



Six Methods to Protect your Business from the Threat of Unmanaged devices

Myron Helgering



Thank you Sponsors



Gold



RECAST SOFTWARE

Silver



Technical Partners



Daalmans
consulting



Secure At Work



About Myron Helgering

Focus

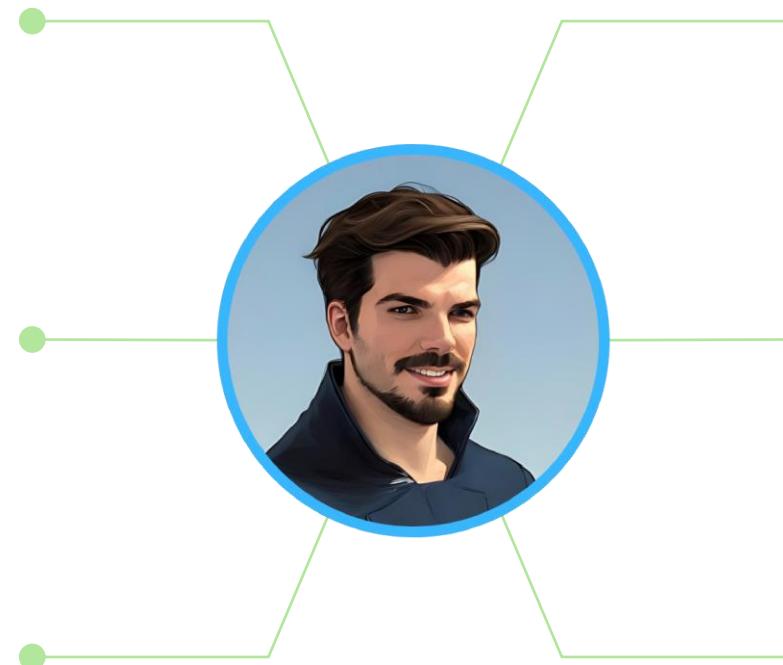
Blogging & Speaking
Microsoft Security MVP

Home

Almere, Netherlands
Wive & Old Rabbit

Work

CTO @ Cloud Life



Hobbies

Snowboarding
Fantasy Geek

Contact

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

My Blog

<https://myronhelgering.com>



Agenda

01

Unmanaged Devices

04

Session Policies

02

Method 1, 2 & 3

05

App Protection Policies

03

App Enforced Restrictions

06

Takeaways & Q&A

What is an unmanaged device?

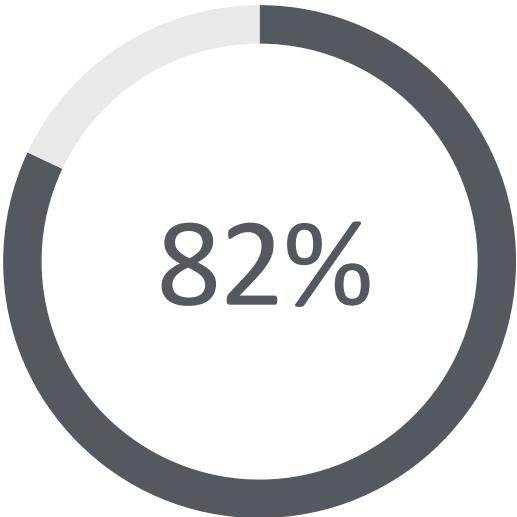
“A device that accesses company apps and data while not being (MDM) managed by the company.”



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

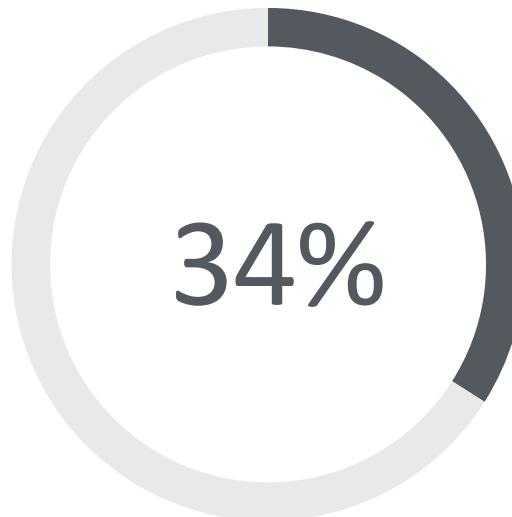


Numbers on unmanaged devices



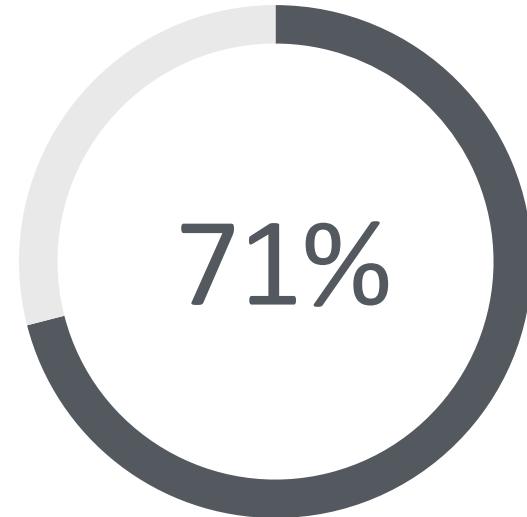
of companies allow the use
of personal devices for work

[Cybersecurity Insiders
BYOD Security Report 2021](#)



of company devices in enterprise
organizations are unmanaged

[Syxsense Vulnerability Gap
Survey 2023](#)



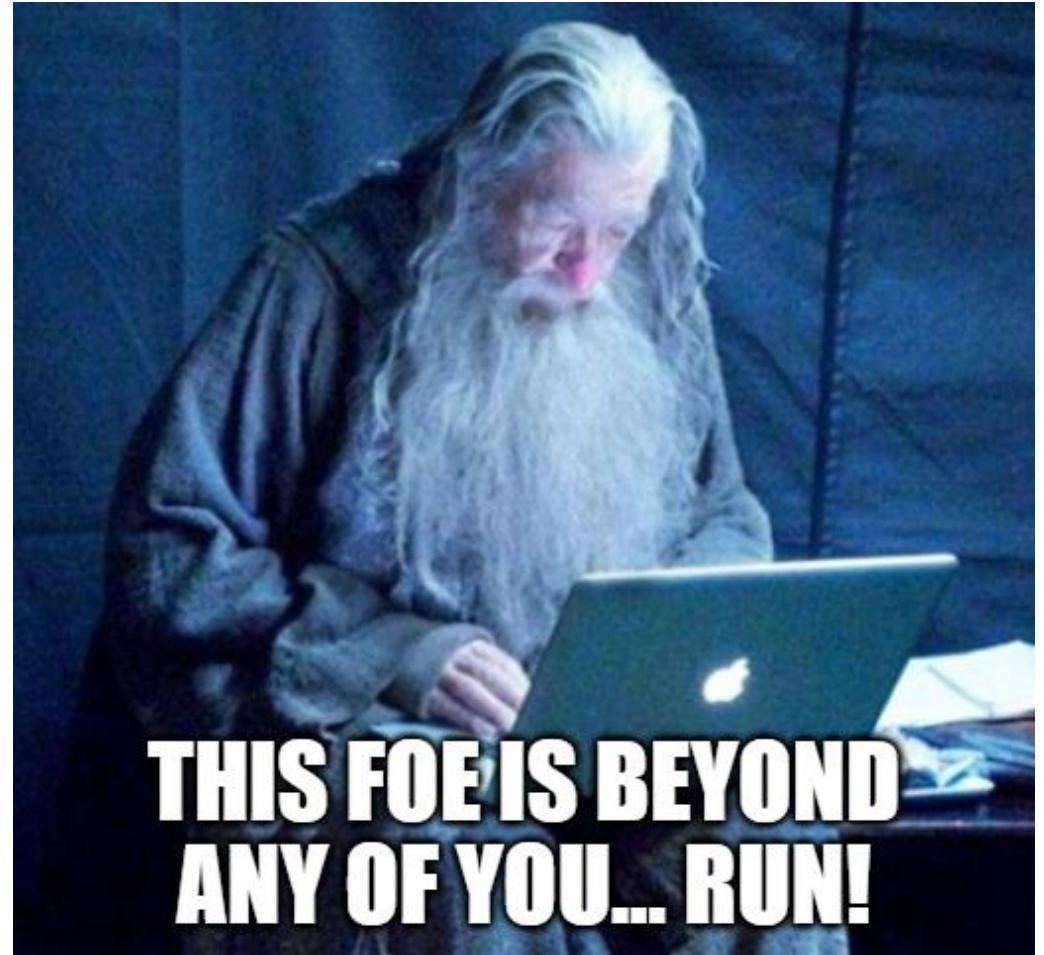
more likely to be infected
on an unmanaged device

[Microsoft Digital Defense
Report 2021](#)



Challenges with unmanaged devices

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





Method 1: Do nothing...

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

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





Example of doing nothing





Method 2: Manage personal devices



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

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



Enrollment during Office sign-in

Stay signed in to all your apps

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

Allow my organization to manage my device

No, sign in to this app only

OK

A blue arrow points from the bottom left towards the 'Allow my organization to manage my device' checkbox, highlighting it.



Personal devices managed by Microsoft Intune

Microsoft Intune admin center

Home > Devices | Windows >

Windows | Windows devices

Search draco-pc

Refresh Export Columns Bulk device actions

OS: Windows Add filters

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

Windows devices

Windows enrollment

Windows policies

- Compliance policies
- Configuration profiles
- Scripts and remediations
- Update rings for Windows 10 and later



Enrollment Restrictions

Type	Platform	versions	Personally owned
Android Enterprise (work profile)	<button>Allow</button> <button>Block</button>	Allow min/max range: <input type="button" value="Min"/> <input type="button" value="Max"/>	<input type="button" value="Allow"/> <button>Block</button>
Android device administrator	<button>Allow</button> <button>Block</button>	Allow min/max range: <input type="button" value="Min"/> <input type="button" value="Max"/>	<input type="button" value="Allow"/> <button>Block</button>
iOS/iPadOS	<button>Allow</button> <button>Block</button>	Allow min/max range: <input type="button" value="Min"/> <input type="button" value="Max"/>	<input type="button" value="Allow"/> <button>Block</button>
macOS	<button>Allow</button> <button>Block</button>	Restriction not supported	<input type="button" value="Allow"/> <button>Block</button>
Windows (MDM) ⓘ	<button>Allow</button> <button>Block</button>	Allow min/max range: <input type="button" value="Min"/> <input type="button" value="Max"/>	<input type="button" value="Allow"/> <button>Block</button>





Example of managing personal devices

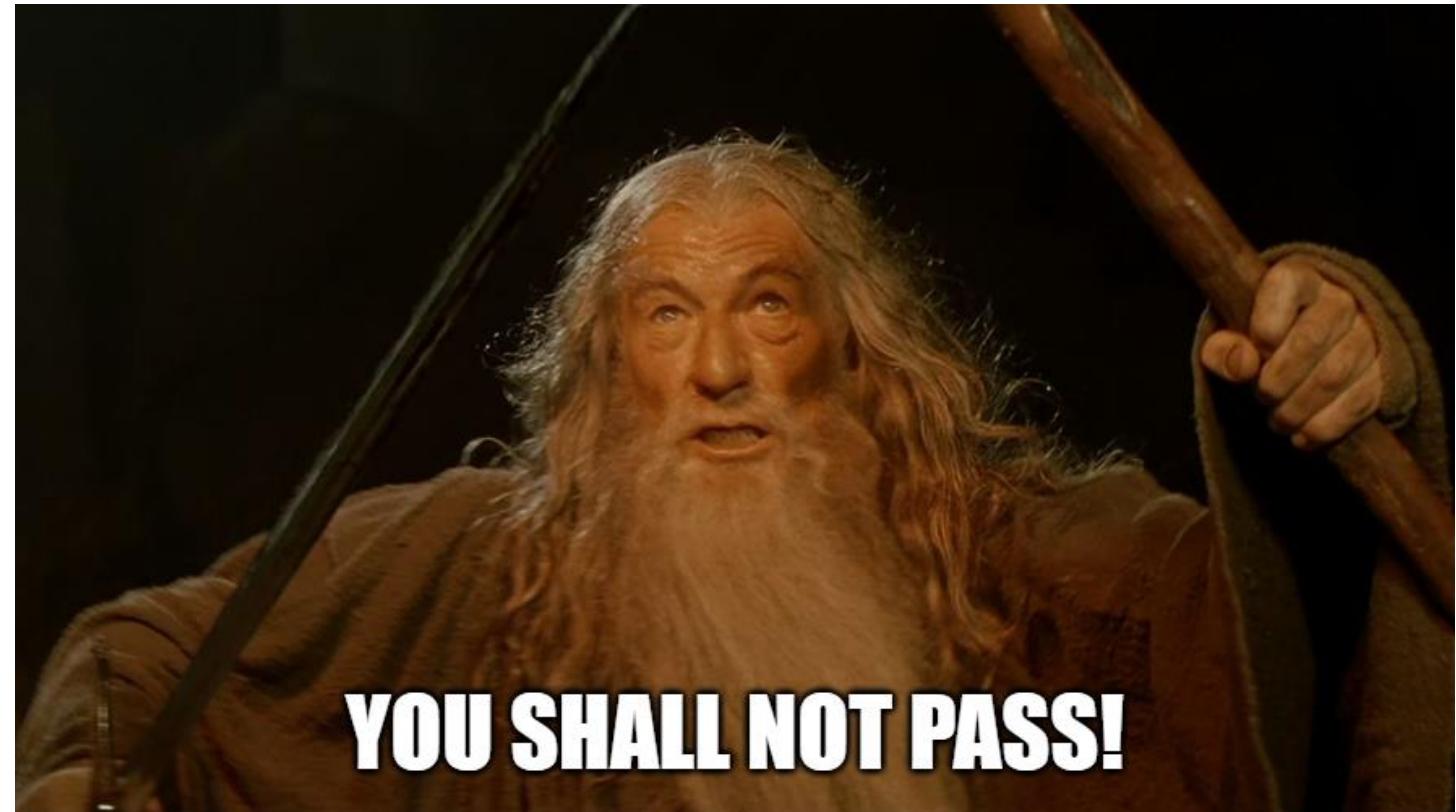


A WELL-EARNED HOLIDAY



Method 3: Block access

- Block access
- Reduces security risks
- Reduces user productivity



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



Block Access with Conditional Access policy

Name *

Block access for unmanaged devices

Assignments

Users ⓘ
All users included and specific users excluded

Target resources ⓘ
All cloud apps

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
2 controls selected

Require device to be marked as compliant

Require Microsoft Entra hybrid joined device



Microsoft

albus.dumbledore@myronhelgering.com

You can't get there from here

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

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

[More details](#)



Some recommendations

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



Method 4: App Enforced Restrictions

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

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





Enable in SharePoint Admin Center (or PowerShell)

Conditional Access policies are created

SharePoint admin center

Access control

Unmanaged devices

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

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

Learn more about controlling access from unmanaged devices.

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

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

Allow limited, web-only access

Block access

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

Learn how to control access to specific sites by using Microsoft PowerShell

Save

Policy Name ↑↓

[SharePoint admin center]Block access from apps on unmanaged devices - 2023/08/21 On

[SharePoint admin center]Use app-enforced Restrictions for browser access - 2023/08/21 On

State ↑↓



Policy 1: Block access from apps on unmanaged devices

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

 Microsoft
albus.dumbledore@myronhelgering.com

You cannot access this right now

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

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

[More details](#)

Policy 2: Use app-enforced restrictions for browser access

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

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



Enable app-enforced restrictions for Exchange Online with Powershell

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Connect-ExchangeOnline
PS C:\WINDOWS\system32> Set-OwaMailBoxPolicy -Identity OwaMailboxPolicy-Default -ConditionalAccessPolicy ReadOnly
PS C:\WINDOWS\system32> Get-OwaMailBoxPolicy | select-object ConditionalAccess*
ConditionalAccessPolicy ConditionalAccessFeatures
-----
ReadOnly {Offline, AttachmentDirectFileAccessOnPrivateComputersEnabled, AttachmentDirectFileAccessO..
.

PS C:\WINDOWS\system32>
```

Set-OwaMailBoxPolicy -Identity OwaMailboxPolicy-Default -ConditionalAccessPolicy ReadOnly



Sensitivity Labels

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

Edit sensitivity label

✓ Name and tooltip
✓ Scope
✓ Items
Groups & sites
● External sharing & conditional access
○ Schematized data assets (preview)
○ Finish

Define external sharing and conditional access settings

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

Control external sharing from labeled SharePoint sites
When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Use Azure AD Conditional Access to protect labeled SharePoint sites
You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.

Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't [hybrid Azure AD joined](#) or enrolled in Intune).
ⓘ For this setting to work, you must also configure the SharePoint feature that blocks or limits access to SharePoint files from unmanaged devices. [Learn more](#)

Allow full access from desktop apps, mobile apps, and the web
 Allow limited, web-only access ⓘ
 Block access ⓘ

[Back](#) [Next](#) [Cancel](#)



Method 5: Session Policies

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

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





Demo

Session Policies with
Microsoft Defender
for Cloud Apps



Conditional Access | Policies

Microsoft Entra ID

« + New policy + New policy from template Upload policy file What if Refresh Preview features Got feedback? ×
i Overview≡ 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

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

All policies**30**

Total

Microsoft-managed policies**1**

out of 30

🔍 Search💡 Add filter

30 out of 30 policies found

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

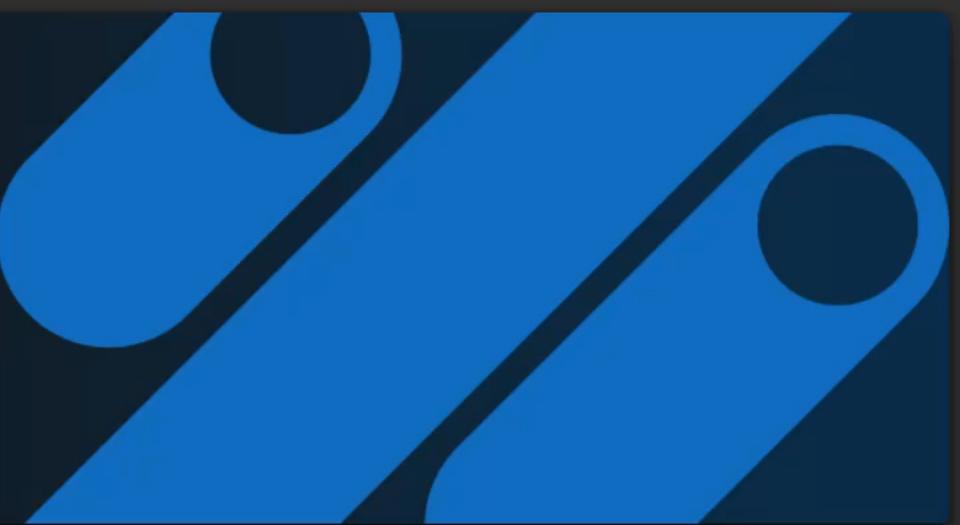
[Home](#)[Incidents & alerts](#)[Hunting](#)[Actions & submissions](#)[Threat intelligence](#)[Learning hub](#)[Trials](#)[Partner catalog](#)[Exposure management](#)[Assets](#)[Endpoints](#)[Identities](#)[Email & collaboration](#)[Cloud apps](#)[Cloud discovery](#)[Cloud app catalog](#)[OAuth apps](#)

Home

[Light mode](#)

Get your SIEM and XDR in one place

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

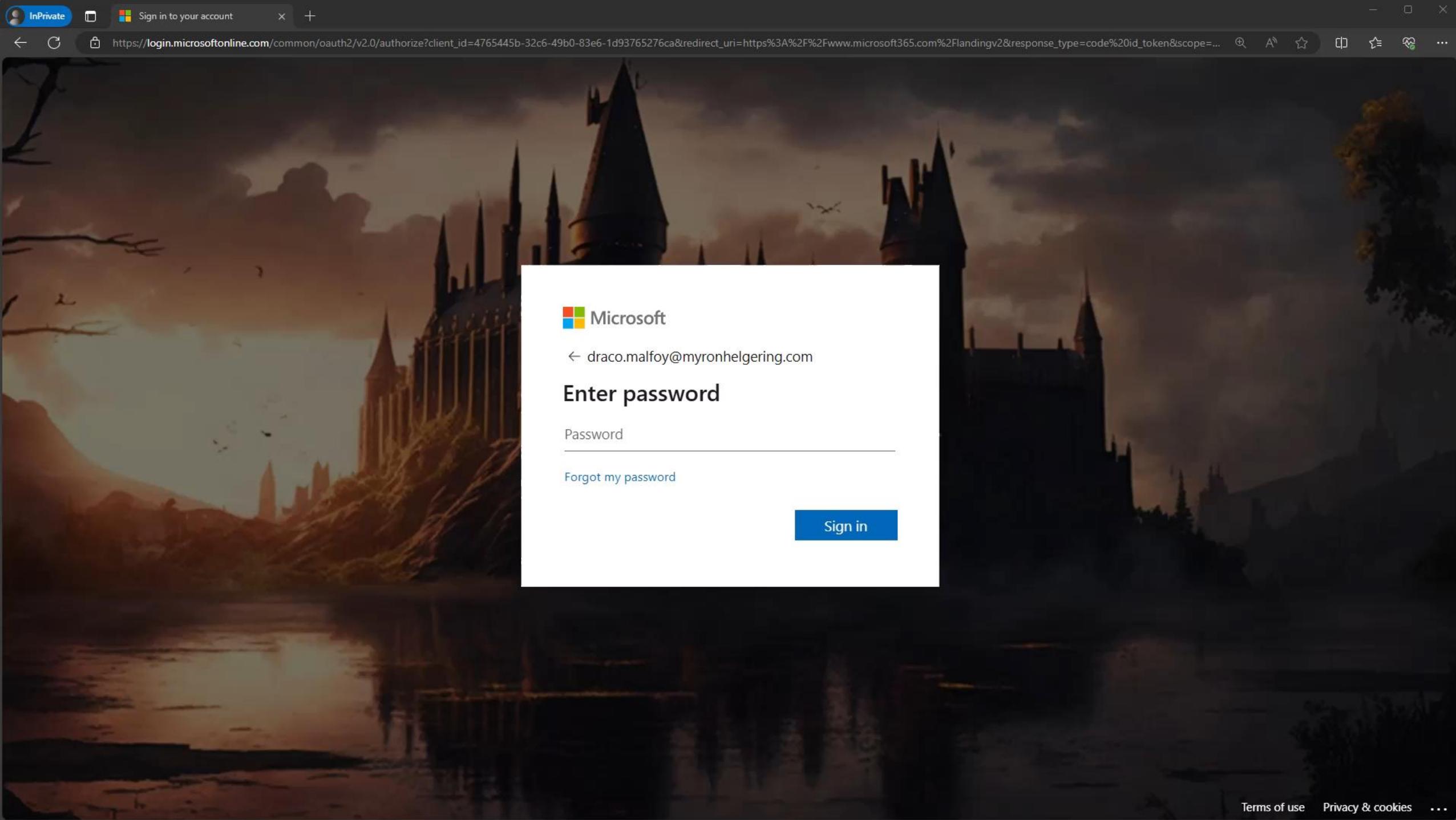
[Connect a workspace](#)[Guided tour](#)[What's new ?](#)[Community](#)[Add cards](#)

Active incidents

No active incidents

No incidents found

[View all incidents](#)





Two ways of protection with session policies

Reverse proxy (Default)

All browsers and operating systems

No user interaction needed

Slower user experience

Easier to bypass controls (dev tools)

Less secure (doesn't support MAM)

Supports all restrictions

In-browser protection (Preview)

Edge for Business with Windows 10/11

Requires Edge profile sign in

Faster user experience

Harder to bypass controls (dev tools)

More secure (supports MAM)

Doesn't support all restrictions yet



Method 6: App Protection Policies

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

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





MAM for Android & iOS

App Protection policy settings

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

The screenshot shows a user interface for managing app protection policies. At the top, there's a navigation bar with a shield icon, the title 'Apps | App protection policies', and a three-dot menu. Below the navigation is a search bar labeled 'Search'. To the right of the search bar are buttons for 'Create policy' (highlighted with a blue arrow), 'Refresh', 'Columns', and 'Export'. A secondary search bar labeled 'Search by policy' is also present. The main area contains a table with columns for 'Policy', 'Deployed', and 'Platform'. Two policies are listed: 'MAM for Android - all users' (Android) and 'MAM for iOS - all users' (iOS/iPadOS). On the left side, there are links for 'Overview', 'All apps', 'Monitor', and sections for 'By platform' (Windows, iOS/iPadOS, macOS, Android) and 'Policy' (highlighted with a blue box).

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



Require app protection policy with Conditional Access

- Authenticator app for iOS
- Company Portal app for Android

Name *

Require app protection policy - Android & iOS

Assignments

Users ⓘ

All users included and specific users excluded

Target resources ⓘ

All cloud apps

Conditions ⓘ

1 condition selected →

Select device platforms

Android

iOS

Access controls

Grant ⓘ

1 control selected →

Require app protection policy

A screenshot of a Conditional Access policy configuration interface. The policy is named "Require app protection policy - Android & iOS". It has no assignments. Under "Target resources", it is set to "All cloud apps". In the "Conditions" section, "Select device platforms" is chosen, and both "Android" and "iOS" are selected. In the "Access controls" section, "Require app protection policy" is selected. Blue arrows point from the text labels to their corresponding configuration fields.



Demo

Mobile Application
Management (MAM)
for Windows



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

Helgering

Welcome to the fresh look for Intune

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

 Give us your feedback



Status

Devices not in compliance
2

Configuration policies with error or conflict
0

Client app install failure
0

Connector errors
0

Service health
Healthy

Account status
Active

[Helgering](#)

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Welcome to the fresh look for Intune

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

Give us your feedback

Status

Devices not in compliance
2

Configuration policies with error or conflict
0

Client app install failure
0

Connector errors
0

Service health
Healthy

Account status
Issues

Conditional Access | Policies

Microsoft Entra ID

« [New policy](#) [New policy from template](#) [Upload policy file](#) [What if](#) [Refresh](#) [Preview features](#) [Got feedback?](#)

[Overview](#)[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](#)

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

[All policies](#)**32**[Microsoft-managed policies](#)**1**

Total

out of 32

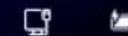
 Search[Add filter](#)

32 out of 32 policies found

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

14:53

Monday, 27 May





What to expect in the future?





Takeaways

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



Bonus Methods!

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



Blogs on unmanaged devices

- [Block access with Conditional Access for Unmanaged Devices](#)
- [Limited Access with Conditional Access for Unmanaged Devices](#)
- [Limited Access with Sensitivity Labels for Unmanaged Devices](#)
- [Limited Access with Session Policies for Unmanaged Devices](#)
- [First look at Mobile Application Management for Windows](#)
- [Mobile Application Management for Android and iOS](#)
- [Blog Series: Unmanaged Devices](#)



in/myronhelgering



myronhelgering.com



Thank You



in/myronhelgering



myronhelgering.com