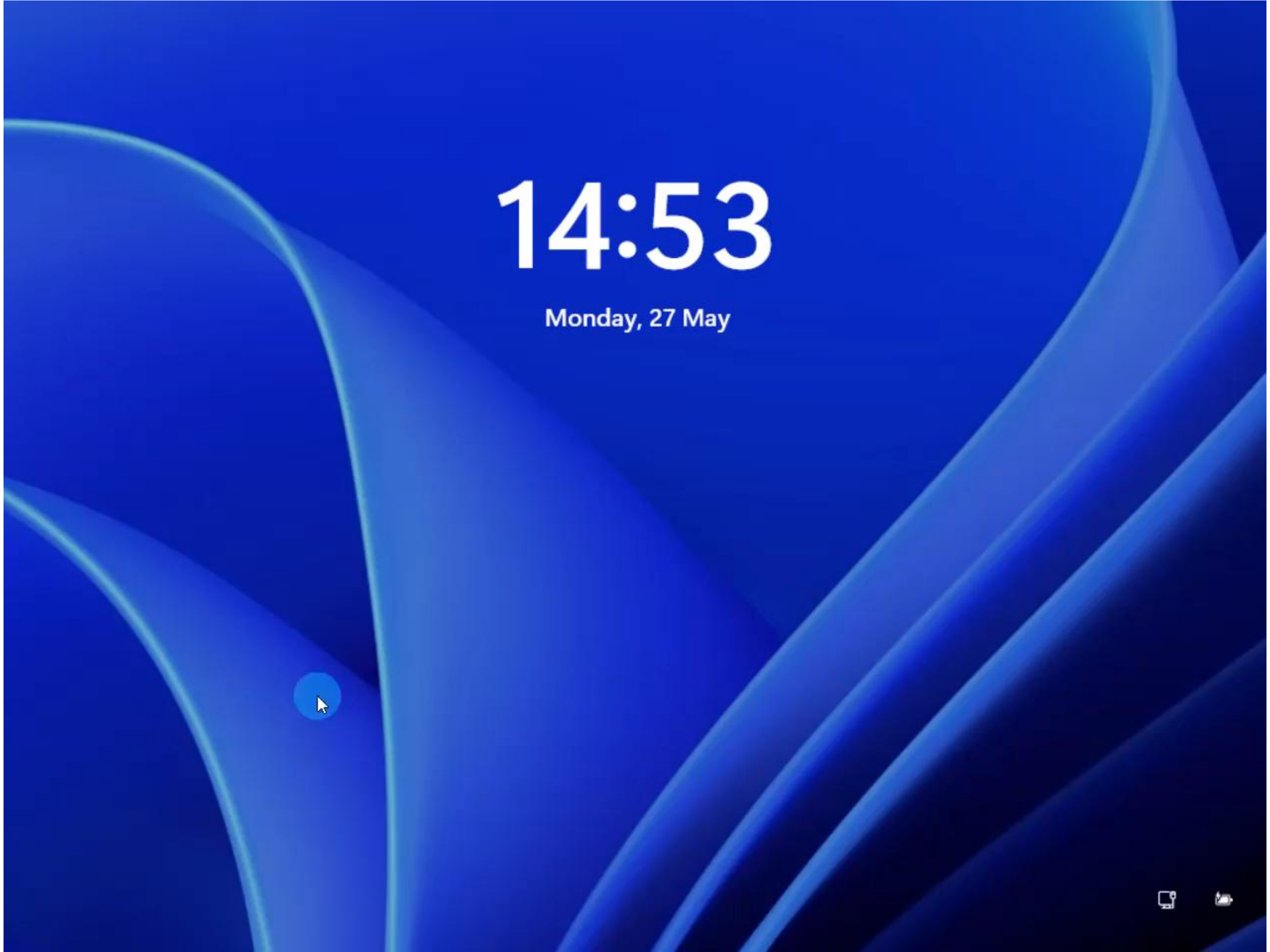
Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more

All policies
32
Total

Microsoft-managed policies
1
out of 32

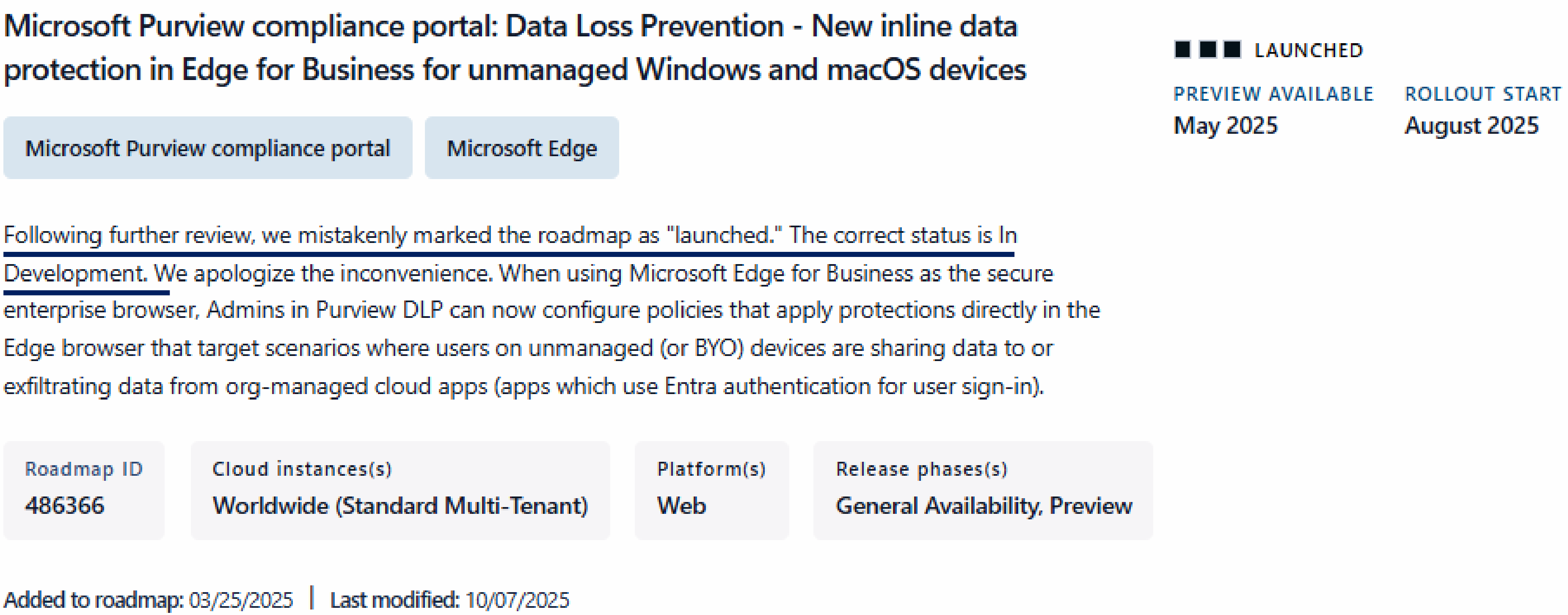
32 out of 32 policies found

| Policy name | Tags | State | Alert | Creation c |
|---|---|---|---|---|
| Multifactor authentication for admins accessing Microsoft Admin Po... | MICROSOFT-MANAGED | Off | | 12/5/2023 |
| Block access for unknown or unsupported device platforms | | Off | | 12/3/2022 |
| Block access for unmanaged devices | | Off | | 8/22/2023 |
| Block access from desktop apps on unmanaged devices | | Off | | 7/9/2023, |
| Block all personal devices (device filters) | | Off | | 8/20/2023 |
| Block legacy authentication | | On | | |
| CA11 - Block access for all locations except Netherlands | | Off | | |
| CA20 - Require MFA | | On | | |
| CA21 - Require MFA - Guests | | On | | |
| CA22 - Require passwordless MFA | | Off | | 12/3/2022 |


14:53
Monday, 27 May

# What to expect in the future?

LIVE! 360
TECH EVENTS WITH PERSPECTIVE



## Microsoft Purview compliance portal: Data Loss Prevention - New inline data protection in Edge for Business for unmanaged Windows and macOS devices

■■■ LAUNCHED

| PREVIEW AVAILABLE | ROLLOUT START |
|---|---|
| May 2025 | August 2025 |

Microsoft Purview compliance portal

Microsoft Edge

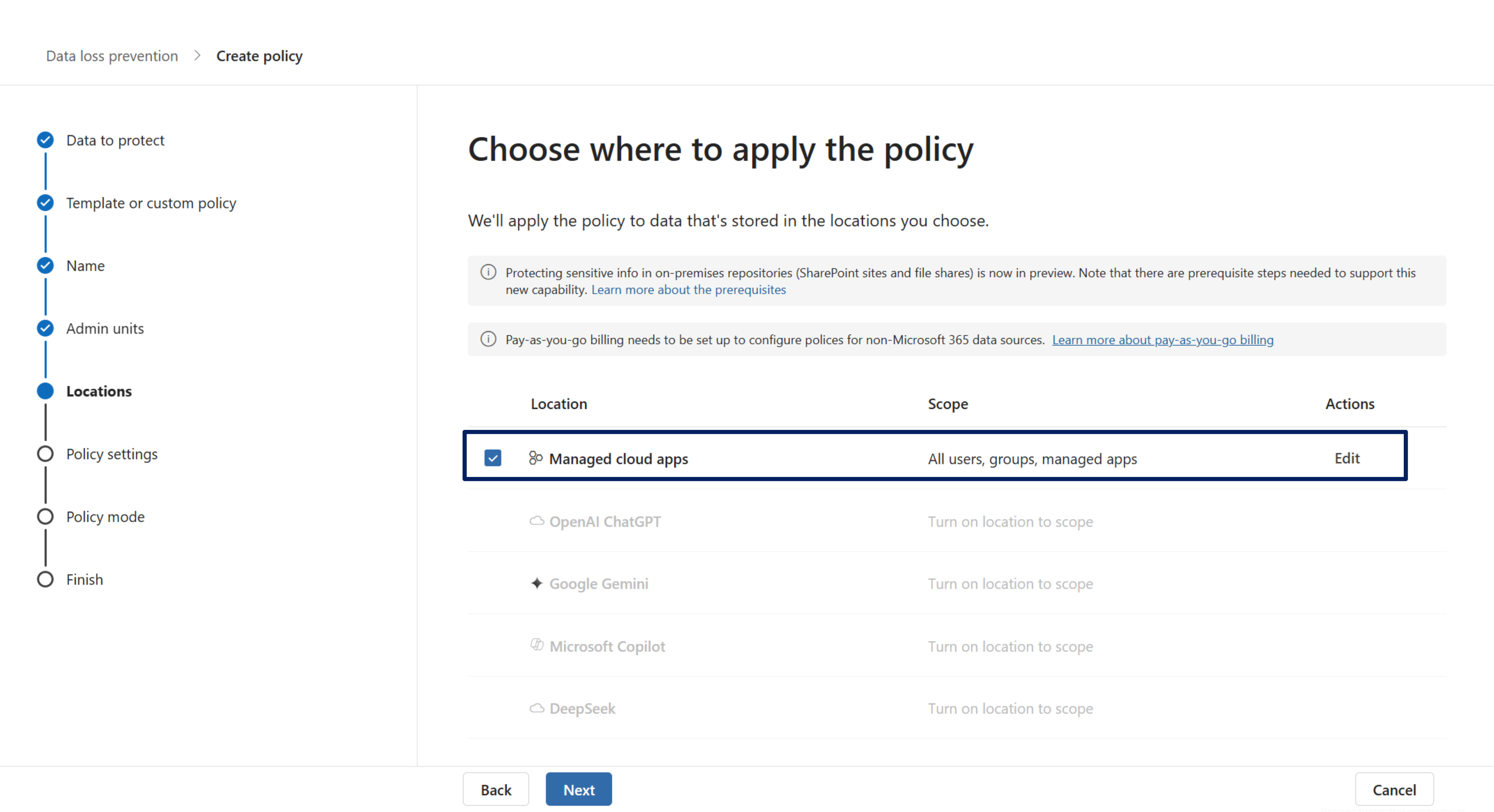
Following further review, we mistakenly marked the roadmap as "launched." The correct status is In Development. We apologize the inconvenience. When using Microsoft Edge for Business as the secure enterprise browser, Admins in Purview DLP can now configure policies that apply protections directly in the Edge browser that target scenarios where users on unmanaged (or BYO) devices are sharing data to or exfiltrating data from org-managed cloud apps (apps which use Entra authentication for user sign-in).

| Roadmap ID | Cloud instances(s) | Platform(s) | Release phases(s) |
|---|---|---|---|
| 486366 | Worldwide (Standard Multi-Tenant) | Web | General Availability, Preview |

**Added to roadmap:** 03/25/2025 | **Last modified:** 10/07/2025

# Requirements

- Enable (or require) in-browser protection
- Conditional Access policy with App Control



Data loss prevention > **Create policy**

- ✓ Data to protect
- ✓ Template or custom policy
- ✓ Name
- ✓ Admin units
- ● **Locations**
- ○ Policy settings
- ○ Policy mode
- ○ Finish

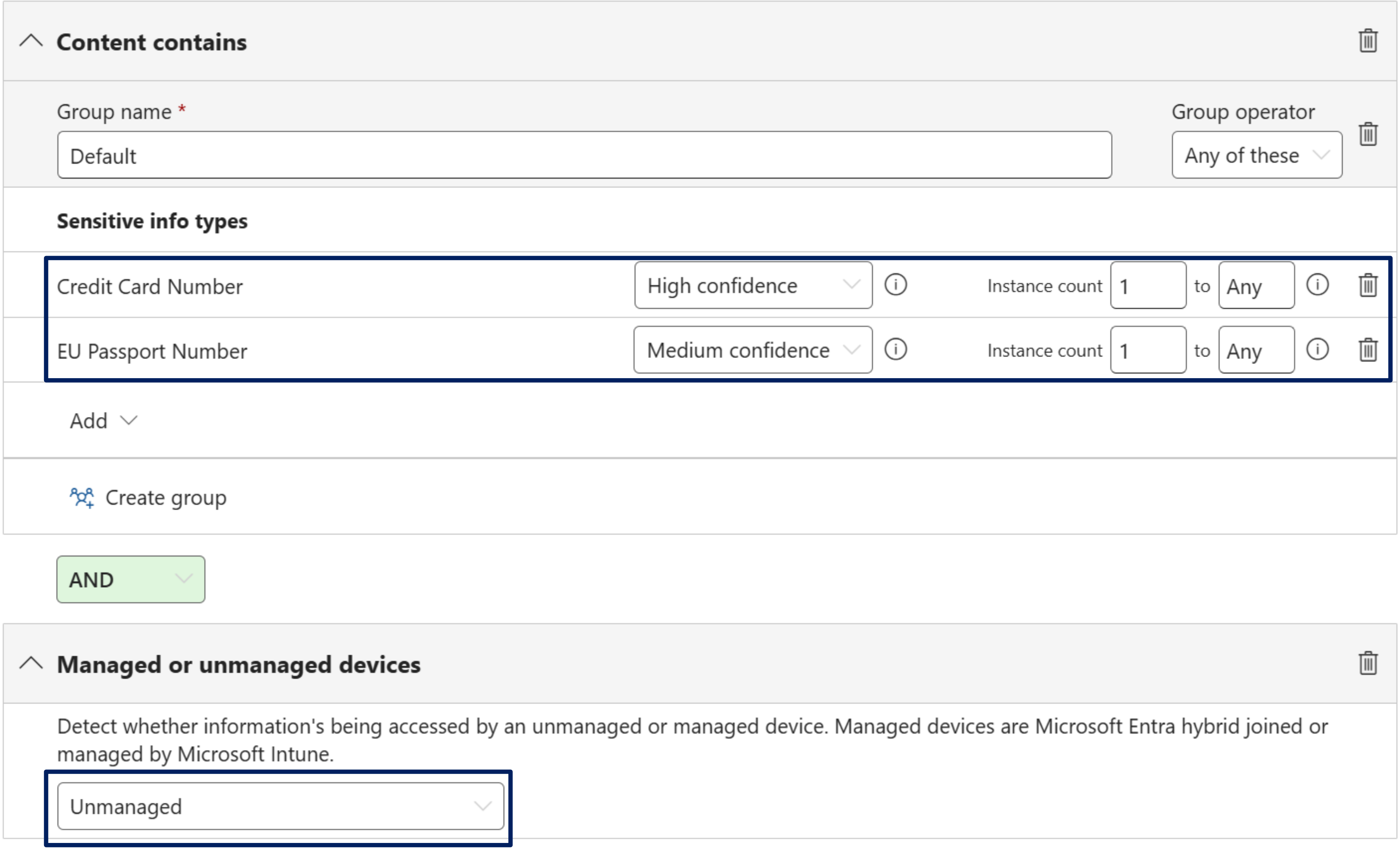
# Choose where to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

ⓘ Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. Learn more about the prerequisites

ⓘ Pay-as-you-go billing needs to be set up to configure polices for non-Microsoft 365 data sources. Learn more about pay-as-you-go billing

| | Location | Scope | Actions |
|---|---|---|---|
| ☑ | **Managed cloud apps** | All users, groups, managed apps | Edit |
| | OpenAI ChatGPT | Turn on location to scope | |
| | Google Gemini | Turn on location to scope | |
| | Microsoft Copilot | Turn on location to scope | |
| | DeepSeek | Turn on location to scope | |



**Content contains**

Group name *

Default

Group operator

Any of these

**Sensitive info types**

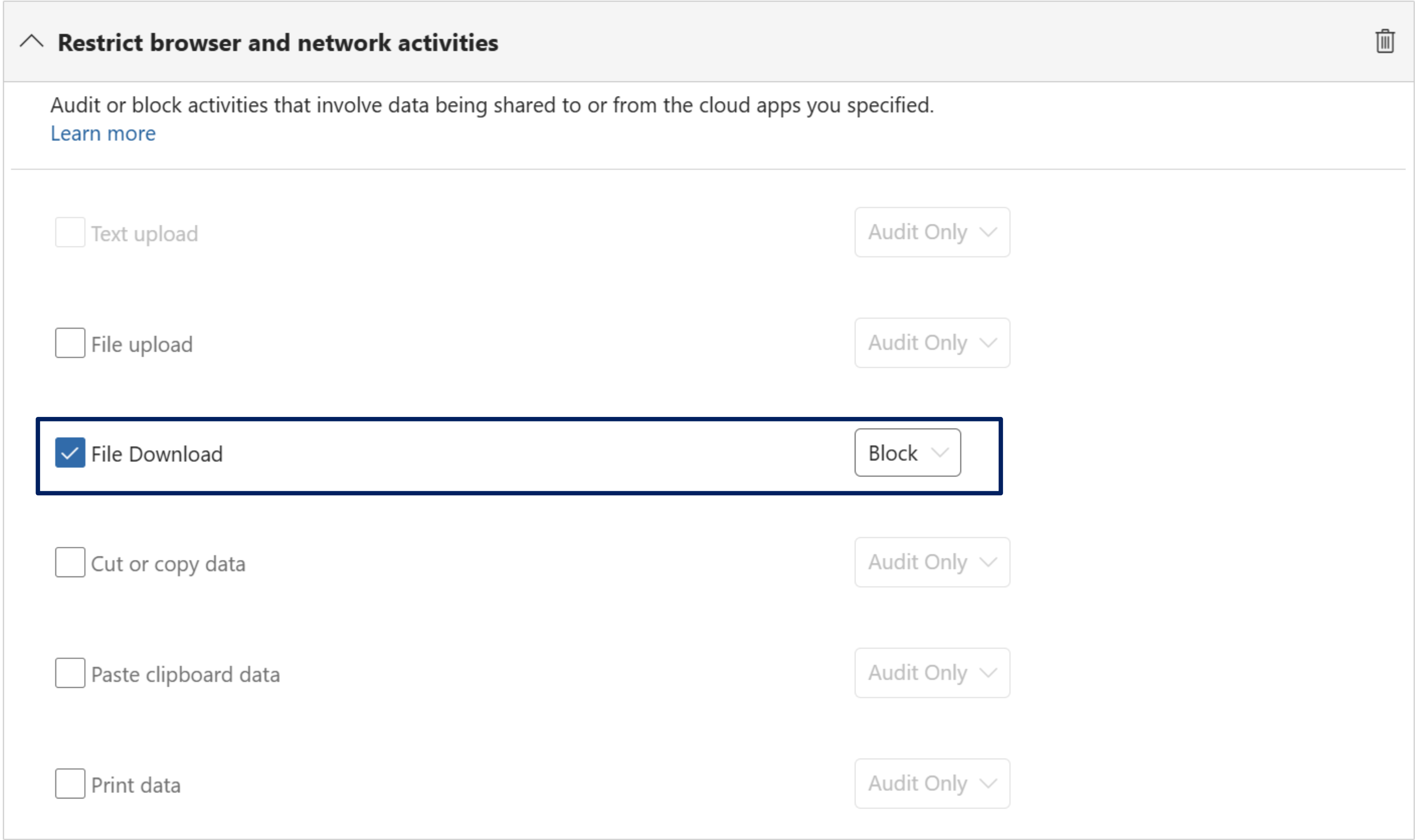
| | | | | |
|---|---|---|---|---|
| Credit Card Number | High confidence | Instance count 1 | to | Any |
| EU Passport Number | Medium confidence | Instance count 1 | to | Any |

AND

**Managed or unmanaged devices**

Detect whether information's being accessed by an unmanaged or managed device. Managed devices are Microsoft Entra hybrid joined or managed by Microsoft Intune.

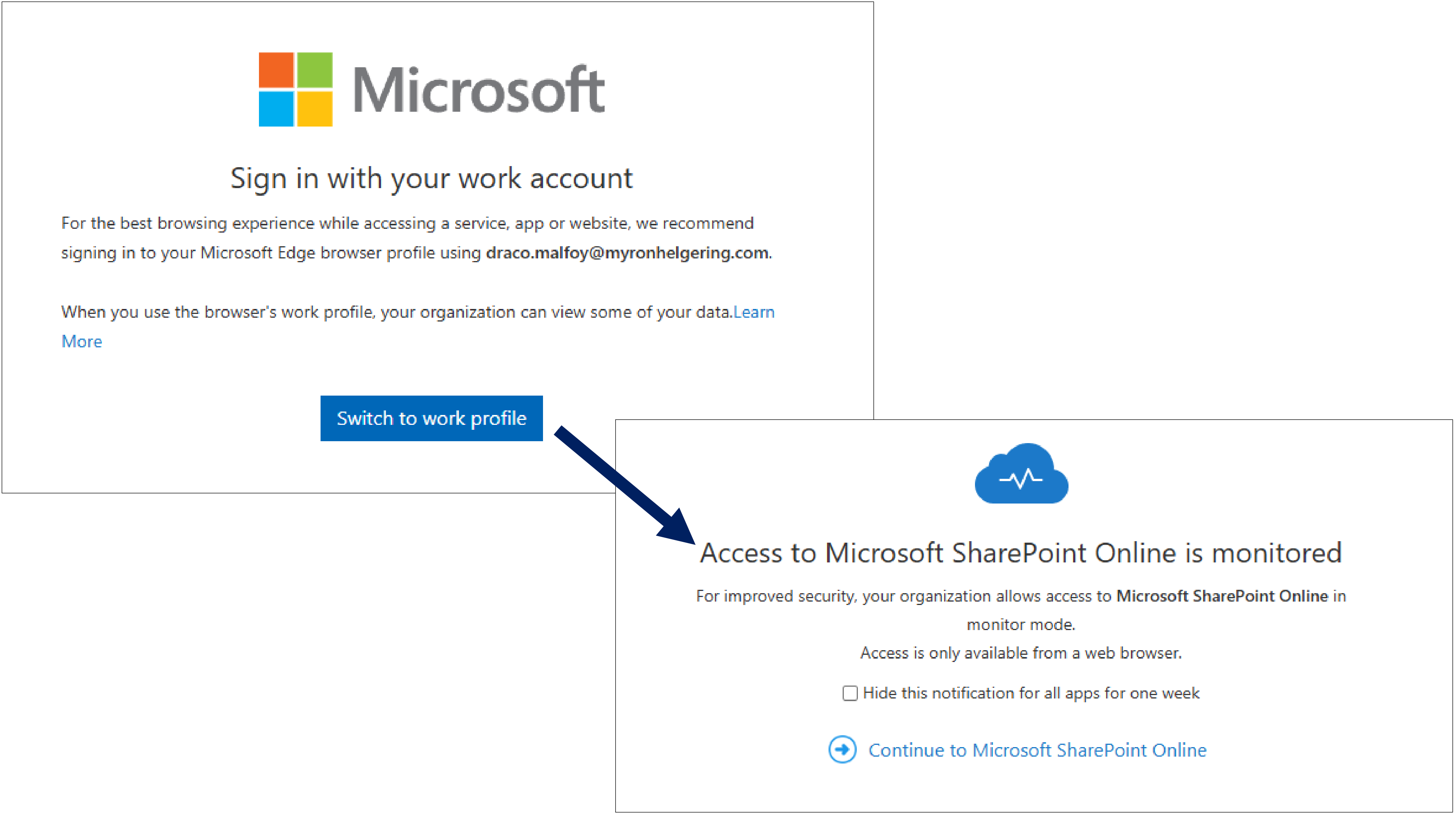
Unmanaged



## Restrict browser and network activities

Audit or block activities that involve data being shared to or from the cloud apps you specified.
Learn more

| | |
|---|---|
| ☐ Text upload | Audit Only |
| ☐ File upload | Audit Only |
| ☑ File Download | Block |
| ☐ Cut or copy data | Audit Only |
| ☐ Paste clipboard data | Audit Only |
| ☐ Print data | Audit Only |



Sign in with your work account

For the best browsing experience while accessing a service, app or website, we recommend signing in to your Microsoft Edge browser profile using **draco.malfoy@myronhelgering.com**.

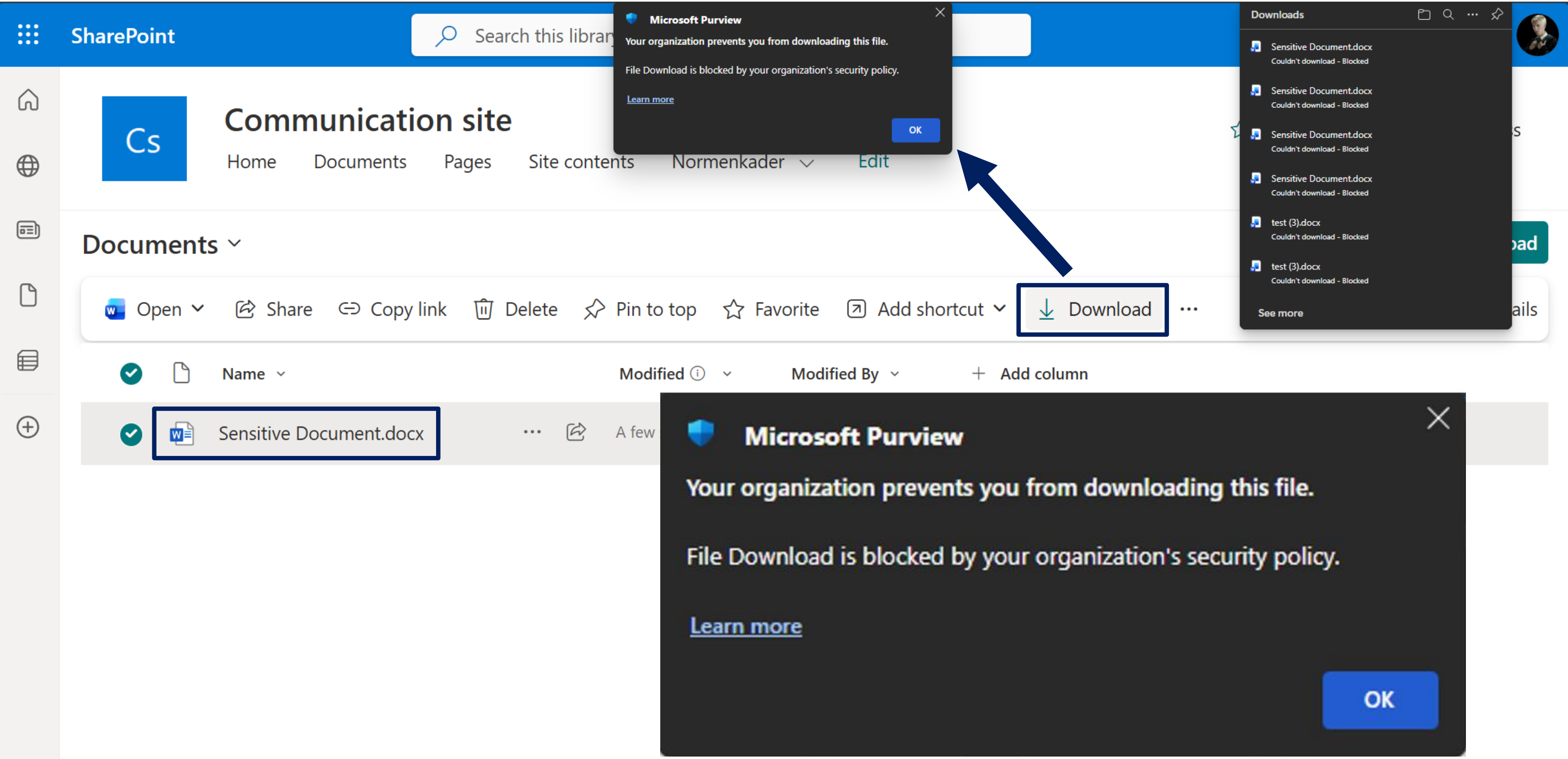
When you use the browser's work profile, your organization can view some of your data.Learn More

Access to Microsoft SharePoint Online is monitored

For improved security, your organization allows access to **Microsoft SharePoint Online** in monitor mode.

Access is only available from a web browser.

☐ Hide this notification for all apps for one week



**Microsoft Purview**

Your organization prevents you from downloading this file.

File Download is blocked by your organization's security policy.

Learn more

Downloads

Sensitive Document.docx
Couldn't download - Blocked

Sensitive Document.docx
Couldn't download - Blocked

Sensitive Document.docx
Couldn't download - Blocked

Sensitive Document.docx
Couldn't download - Blocked

test (3).docx
Couldn't download - Blocked

test (3).docx
Couldn't download - Blocked

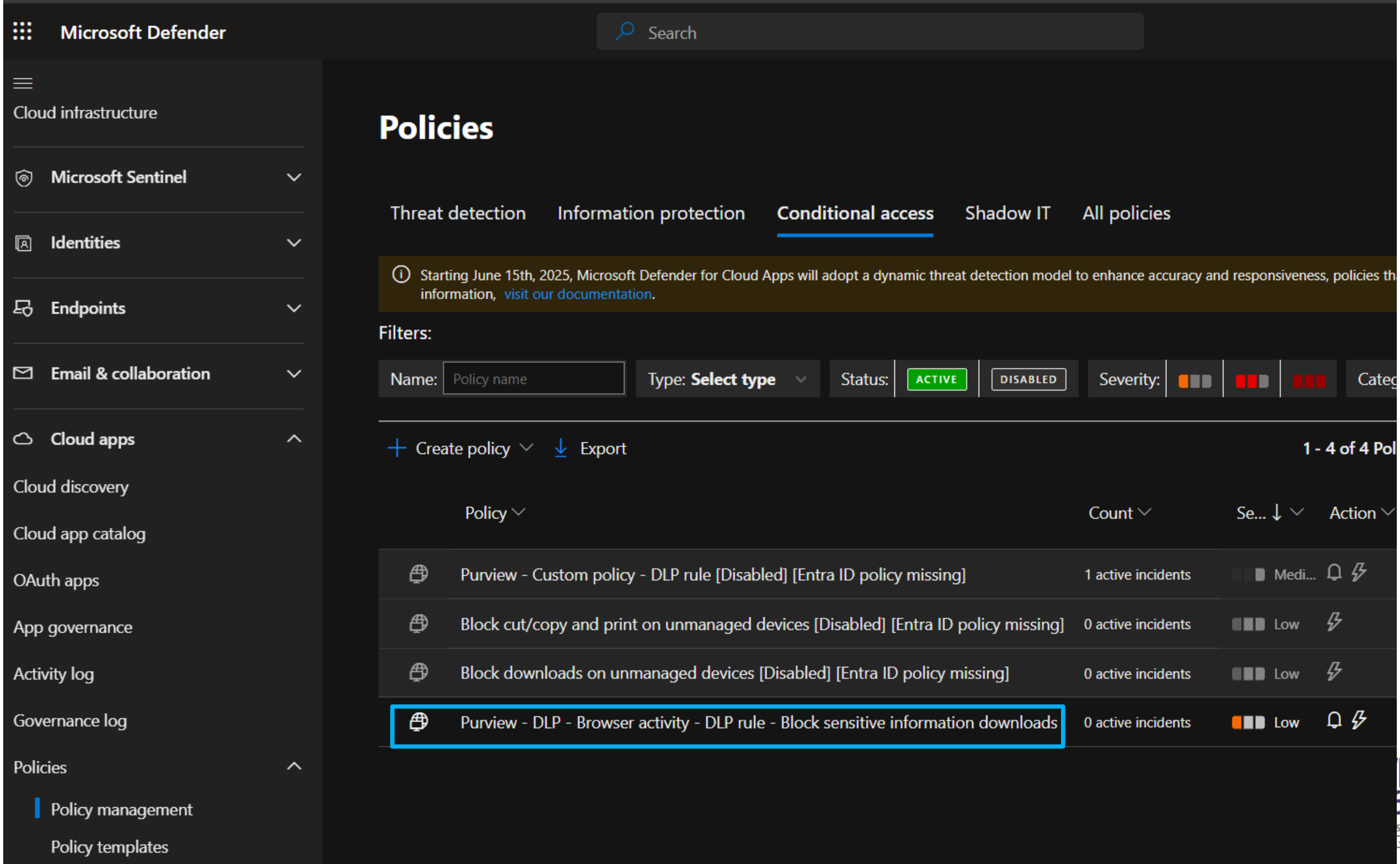
**Microsoft Purview**

Your organization prevents you from downloading this file.

File Download is blocked by your organization's security policy.

Learn more

OK



# Policies

ⓘ Starting June 15th, 2025, Microsoft Defender for Cloud Apps will adopt a dynamic threat detection model to enhance accuracy and responsiveness, policies th
information, visit our documentation.

Filters:

Name: Policy name | Type: **Select type** | Status: ACTIVE DISABLED | Severity: | Categ

**1 - 4 of 4 Pol**

| Policy | Count | Se... | Action |
|---|---|---|---|
| Purview - Custom policy - DLP rule [Disabled] [Entra ID policy missing] | 1 active incidents | Medi... | |
| Block cut/copy and print on unmanaged devices [Disabled] [Entra ID policy missing] | 0 active incidents | Low | |
| Block downloads on unmanaged devices [Disabled] [Entra ID policy missing] | 0 active incidents | Low | |
| Purview - DLP - Browser activity - DLP rule - Block sensitive information downloads | 0 active incidents | Low | |

# Takeaways

- ✗ Don't do nothing
- ! Don’t (completely) manage personal devices
- ! Consider blocking unmanaged devices
- ✓ Enforce app enforced restrictions (with CA or Sensitivity Labels)
- ✓ Enforce session policies (with MDA)
- ✓ Enforce app protection policies (with MAM)

# Bonus Methods!

- ✓ Personally owned work profiles
- ✗ Windows Information Protection (WIP)
- ! Endpoint Data Loss Prevention (DLP)

# Blogs on unmanaged devices

Block access with Conditional Access for Unmanaged Devices

Limited Access with App-enforced Restrictions for Unmanaged Devices

Limited Access with Sensitivity Labels for Unmanaged Devices

Limited Access with Session Policies for Unmanaged Devices

First look at Mobile Application Management for Windows

Mobile Application Management for Android and iOS

Blog Series: Unmanaged Devices

in/myronhelgering myronhelgering.com

# Time for questions!

# Other sessions @ Live! 360

- Wednesday, November 19, 2025
  - Automated Data Security: Identifying Sensitive Data with Microsoft Purview **(9:30am – 10:45am)**
- Thursday, November 20, 2025
  - Six Methods to Protect your Business from the Threat of Unmanaged Devices **(1:00pm – 2:15pm)**
  - The Challenge of Providing Secure Access to External Admins **(2:30pm – 3:45pm)**

# 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!

LIVE! 360
TECH EVENTS WITH PERSPECTIVE

# Thank you!

LIVE!
360
TECH EVENTS WITH PERSPECTIVE