



November 13-15, Oslo Spektrum

Florian Salzmann & Jannik Reinhard

MAM: Bring Your Own Device to Success

About "Jannik Reinhard"

Focus

AI 🤖, Workspace 🏢, Cloud ☁

From

Germany 🇩🇪

My Blog

Jannikreinhard.com



Certifications

Dual MVP + many MS Certifications



Hobbies

Various Sports 🚴🏊⚽
Blogging 📝
Speaking 🎤
Traveling ✈

Contact

- X (formerly Twitter) 🐦
- LinkedIn 💼
- Blog 📝
- Email ✉



About “Florian Salzmänn”

Focus

Endpoint Management / Intune

From

Switzerland CH

My Blog

scloud.work



Hobbies

Travel ✈️
Tech 🖥️
Wine 🍷

Contact

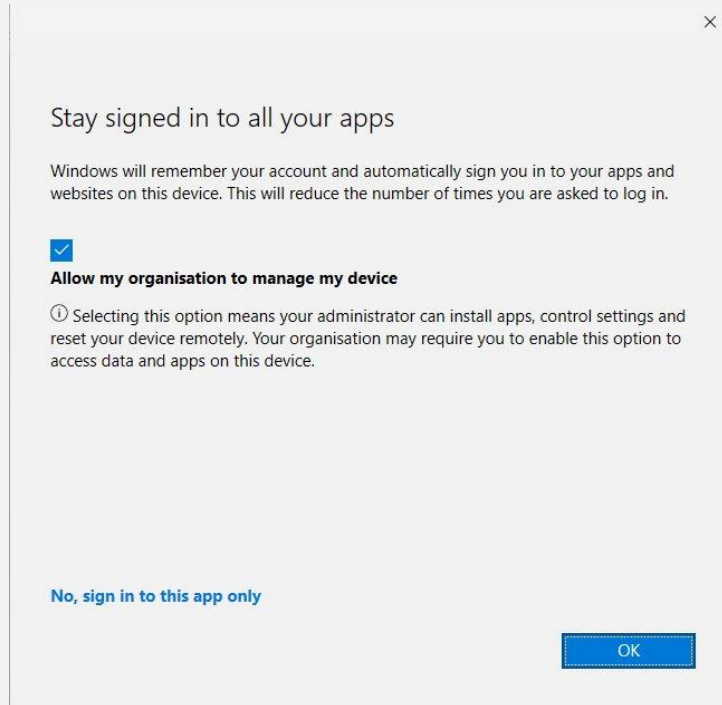
@FlorianSLZ






Agenda

- Securing Corporate Data on Personal Devices
- Mobile Application Management (MAM)
- MAM for Windows
- MAM for Mobile
- MAM for the Rest
- Demo

Have you seen this prompt before?



Don't wonder you will find them here!

<input type="checkbox"/>	Name 	Enabled	OS	Version	Join type	Owner	MDM	Security settings m...	Compliant
<input type="checkbox"/>	 DESKTOP-3JPGJIN	 Yes	Windows	10.0.19045.4842	Microsoft Entra registered	Adele Vance	None	N/A	N/A

Improvements on the way!

×

Automatically sign in to all desktop apps, websites, and services on this device?

Selecting **Yes, all apps** will:

- Allow us to use your work or school account to sign you in to other desktop apps, websites, and services you use on this device.
- Register this device with your organization, allowing your organization to view device information like the device's name.

Is **this a shared device**? If so, consider signing in to this app only.

Your organization also needs to manage this device to access some enterprise resources. Allowing this will enable your IT admin to perform various operations remotely like controlling settings, installing apps, and resetting this device.

☒ Allow my organization to manage this device.

[Learn more](#)

No, this app only

Yes, all apps

“Solution”

[Home](#) > [Devices | Enrollment](#) > [Enrollment restrictions](#) > [All Users | Properties](#) >

Edit restriction

Device type restriction

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)	<div>AllowBlock</div>	Allow min/max range: <div>MinMax</div>	<div>AllowBlock</div>	<div>Manufacturer name</div>
Android device administrator	<div>AllowBlock</div>	Allow min/max range: <div>MinMax</div>	<div>AllowBlock</div>	<div>Manufacturer name</div>
iOS/iPadOS	<div>AllowBlock</div>	Allow min/max range: <div>MinMax</div>	<div>AllowBlock</div>	Restriction not supported
macOS	<div>AllowBlock</div>	Restriction not supported	<div>AllowBlock</div>	Restriction not supported
Windows (MDM) ⓘ	<div>AllowBlock</div>	Allow min/max range: <div>MinMax</div>	<div>AllowBlock</div>	Restriction not supported

Security become more and more important!

Securing Corporate Data on Personal Devices



Growing use of personal devices in the workplace



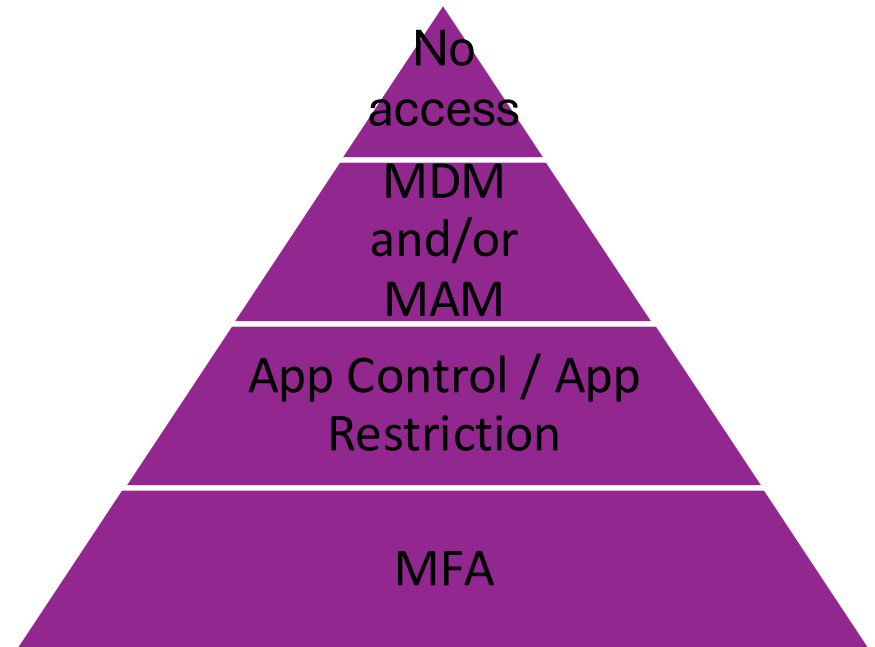
Risks associated with unmanaged devices



Benefits of a multi-layered security approach

Multi-Layered Security Approach

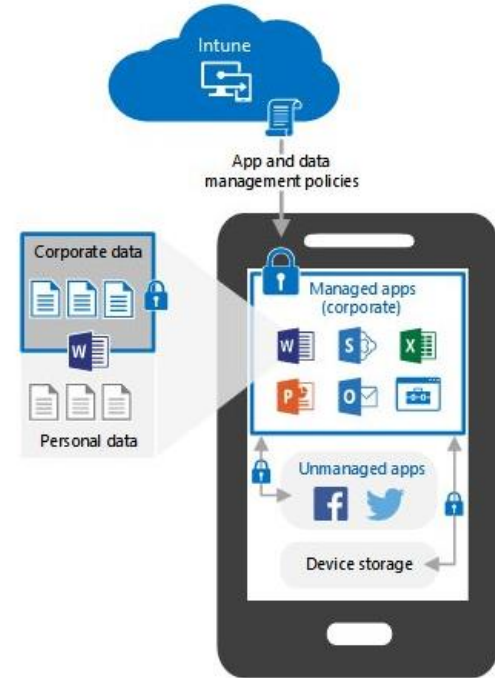
- Block all corporate data access
- MDM and/or MAM
- Access through browser with control
- Enforce MFA



What is MAM?

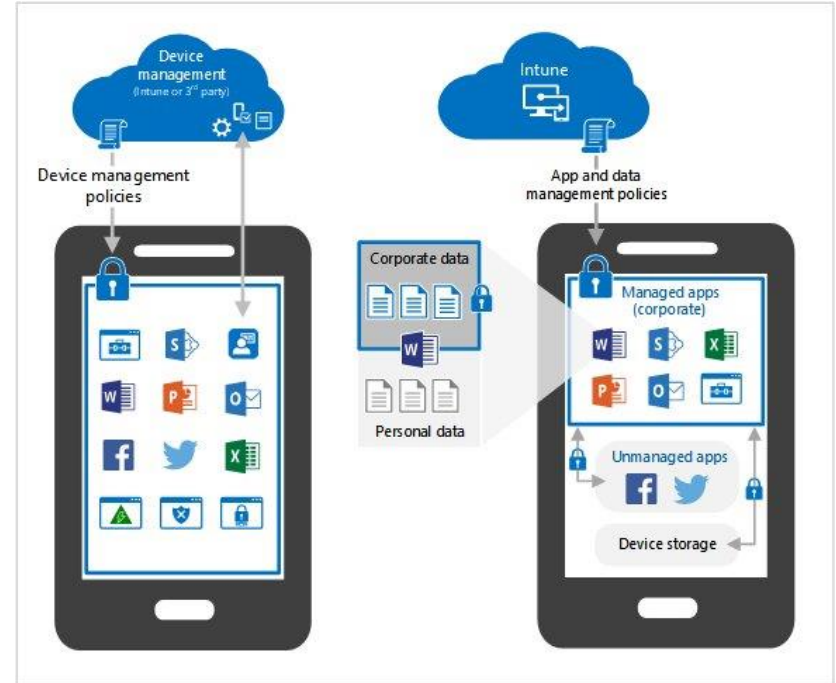
Mobile Application Management (MAM)

- What is MAM?
 - Manage the application
 - Secure data on personal devices
- Key Features
 - Control with App Protection
 - Data Encryption
 - Copy/Paste Control
 - Selective Wiping

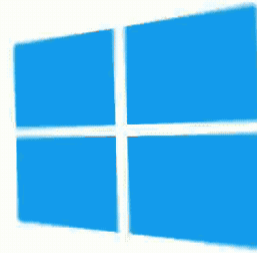
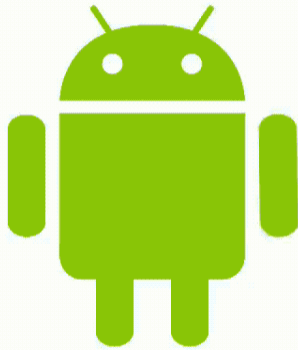


Differences between MAM/MDM

- Differences between MAM/MDM
 - Mobile **Application** Management
 - Mobile **Device** Management



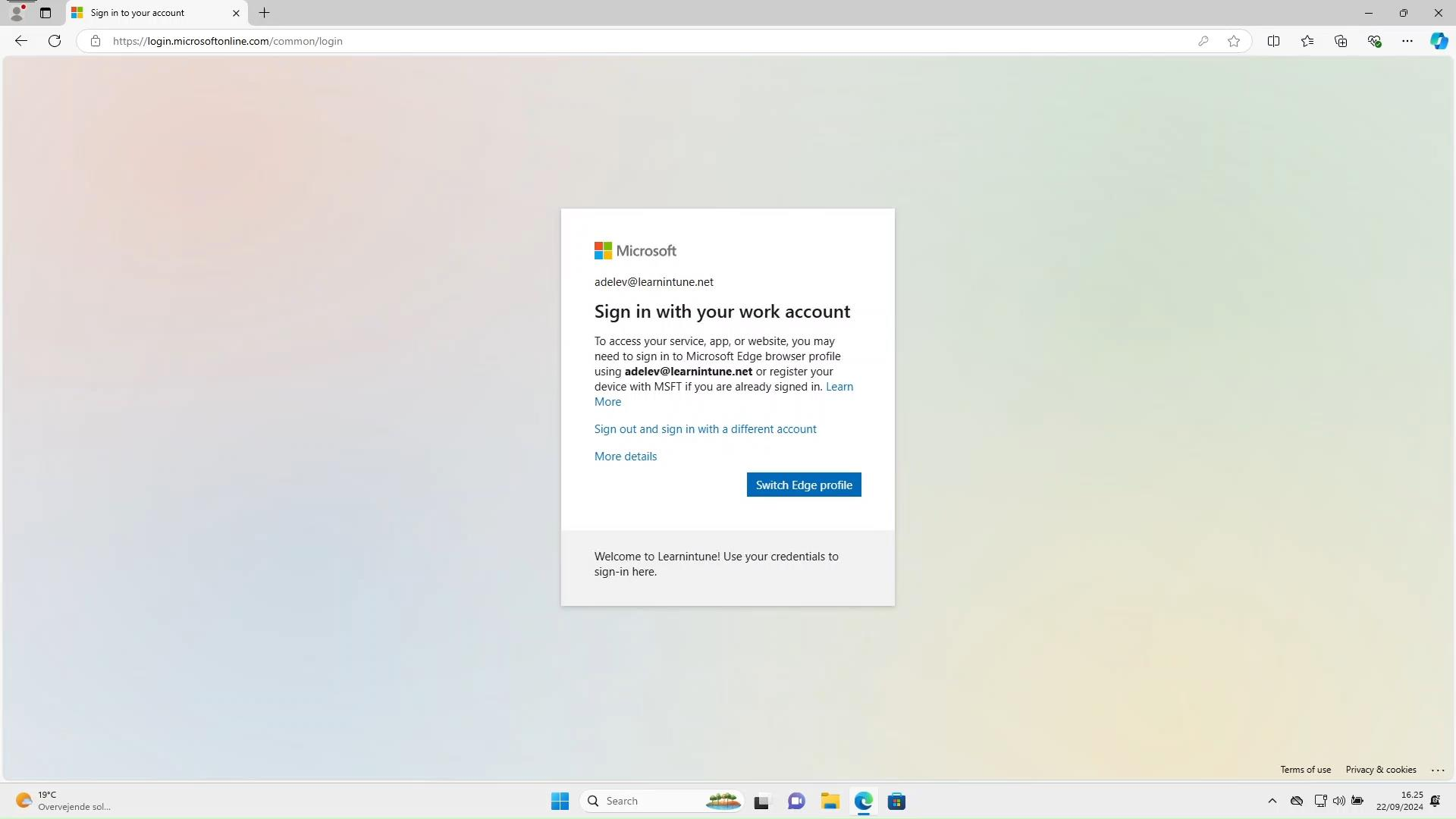
Supported Operating Systems



MAM for Windows

MAM for Windows

- Key Points
 - Controlled data access
 - Run in Container
- Limitations
 - Only available for Edge on Windows
 - Enrolment experience for the end-user



adelev@learnintune.net

Sign in with your work account

To access your service, app, or website, you may need to sign in to Microsoft Edge browser profile using **adelev@learnintune.net** or register your device with MSFT if you are already signed in. [Learn More](#)

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

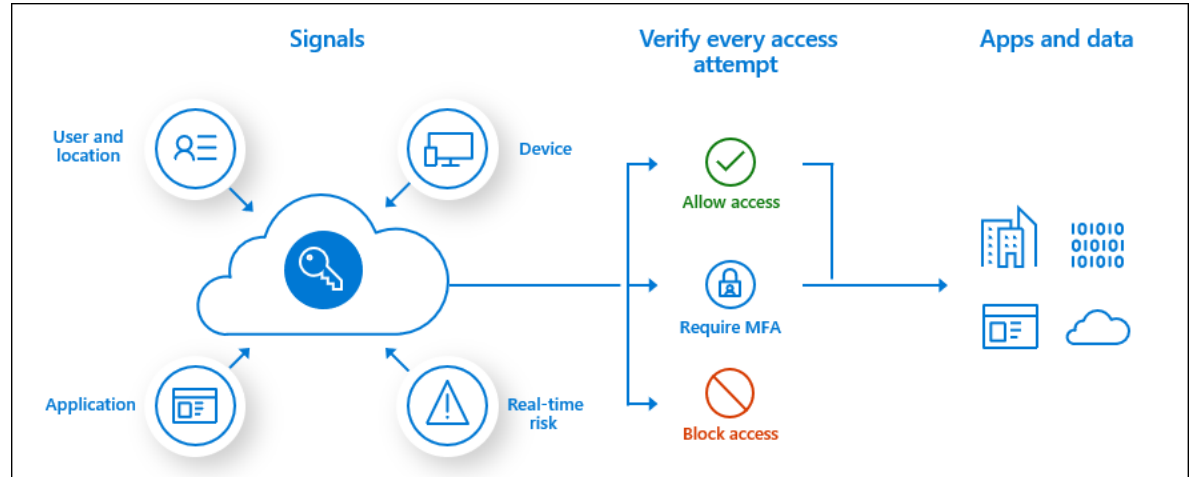
[More details](#)

Switch Edge profile

Welcome to Learnintune! Use your credentials to sign-in here.

Interaction with conditional Access

- Ensure comprehensive security across all access points
 - Key Components
 - Conditions
 - Controls
 - Policies



MAM for Mobile

07:32



-



Finace



Healthcare&Fit...



YouTube



Social



News



Sport



Home



Shops



Foto & Audio



Work



Travel



Asana



1Password



mobile access



HA Davos

Search



Let's also have a look at the admin experience

Apps - Microsoft Intune admin ce

https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/AppsMenu/~-/appProtection

Microsoft Intune admin center

Globaladm@learnintun...MSFT (LEARNINTUNE.NET)

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home > Apps

Apps | App protection policies

Search

Create policy

Refresh

Columns

Export

App protection report: WIP via MDM

Overview

All apps

Monitor

By platform

- Windows
- iOS/iPadOS
- macOS
- Android

Policy

- App protection policies
- App configuration policies
 - iOS app provisioning profiles
 - S mode supplemental policies
 - Policies for Office apps
 - Policy sets
 - Quiet time
- Other
 - App selective wipe
 - App categories
 - E-books
 - Filters
- Help and support
 - Help and support

Important:

On June 1, 2024 Apps with an SDK older than 17.7.0 will no longer get App Protection Policy updates and users will be blocked from launching the app. Please ensure users are updating their apps and your line of business apps are using a recent SDK or wrapper. [Learn More](#)

Search by policy

Policy	Deployed	Updated	Platform	Management type	Apps
You have no policies.					

New - Microsoft Entra admin center

+

←

↺

https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade

🏠

🔊

☆

🖨

🔖

🔒

🌐

...

🔍

Globaladm@learnintun...
MSFT (LEARNINTUNE.NET)

Microsoft Entra admin center

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

🔔

⚙

?

🗨

Home

What's new

Diagnose & solve problems

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Roles & admins

Protection

Identity Protection

Conditional Access

Authentication methods

Password reset

Custom security attributes

Risky activities

Identity Governance

External Identities

Show more

Learn & support

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 *
Example: 'Device compliance app policy'

Assignments

Users
0 users and groups selected

Target resources
No target resources selected

Network NEW
Not configured

Conditions
0 conditions selected

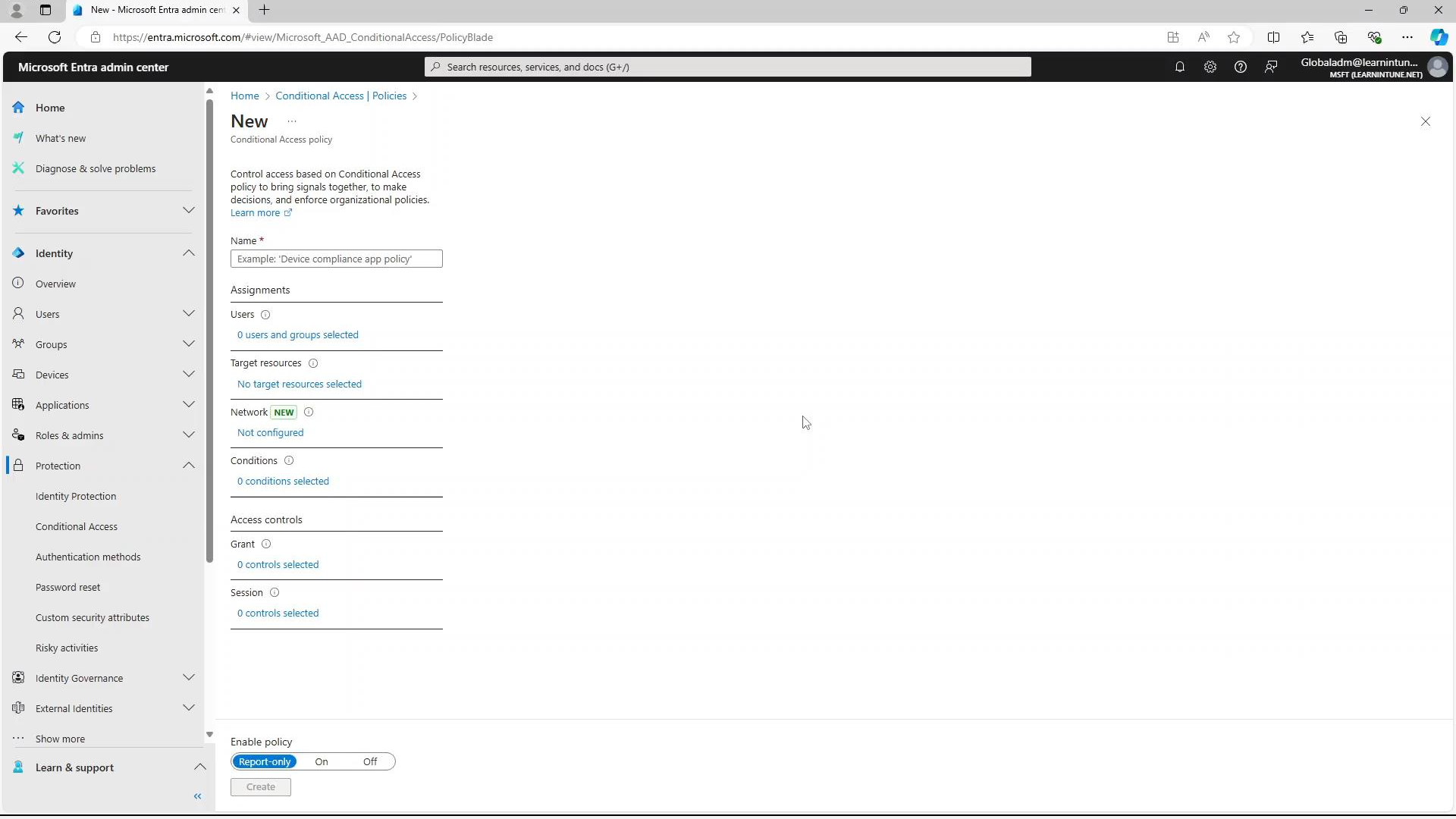
Access controls

Grant
0 controls selected

Session
0 controls selected

Enable policy
Report-only On Off

Create



Selective Wipe

Selective Wipe

- **Managed Applications**
- **Wipe Requests**
 - Device based
- **User-Level**
 - Across all platforms
- **Things to consider**
 - Internet access
 - Up to 30 min delay
 - Access the application

Selective Wipe

- Performing Wipe Requests

Create wipe request ...

Select a user and one or more devices to selectively remove company app data.

User

Adele Vance

[Select user](#)

Device

☐

Device name

Device type

☐

DESKTOP-3JPGJIN

Desktop

User ↑↓	State ↑↓	App ↑↓	Device name ↑↓	Device type ↑↓	Time ↑↓
Adele Vance	 pending	Microsoft Edge	DESKTOP-3JPGJIN	Desktop	9/13/24, 4:38 PM

Selective Wipe

Microsoft Edge Application Management

Org data removal

Your organization is now removing its data associated with Microsoft Edge because your account AdeleV@learnintune.net is disabled.

OK

Troubleshooting

Logs & Troubleshooting

Edge DLP Internals

Feature Status #

Feature Flags for Data Loss Prevention #		Status of Data Loss Prevention Providers #	
Feature Flag Name	Feature Flag State	Provider Name	Provider State
msDataProtection	Enabled	Window Information Protection (WIP)	Not Available
msEndpointDlp	Enabled		
msMdatpWebSiteDlp	Enabled	Endpoint DLP	Not Available
msMdatpWebSiteDlpv2	Not Enabled		
msMdatpWebSiteDlpMac	Not Enabled	Endpoint DLP (WebSite)	Not Available
msEgressPaste	Not Enabled		
msEgressPasteMac	Not Enabled	Insider Risk Management (IRM)	Not Available
msIrm	Enabled		
msIrmv2	Enabled	Mam Intune Data Loss Prevention (Mam Dlp)	Available
msMamDlp	Enabled		
msMamDlpMac	Not Enabled	SaaS DLP	Not Available
msSaasDlp	Enabled		
msSaasAndEndpointDlp	Not Enabled		

Policies Per tab #

[Return Top List](#)

Policies

MAM DLP Policies #

MAM DLP Policy Settings	
Edge identity:	@0kybc.onmicrosoft.com
Printing policy:	Block
Data receipt policy:	NoSources
Data transmission policy:	NoDestinations
Cut/copy/paste policy:	NoDestinationsAndSources

Edge://edge-dlp-internals

MAM Internals

Feature Flags:

- msCloudPolicyMam: enabled

Account Creation links

user@domain.com https://www.bing.com

Deep Link: [about:blank](#)

External Link: [about:blank](#)

Utilities

Simulate Healthcheck: Missing Policy Warn Simulate Health Check

Simulate Idle: In 5 seconds

Edge://mam-internals

AppData > Local > Microsoft > Edge > User Data >			
Name	Date modified	Type	Size
Nurturing	22/10/2023 19:43	File folder	
OriginTrials	22/10/2023 19:45	File folder	
PKIMetadata	22/10/2023 19:43	File folder	
Profile 1	28/10/2023 19:05	File folder	
RecoveryImproved	22/10/2023 19:43	File folder	
Safe Browsing	22/10/2023 19:43	File folder	
SafetyTips	22/10/2023 19:43	File folder	
ShaderCache	22/10/2023 19:43	File folder	
SmartScreen	22/10/2023 19:43	File folder	
Speech Recognition	22/10/2023 19:43	File folder	
Subresource Filter	22/10/2023 19:43	File folder	
Trust Protection Lists	22/10/2023 19:43	File folder	
TrustTokenKeyCommitments	22/10/2023 19:43	File folder	
Web Notifications Deny List	22/10/2023 19:43	File folder	
WidevineCdm	22/10/2023 19:43	File folder	
WorkspacesNavigationComponent	22/10/2023 19:43	File folder	
ZxcvbnData	22/10/2023 19:43	File folder	
BrowserMetrics-spare.pma	22/10/2023 19:45	PMA File	4,096 KB
First Run	22/10/2023 19:43	File	0 KB
FirstLaunchAfterInstallation	22/10/2023 19:43	File	0 KB
Last Browser	22/10/2023 19:44	File	1 KB
Last Version	22/10/2023 19:43	File	1 KB
Local State	28/10/2023 19:03	File	42 KB
lockfile	22/10/2023 19:43	File	0 KB
MamCache.json	28/10/2023 18:52	JSON File	34 KB
MamLog	28/10/2023 18:52	Text Document	5 KB
Variations	22/10/2023 19:44	File	1 KB

MamLog & MamCache

Selective Wipe - MamLog

[2024-09-13T13:56:37.308Z] [INFO] Requested check-in to the MAM Service for UserID:15b1e172-31ba-475a-9795-2f0eef46a184 is complete. (client-request-id:42bc5a34-1b76-43c8-9a1d-fa6fa9c539cd)

[2024-09-13T13:56:37.322Z] [INFO] Check-in for UserID:15b1e172-31ba-475a-9795-2f0eef46a184 is complete with a remote wipe command.

[2024-09-13T13:56:37.322Z] [INFO] Received a remote selective wipe command for UserID:15b1e172-31ba-475a-9795-2f0eef46a184.

[2024-09-13T13:56:37.322Z] [INFO] Remote Wipe 6b13f4a6-ee25-45df-bd27-66a97b0a580d for UserID:15b1e172-31ba-475a-9795-2f0eef46a184.

[2024-09-13T13:56:37.352Z] [INFO] Queuing unenrollment to wipe UserID:15b1e172-31ba-475a-9795-2f0eef46a184 to run as soon as possible.

[2024-09-13T13:56:37.352Z] [INFO] Application protection enforcement action 6b13f4a6-ee25-45df-bd27-66a97b0a580d for UserID:15b1e172-31ba-475a-9795-2f0eef46a184 is complete.

[2024-09-13T13:56:37.352Z] [INFO] Wiping UserID:15b1e172-31ba-475a-9795-2f0eef46a184.

[2024-09-13T13:56:37.482Z] [INFO] Unenrollment request to MAM Service for UserID:15b1e172-31ba-475a-9795-2f0eef46a184 complete. (client-request-id:127914c4-c6cf-454f-8f85-0ce3985a03cb)

[2024-09-13T13:56:37.482Z] [INFO] Successfully deleted application instance for UserID:15b1e172-31ba-475a-9795-2f0eef46a184. (client-request-id:127914c4-c6cf-454f-8f85-0ce3985a03cb)

[2024-09-13T13:56:37.483Z] [INFO] Telemetry collector for general events changed to Global.

[2024-09-13T13:56:37.483Z] [INFO] Removed the service location session state for UserID:15b1e172-31ba-475a-9795-2f0eef46a184.

[2024-09-13T13:56:37.483Z] [INFO] Removing Application Protection for unenrolled UserID:15b1e172-31ba-475a-9795-2f0eef46a184.

What's about MacOS and Linux?

App Enforced Restrictions

What are App Enforced Restrictions?

- Blocking offline access to SharePoint and Exchange Online

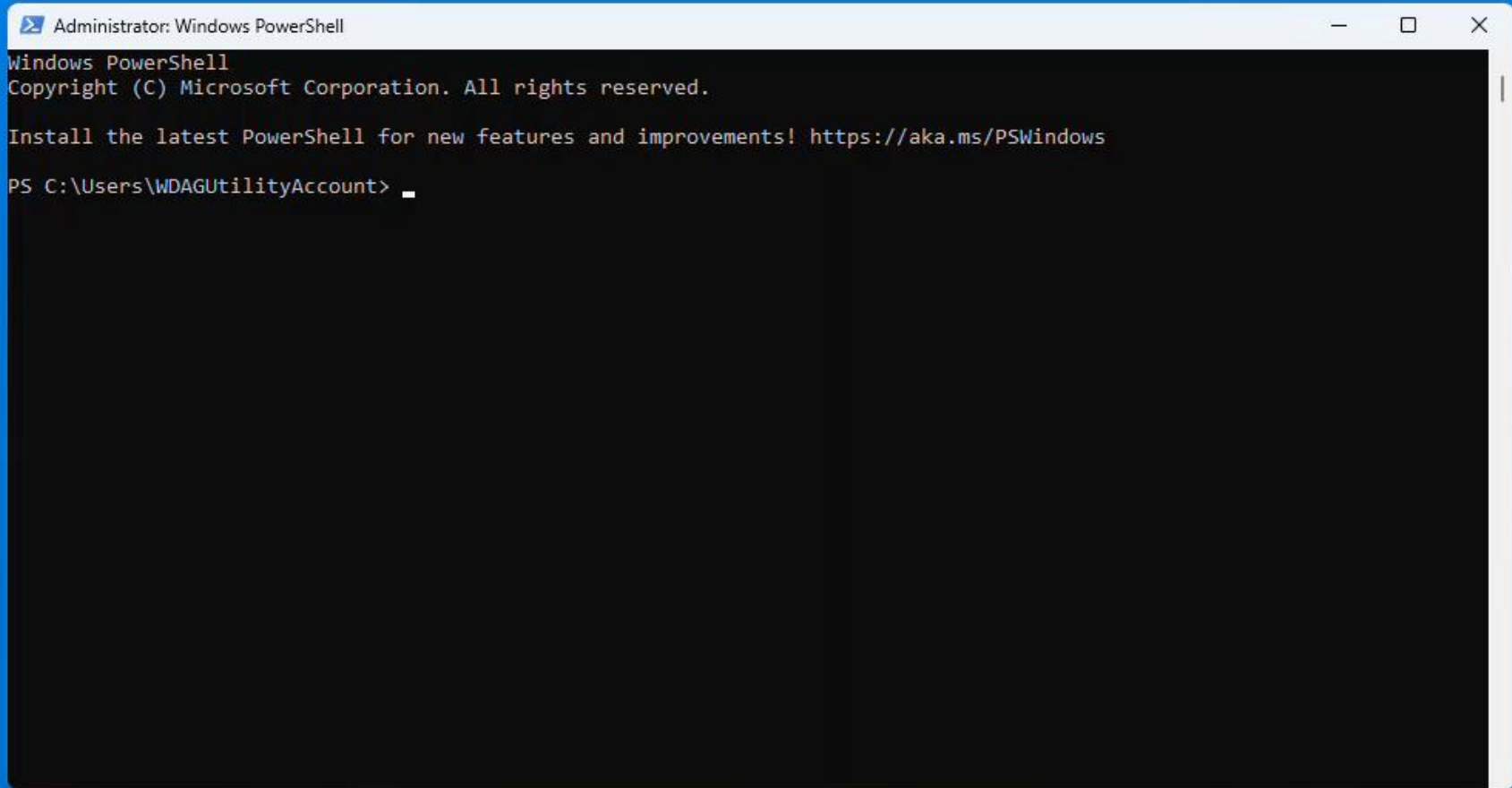
Demo: App Restrictions for Exchange

- How to configure
- Enduser experience (offline access block)

```
Install-Module -Name ExchangeOnlineManagement
```

```
Get-OwaMailboxPolicy | ft Name
```

```
Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default -ConditionalAccessPolicy ReadOnly
```

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window has a white title bar with standard Windows window controls (minimize, maximize, close). The main area is black with white text. The text displayed is: "Windows PowerShell", "Copyright (C) Microsoft Corporation. All rights reserved.", "Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows", and the prompt "PS C:\Users\WDAGUtilityAccount> _".

```
Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\WDAGUtilityAccount> _
```

Activate Policy for Mailbox Policy

CA06 - Office365: AppEnforcedR

Conditional Access policy

 Delete  View policy information

excluded

Target resources ⓘ

1 resource included

Network **NEW** ⓘ

Not configured

Conditions ⓘ

2 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

Use app enforced restrictions

Enable policy

Report-only **On** Off

Save

Session



Control access based on session controls to enable limited experiences within specific cloud applications. [Learn more](#)

☒ Use app enforced restrictions ⓘ

☐ Use Conditional Access App Control ⓘ

☐ Sign-in frequency ⓘ

☐ Persistent browser session ⓘ

☐ Customize continuous access evaluation ⓘ

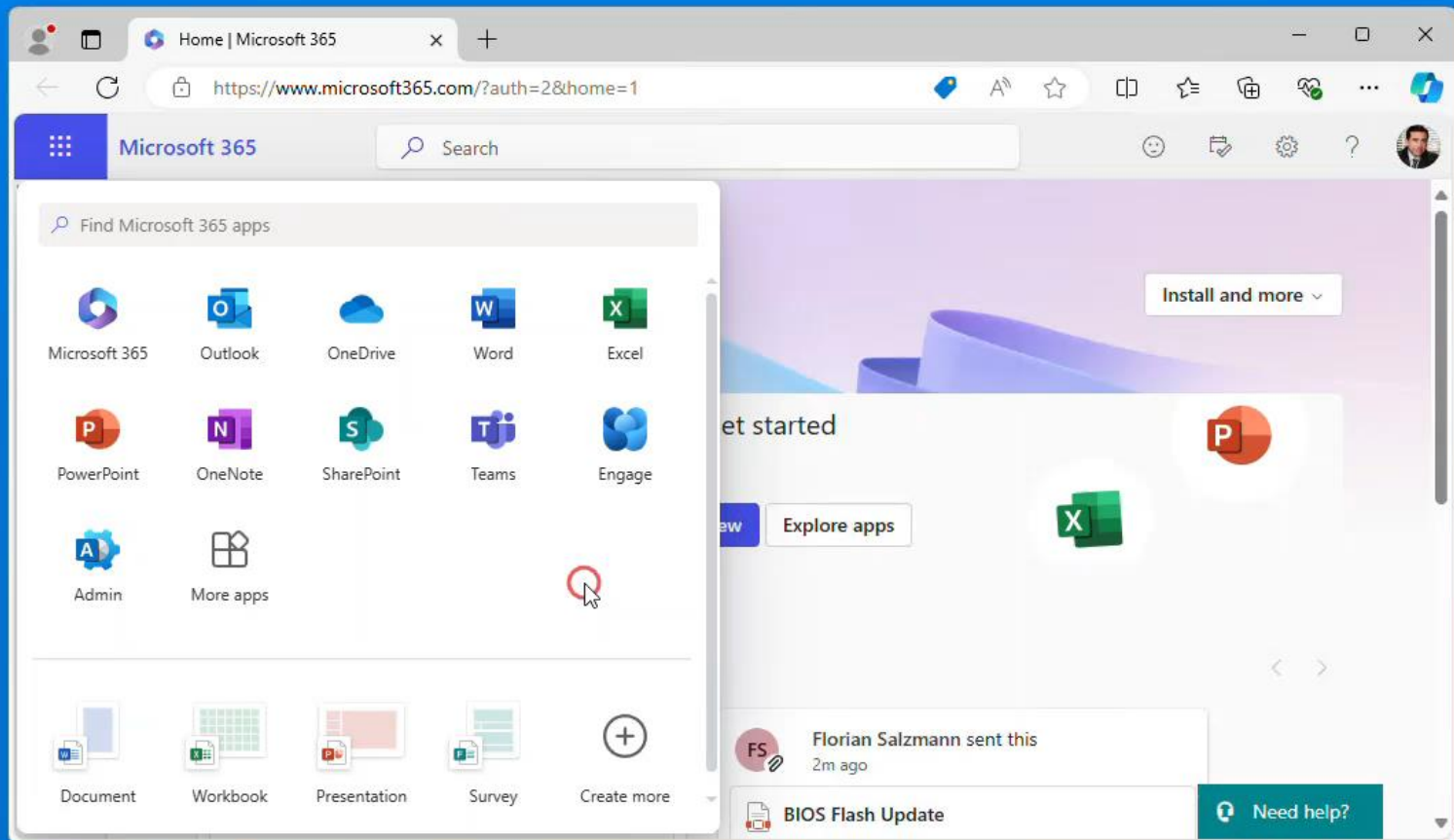
☐ Disable resilience defaults ⓘ

☐ Require token protection for sign-in sessions (Preview) ⓘ

☐ Use Global Secure Access security profile ⓘ

i This option only works with Global Secure Access resources.

Select



App Enforced Restrictions – Exchange Online Enduser Experience

Restriction for a single site

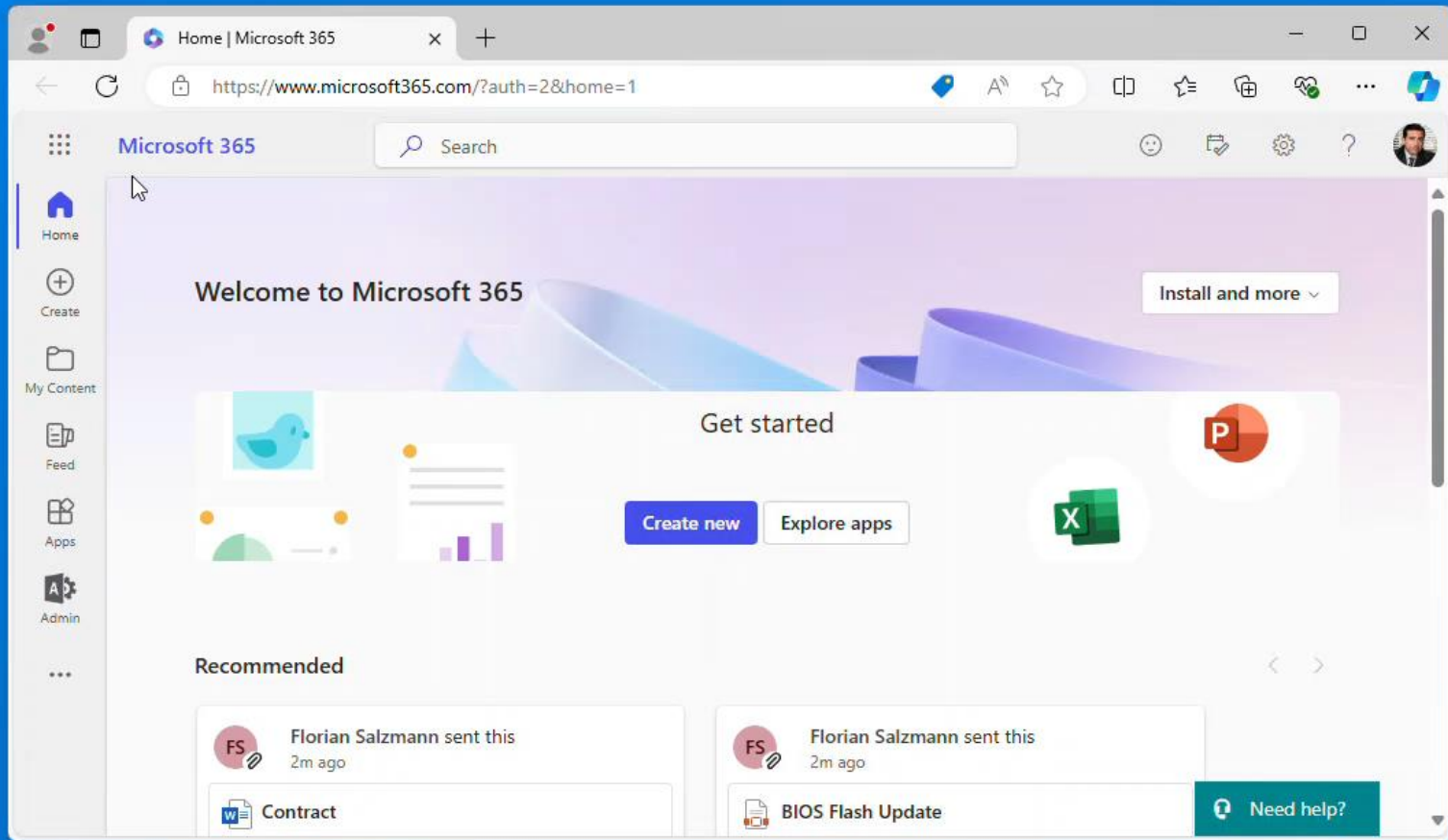
- Set-SPOSite -ConditionalAccessPolicy
 - BlockAccess
 - AllowLimitedAccess

```
Install-Module -Name Microsoft.Online.SharePoint.PowerShell
```

```
Connect-SPOService -URL https://xxx-admin.sharepoint.com/
```

```
Set-SPOSite -Identity https://xxx.sharepoint.com/sites/RD -ConditionalAccessPolicy  
AllowLimitedAccess
```

```
Get-SPOSite -Identity https://xxx.sharepoint.com/sites/RD | Select ConditionalAccessPolicy
```

App Enforced Restrictions – SharePoint Online

Enduser Experience

Conclusion

Conclusion – MAM for Windows

- **Require App Protection Policy**
- **Blocking Office 365 desktop apps**
- **The end-user experience when enrolling a device into MAM**
- **Where to look for logs and troubleshooting?**
- **Non mobile and windows**

Thank you!



NIC
EMPOWER

November 13-15, Oslo Spektrum

Chapter

Dark tile

- Talking points

White tile

- Talking points

Dark, media right

White, media right

