

Session: Applying DLP Controls to Cloud Apps Using Edge for Business



International Data Security User Group
Monday 13 July 2026

Agenda

- Introduction
- Edge for Business and unified policy management
- Data Loss Prevention for Managed Cloud Apps
- Inline browser DLP
- Additional Edge for Business capabilities
- Q&A

About me

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



Myron Helgering



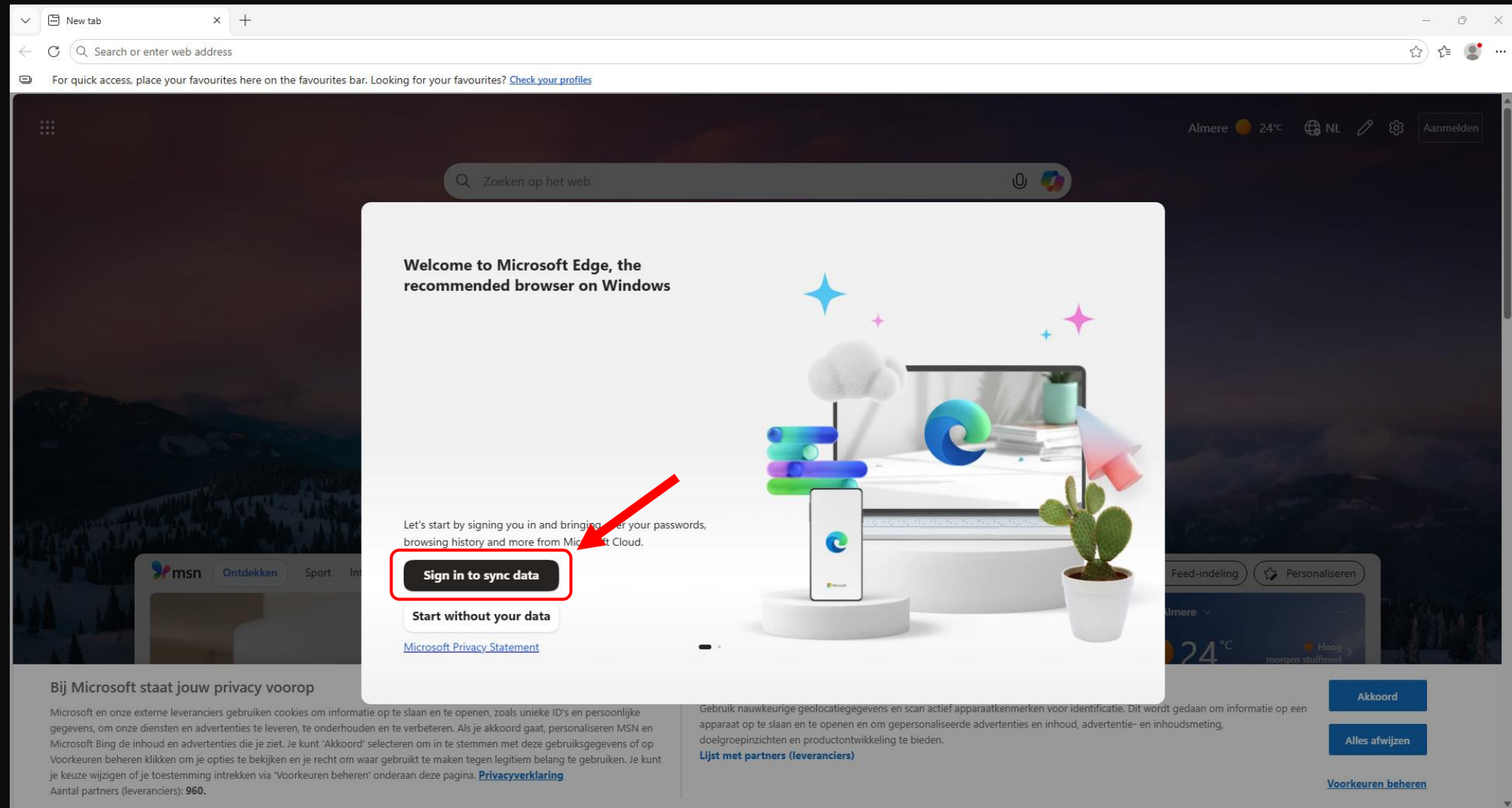
[in/myronhelgering](https://www.linkedin.com/in/myronhelgering)



myronhelgering.com

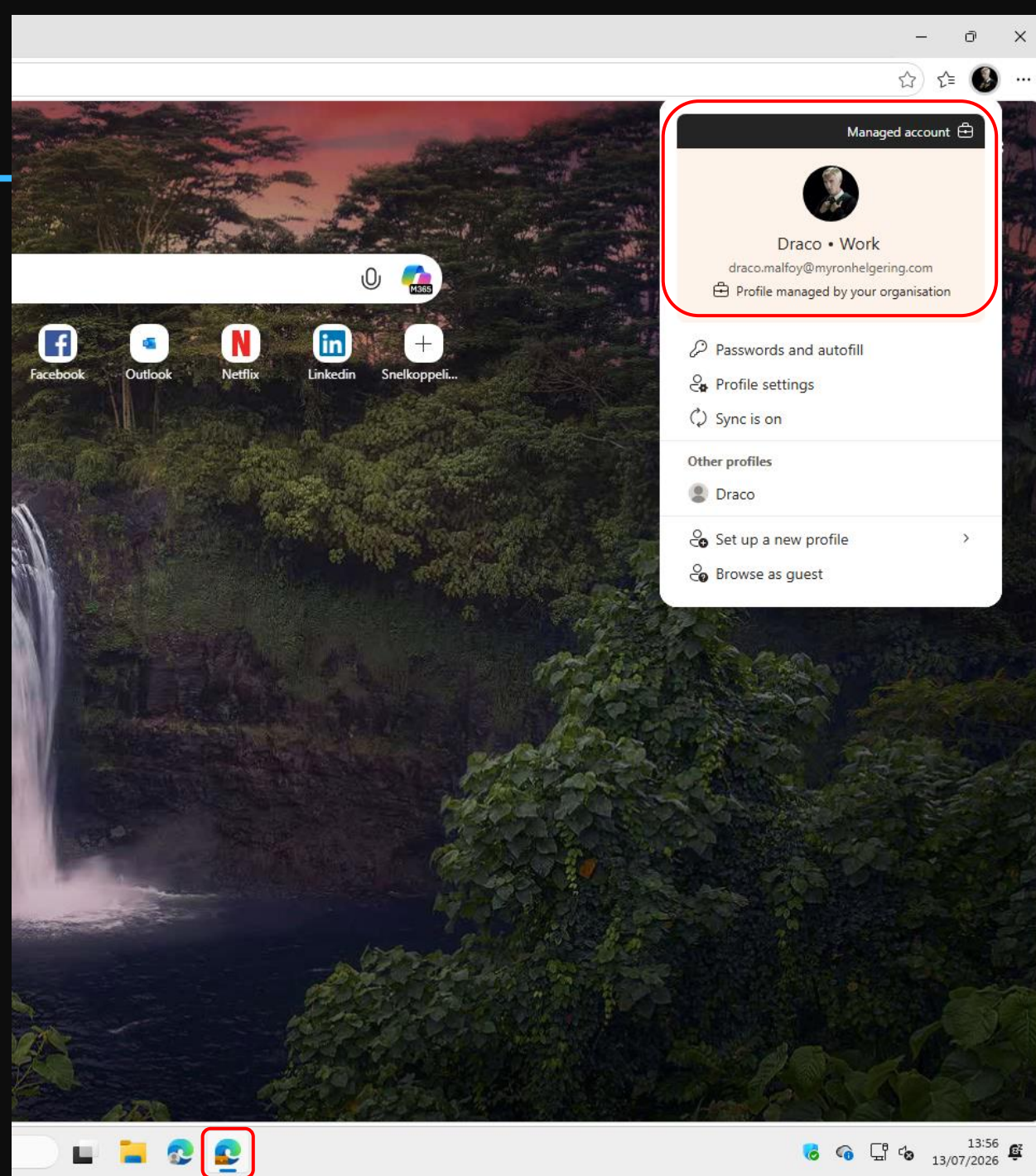


What is Edge for Business compared to Edge?



Edge for Business

- Isolated work container
- Separation of work vs. personal
- Automatic profile switching
- Enterprise policy control



Options for Edge configurations

The image displays two overlapping windows from a Windows operating system. The background window is the 'Settings picker' in Windows 11, showing a search for 'microsoft edge' with a list of settings categories like 'Cast', 'Content settings', and 'Extensions'. The foreground window is the 'Group Policy Management Editor', showing the 'Microsoft Edge' policy folder expanded under 'Administrative Templates'. The 'Microsoft Edge' folder contains sub-folders for 'Cast', 'Content settings', 'Default search provider', 'Extensions', 'HTTP authentication', 'Native Messaging', 'Password manager and protection', 'Printing', 'Proxy server', 'SmartScreen settings', and 'Startup, home page and new tab page'. The 'Startup, home page and new tab page' folder is expanded, showing a list of policies with their current state (e.g., 'Not configured').

Group Policy Management Editor - Microsoft Edge Policies

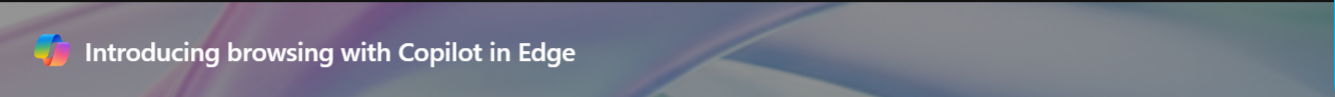
Setting	State
Cast	
Content settings	
Default search provider	
Extensions	
HTTP authentication	
Native Messaging	
Password manager and protection	
Printing	
Proxy server	
SmartScreen settings	
Startup, home page and new tab page	
Enable deleting browser and download history	Not configured
Allow file selection dialogs	Not configured
Always open PDF files externally	Not configured
Set application locale	Not configured
Allow or block audio capture	Not configured
Sites that can access audio capture devices without requesti...	Not configured
Automatically import another browser's data and settings at...	Not configured

Settings picker - Search results for 'microsoft edge'

- Cast
- Content settings
- Default search provider
- Extensions
- HTTP authentication
- Native Messaging
- Password manager and protection
- Printing
- Proxy server
- SmartScreen settings
- Startup, home page and new tab page
- Enable deleting browser and download history (User)
- Allow file selection dialogs (User)
- Always open PDF files externally (User)
- Set application locale (User)
- Allow or block audio capture (User)
- Sites that can access audio capture devices without requesti... (User)
- Automatically import another browser's data and settings at... (User)

- Home
- Copilot
- Agents
- Users
- Groups
- Roles
- Resources
- Marketplace
- Billing
- Support
- Settings
- Domains
- Search & intelligence
- Org settings
- Microsoft 365 Backup
- Integrated apps
- Directory sync errors
- Viva
- Partner relationships
- Microsoft Edge
- Setup
- Reports
- Health
- Admin centers

Microsoft Edge for Business



Dashboard Configuration policies Site lists Connectors Copilot Resources

Provide Feedback

Manage browser settings for your organization with configuration policies. If a user is assigned to multiple policies with conflicting settings, then the setting of the highest priority policy is applied.

Create policy Refresh

	Priority ↑	Name	Policy type	Scope	Platforms	Last modified date	Modified by
☐	0	Helgering Edge Configuration policy	Cloud	User	Windows macOS iOS Android	2026-05-26	Myron Helgering
☐	1	Purview - Allow Purview collection policies to apply to all users This policy is automatically created, scoped to all users, and allows for Purview collection policies to be applied to users on managed devices. It doesn't block user activities.	Cloud	Tenant	Windows macOS iOS Android	2026-05-03	Myron Helgering
☐	2	Purview - Block use of browsers where DLP protections for unmanaged Generative AI apps don't apply. This policy is automatically created and updated to include the users scoped in DLP policies targeting unmanaged generative AI apps in the browser. It blocks users from sharing data in browsers where the protections don't apply. Apps that aren't covered by these protections can still be accessed using either Edge or Chrome.	Cloud	User	Windows macOS iOS Android	2026-05-03	Myron Helgering
☐	3	Monitoring Policy This policy was auto-created from the monitoring page. To delete this policy, visit the monitoring page.	Cloud	Tenant	Windows macOS iOS Android	2026-05-25	Myron Helgering



Edge for Business unified policy management

- Update management
- Connector management
- Extension management
- Copilot management
- Configuration policy management
 - Support for Windows 10/11, MacOS, Android & iOS
 - Support for managed and unmanaged devices
- Browser insights and reporting



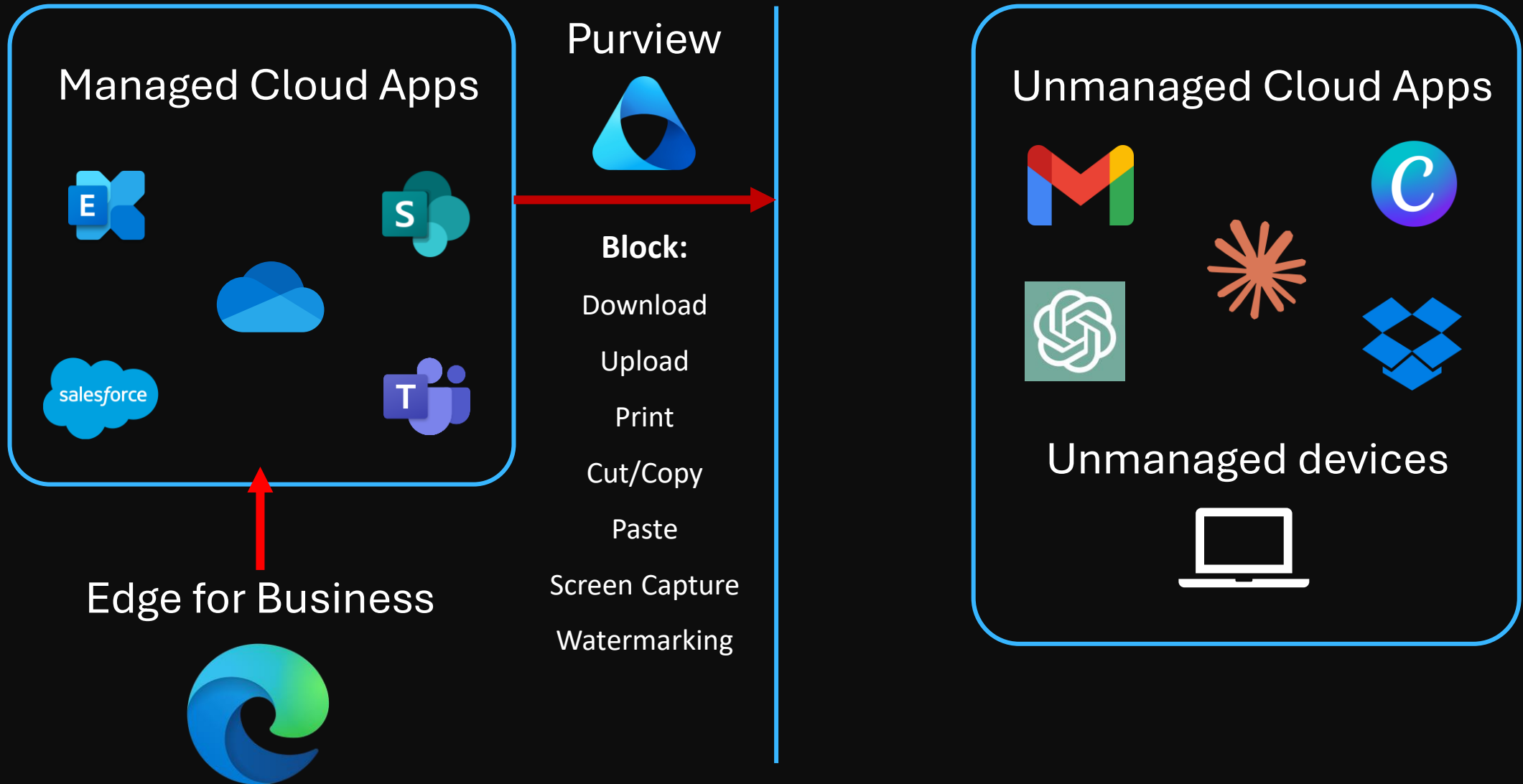
**Let's dive into some new
Edge for Business
features!**



Next section

- ✓ Edge for Business unified policy management
- ➔ DLP for Managed Cloud Apps

DLP for Managed Cloud Apps





Session
Policies

Endpoint
DLP

App
protection
policies

Inline
network DLP

DLP for
Managed
Cloud Apps

App
enforced
restrictions

Inline
browser DLP

Compare similar DLP features

DLP feature	Enforcement	Requirement	Device Type
Endpoint DLP	Device	MDE onboarding	Managed
MAM for Windows	Application	MAM registration	Unmanaged
Session Policies (in MDA)	Session	MDA proxy or Edge for Business	Managed and Unmanaged
DLP for Managed Cloud Apps	Session	Edge for Business	Managed and Unmanaged



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's new

Refresh

Review features

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

Microsoft-managed policies

Policies created 1

3

User created policies

Policies created 1

33

Search

Add filter

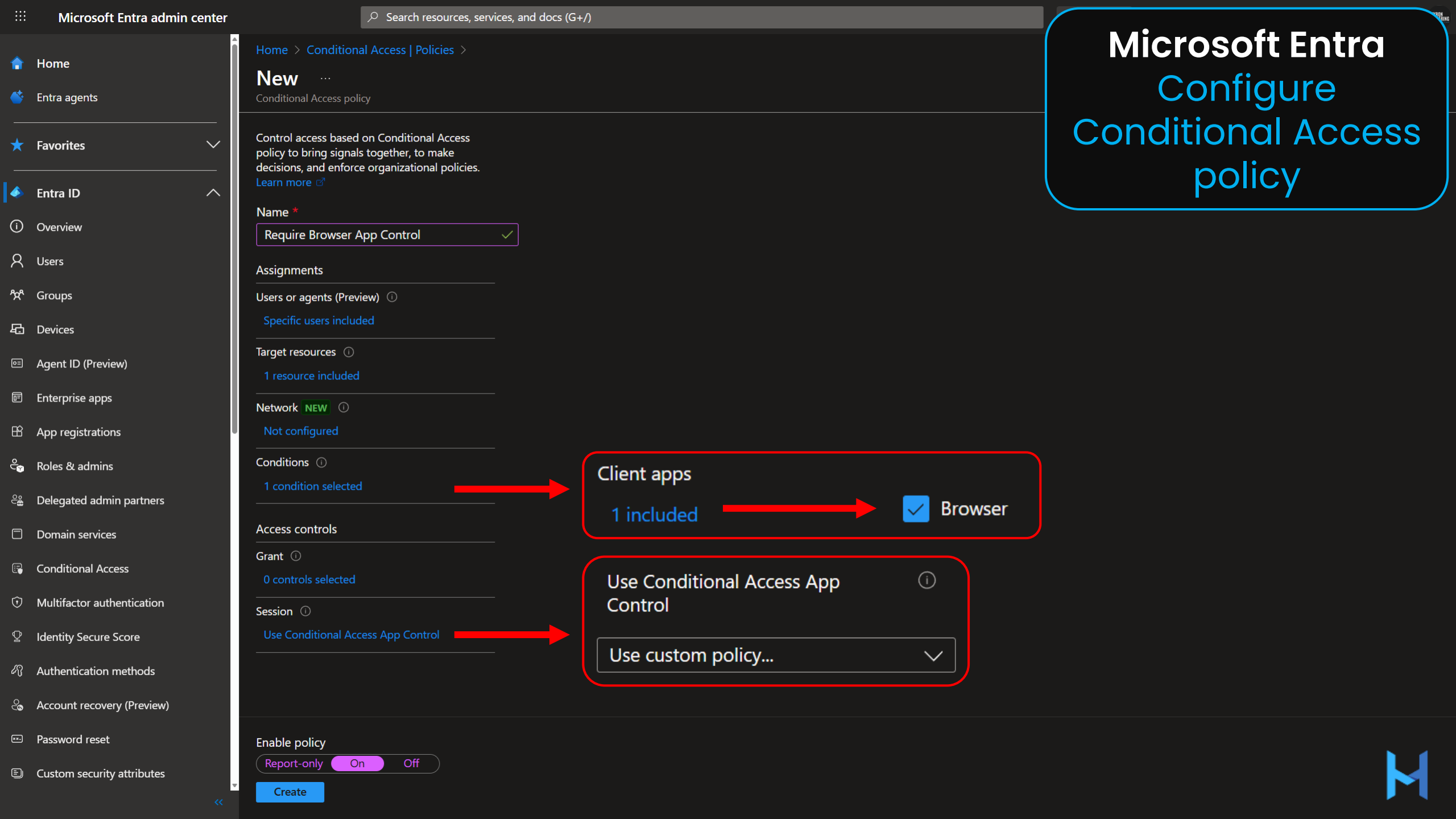
36 out of 36 policies found

Policy name	Created by	State	Alert
Block legacy authentication		On	
Multifactor authentication for admin accessing Microsoft admin center		On	
Prevent legacy multifactor authentication for admin		On	
Block access for unknown or unsupported device platform		On	
Block access for unmanaged device		On	
Block access from desktop app on unmanaged device		On	
Block all personal device device flows		On	
Block legacy authentication		On	
Grant Block access for all locations except Netherlands		On	

Microsoft Entra

Create Conditional Access policy

H



Microsoft Entra
Configure
Conditional Access
policy

Client apps

1 included

☒ Browser

Use Conditional Access App Control

Use custom policy...



Microsoft Defender

Enable in-browser protection

-  Home
-  Incidents
-  Advanced hunting
-  All Solutions

 Find Defender solutions

-  Home
-  Exposure management
-  Investigation & response
-  Threat intelligence
-  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
-  Settings

- Settings > Cloud apps
- 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](#) .



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

Edge for Business protection

PREVIEW FEATURE

Turn on Edge for Business browser protection to provide end users with a faster, more secure browsing 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](#).

Microsoft Defender
Enable in-browser
protection



Microsoft Purview
Create DLP policy
for Managed Cloud
Apps

Scope for managed app

You need to select both the apps you want to monitor and the users or groups whose activity you want to detect.

Users and groups

☒ **All users and groups**

☐ Exclude users and groups

☐ **Specific users and groups**

AND

Managed Apps

+ Include managed apps

✕ Remove all

2 items selected

Name	Type	
Office 365 SharePoint Online	Applications	✕
Office 365 Exchange Online	Applications	✕

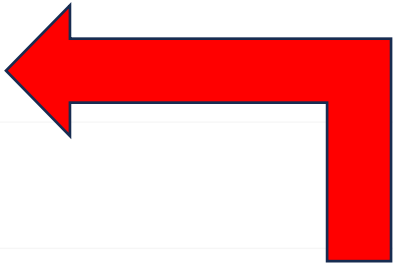
NEW



Back

Done

Cancel



Edit

Cancel



Microsoft Purview

DLP Policy 1: Block file downloads

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 [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 ▾

☒ File Download

Block ▾

☐ Cut or copy data

Audit Only ▾

☐ Paste clipboard data

Audit Only ▾

☐ Print data

Audit Only ▾

Save

Cancel



Microsoft Purview
Block “sensitive” file
downloads with DLP
policy (optional)

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



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 rules. You 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

DLP Rule 1

^ 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

☐ File upload

☐ File Download

☐ Cut or copy data

☐ Paste clipboard data

☒ Print data

Audit Only ▾

Audit Only ▾

Audit Only ▾

Audit Only ▾

Audit Only ▾

Block ▾

^ 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

☐ File upload

☐ File Download

☒ Cut or copy data

☐ Paste clipboard data

☐ Print data

Audit Only ▾

Audit Only ▾

Audit Only ▾

Block ▾

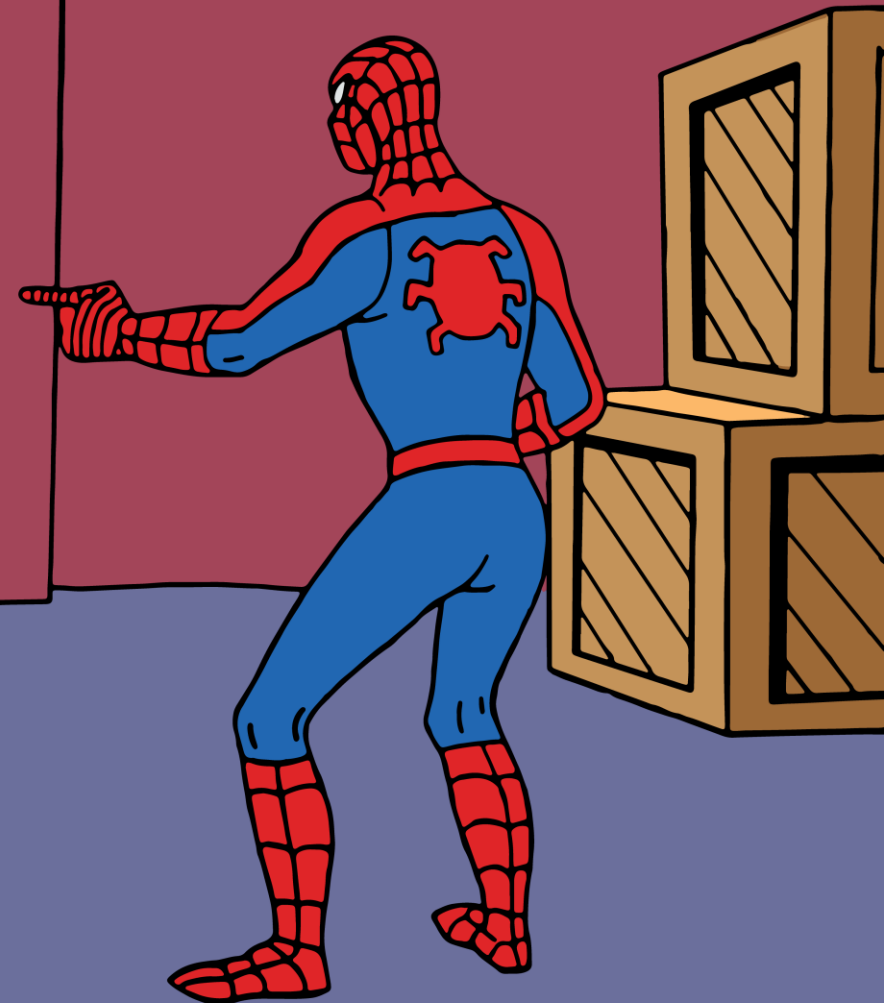
Audit Only ▾

Audit Only ▾

Microsoft Purview
DLP Policy 2: Block activities



DLP for Managed
Cloud Apps



Session Policies

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: 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



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

Not configured

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

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

Enabled

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

Policy applies to

Windows macOS

Enable browser-based tenant restrictions

Not configured

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

Protected Clipboard

Preview

Shared Boundary

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

Policy applies to

Windows macOS

Screen capture protection

Preview

Enabled

Restricts screenshots and recordings of protected content.

Policy applies to

Windows macOS

M365 admin center
Configure Edge for
Business policy



Security settings

Connected feature control

Secure password deployment



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

M365 admin center
Configure Edge for
Business policy



Scenario

- Draco Malfoy is a student working from a personal (unmanaged) device.
- Draco got access to the herbology exam answers and wants to print them so he can cheat during the finals exam.



Demo: DLP for Managed Cloud Apps

1. Conditional Access policy
2. Enabled in-browser protection
3. DLP for Managed Cloud Apps policies
4. Edge for Business policy





Recycle Bin



Microsoft Edge



Google Chrome



Learn about this picture



Lichte regen
Morgen



Q Search



17:03
16/05/2026

Section A – Mul

Correct Answer: B

User Experience
Screen recording
blooper

User Experience

Watermarking

Protection

Hogwarts School of Witchcraft and Wizardry

HERBOLOGY – ORDINARY WIZARDING LEVEL (O.W.L.) PRACTICE EXAMINATION

PROFESSOR POMONA SPROUT

GREENHOUSE THREE – RESTRICTED FLORA MODULE

Section A – Multiple Choice

1. Which condition is essential for safely repotting a mature Mandrake?

- A. Direct sunlight and warm soil
- B. Full moon illumination
- C. Protective earmuffs and dragon-hide gloves
- D. A cooling charm on the roots

Correct Answer: C

2. What is the primary magical property of Gillyweed?

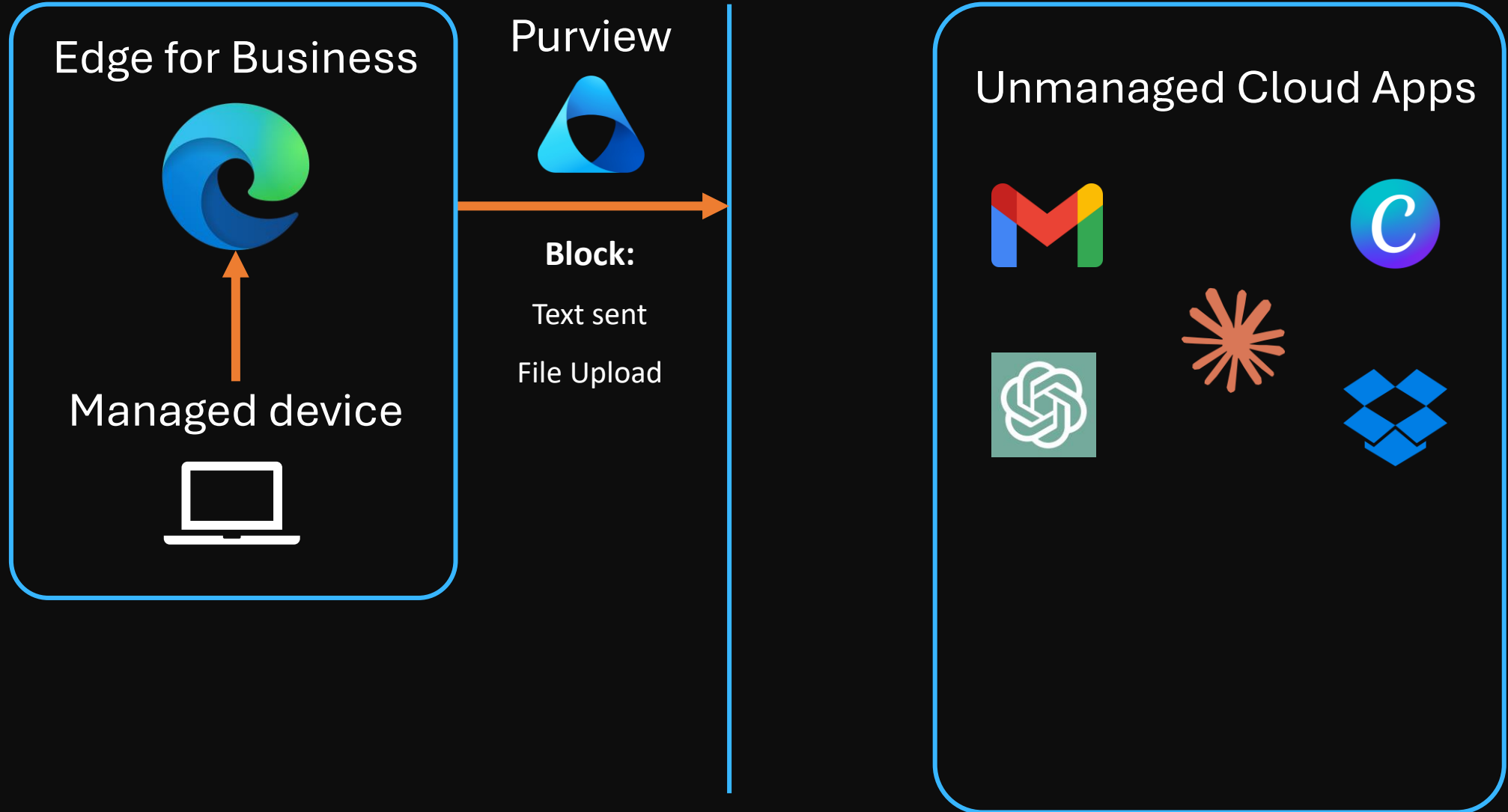
- A. Inducing temporary invisibility
- B. Allowing underwater respiration
- C. Enhancing night vision
- D. Neutralizing minor poisons

Correct Answer: B

Next section

- ✓ Edge for Business unified policy management
- ✓ DLP for Managed Cloud Apps
- ➔ Inline browser DLP

Inline browser DLP



Home

Solutions

Agents

Learn

Usage center (preview)

Settings

DSPM

DSPM for AI (classic)

Data Loss Prevention

Data Loss Prevention

Overview

Policies

Recommendations

Alerts

Classifiers

Explorers

Diagnostics

Posture reports

Security Store

Related solutions

Data Security Investigations

Information Protection

Insider Risk Management

Policies

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to prevent data from being shared with the wrong people. [Learn more about DLP](#)

Some data loss prevention policy features are pay-as-you-go. Your org will be charged based on usage. [Learn more about pay-as-you-go billing](#)

What info do you want to protect?

Let us know what type of data you want your policy to cover, and we'll guide you through a tailored setup experience. [Learn more about these options](#)

Enterprise applications & devices

Includes protection for data across all connected sources in your organization — including Microsoft 365 locations, Microsoft Copilot experiences, data connectors, enterprise-registered apps, and managed apps accessed with the Edge for Business browser.

Inline web traffic

Includes protection for data transferred in real-time with unmanaged cloud apps through the Edge for Business browser and network SASE/SSE integrations.

NEW

Search

Customize columns

status (preview)

Last modified

pletedJan 24, 2026 4:10 PM

pletedJan 31, 2026 6:38 PM

pletedJan 31, 2026 6:40 PM

pletedApr 20, 2026 9:38 AM

Microsoft Purview

Search for solutions, users, articles, and more

Data loss prevention > Create policy

Template or custom

Name

Cloud apps

Policy settings

Policy mode

Finish

Choose data sources

Select up to 100 data sources where you want to detect your specified data and activities.

Q Search

Unmanaged cloud apps 0 / 37K

Adaptive app scopes 3 / 5

Category: Any

0 / 37K selected

☐	Name	Category
☐	4chan 4chan is an image-based bulletin board where users can post comments and share images.	Content sharing
☐	Amazon Amazon is an international e-commerce website for consumers, sellers, and content creators.	E-commerce
☐	Amazon S3 (Simple Storage Service) Amazon Simple Storage Service Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.	Cloud storage
☐	Anthropic Claude Anthropic Claude is a nextgeneration AI built for safe, accurate, and secure work. The platform emphasizes productivity, collaboration, and responsible AI design.	Generative AI
☐	Atlassian Bitbucket Bitbucket is a Git and Mercurial code management and collaboration platform used by professional teams to build, test and deploy software.	Code hosting

Add (3)

Cancel

Back

Next

Cancel

Microsoft Purview

Select Unmanaged Cloud Apps

- ✓ Template or custom
- ✓ Name
- **Cloud apps**
- Policy settings
- Policy mode
- Finish

Choose data sources

Select up to 100 data sources where you want to detect your specified data and activities.

☁ Unmanaged cloud apps 0 / 100

Adaptive app scopes 3 / 5

✕ 3 / 5 selected

 Name

- ☒  **All unmanaged AI apps**
All unmanaged cloud apps categorized as generative AI. Includes Anthropic Claude, ChatGPT, Google Gemini, DeepSeek, and more.
 - ☒  **All unmanaged cloud storage apps**
All unmanaged cloud apps categorized as cloud storage. Includes Box, Dropbox, Google Drive, and more.
 - ☒  **All unmanaged collaboration apps**
All unmanaged cloud apps categorized as collaboration. Includes Google Workspace, Figma, Slack, Zoho, and more.
 - ☐  **All unmanaged social network apps**
All unmanaged cloud apps categorized as social network. Includes Facebook, LinkedIn, Reddit, X, and more.
 - ☐  **All unmanaged webmail apps**
All unmanaged cloud apps categorized as webmail. Includes Gmail, Yahoo! Mail, Zoho Mail, and more.

Add (3)

Cancel

[Back](#)

Cancel



- ✓ Template or custom policy
- ✓ Name

Choose where to enforce the policy

Choose whether you want to detect sensitive data shared with the selected cloud apps through browser or network capabilities.

Link an Azure subscription for pay-as-you-go billing

The subscription you select will be used to manage all pay-as-you-go capabilities in Microsoft Purview. Your org will only pay for the features used —no upfront costs, no commitment. [What capabilities are pay-as-you-go?](#)

Country/region *

Azure subscription *

Visual Studio Enterprise Subscription – MPN

Resource group *

RG_Purview-costs

The resource will be created under the selected resource group and pay-as-you-go feature usage will be billed to the selected Azure subscription.

I acknowledge that I have read, understood, and agree to the [Terms and Conditions](#) & terms of [Data Flow Disclosure](#)

Enable Cancel



Microsoft Purview

Configure policy conditions

Data loss prevention > Create policy

✓ Template or custom policy

✓ Name

✓ Cloud apps

● **Policy settings**

● Advanced DLP rules

○ Policy mode

○ Finish

Create rule

Use rules to define the type of sensitive information you want to protect. If the content matches many rules, the most restrictive rule applies.

Name * ⓘ

Prevent sensitive information sharing with unmanaged cloud apps

Description

^ Conditions

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 groups to exclude or include items. [Learn how the condition builder works](#)

☐ Quick summary

^ Content contains



Group name *

Default

Group operator

Any of these ▾



Sensitive info types

Credit Card Number

High confidence ▾ ⓘ

Instance count

1

to

Any ⓘ



Sensitivity labels

Confidential/Internal only



Add ▾

Create group

Save

Cancel





Microsoft Purview

Configure policy actions

Data loss prevention > Create policy

✓ Template or custom policy

✓ Name

✓ Cloud apps

● **Policy settings**

● Advanced DLP rules

○ Policy mode

○ Finish

Create rule

^ 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 sent to or shared with cloud or AI apps

Block ▾

☒ File uploaded to or shared with cloud or AI apps

Block ▾

☐ Text received from cloud or AI app

Block ▾

☐ File received from cloud or AI app

Block ▾

+ Add an action ▾

^ User notifications

User notifications inform your users when activities are blocked.

 Inline notifications will automatically be displayed when activities are blocked in Edge for Business and with some network integrations. [Learn more about inline notifications](#)

Send an email notification when activities are blocked

☐ Off

Save

Cancel



In-transit costs

€0.43/10K requests

A request is each network call a device, or browser makes to a website or API. This definition doesn't include the responses to the requests.

Example: organization of 1k users

1 user does 100 requests (per day)

100.000 requests (per day) = €4.30 per day

€94 per month (22 workdays)

Microsoft 365 admin center

Search

M365 admin center
Security groups are auto-created

Home

Copilot

Agents

Users

Groups

Active groups

Deleted groups

Shared mailboxes

Marketplace

Billing

Setup

Admin centers

Security

Customize navigation

Show all

Active groups

About GroupsWhere to store files

purview

Add a groupExport search resultsRefresh2 itemsFilter

	Name ↑	Email	Type	Sync status	Membership type	Privacy	Created on
☐	Purview DLP browser protection - excluded users	:	Security	☁	Assigned		May 3, 2026 at 2:17 PM
☐	Purview DLP browser protection - included users	:	Security	☁	Assigned		May 3, 2026 at 2:17 PM

M365 admin center
Edge policies are auto-created

Home > Microsoft Edge for Business

Microsoft Edge for Business

Dashboard Configuration policies Site lists Connectors Copilot Resources

Manage browser settings for your organization with configuration policies. If a user is assigned to multiple policies with conflicting settings, then the setting of the highest priority policy is applied.

Allows Purview to collect the browser events

+ Create policy Refresh

	Priority ↑	Name	Policy type	Scope	Platforms	Last modified date	Modified by
☐	1	Purview - Allow Purview collection policies to apply to all users This policy is automatically created, scoped to all users, and allows for Purview collection policies to be applied to users on managed devices. It doesn't block user activities.	Cloud	Tenant	Windows macOS iOS Android	2026-05-03	Myron Helgering
☐	2	Purview - Block use of browsers where DLP protections for unmanaged Generative AI apps don't apply. This policy is automatically created and updated to include the users scoped in DLP policies targeting unmanaged generative AI apps in the browser. It blocks users from sharing data in browsers where the protections don't apply. Apps that aren't covered by these protections can still be accessed using either Edge or Chrome.	Cloud	User	Windows macOS iOS Android	2026-05-03	Myron Helgering

Blocks browsers where Purview DLP can't protect data



Microsoft Intune
Intune policies are
auto-created

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

- Home > Devices
- Devices | Configuration
- Search
- macOS
 - Android
 - Linux
 - Device onboarding
 - Enrollment
 - Manage devices
 - Configuration**
 - Compliance
 - Conditional access
 - Scripts and remediations
 - Group Policy analytics
 - eSIM cellular profiles (preview)
 - Policy sets
 - Device categories
 - Partner portals
 - Manage Windows 365 Cloud PCs
 - Cloud PC Overview
 - Monitor Cloud PCs (preview)
 - All Cloud PCs
- Add or remove favorites by pressing Ctrl+Shift+F

Policies Import ADMX Monitor

+ Create Refresh Export Columns

edge policy Add filters

Blocks access to GenAI sites in Chrome

2 policies

Policy name	Platform	Policy type
Edge policy to block use of unmanaged GenAI apps in browsers where in-browser protections don't apply	Windows 10 and later	Setting
Edge policy to block use of browsers where Purview DLP protections for unmanaged AI apps don't apply	Windows 10 and later	Custom

Blocks 15+ browser apps through AppLocker



Scenario

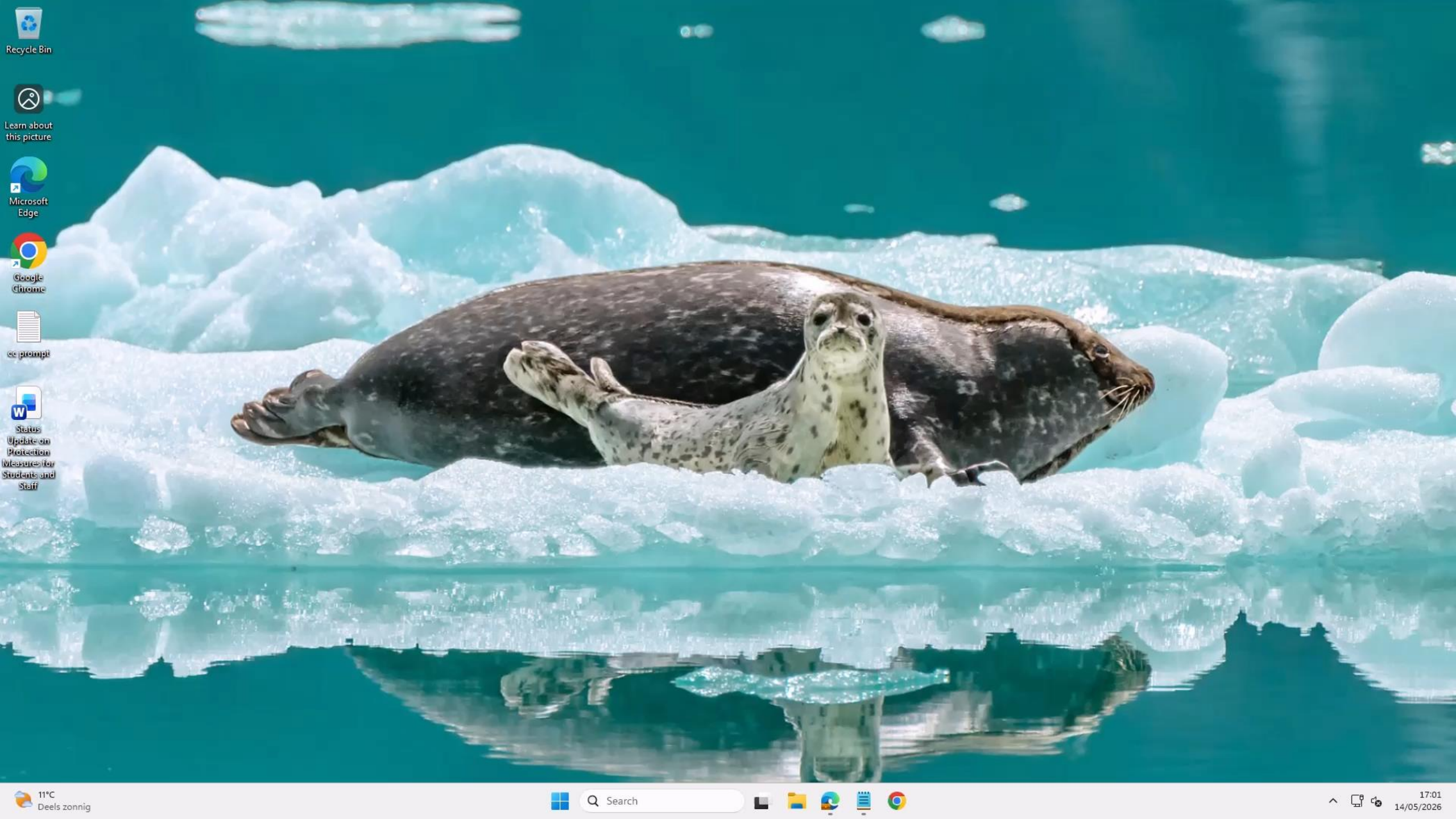
- Albus Dumbledore is a teacher and is working from a corporate Intune-managed device.
- Albus is working overtime and wants a late-night snack.
- Albus wants ChatGPT to quickly summarize a file before his snack arrives.



Demo: Inline browser DLP

1. Inline browser DLP policy
2. Pay-as-you-go Azure subscription





Recycle Bin

Learn about
this picture

Microsoft
Edge

Google
Chrome

cc prompt

Status
Update on
Protection
Measures for
Students and
Staff

11°C
Deels zonnig

Search

17:01
14/05/2026

Unmanaged cloud apps

Your organization doesn't manage the account. You can use policies for unmanaged cloud app DLP feature only applies to version and available DLP features see

To create a DLP policy that helps protect permissions for [Microsoft Intune](#) admin

Browser policies in Edge for Business s

- Adobe Firefly
- CapCut
- ChatGPT (consumer)
- Cohere
- DeepAI
- DeepL
- DeepSeek
- Google Gemini
- Grok (xAI)
- Meta AI
- Microsoft Copilot 365 Chat
- Notion AI
- Otter.ai
- Perplexity AI
- QwenAI
- Qwen Chat
- Runway
- Textcortex
- Textcortex Zenochat
- You (You.com)
- Zapier

Choose data sources

Select up to 100 data sources where you want to detect your specified data and activities.

Q Search

Unmanaged cloud apps 0 / 37K

Adaptive app scopes 3 / 5

Category: Any

☐	Name	Category
☐	4chan 4chan is an image-based bulletin board where users can post comments and share images.	Content sharing
☐	Amazon Amazon is an international e-commerce website for consumers, sellers, and content creators.	E-commerce
☐	Amazon S3 (Simple Storage Service) Amazon Simple Storage Service offers industry-leading performance, availability, and security.	
☐	Anthropic Claude Anthropic Claude is a large language model. The platform emphasizes safety and control.	
☐	Atlassian Bitbucket Bitbucket is a Git and Mercurial code hosting platform used by professional developers.	

0 / 37K selected

Choose data sources

Select up to 100 data sources where you want to detect your specified data and activities.

Q Search

Unmanaged cloud apps 0 / 100

Adaptive app scopes 3 / 5

☐ Name

☒ All unmanaged AI apps
All unmanaged cloud apps categorized as generative AI. Includes Anthropic Claude, ChatGPT, Google Gemini, DeepSeek, and more.

☒ All unmanaged cloud storage apps
All unmanaged cloud apps categorized as cloud storage. Includes Box, Dropbox, Google Drive, and more.

☒ All unmanaged collaboration apps
All unmanaged cloud apps categorized as collaboration. Includes Google Workspace, Figma, Slack, Zoho, and more.

☐ All unmanaged social network apps
All unmanaged cloud apps categorized as social network. Includes Facebook, LinkedIn, Reddit, X, and more.

☐ All unmanaged webmail apps
All unmanaged cloud apps categorized as webmail. Includes Gmail, Yahoo! Mail, Zoho Mail, and more.

3 / 5 selected

Add (3)

Cancel



Free plan · Upgrade

☀ Good afternoon, Albus Dumbledore

How can I help you today?

+

Sonnet 4.6

- Write
- Learn
- Code
- Life stuff
- Claude's choice



Start

We need Inline Network DLP

Microsoft Purview

Search for solutions, users, articles, and more

Copilot

Data loss prevention > Create policy

Template or custom policy

Name

Cloud apps

Enforcement options

Policy settings

Policy mode

Finish

Choose where to enforce the policy

Choose whether you want to detect sensitive data shared with the selected cloud apps through browser, network, or both. [Learn more about enforcement options](#)

Protecting cloud app activity with the Edge for Business browser or network are pay-as-you-go capabilities. Your org will be charged based on usage. [Learn more about pay-as-you-go billing](#)

If you choose to integrate with non-Microsoft partners, they will be able to access and possibly store some policy configuration, including user identifiers. Their terms, conditions, and privacy policy will govern the usage and storage of this data. [Learn more](#)

☒ On **Edge for Business**
Detect and protect sensitive data shared with unmanaged cloud apps, including AI apps. Applies to data shared through Microsoft Edge for Business when the user is on a managed work device. [Learn more about which apps are supported](#)

☐ Off **Network and non-Microsoft secure browsers**
Detect and protect sensitive data shared with unmanaged cloud apps through browsers, apps, APIs, and more with Microsoft Entra Global Secure Access (GSA), other integrated Secure Access Service Edge (SASE) / Secure Service Edge (SSE), and non-Microsoft secure browser providers. [View available integrations](#)

Back Next Cancel

apps by targeting data
the web traffic (preview) and

work option only

Next section

- ✓ Edge for Business unified policy management
- ✓ DLP for Managed Cloud Apps
- ✓ Inline browser DLP
- ➔ Additional Edge for Business capabilities

Microsoft 365 admin center

Home > Microsoft Edge for Business > Policy: Helgering Edge Co

Manage a configuration policy for Microsoft Edge

Basics

Settings

Extensions

Assignments

Finish

Default extension settings

These are the default settings for Microsoft Edge. [Learn more about Microsoft Edge settings.](#)

Installation settings

Allow these types of extensions

External extensions

Install sources

Permissions and URLs

Blocked hosts

Allowed hosts

Blocked extensions

Extension requests

Unmanaged extensions

Block extensions by publisher

Message for users with blocked extensions

Example: Your IT administrator has blocked the following extensions from being installed on your device.

0/1000 characters

Manage request settings

Control whether Microsoft Edge sends data about blocked extensions to the Microsoft Edge management service. If enabled, users can request blocked extensions. If disabled, users can't request blocked extensions.

Note: You must have at least one blocked extension to allow users to request blocked extensions.

Enabled

☒ Notify me about incoming requests by email

Email

helgering@microsoft.com

Frequency of email notifications

Daily

Save

M365 admin center

Allow users to request blocked extensions

Cancel

Scenario

- Albus wants to be able to translate text written in the mermaid language.
- Albus keeps forgetting his online passwords and heard about a magical vault called Keeper.
- Albus thinks Edge extensions could help him solve both problems.



Demo: extension management with Edge for Business

1. Edge for Business policy





Edge Add-ons

Discover Extensions Themes



Keeper® Password Manager & Digital Vault

Featured

Get

Compatible with your browser

Extension | Keeper Security Inc

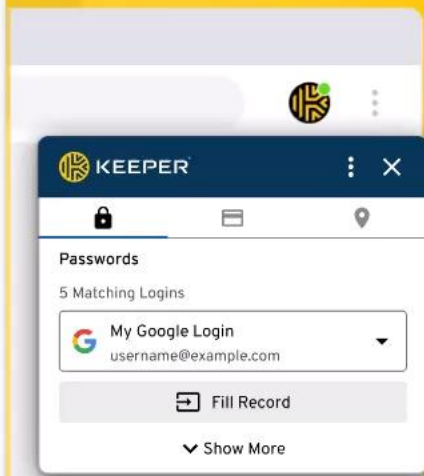
★★★★☆ (189) | 1.700.000+ Users | Productivity



Over 200,000 Reviews
★★★★★
4.9 Stars

#1 Rated Password Manager

Trusted by millions of customers to secure their passwords, passkeys and digital life.



Autofill Every Login

Keeper automatically fills in usernames and passwords - including 2FA codes.

Version 17.9.0
Updated May 6, 2026
[Available in 19 languages](#)

Developer
[More add-ons from Keeper Security Inc \(1\)](#)

Report abuse

Description

- Home
- Copilot
- Agents
- Users
- Groups
- Roles
- Resources
- Marketplace
- Billing
- Support
- Settings
 - Domains
 - Search & intelligence
 - Org settings
 - Microsoft 365 Backup
 - Integrated apps
 - Directory sync errors

Helgering Edge Configuration policy

 **Introducing browsing with Copilot in Edge** [Learn more](#) [Join Preview](#)

Export Delete

Provide Feedback

Properties Managed extensions Customization Settings

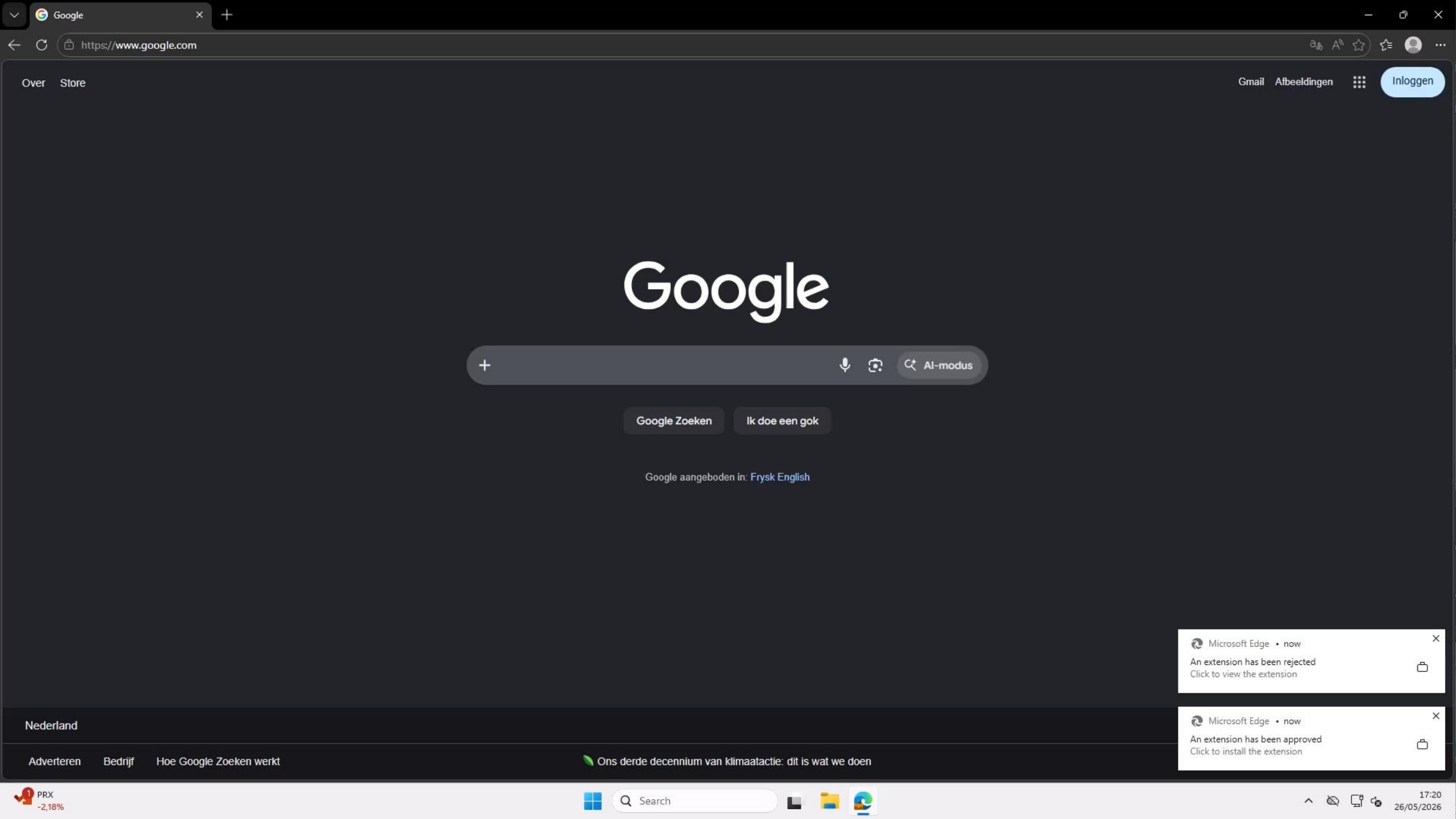
- Extensions
- Requests

Manage request settings Refresh Search

	Name ↑	Number of requests	Last requested
☐	Keeper® Password Manager & Digital Vault	2	26/05/2026, 17:15:53
☐	Translator	3	26/05/2026, 17:16:18

Support

Feedback



Over Store

Gmail Afbeeldingen Inloggen

Google

+

AI-modus

Google Zoeken Ik doe een gok

Google aangeboden in: Frysk English

Nederland
Adverteren Bedrijf Hoe Google Zoeken werkt

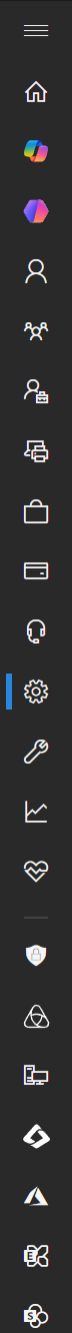
Ons derde decennium van klimaatactie: dit is wat we doen

Microsoft Edge • now

An extension has been rejected
Click to view the extension

Microsoft Edge • now

An extension has been approved
Click to install the extension



☒ 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 restricts 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

M365 admin center
Enable Protected
Downloads for
MAM-registered
devices



Microsoft Edge

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

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**

```
#edge-dlp-protected-downloads
```

Enabled

- **Allow MAM enrollment on managed devices**

```
#edge-allow-mam-on-mdm
```

Enabled

Temporarily unexpire M146 flags.

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

Default

Temporarily unexpire M147 flags.

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

Default

Enable benchmarking

```
#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.docx

https://helgering-my.sharepoint.com/:w/g/personal/cho_chang_myronhelgering_com/IQDvXVWLm_GtQ7QE6lJxgXQjAb_Yg9-m2BgQq_IsfqI69Fw

Hogwarts_House_Rules

Search for tools, help, and more (Alt + Q)

CC

FileHomeInsertLayoutReferencesReviewViewHelp

CommentsCatch upEditingShare

UndoFontFaceSizeColorTextBackgroundText BordersTableInsertImageMoreNormalFindDictateSensitivityEditor

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.

Page 1 of 1119 wordsEnglish (U.S.)Text Predictions: OnEditor Suggestions: Showing

110%Fit

Give Feedback to Microsoft

Session recap

- ✓ Edge for Business unified policy management
- ✓ DLP for Managed Cloud Apps
- ✓ Inline browser DLP
- ✓ Additional Edge for Business capabilities

Questions?
Thank you!



[in/myronhelgering](https://www.linkedin.com/company/myronhelgering)



myronhelgering.com