
# Lessons Learned from many Conditional Access implementations

*Kenneth van Surksum*

# Sponsors


onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

**David O'Brien** • 1st
ARGOS writes your cloud audit report for you! | Founder of ARGOS ...
3w

I mostly get it second hand now, through conversations with consultants using ARGOS, but they typically tell us that the two most common things are "glad I excluded my own user, because I just locked
are excl
include interac
Systems on tha

**Sander Berkouwer** • 1st
Entraordinary Identity Architect | DirTeam
(edited) 4w

A Conditional Access policy with:
Lessons Learned from many Conditional Access implementations

**Jop Gommans** • 1st
Technical project lead
3w

Be careful with creating too many device filters in policies, they might not always work in the way (order) you might think.
Came across this is wanting to create a very explicit policy with a couple of exclusions/inclusions in the device type queries where it worked differently than expected, since those queries (each line) did an "or" instead of an "and"

MODERN ENDPOINT MANAGEMENT SUMMIT 2026

# Agenda


- The obvious
- Conditional Acces implementation
- Block challenges
- Filters
- IP Locations

# THE OBVIOUS

- Naming
- Versioning
- Break Glass accounts
- Some “gotchas”

# THE OBVIOUS


- Even though MS recommends less is better when it comes to CA policies, I prefer granularity
- Conditional Access policy per functionality
- For each Conditional Access policy there is a specific exclude group (which also includes the Breakglass accounts) – protect those groups with Restricted Management Administrative Units (RMUA)
- Therefore, if exceptions are made, they can be very specific
- [illegible] Azure AD P2
- Naming convention is very important, follow MS best practices

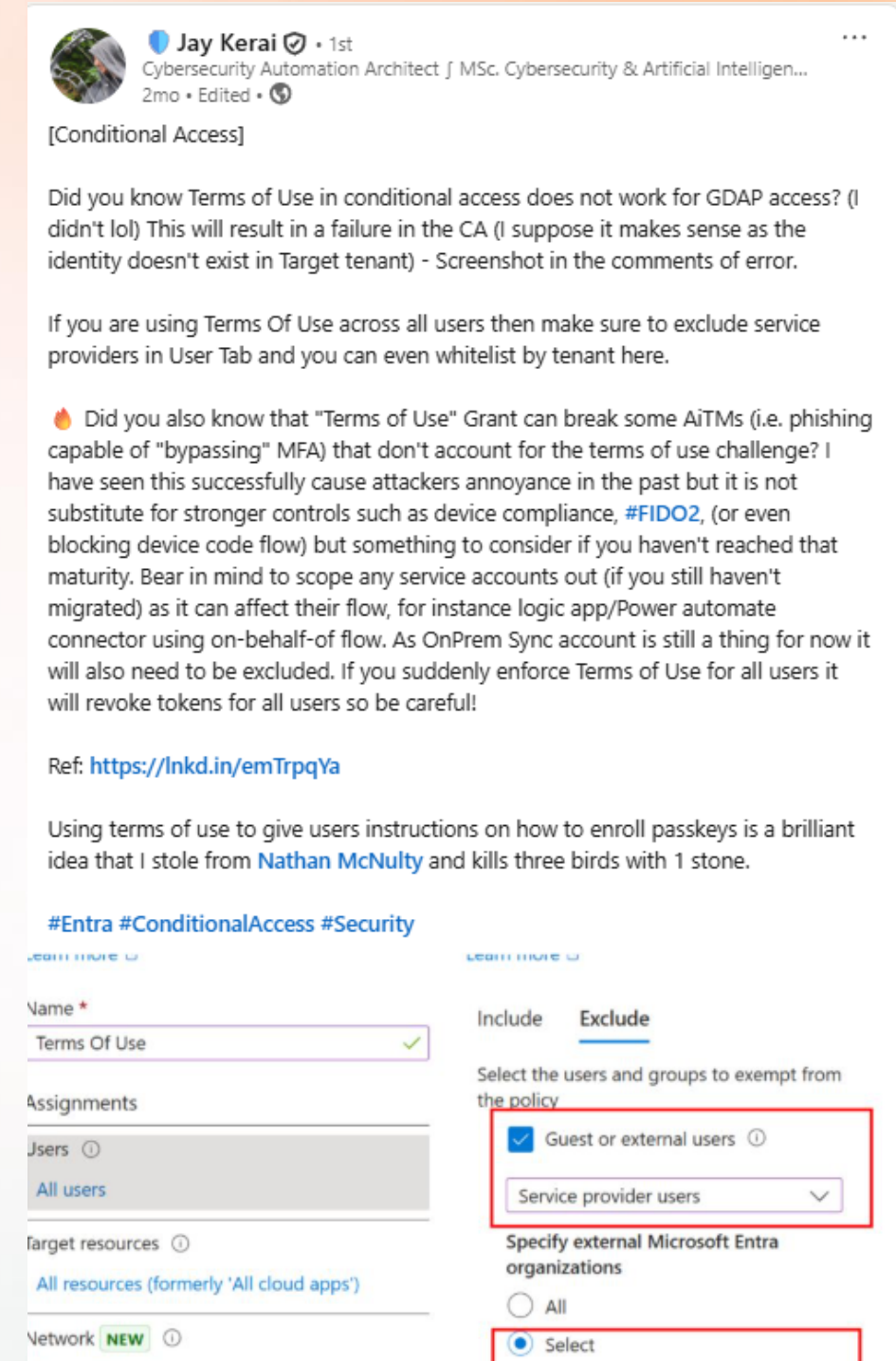
<SN>- <Cloud app>: <Response> For <Principal> When <Conditions>

- The Conditional Access policies are numbered, and versioned
  - CAP = Conditional Access Prerequisite
  - CAU = Conditional Access User
  - CAD = Conditional Access Device
  - CAL = Conditional Access Location
  - CAC = Conditional Access Custom
- Example: CAD007-O365: Session set Sign-in Frequency for Apps for All users when Modern Auth Clients and Non-Compliant-v1.0

# Gotcha's

- **Using Terms of use in combination with GDAP Access**

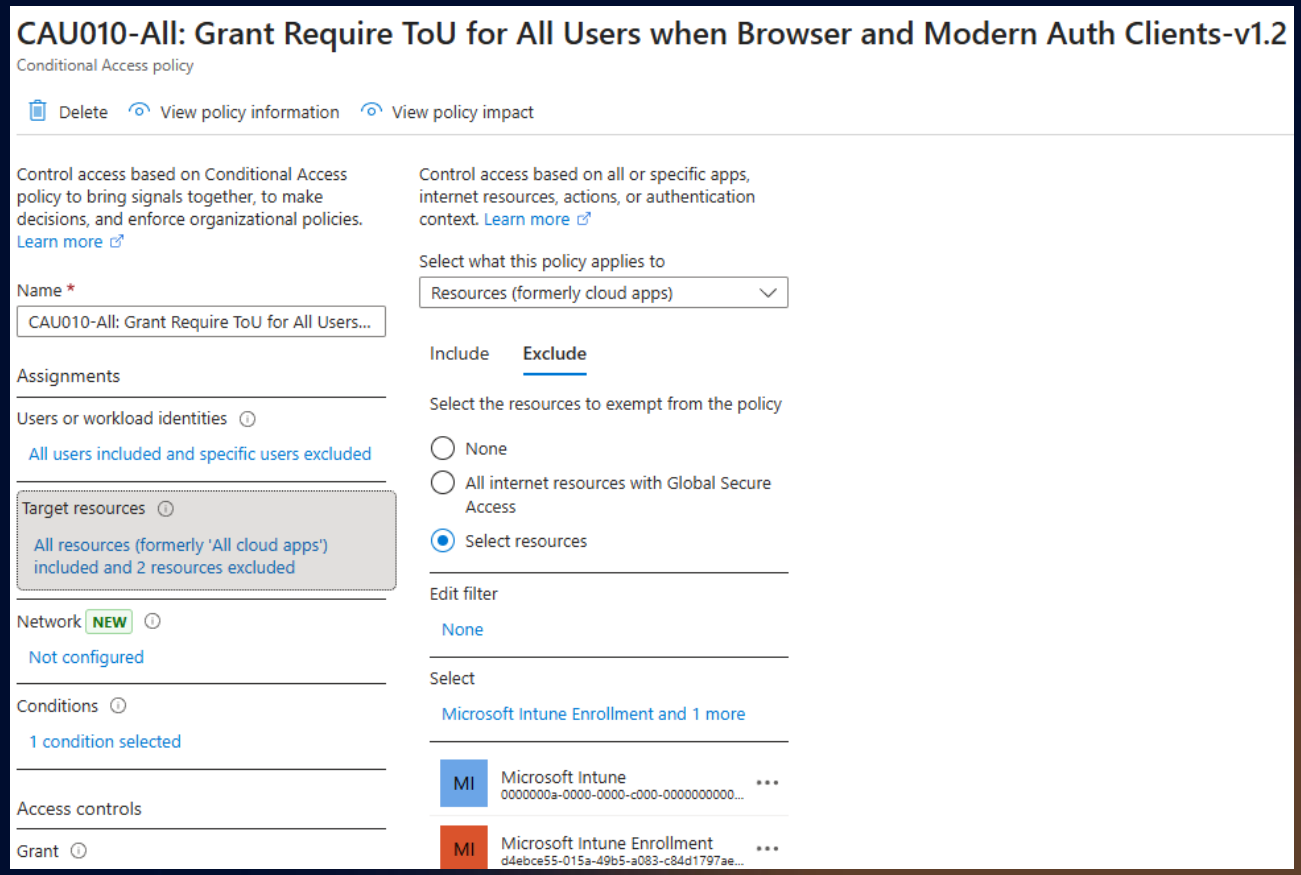
- **Source: Jay Kerai on LinkedIn**



# Gotcha's

- The Intune Enrollment app must be excluded from any Conditional Access policy requiring Terms of Use because it isn't supported.

- **Source:** Windows Autopilot known issues | Microsoft Learn



# Gotcha's


After administrators evaluate the policy settings using policy impact or report-only mode, they can move the **Enable policy** toggle from **Report-only** to **On**.

> ⓘ **Note**
>
> You can enroll your new devices to Intune even if you select **Require device to be marked as compliant** for **All users** and **All resources (formerly 'All cloud apps')** using the previous steps. **Require device to be marked as compliant** control does not block Intune enrollment.

# Gotcha's

- **Remote Help on Windows**

## Building a Conditional Access policy

After the Remote Help service principal is created, learn more on how to set up a conditional access policy.

To apply conditional access policies to Remote Help, follow these steps:

1. Navigate to the conditional access policy that you created.
2. Select **Target resources**
   a. Select **Resources (formerly cloud apps)** to specify what this policy applies to.
   b. Select **Exclude**.
   c. Select **Select resources**.
   d. Under **Select**, check the **RemoteAssistanceService** with the app ID of 1dee7b72-b80d-4e56-933d-8b6b04f9a3e2

- Source: Using Remote Help on Windows to assist authenticated users. - Microsoft Intune | Microsoft Learn

# Gotcha's


## Teams Phones

### When and when not to require compliant shared devices

> **Note**
>
> Device compliance requires an Intune license.

When enrolling shared devices into Intune, you can configure dev
that only compliant devices can access your corporate resources.
Access policies based on device compliance. For more informatio

> **Note**
>
> Shared devices being used for *hot-desking* should be excluded from compliance policies. Compliance policies prevent the devices from enrolling into the hot desk user account. **Instead, use named locations to secure these devices**. To increase security, you can also **require multi-factor authentication** for *hot-desking users / user accounts* in addition to the named location policies.

### Exclude shared devices from sign-in frequency conditions

In Conditional Access, you can configure sign-in frequency to require users to sign in again to access a resource after a specified time period. If sign-in frequency is enforced for phone resource accounts, shared devices sign out until they're signed in again by an admin. Microsoft recommends excluding shared devices from any sign-in frequency policies.

- Source: Authentication best practices for Teams phones - Microsoft Teams | Microsoft Learn

# Gotcha's

## Microsoft Defender for Endpoint

> **Note**
>
> You can use the Microsoft Defender for Endpoint app along with the **Approved Client app** , **App Protection policy** and **Compliant Device** (Require device to be marked as compliant) controls in Microsoft Entra Conditional Access policies. There's no exclusion required for the Microsoft Defender for Endpoint app while setting up Conditional Access. Although Microsoft Defender for Endpoint on Android & iOS (App ID - dd47d17a-3194-4d86-bfd5-c6ae6f5651e3) isn't an approved app, it is able to report device security posture in all the three grant permissions.
>
> However, internally Defender requests **MSGraph/User.read** scope and **Intune Tunnel** scope (in case of Defender+Tunnel scenarios). So these scopes must be excluded*. To exclude MSGraph/User.read scope, any one cloud app can be excluded. To exclude Tunnel scope, you need to exclude 'Microsoft Tunnel Gateway'.These permission and exclusions enables the flow for compliance information to Conditional Access.

- Source: Configure Conditional Access in Microsoft Defender for Endpoint - Microsoft Defender for Endpoint | Microsoft Learn

# Gotcha's

## Microsoft Defender mobile app

## *New-MgServicePrincipal*

### Microsoft Defender mobile app exclusion from Conditional Access (CA) Policies

The Microsoft Defender mobile app is a security app that needs to constantly be running in the background to report the device security posture. This security posture is used in the Compliance and App Protection policies to secure the managed apps and ensure that corporate data is accessed only in a secured device. However, with restrictive Conditional Access policies such as having Block policies based on certain locations, or enforcing frequent sign ins can result in Defender blocked from reporting posture. If the Defender app fails to report the device posture this can lead to situation where the device is under a threat, leading to vulnerability of corporate data on the device. To ensure seamless protection, we recommend excluding the Defender app from the blocking Conditional Access Policy.

#### Apps required to exclude

1. **MicrosoftDefenderATP XPlat app (a0e84e36-b067-4d5c-ab4a-3db38e598ae2)**: MicrosoftDefenderATP XPlat app is the application responsible for forwarding Defender risk signals to the Defender backend. However, the presence of restrictive CA policies can result in Defender blocked from reporting signals. In these scenarios, we recommend excluding the MicrosoftDefenderATP XPlat app. Note, that **MicrosoftDefenderATP XPlat app** is also used by other platforms like Mac and Linux. So if the policy is same for these platforms, it is better to create a separate Conditional Access policy for Mobile.

2. **Microsoft Defender for Mobile TVM app (e724aa31-0f56-4018-b8be-f8cb82ca1196)**: Microsoft Defender for Mobile TVM (Threat and Vulnerability Management) is the service, which provides the vulnerability assessment for the installed apps on the iOS devices. However, the presence of restrictive CA policies can result in Defender blocked from communicating the onboarding requests to the TVM backend services. This service should be excluded if MDVM (Vulnerability Assessment) is used in the organization.

- Source: Resources for Microsoft Defender for Endpoint for mobile devices - Microsoft Defender for Endpoint | Microsoft Learn

# Gotcha's

## Azure Virtual Desktop

> **Important**
>
> - The clients used to access Azure Virtual Desktop use the **Microsoft Remote Desktop** Entra ID app to authenticate to the session host today. An upcoming change will transition the authentication to the **Windows Cloud Login** Entra ID app. To ensure a smooth transition, you need to add both Entra ID apps to your CA policies.
> - Don't select the app called Azure Virtual Desktop Azure Resource Manager Provider (app ID `50e95039-b200-4007-bc97-8d5790743a63`). This app is only used for retrieving the user feed and shouldn't have multifactor authentication.

### Configure sign-in frequency

Sign-in frequency policies let you configure how often users are required to sign-in when accessing Microsoft Entra-based resources. This can help secure your environment and is especially important for personal devices, where the local OS may not require MFA or may not lock automatically after inactivity. Users are prompted to authenticate only when a new access token is requested from Microsoft Entra ID when accessing a resource.

Sign-in frequency policies result in different behavior based on the Microsoft Entra app selected:

Expand table

| App name | App ID | Behavior |
|---|---|---|
| **Azure Virtual Desktop** | 9cdead84-a844-4324-93f2-b2e6bb768d07 | Enforces reauthentication when a user subscribes to Azure Virtual Desktop, manually refreshes their list of resources and authenticates to the Azure Virtual Desktop Gateway during a connection.<br><br>Once the reauthentication period is over, background feed refresh and diagnostics upload silently fails until a user completes their next interactive sign in to Microsoft Entra. |
| **Microsoft Remote Desktop** | a4a365df-50f1-4397-bc59-1a1564b8bb9c | Enforces reauthentication when a user signs in to a session host when single sign-on is enabled.<br><br>Both apps should be configured together as the Azure Virtual Desktop clients will soon switch from using the Microsoft Remote Desktop app to the Windows Cloud Login app to authenticate to the session host. |
| **Windows Cloud Login** | 270efc09-cd0d-444b-a71f-39af4910ec45 | |

- Source: Enforce Microsoft Entra multifactor authentication for Azure Virtual Desktop using Conditional Access - Azure | Microsoft Learn

# Gotcha's


## Microsoft Purview

### Conditional Access policies and encrypted documents

If your organization has implemented Microsoft Entra Conditional Access policies that include **Microsoft Rights Management Services** and the policy extends to external users who need to open documents encrypted by your organization:

- For external users who have a Microsoft Entra account in their own tenant, we recommend you use External Identities cross-tenant access settings to configure trust settings for MFA claims from one, many, or all external Microsoft Entra organizations.
- For external users not covered by the previous entry, for example, users who don't have a Microsoft Entra account or you haven't configured cross-tenant access settings for trust settings, these external users must have a guest account in your tenant.

Without one of these configurations, external users can't open the encrypted content and see an error message. The message text might inform them that their account needs to be added as an external user in the tenant, with the incorrect instruction for this scenario to **Sign out and sign in again with a different Microsoft Entra user account.**

If you can't meet these configuration requirements for external users who need to open content encrypted by your organization, you must either remove Microsoft Rights Management Services from the Conditional Access policies, or exclude external users from the policies.

For more information, see the frequently asked question, I see Azure Information Protection is listed as an available cloud app for conditional access—how does this work?

- Source: Microsoft Entra configuration for content encrypted by Microsoft Purview Information Protection | Microsoft Learn & Conditional Access MFA Gives Outlook Desktop a Problem

# Gotcha's

## Subscription Activation


### Subscription activation

Organizations that use the Subscription Activation feature to enable users to "step-up" from one version of Windows to another and use Conditional Access policies to control access need to exclude one of the following cloud apps from their Conditional Access policies using **Select Excluded Cloud Apps**:

- Universal Store Service APIs and Web Application, AppID 45a330b1-b1ec-4cc1-9161-9f03992aa49f.
- Windows Store for Business, AppID 45a330b1-b1ec-4cc1-9161-9f03992aa49f.

Although the app ID is the same in both instances, the name of the cloud app depends on the tenant.

When a device is offline for an extended period of time, the device might not reactivate automatically if this Conditional Access exclusion isn't in place. Setting this Conditional Access exclusion ensures that Subscription Activation continues to work seamlessly.

Starting with Windows 11, version 23H2 with KB5034848 or later, users are prompted for authentication with a toast notification when Subscription Activation needs to reactivate. The toast notification shows the following message:

> **Your account requires authentication**
>
> **Please sign in to your work or school account to verify your information.**

Additionally, in the Activation pane, the following message might appear:

> **Please sign in to your work or school account to verify your information.**

The prompt for authentication usually occurs when a device is offline for an extended period of time. This change eliminates the need for an exclusion in the Conditional Access policy for Windows 11, version 23H2 with KB5034848 or later. A Conditional Access policy can still be used with Windows 11, version 23H2 with KB5034848 or later if the prompt for user authentication via a toast notification isn't desired.

- Source: Require compliant, hybrid joined devices, or MFA - Microsoft Entra ID | Microsoft Learn & Subscription activation Issues and the Windows Store API

# Gotcha’s

## Defender for Cloud Apps

### Internal Session Controls application notice

The Enterprise application 'Microsoft Defender for Cloud Apps – Session Controls' is used internally by the Conditional Access App Control service.
Ensure there's no CA policy restricting access to this application. For policies that restrict all or certain applications, ensure this application is listed as an exception or confirm that the blocking policy is deliberate.

For more information, see Sample: Create Microsoft Entra ID Conditional Access policies for use with Defender for Cloud Apps.

For more information, see Conditional Access policies and Building a Conditional Access policy.

**Note**

Microsoft Defender for Cloud Apps utilizes the application **Microsoft Defender for Cloud Apps - Session Controls** as part of the Conditional Access App Control service for user sign-in. This application is located within the 'Enterprise Applications' section of Entra ID. To protect your SaaS applications with Session Controls, you must allow access to this application.

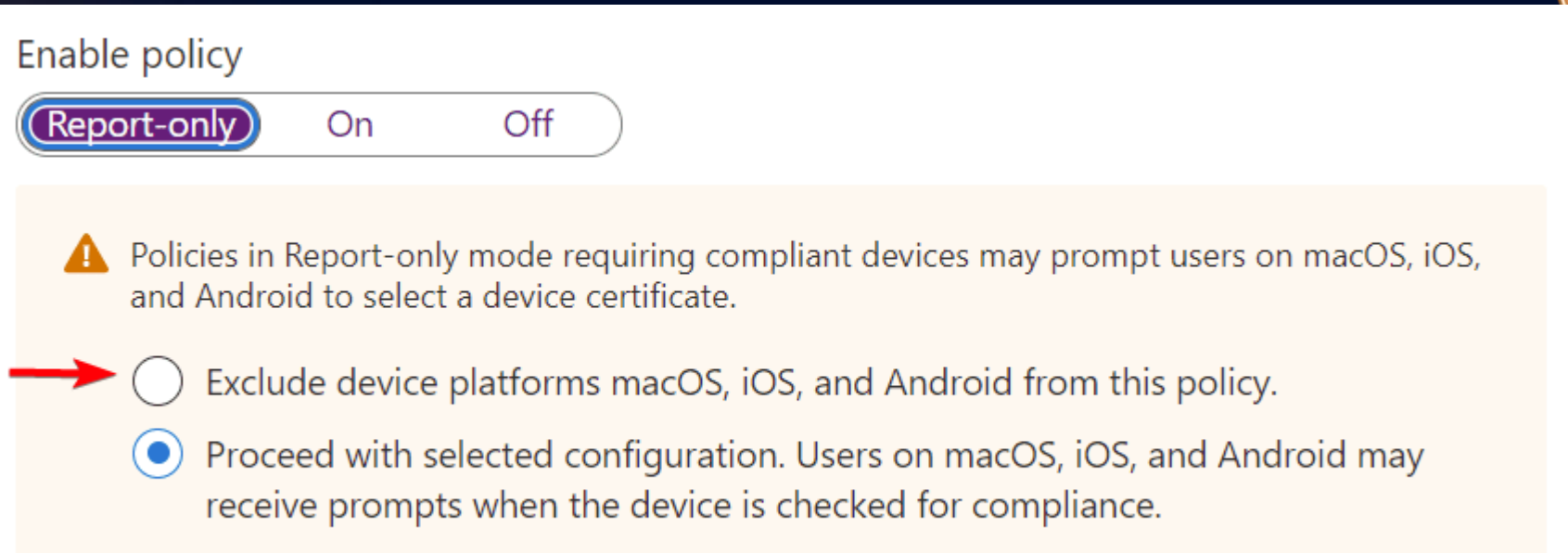
If you have any Conditional Access policies that have **“Block Access”** selected in the **“Grant Access”** Control under a Microsoft Entra ID Conditional Access policy scoped to this app, end users will not be able to access the protected applications under session controls.

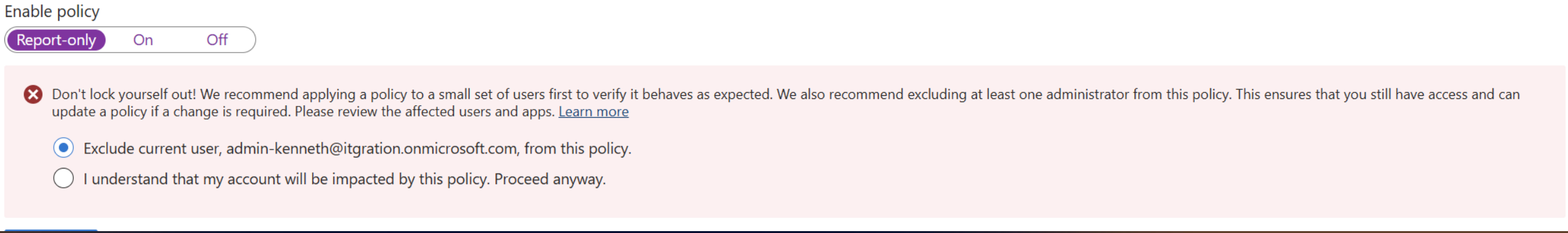
It's important to ensure that this application isn't unintentionally restricted by any Conditional Access policies. For policies that restrict all or certain applications, please ensure this application is listed as an exception in the **Target resources** or confirm that the blocking policy is deliberate.

To ensure your location-based conditional access policies function correctly, include the **Microsoft Defender for Cloud Apps – Session Controls** application in those policies.

- Source: What's new - Microsoft Defender for Cloud Apps | Microsoft Learn & Create session policies - Microsoft Defender for Cloud Apps | Microsoft Learn

# THE OBVIOUS


Enable policy
Report-only
On
Off
Policies in Report-only mode requiring compliant devices may prompt users on macOS, iOS, and Android to select a device certificate.
Exclude device platforms macOS, iOS, and Android from this policy.
Proceed with selected configuration. Users on macOS, iOS, and Android may receive prompts when the device is checked for compliance.


Enable policy
Report-only
On
Off
Don't lock yourself out! We recommend applying a policy to a small set of users first to verify it behaves as expected. We also recommend excluding at least one administrator from this policy. This ensures that you still have access and can update a policy if a change is required. Please review the affected users and apps. Learn more
Exclude current user, admin-kenneth@itgration.onmicrosoft.com, from this policy.
I understand that my account will be impacted by this policy. Proceed anyway.

# about://me

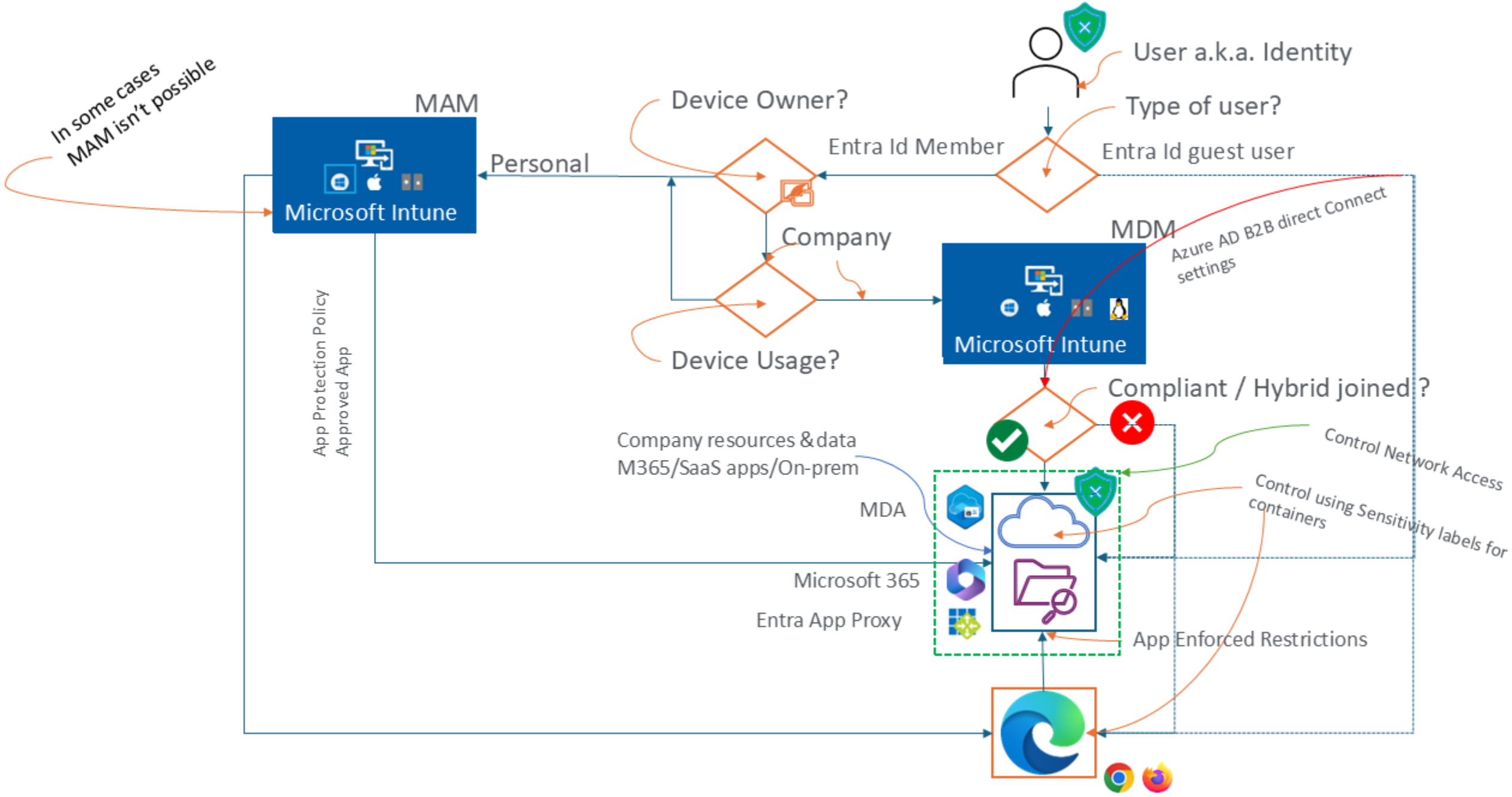
**Kenneth van Surksum**
Microsoft Security MVP · Intune, Identity & Access

**Role**
Modern Workplace Consultant at Secure At Work

**Focus**
Intune · Entra· Security

**Blog, Hobbies and more**
https://vansurksum.com


# Implementation


In some cases
MAM isn't possible
MAM
Microsoft Intune
Personal
Device Owner?
Entra Id Member
User a.k.a. Identity
Type of user?
Entra Id guest user
Company
Device Usage?
MDM
Microsoft Intune
Azure AD B2B direct Connect settings
App Protection Policy
Approved App
Compliant / Hybrid joined ?
Company resources & data
M365/SaaS apps/On-prem
MDA
Microsoft 365
Entra App Proxy
Control Network Access
Control using Sensitivity labels for containers
App Enforced Restrictions

# IMPLEMENTATION


- Approach
  - Make a copy of every CA policy and make it a Learn policy, which stays in Report-only mode during your migration, this policy is scoped to All Users
  - You can now target Groups in your CA Policies which you are going to activate


# Filters

# FILTERS


- **You cannot filter on device properties you don't receive in the first place**

> **Note**
>
> Microsoft Entra ID uses device authentication to evaluate device filter rules. For a device that is unregistered with Microsoft Entra ID, all device properties are considered as null values and the device attributes cannot be determined since the device does not exist in the directory. The best way to target policies for unregistered devices is by using the negative operator since the configured filter rule would apply. If you were to use a positive operator, the filter rule would only apply when a device exists in the directory and the configured rule matches the attribute on the device.

- **Source:** Filter for devices as a condition in Conditional Access policy - Microsoft Entra ID | Microsoft Learn


# Block challenges

Control access based on all or specific apps, internet resources, actions, or authentication context. Learn more

Select what this policy applies to

Resources (formerly cloud apps)

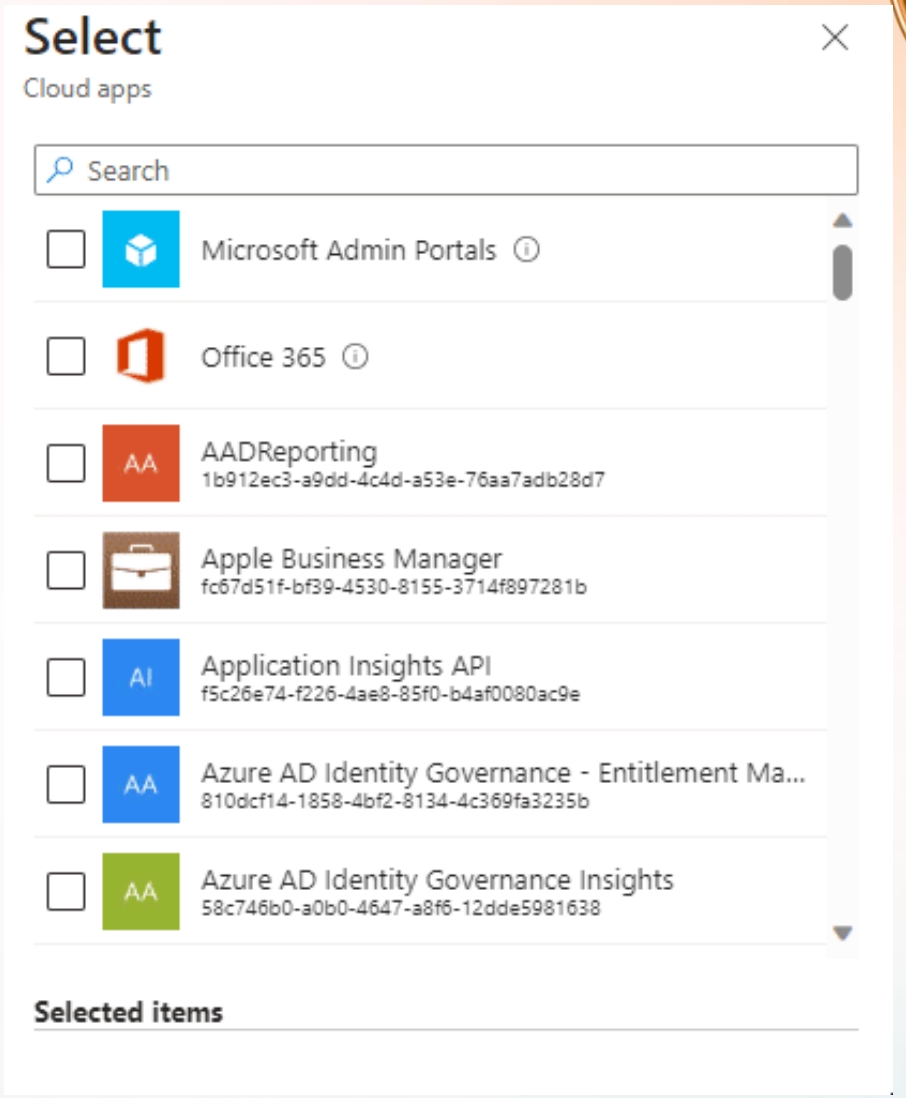
Include | Exclude

- None
- All internet resources with Global Secure Access
- All resources (formerly 'All cloud apps')
- Select resources

Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal.
Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All resources" are selected. Learn more

To create a Conditional Access policy targeting members in your tenant with Global Secure Access (GSA) as a resource, make sure GSA is deployed in your tenant. Learn more

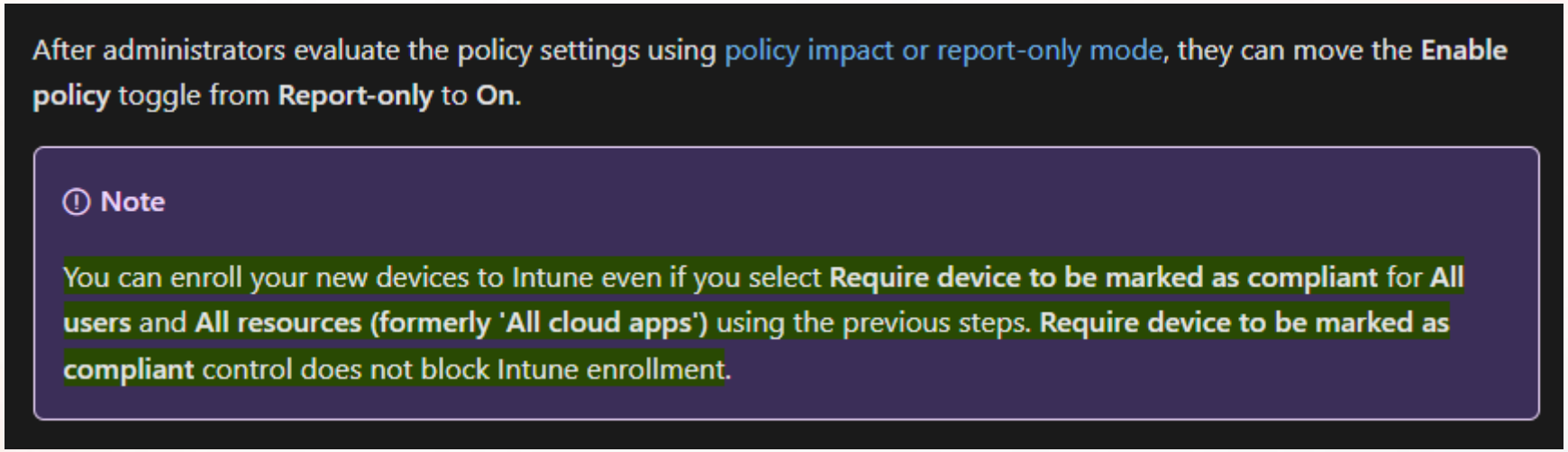
≠



# ALL RESOURCE (ALL CLOUD APPS) AND BLOCK CHALLENGES


## Requested scenario's

- Only give Guest users access to Office 365
- Only allow access to CloudPC from unmanaged device



# ALL RESOURCE (ALL CLOUD APPS) AND BLOCK CHALLENGES


## Conditional Access behavior when an all resources policy has an app exclusion

If any app is excluded from the policy, in order to not inadvertently block user access, certain low privilege scopes are excluded from policy enforcement. These scopes allow calls to the underlying Graph APIs, like `Windows Azure Active Directory` (00000002-0000-0000-c000-000000000000) and `Microsoft Graph` (00000003-0000-0000-c000-000000000000), to access user profile and group membership information commonly used by applications as part of authentication. For example: when Outlook requests a token for Exchange, it also asks for the `User.Read` scope to be able to display the basic account information of the current user.

Most apps have a similar dependency, which is why these low privilege scopes are automatically excluded whenever there's an app exclusion in an **All resources** policy. These low privilege scope exclusions don't allow data access beyond basic user profile and group information. The excluded scopes are listed as follows, consent is still required for apps to use these permissions.

- Native clients and Single page applications (SPAs) have access to the following low privilege scopes:
  - Azure AD Graph: `email`, `offline_access`, `openid`, `profile`, `User.Read`
  - Microsoft Graph: `email`, `offline_access`, `openid`, `profile`, `User.Read`, `People.Read`
- Confidential clients have access to the following low privilege scopes, if they're excluded from an **All resources** policy:
  - Azure AD Graph: `email`, `offline_access`, `openid`, `profile`, `User.Read`, `User.Read.All`, `User.ReadBasic.All`
  - Microsoft Graph: `email`, `offline_access`, `openid`, `profile`, `User.Read`, `User.Read.All`, `User.ReadBasic.All`, `People.Read`, `People.Read.All`, `GroupMember.Read.All`, `Member.Read.Hidden`

For more information on the scopes mentioned, see Microsoft Graph permissions reference and Scopes and permissions in the Microsoft identity platform.

D | Microsoft Learn

## All resources

Applying a Conditional Access policy to **All resources (formerly 'All cloud apps')** without any app exclusions enforces the policy for all token requests from websites and services, including Global Secure Access traffic forwarding profiles. This option includes applications that aren't individually targetable in Conditional Access policy, such as `Windows Azure Active Directory` (00000002-0000-0000-c000-000000000000).

> **Important**
>
> Microsoft recommends creating a baseline multifactor authentication policy targeting all users and all resources (without any app exclusions), like the one explained in Require multifactor authentication for all users.

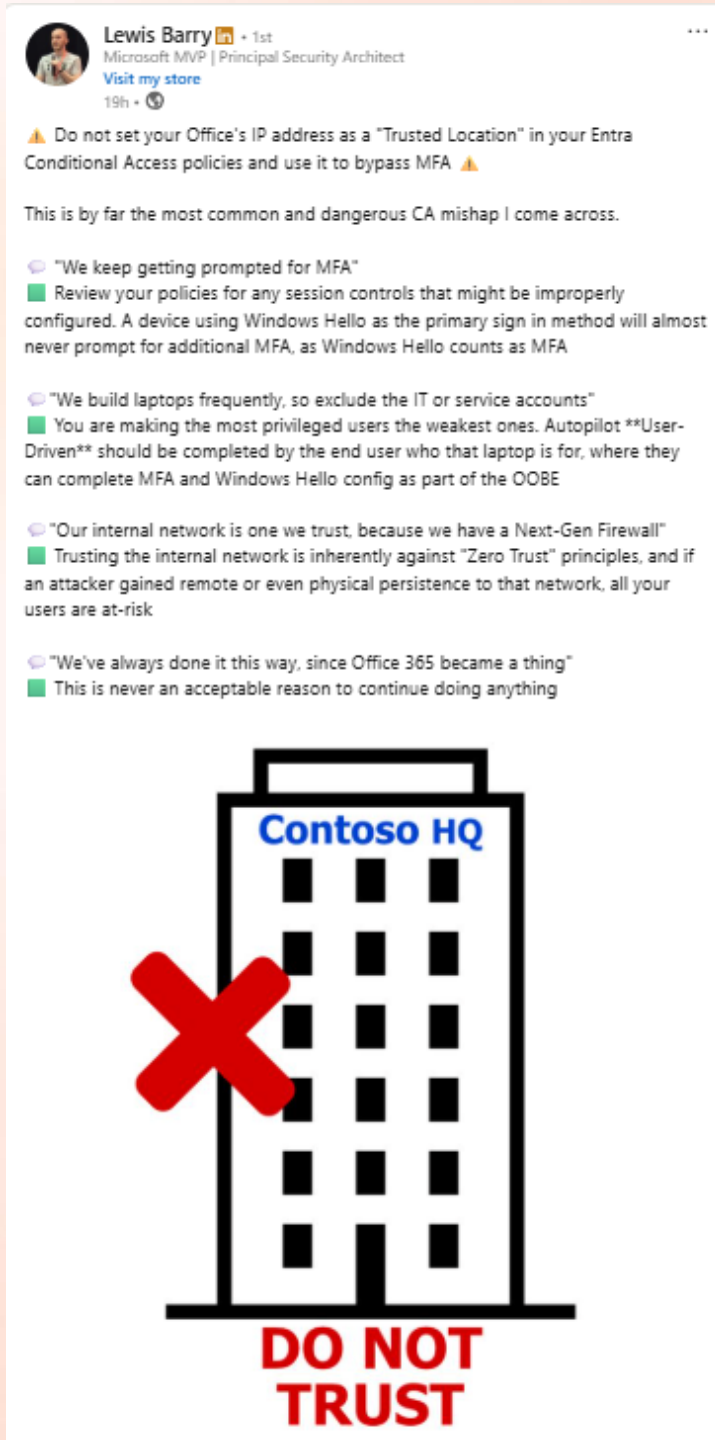
# Configuring Conditional Access for Guest Users: Allowing Only Office 365 and Essential Apps

https://www.vansurksum.com/2025/10/12/configuring-conditional-access-for-guest-users-allowing-only-office-365-and-essential-apps/


# IP Locations

# IP LOCATIONS

- IP versus GPS
- eSim while on holiday
- Guest network uses same IP breakout as corporate network

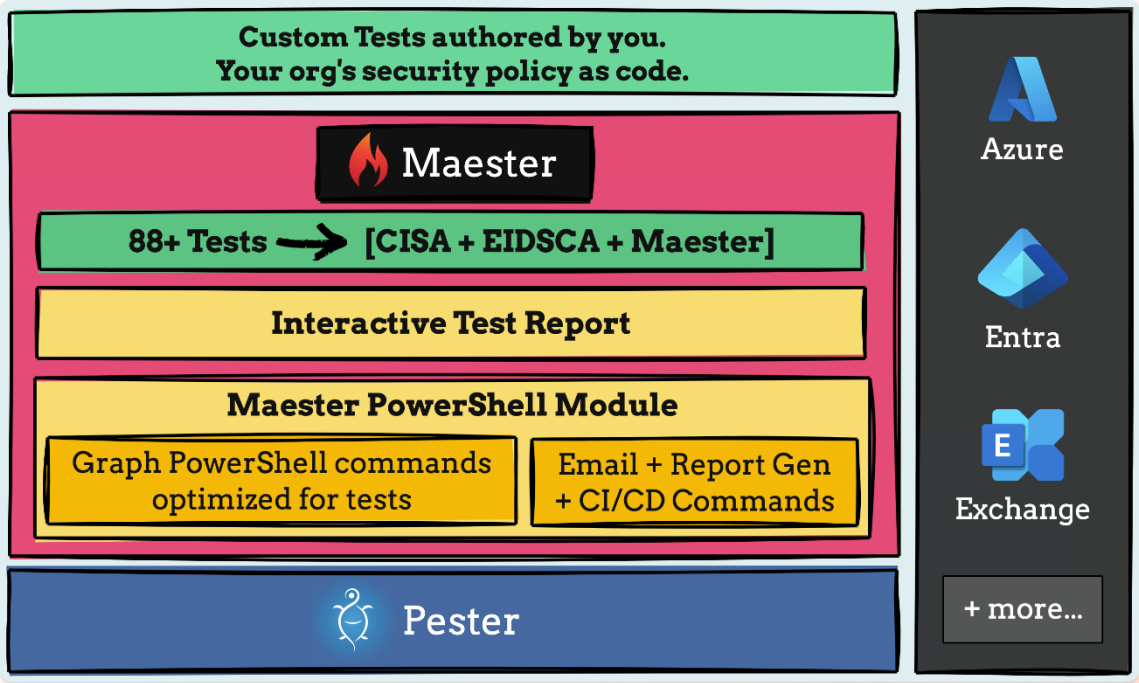



# Monitoring

# MONITORING

- **Workbooks**
  - Advanced Workbooks for Conditional Access | by Christopher Brumm | Medium

- **Maester**



# MONITORING


- **Member added to group starting with AAD_UA_CA**

```
AuditLogs
| where OperationName == "Add member to group"
| extend Type = tostring(TargetResources[0].type)
| where Type == "User"
| extend ['GroupName'] =
tostring(parse_json(tostring(parse_json(tostring(TargetResources[0].modifiedProperties))[1].newValue)))
| where ['GroupName'] startswith "AAD_UA_CA"
| extend UserAdded = tostring(TargetResources[0].userPrincipalName)
| where isnotempty(UserAdded)
| summarize ['UsersAdded']=make_set(UserAdded) by ['GroupName'], startofday(TimeGenerated)
| sort by ['GroupName'] asc, TimeGenerated desc
```

# MONITORING


- **Member added to group with name AAD_UA_ConAcc_Breakglass**

```
AuditLogs
| where OperationName == "Add member to group"
| extend Type = tostring(TargetResources[0].type)
| where Type == "User"
| extend ['GroupName'] = tostring(parse_json(tostring(parse_json(tostring(TargetResources[0].modifiedProperties))[1].newValue)))
| where ['GroupName'] startswith "AAD_UA_ConAcc-Breakglass"
| extend UserAdded = tostring(TargetResources[0].userPrincipalName)
| where isnotempty(UserAdded)
| summarize ['UsersAdded']=make_set(UserAdded) by ['GroupName'], startofday(TimeGenerated)
| sort by ['GroupName'] asc, TimeGenerated desc
```

# Conditional Access Baseline October 2025 (v2025-10) Available on GitHub

[Conditional Access Baseline October 2025 (v2025-10) Available on GitHub - Modern Workplace Blog]

October 18, 2025 | Kenneth van Surksum | https://vansurksum.com

# Please rate this session on Sched.com

SCHED

MODERN ENDPOINT MANAGEMENT SUMMIT 2026

# We would love to hear what you liked and how we could improve!