How to Protect your Business from the Threat of Unmanaged Devices

Myron Helgering

Thank you Sponsors

Gold

robopack

SUPER VISION

AvePoint®

controlUP

inforcer

Recast

Silver

PATCH MY PC

Technical Partners

CONSULTEQ

PROXSYS

SecMinds SOLUTIONS

Secure At Work

About Myron Helgering

Focus

Blogging & Speaking

Microsoft Security MVP

Home

Almere, Netherlands

Wive

Work

Tech Lead Security @ Pink Elephant

Hobbies

Snowboarding

Fantasy Geek

Contact

LinkedIn: in/myronhelgering

My Blog

https://myronhelgering.com

Agenda

01 Unmanaged Devices

02 Customer landscape and solution requirements

03 MAM for Windows and MTD Connector

04 Session policies and In-browser protection

05 Inline DLP policies and Edge for Business configuration policies

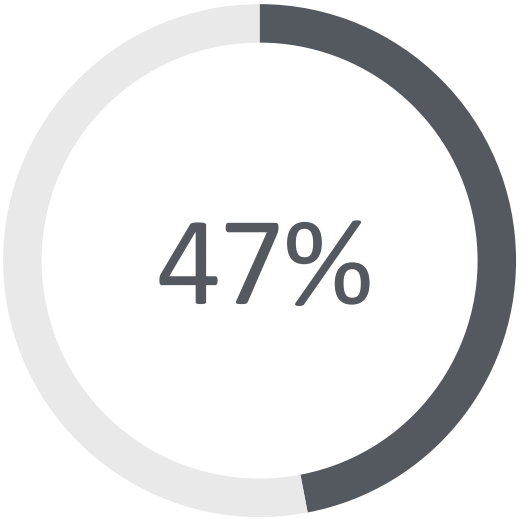
06 Takeaways & Q&A

What is an unmanaged device?

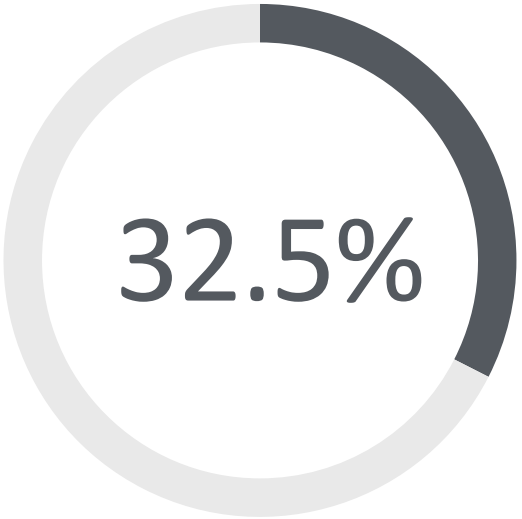
"A device that accesses company apps and data
while not being (MDM) managed by the company."

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

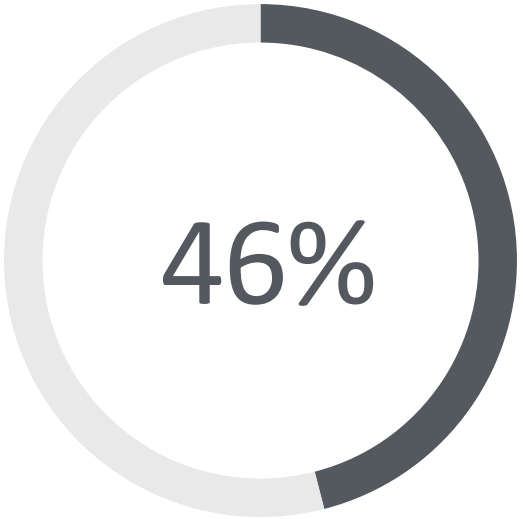
Numbers on unmanaged devices



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

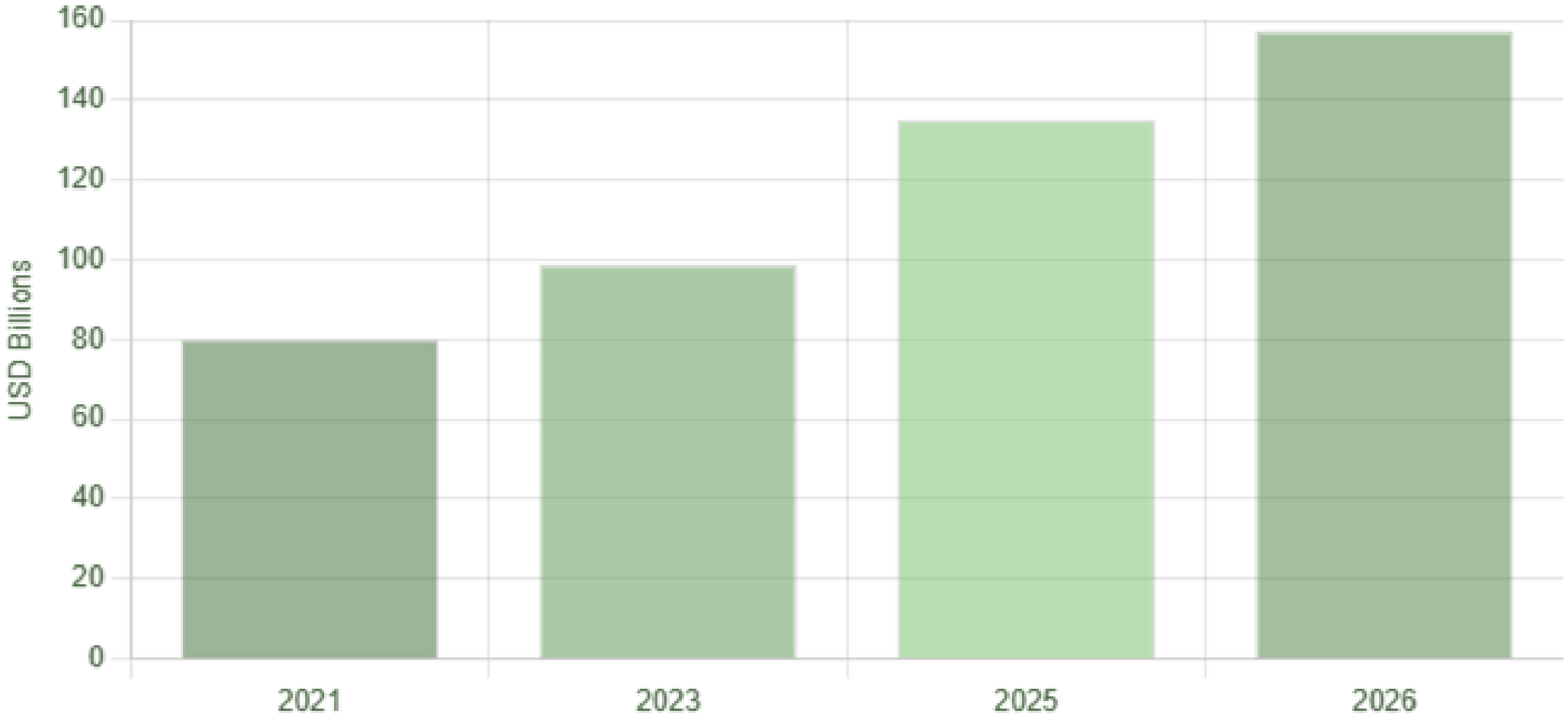
Numbers on unmanaged devices

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

Customer landscape

Corporate devices

macOS

iOS

MDM-managed by Intune

Personal devices

iOS

MAM-protected by Intune

Personal devices

macOS

Client app access blocked through Conditional Access

Personal devices

macOS

Full access through browser

Solution requirements

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

MAM for Windows and MTD Connector

Microsoft Intune admin center

Copilot

Microsoft Intune
Create new Mobile Threat Defense (MTD) connector

Connectors and tokens | Mobile Threat Defense

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

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

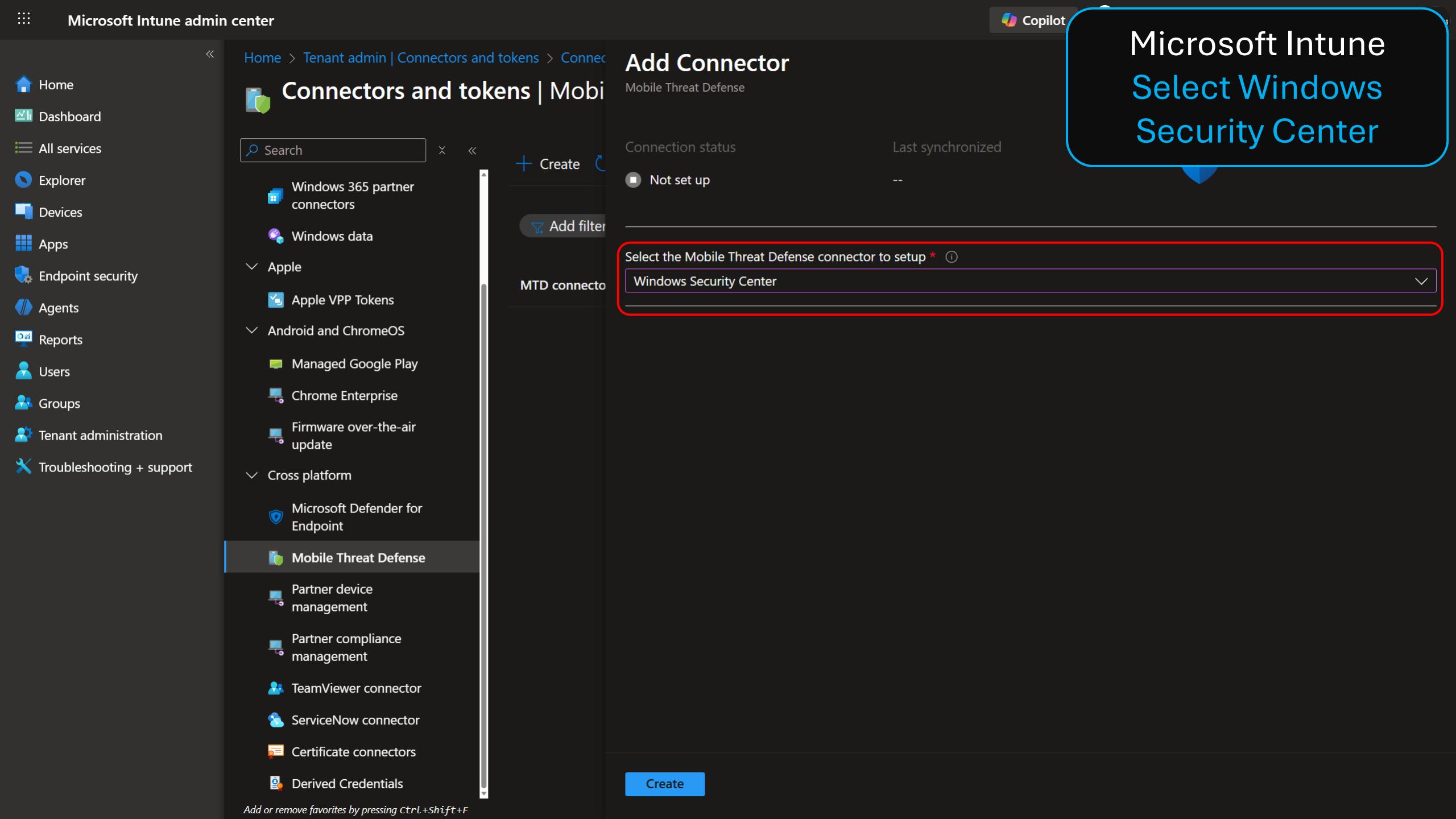
Create | Refresh | Columns

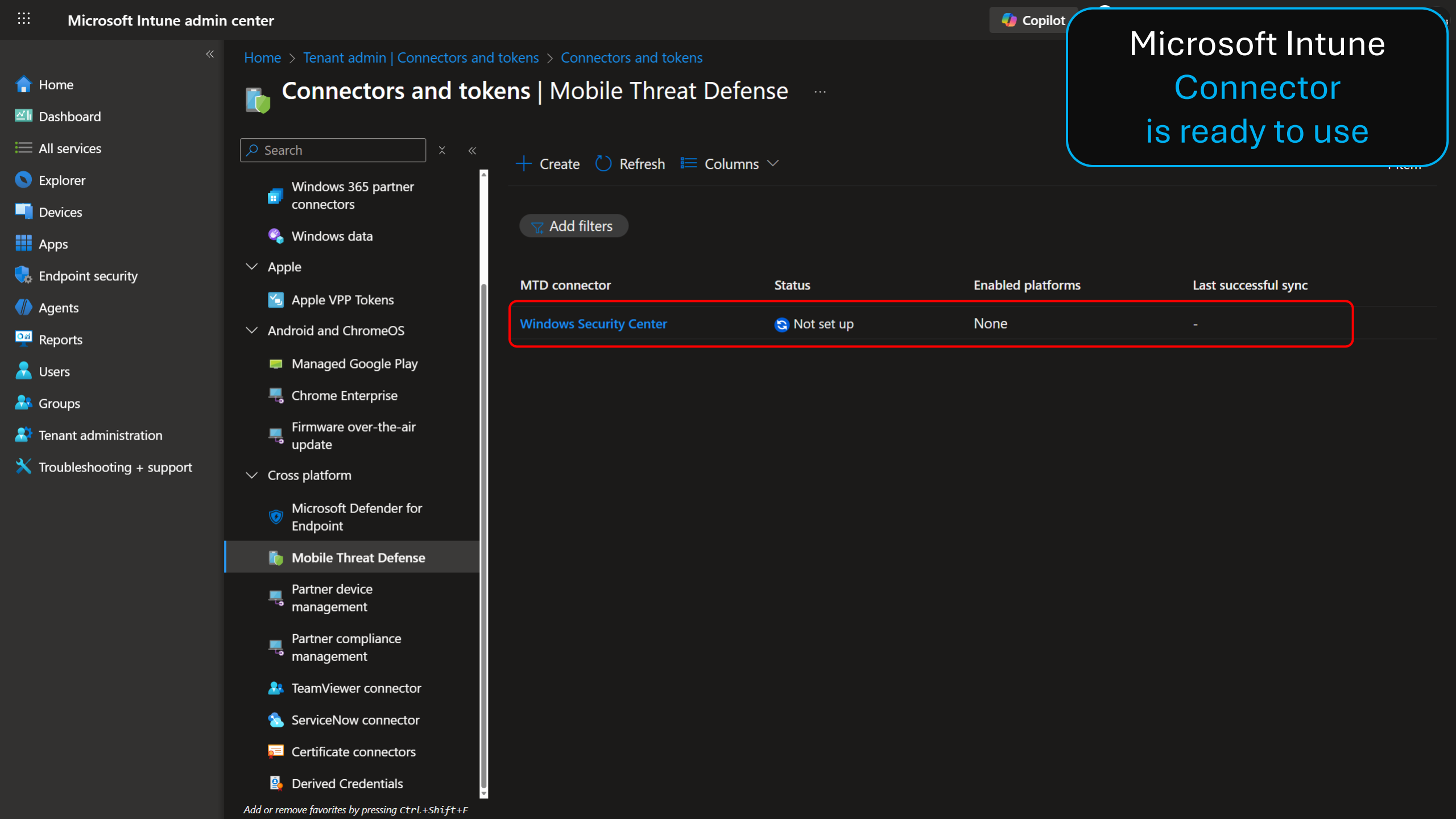
Add filters

MTD connector	Status	Enabled platforms	Last successful sync

No results found

Add or remove favorites by pressing Ctrl+Shift+F


Microsoft Intune admin center
Copilot
Microsoft Intune
Select Windows
Security Center
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Tenant admin | Connectors and tokens > Connec
Connectors and tokens | Mobi
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
Add or remove favorites by pressing Ctrl+Shift+F
Create
Add filter
MTD connecto
Add Connector
Mobile Threat Defense
Connection status
Not set up
Last synchronized
--
Select the Mobile Threat Defense connector to setup *
Windows Security Center
Create


Microsoft Intune admin center
Copilot
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
Add or remove favorites by pressing Ctrl+Shift+F
Create
Refresh
Columns
Add filters
MTD connector
Status
Enabled platforms
Last successful sync
Windows Security Center
Not set up
None
-

Microsoft Intune admin center

Copilot

Microsoft Intune
Create app protection policy for Windows

Home > Apps

Apps | Protection

Search

- 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

Create | Refresh | Export | Columns | App protection report: W

- iOS/iPadOS
- Android
- Windows
- Windows Information Protection

Add filters

Deployed	Last modified	Platform	Management type

You have no policies.

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

Add or remove favorites by pressing Ctrl+Shift+F

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

Create policy

Basics | 2 Apps | 3 Data protection | 4 Health Checks | 5 Assignments | 6 Review + create

+ Select apps

Apps	Remove
No apps selected	

Previous Next

Select apps to target

Search by Windows App Id

Microsoft Edge

Selected Apps

No Apps selected

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

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

Microsoft Intune Configure Health Checks settings

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

Create policy ...

Basics | Apps | Data protection | 4 Health Checks | 5 Assignments | 6 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 acounts 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 ...

Previous Next

nistration

ting + support

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 Create Conditional Access policy

Conditional Access | Policies

Microsoft Entra ID

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 Configure Conditional Access policy

Microsoft Entra admin center

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

- 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
- Account recovery (Preview)
- Password reset
- Custom security attributes

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

- MTD Connector
- App Protection policy
- Conditional Access policy


15:17
Saturday, 31 January

Old user experience

Stay signed i

Windows will remem
websites on this dev
on your device.

Allow my orga

No, sign in to this a

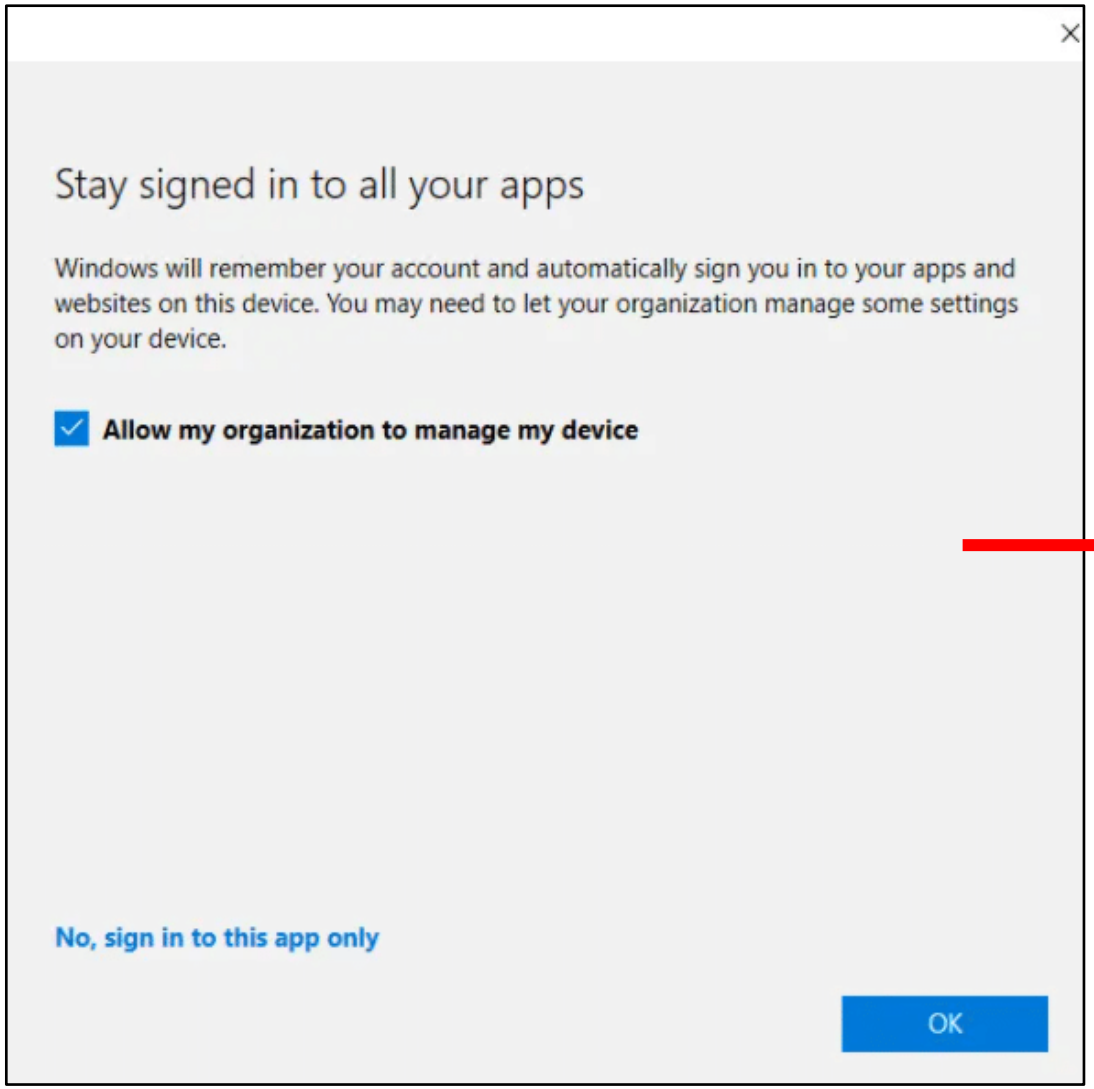
OK

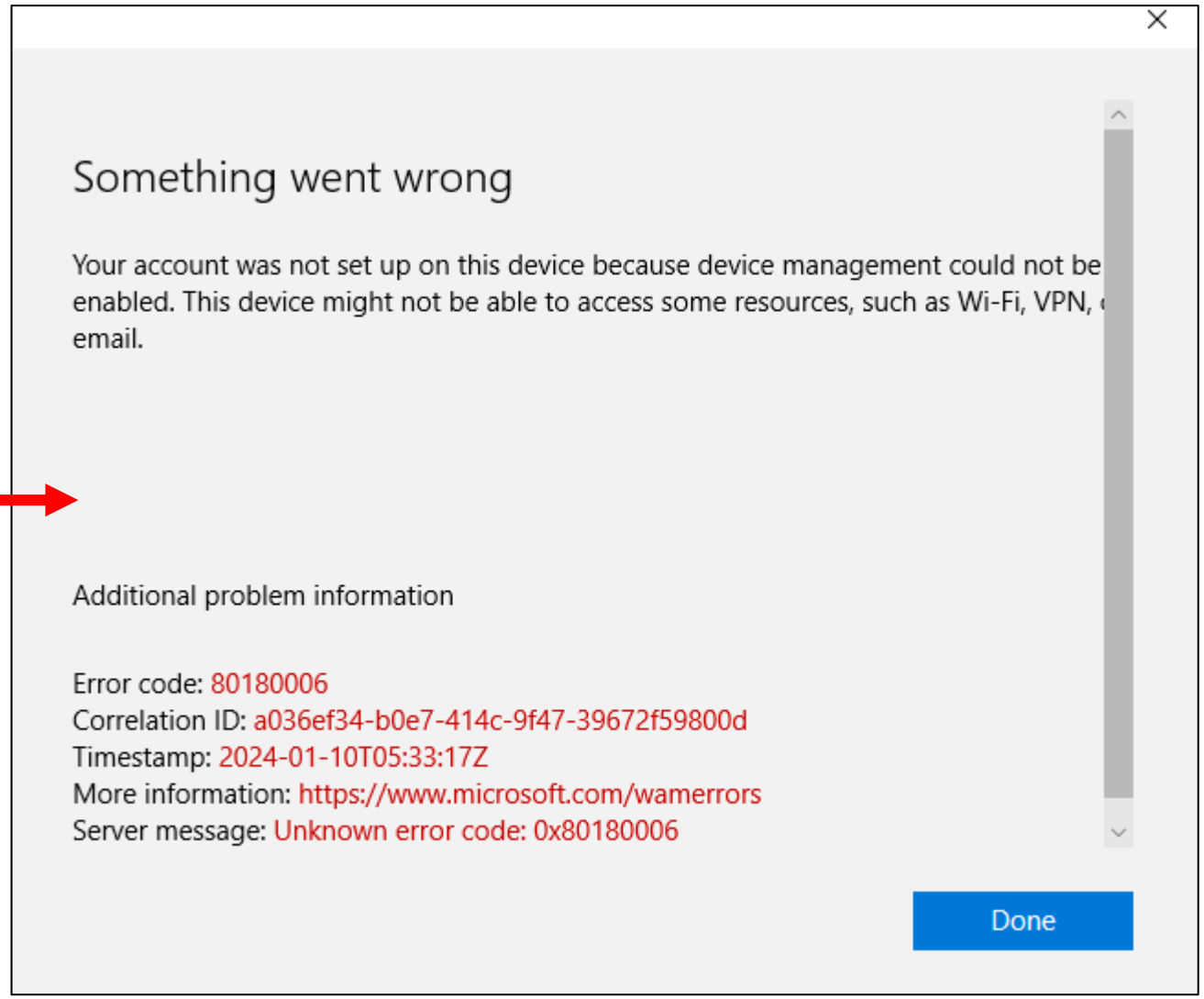
1 Platform settings 2 Review + save

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

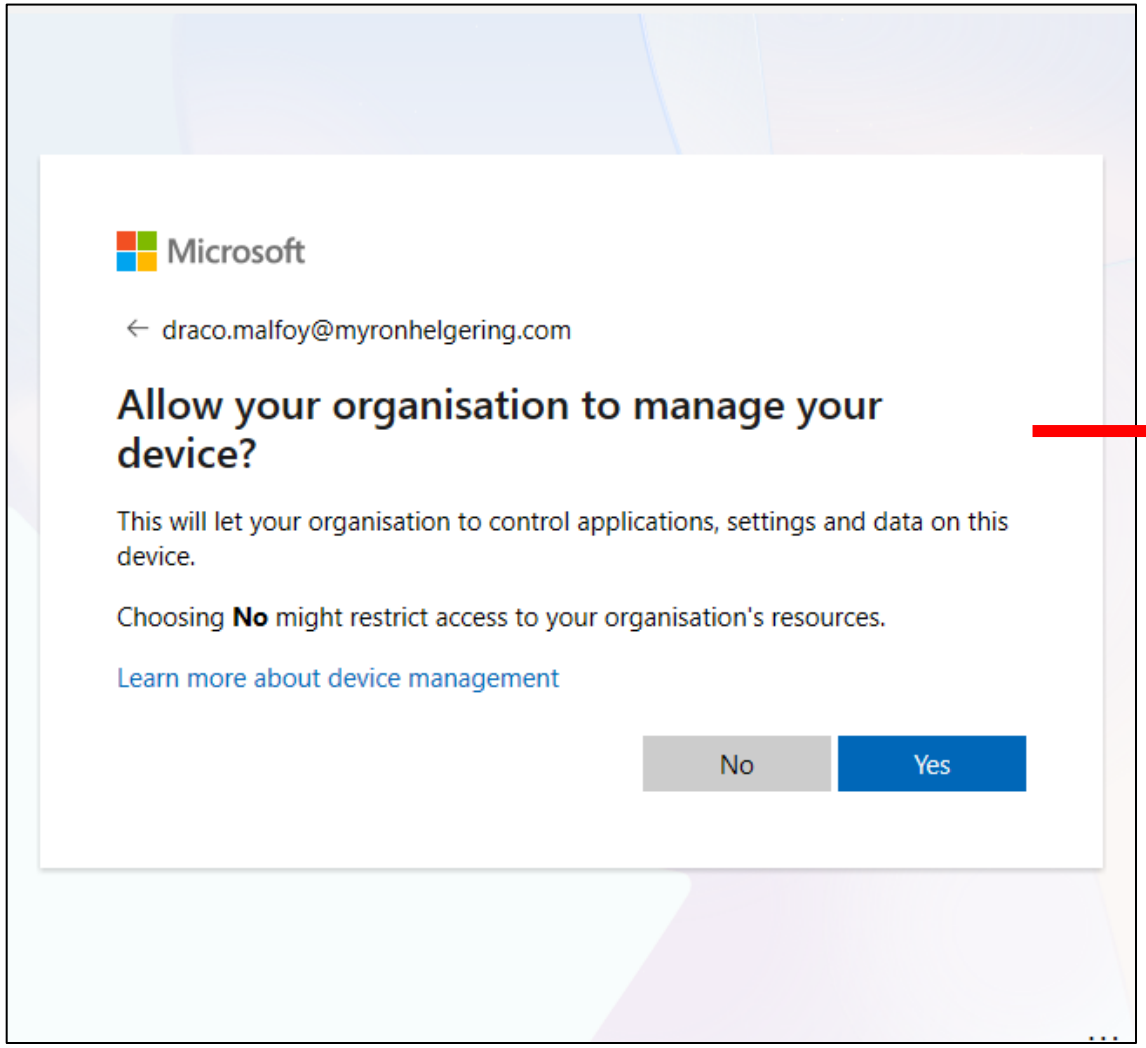
Type	Platform	versions	Personally owned	Device manufacturer
Android Enterprise (work profile)	Allow / Block	Allow min/max range: Min Max	Allow / Block	Manufacturer name
Android device administrator	Allow / Block	Allow min/max range: Min Max	Allow / Block	Manufacturer name
iOS/iPadOS	Allow / Block	Allow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

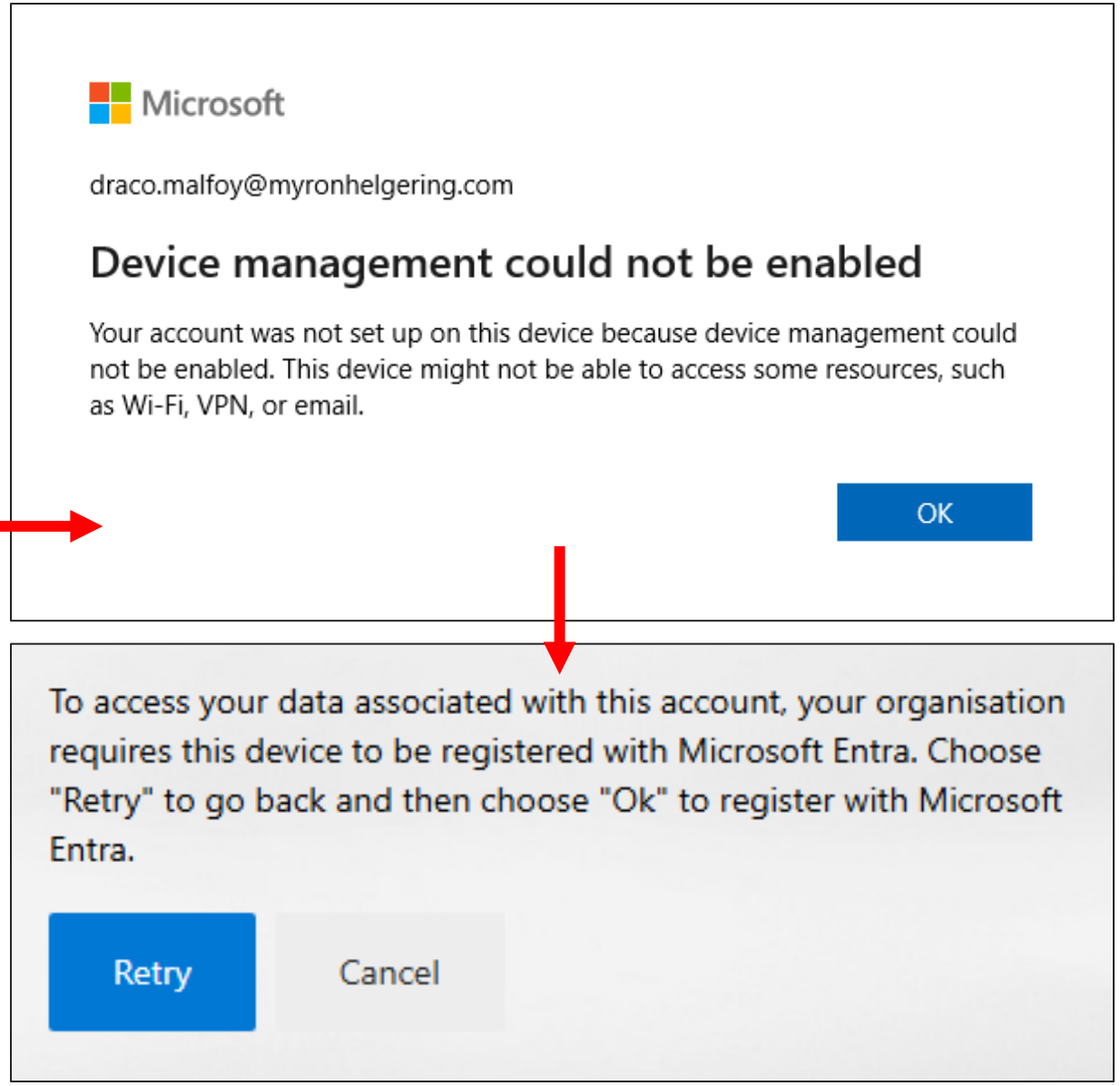
Old user experience

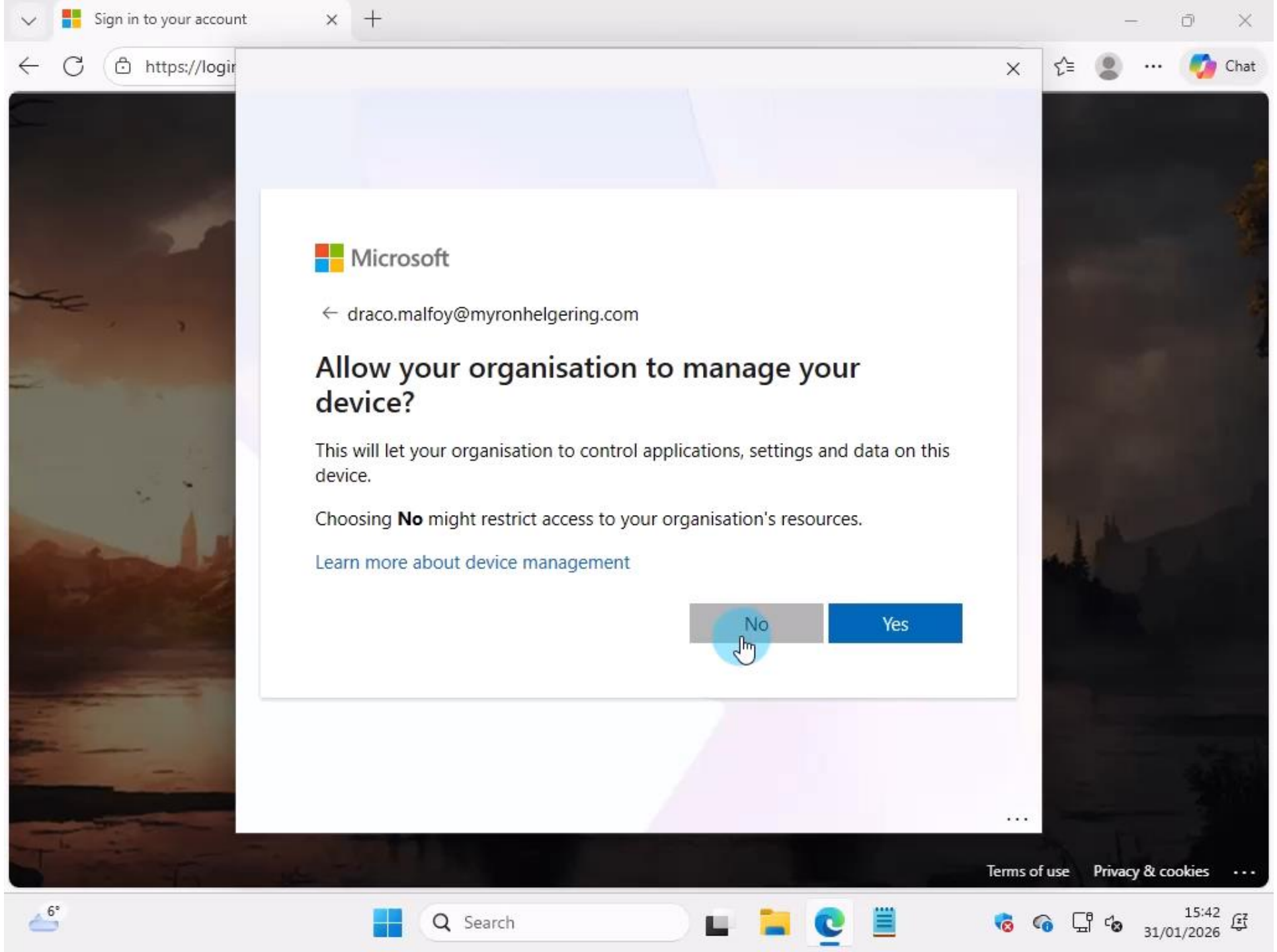




New user experience






Sign in to your account
https://logi
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
Search
15:42
31/01/2026

Session policies and in-browser protection

Microsoft Entra Create Conditional Access policy

Conditional Access | Policies

Microsoft Entra ID

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 Configure Conditional Access policy

Microsoft Entra admin center

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

- 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
- Account recovery (Preview)
- Password reset
- Custom security attributes

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 session policy for unmanaged dev...

Assignments

Users or agents (Preview)

Specific users included

Target resources

1 resource included

Network NEW

Not configured

Conditions

1 condition selected

Access controls

Grant

0 controls selected

Session

Use Conditional Access App Control

Client apps

1 included

Browser

Use Conditional Access App Control

Use custom policy...

Enable policy

Report-only On Off

Create

Microsoft Defender

Search

Microsoft Defender
Session Policy 1: Block file downloads

- 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

Policy name *

MDA - Block file downloads on unmanaged devices

Policy severity *

Category *

DLP

Description

Session control type *

Select the type of contr

Control file download (

Activity source

Add activity filters to the policy

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

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

Microsoft Defender
Session Policy 2:
Block activities

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

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

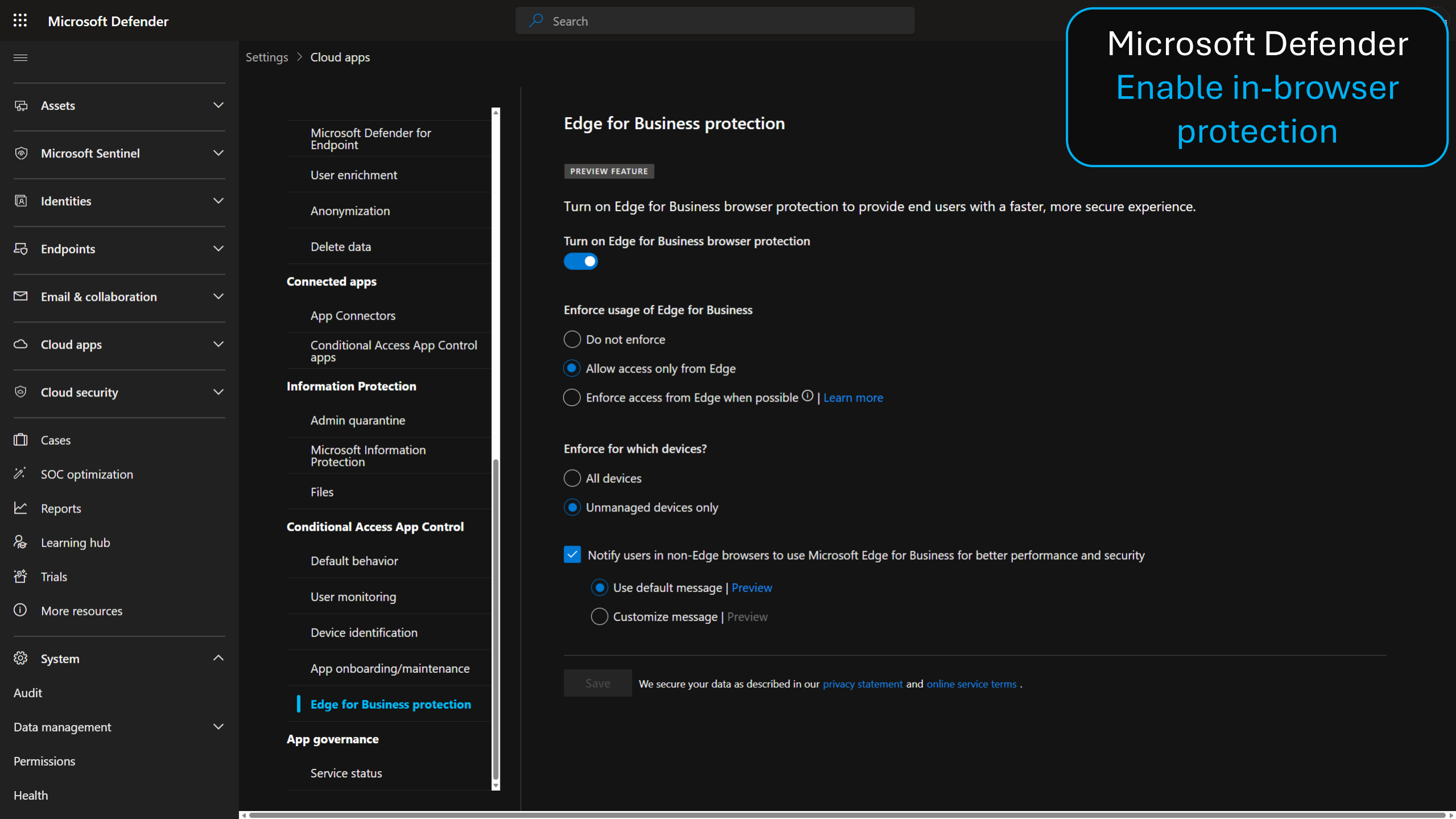
App | Manual onboarding | equals | Microsoft 365

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	In-browser protection
General available	Still in preview (after 1,5 years)
All browsers and operating systems	Edge with Windows 10/11 or MacOS
No user interaction required	Requires Edge profile sign in
Slower user experience	Faster user experience
N/A	Supports MAM & DLP restrictions


Microsoft Defender
Search
Microsoft Defender
Enable in-browser protection
Settings > Cloud apps
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Cloud security
Cases
SOC optimization
Reports
Learning hub
Trials
More resources
System
Audit
Data management
Permissions
Health
Microsoft Defender for Endpoint
User enrichment
Anonymization
Delete data
Connected apps
App Connectors
Conditional Access App Control apps
Information Protection
Admin quarantine
Microsoft Information Protection
Files
Conditional Access App Control
Default behavior
User monitoring
Device identification
App onboarding/maintenance
Edge for Business protection
App governance
Service status
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

Microsoft Defender
Enable in-browser 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

Demo

- Conditional Access policy
- Session policies
- In-browser protection


Draco Malfoy
Enter your PIN
PIN
I forgot my PIN

Inline DLP policies and Edge for Business configuration policies

Announcement Inline Data Protection

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

■■■ LAUNCHED

PREVIEW AVAILABLE
May 2025

ROLLOUT START
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

Microsoft Purview
Create Data Loss Prevention 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	
NEW ☑ **Managed cloud apps**	All users, groups, managed apps	Edit

Back Next Cancel

Define the conditions that must be met for this policy to be applied. Include specific content, senders, and recipients that you want the rule to detect. For more complex rules, create gr
works

Quick summary

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

Add condition Add group

Actions

Use actions to protect content when the conditions are met.

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
- [x] File Download — Block
- [ ] Cut or copy data — Audit Only
- [ ] Paste clipboard data — Audit Only
- [ ] Print data — Audit Only

Save Cancel

Microsoft Purview
DLP Policy 1:
Block file downloads

Customize advanced DLP rules

Microsoft Purview
DLP Policy 2:
Block activities

The rules here are made up of conditions and actions that define the protection req
can edit existing rules or create new ones.

+ Create rule

2 items

Name	Status
Block print action on unmanaged devices	On
Block cut/copy action on unmanaged devices	On

Back Next Cancel

DLP Rule 2

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	Audit Only
Cut or copy data	Block
Paste clipboard data	Audit Only
Print data	Audit Only

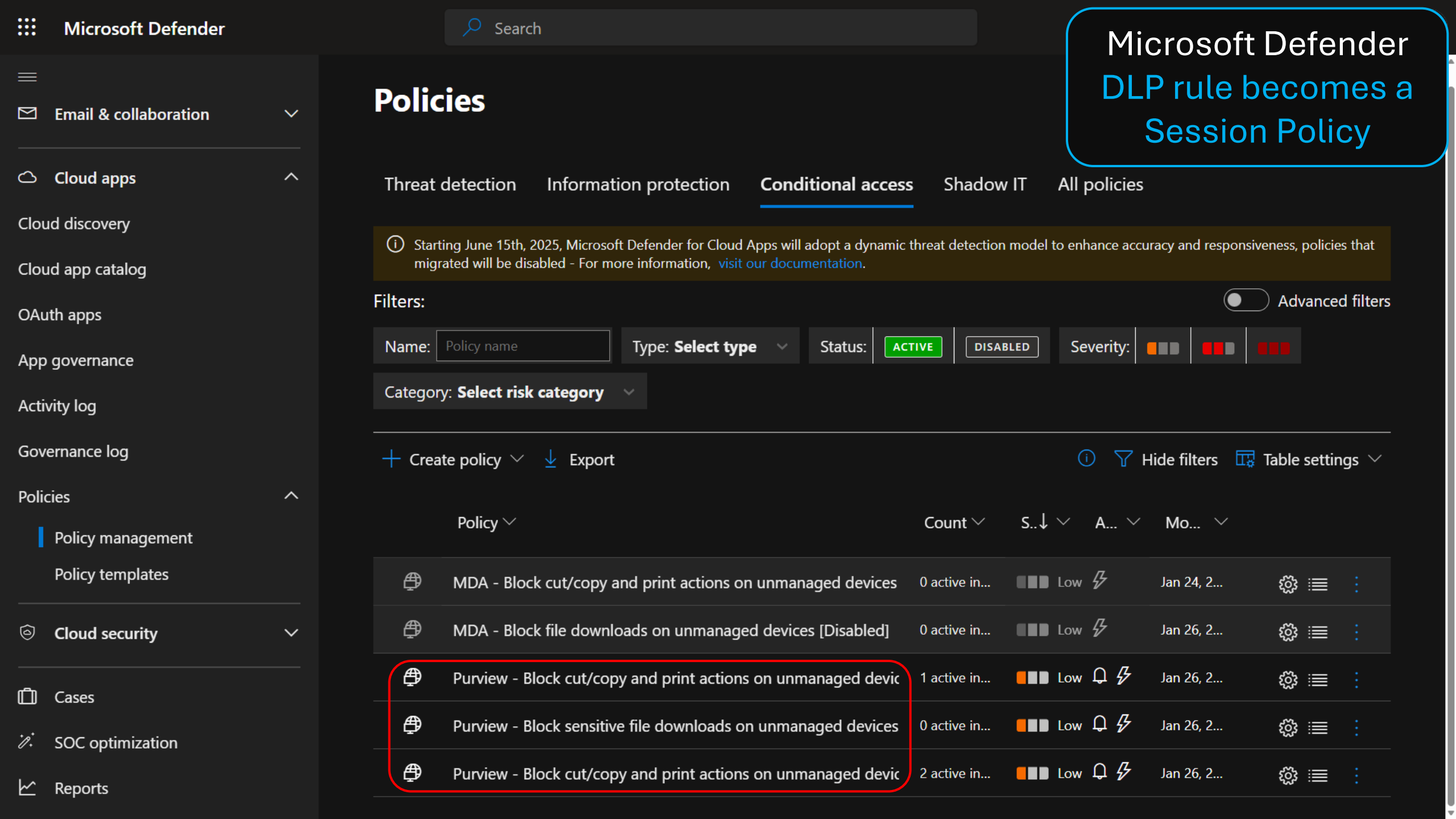
DLP Rule 1

Restrict browser and network activities

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

Text upload	
File upload	
File Download	
Cut or copy data	Audit Only
Paste clipboard data	Audit Only
Print data	Block

Microsoft Purview
DLP Policy 2:
Block activities


Microsoft Defender
Search
Microsoft Defender
DLP rule becomes a
Session Policy
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
Reports
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: Policy 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

M365 admin center
Configure Edge for Business policy

Helgering Edge Configuration policy

Export Delete

Properties | Managed extensions | Customization Settings

- Enterprise secure AI
- Organization branding
- Automatic profile switching
- Security settings
- Connected feature control
- Secure password deployment

Configure settings to protect against security vulnerabilities and improve your security posture. In the event of a zero-day vulnerability, we highly recommend enabling enhanced security mode.

Raise Edge protection levels

Turn on enhanced security mode to gain an extra layer of protection and help reduce the risk of an attack caused by memory-related vulnerabilities. This will not restart any devices. Learn more about Enhanced Security Mode.

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.

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

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

M365 admin center
Configure Edge for Business policy

Security settings
Connected feature control
Secure password deployment

will not restart any devices. Learn more about Enhanced Security Mode.

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

Demo

- Conditional Access policy
- Data Loss Prevention policies
- Edge for Business configuration policy
- In-browser protection


Recycle Bin
Learn about this picture
Microsoft Edge
Google Chrome
Personal - Edge
Search
19:57
31/01/2026

User Experience

Screen recording blooper

User Experience Watermarking Protection

Delete | Archive | Report | Move to | Zoom

New Employees

Albus Dumbledore
To: Draco Malfoy

Reply | Reply all | Forward

Sun 5/26/2024 2:51 PM

New Employees.docx
14 KB

Start reply with: They have been added. | This has been updated. | This has been completed.

Hello Draco,

Please add these passport numbers to the HR database as we have hired some new employees.

Johan Bergen: P4366918
Melissa Lakerhof: XN5004216
Najib Yare: BB0979829

Thank you,

Albus

p.s. I have also attached a file with the same numbers

Reply | Forward

Microsoft Purview
Block “sensitive” file downloads with DLP policy

Content contains

Group name *

Default

Sensitive info types

Credit Card Number — Medium confidence — Instance count 1 to Any

Sensitivity labels

Confidential/Internal only

Add

Create group

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

Save Cancel

Microsoft Defender

Search

Microsoft Defender
Block “sensitive” file downloads with session policy

- 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

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

MAM for Windows vs Session & DLP policies

MAM for Windows	Session & DLP policies
Intune license (M365 E3 or BP)	M365 E5 license
Device health checks	N/A
Remote selective wipe	N/A
Data protection restrictions	Data protection restrictions
Allow copy/paste within Edge	Protected clipboard with boundaries
N/A	macOS support
Unmanaged devices only	Support for any device
App level targeting (Edge only)	Granular cloud-app targeting
N/A	Screen capture and watermark protection
N/A	Protection based on sensitive files

Thank You

in/myronhelgering

myronhelgering.com