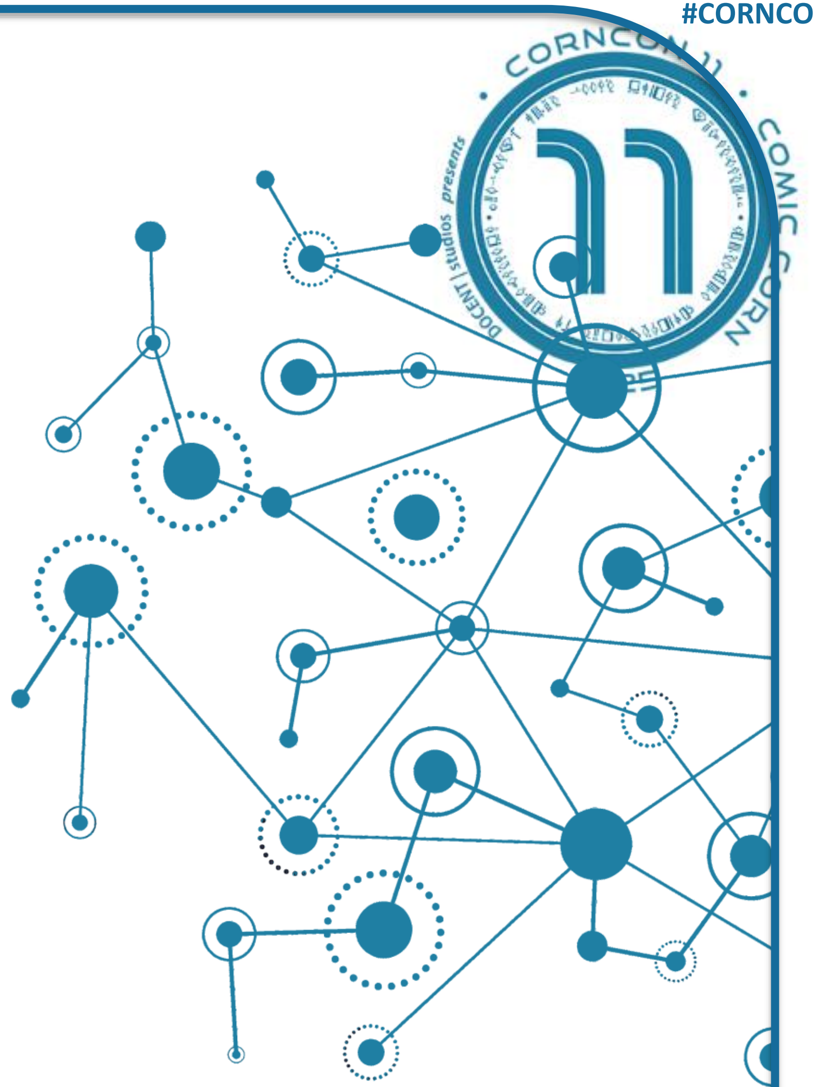
#CORNCON

DOCENT | studios

CornCon 11

*Manifest your inner Cyber Superhero*



# Abusing Holes In Conditional Access

Brandon Colley

@techBrandon

2025 CORNCON
CYBERSECURITY
CONFERENCE

# whoami

- Brandon Colley
  - @techBrandon (LinkedIn, Twitter, GitHub, etc)
  - Founder of BNR Consulting
  - Senior Security Consultant - TrustedSec

# Agenda

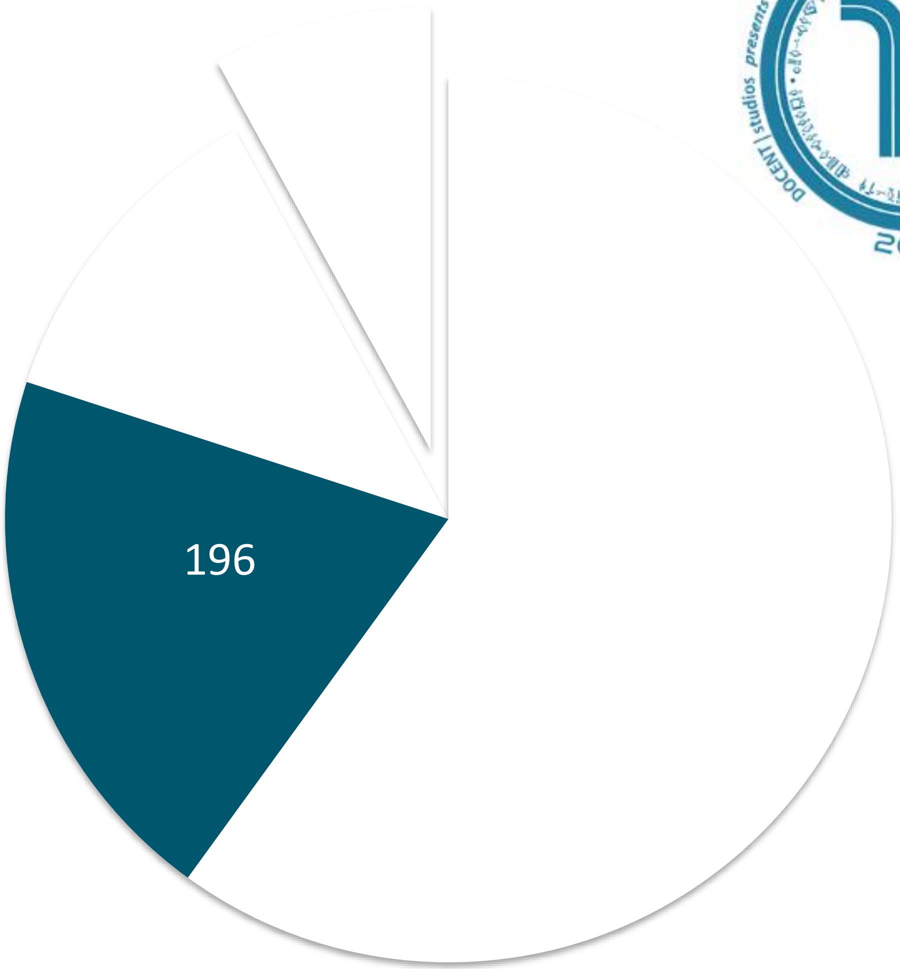
- Common Misconfigurations
- Exploitation Techniques
- Evaluating Your Risk

# Mission

- Identify Misconfiguration
- Understand the Adversary
- Improved Arsenal
- Incite Change
- Smile

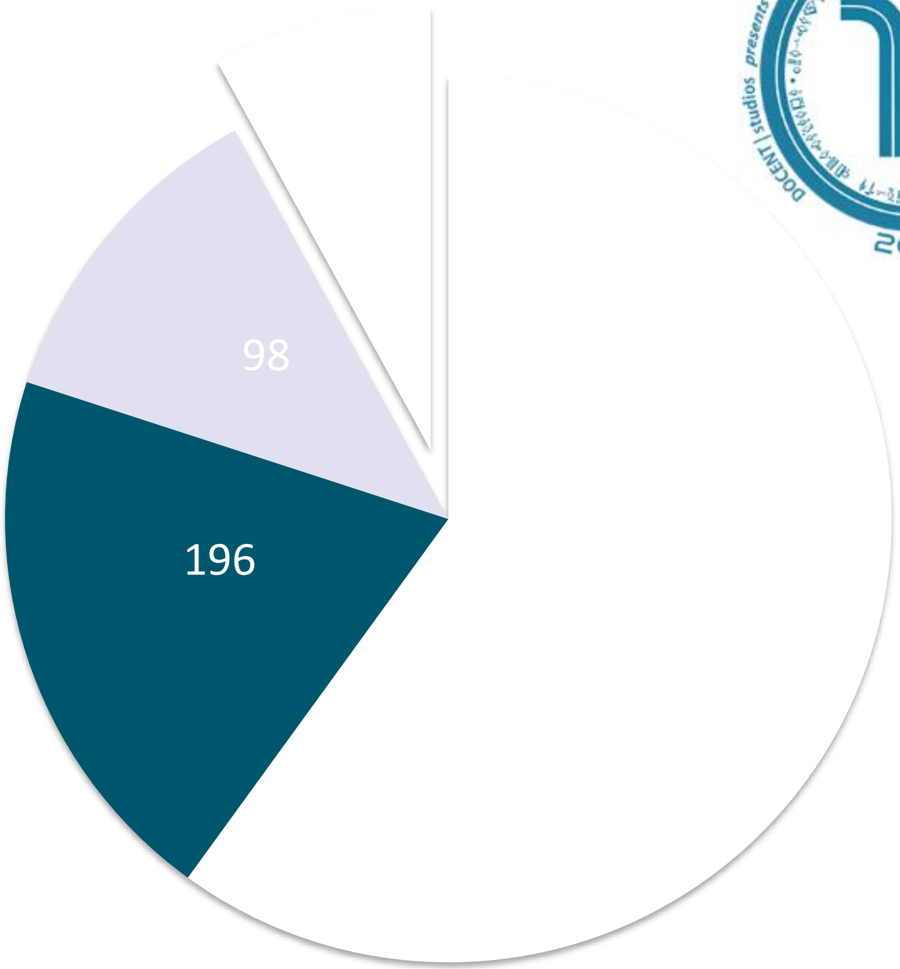
# Large Number of Policies

- 196



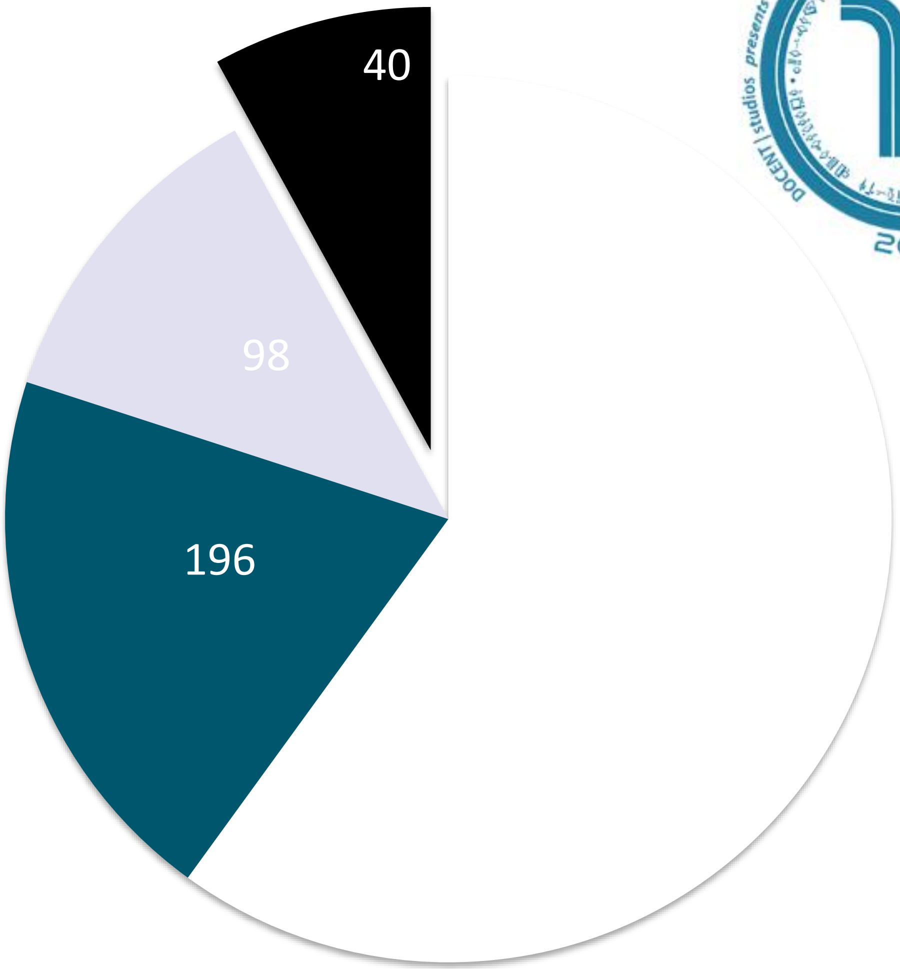
# Large Number of Policies

- 196
- 98



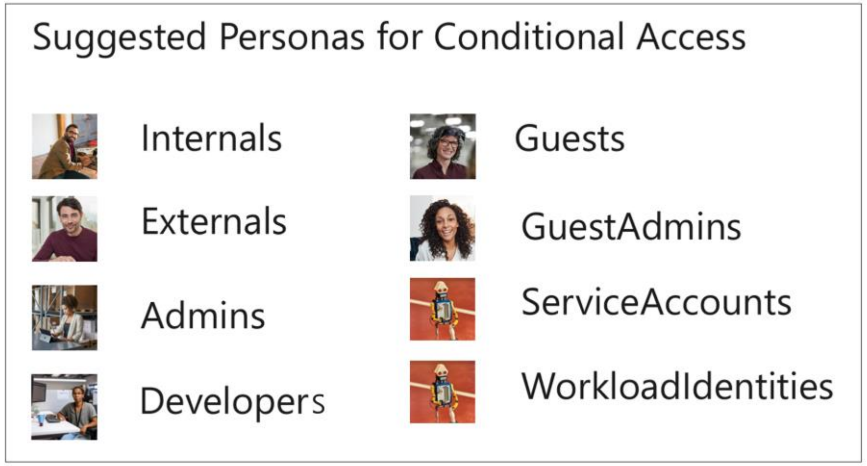
# Large Number of Policies

- 196
- 98
- 40



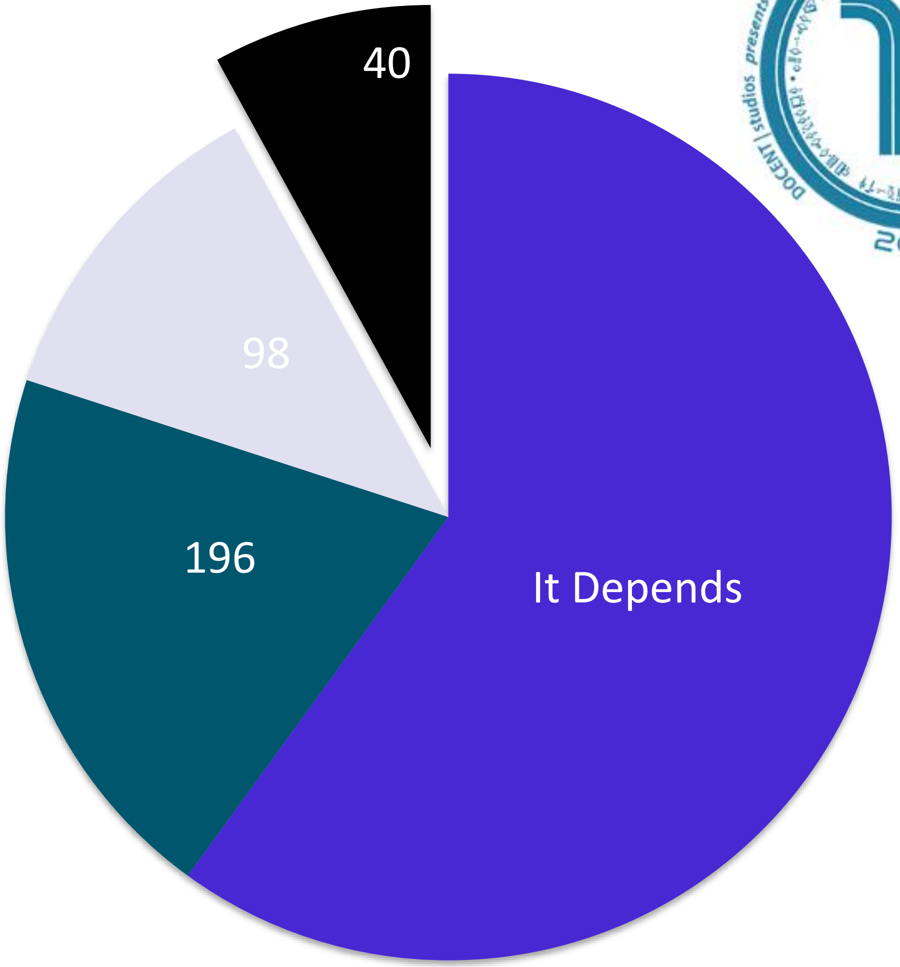
# Large Number of Policies

- 196
- 98
- 40
- ?



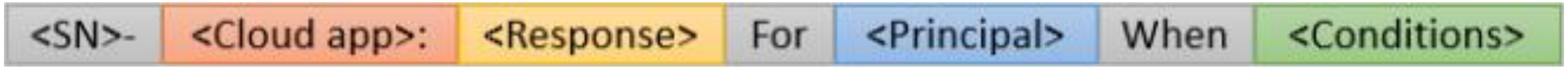
Suggested Personas for Conditional Access

- Internals
- Externals
- Admins
- Developers
- Guests
- GuestAdmins
- ServiceAccounts
- WorkloadIdentities

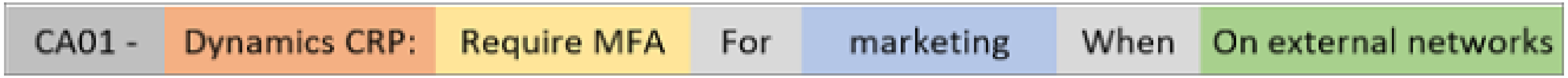


# Large Number of Policies

- Framework
- Naming standards



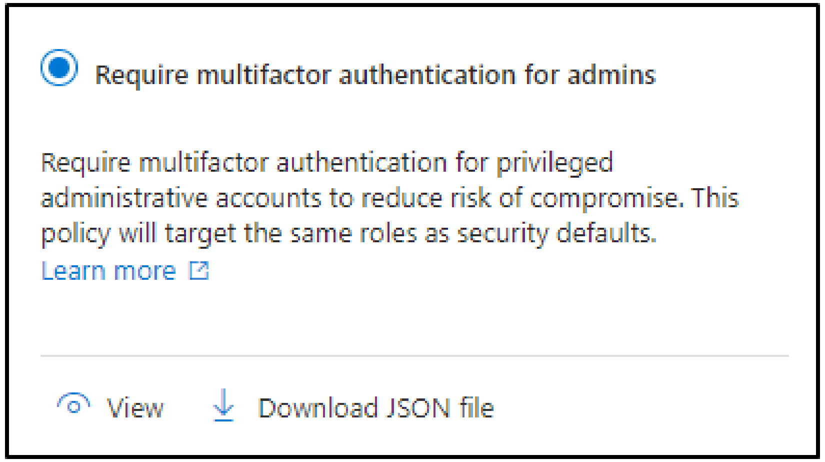
| | | | | | | |
|---|---|---|---|---|---|---|
| <SN>- | <Cloud app>: | <Response> | For | <Principal> | When | <Conditions> |



| | | | | | | |
|---|---|---|---|---|---|---|
| CA01 - | Dynamics CRP: | Require MFA | For | marketing | When | On external networks |

# Require MFA For Admins

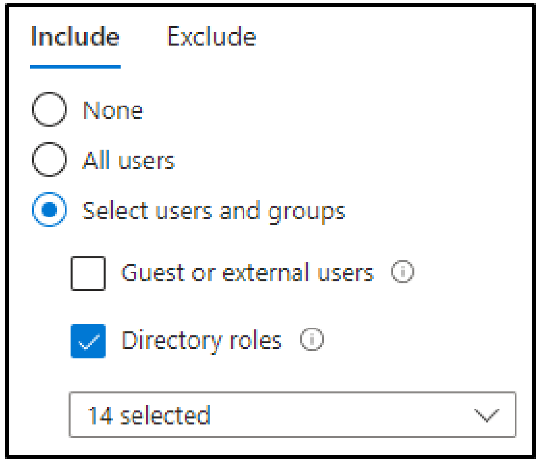
- 14 Default Roles
  - Global Administrator
  - Security Administrator
  - SharePoint Administrator
  - Exchange Administrator
  - Conditional Access Administrator
  - Helpdesk Administrator
  - Billing Administrator
  - User Administrator
  - Authentication Administrator
  - Application Administrator
  - Cloud Application Administrator
  - Password Administrator
  - Privileged Authentication Administrator
  - Privileged Role Administrator



● Require multifactor authentication for admins

Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as security defaults.

Learn more



○ None

○ All users

● Select users and groups

□ Guest or external users

☑ Directory roles

14 selected

# Require MFA For Admins

- Add (at least) These:
  - Authentication Policy Administrator
  - Directory Writers
  - External Identity Provider Administrator
  - Hybrid Identity Administrator
  - Identity Governance Administrator
  - Intune Administrator

# Require MFA For Admins

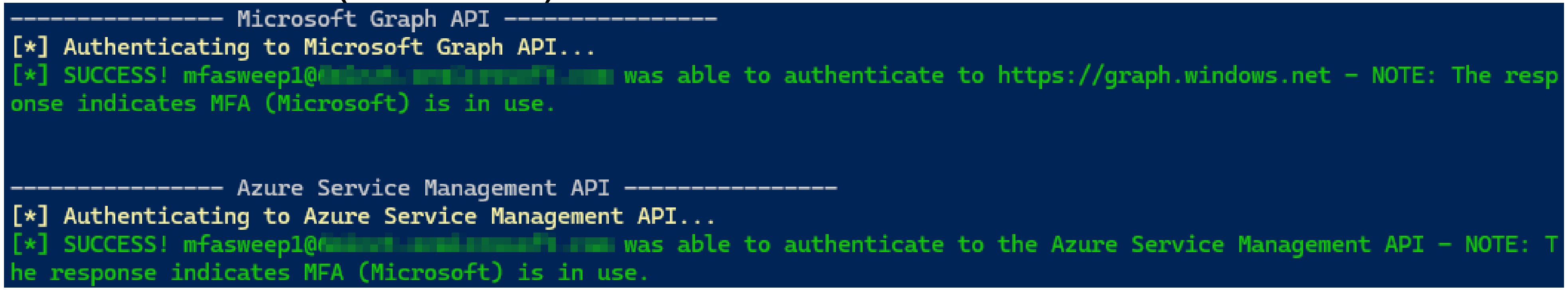
- Add (at least) These:
  - Authentication Policy Administrator
  - Directory Writers PRIVILEGED
  - External Identity Provider Administrator PRIVILEGED
  - Hybrid Identity Administrator PRIVILEGED
  - Identity Governance Administrator
  - Intune Administrator PRIVILEGED

# MFASweep Demo

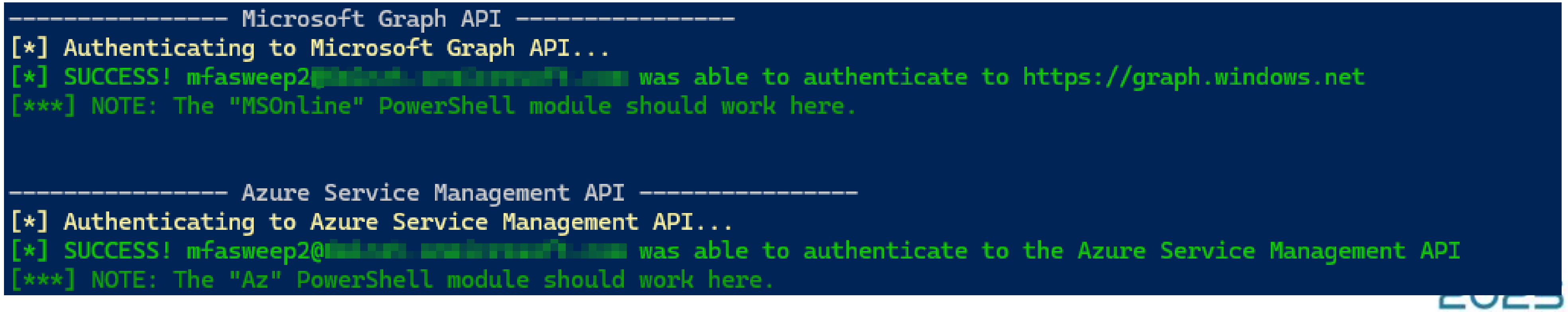
- https://github.com/dafthack/MFASweep
  - Beau Bullock (dafthack)
    - Microsoft Graph API
    - Azure Service Management API
    - Microsoft 365 Exchange Web Services
    - Microsoft 365 Web Portal w/ 6 device types (Windows, Linux, MacOS, Android Phone, iPhone, Windows Phone)
    - Microsoft 365 Active Sync
    - ADFS

# MFASweep Demo

- https://github.com/dafthack/MFASweep
  - Beau Bullock (dafthack)



```
---------------- Microsoft Graph API ----------------
[*] Authenticating to Microsoft Graph API...
[*] SUCCESS! mfasweep1@[redacted] was able to authenticate to https://graph.windows.net - NOTE: The resp
onse indicates MFA (Microsoft) is in use.


---------------- Azure Service Management API ----------------
[*] Authenticating to Azure Service Management API...
[*] SUCCESS! mfasweep1@[redacted] was able to authenticate to the Azure Service Management API - NOTE: T
he response indicates MFA (Microsoft) is in use.
```

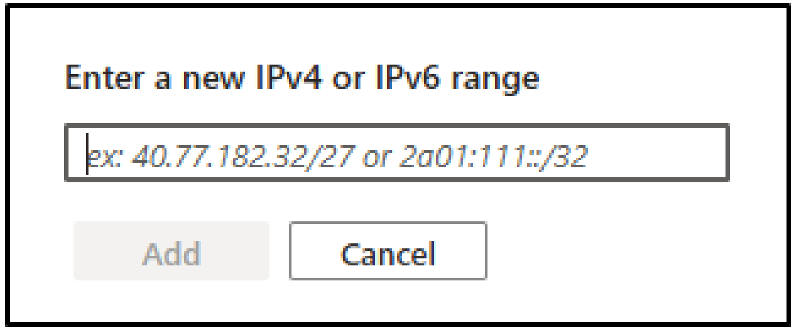


```
---------------- Microsoft Graph API ----------------
[*] Authenticating to Microsoft Graph API...
[*] SUCCESS! mfasweep2[redacted] was able to authenticate to https://graph.windows.net
[***] NOTE: The "MSOnline" PowerShell module should work here.


---------------- Azure Service Management API ----------------
[*] Authenticating to Azure Service Management API...
[*] SUCCESS! mfasweep2@[redacted] was able to authenticate to the Azure Service Management API
[***] NOTE: The "Az" PowerShell module should work here.
```

# Conditions

# Location(Network) Based Conditions

- Named Locations
  - IP range configuration

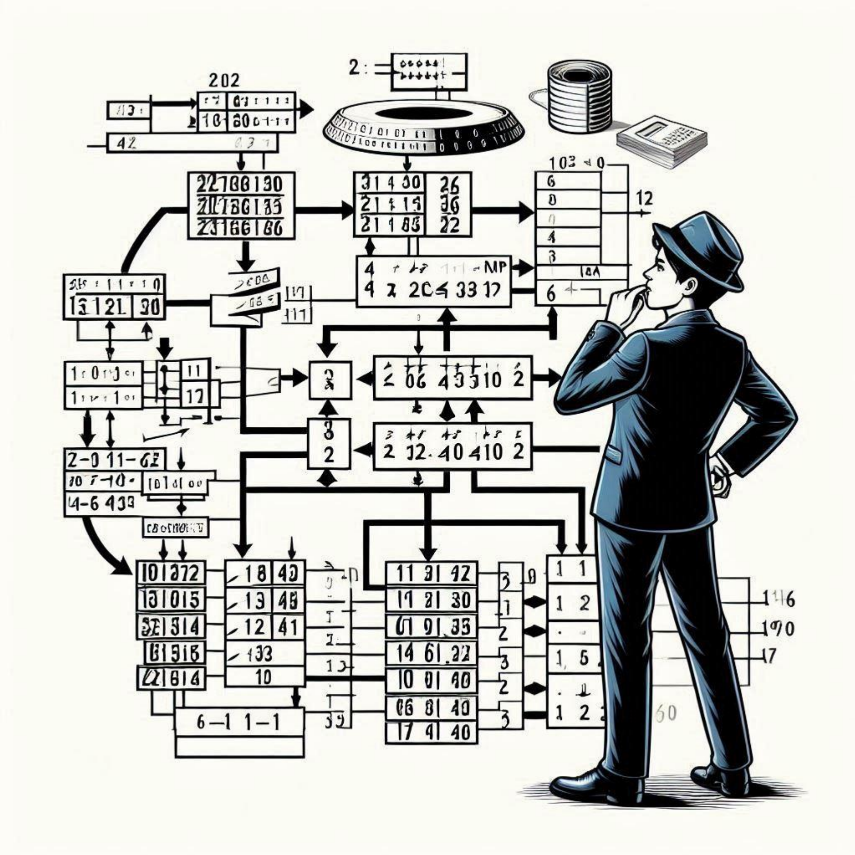


Enter a new IPv4 or IPv6 range

ex: 40.77.182.32/27 or 2a01:111::/32

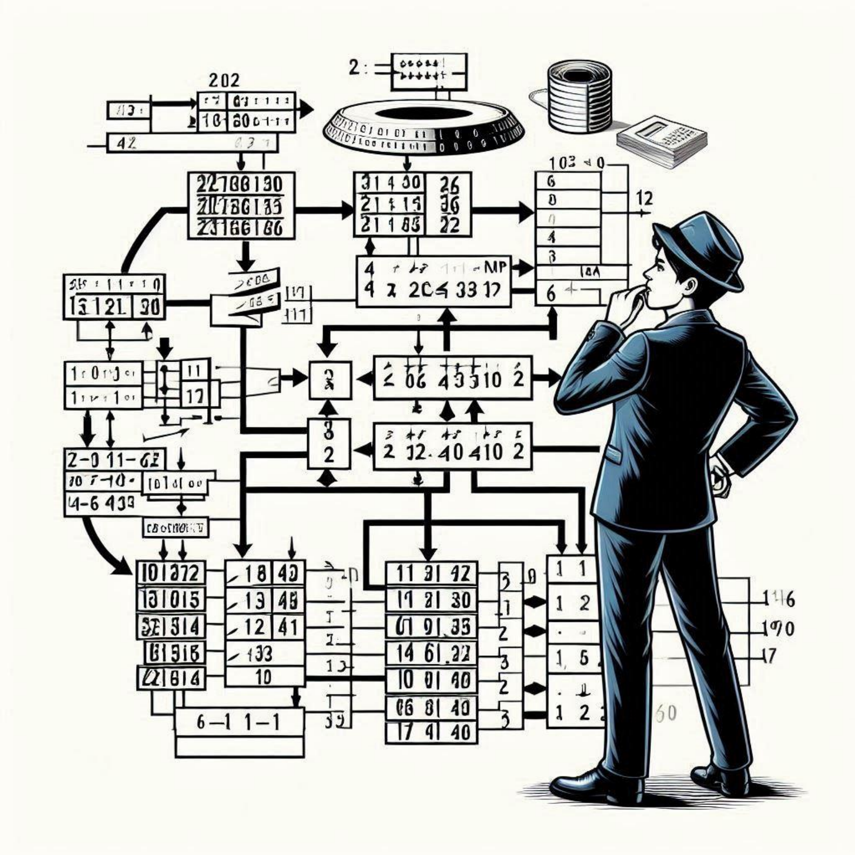
# Location(Network) Based Conditions

- Named Locations
  - IP range configuration



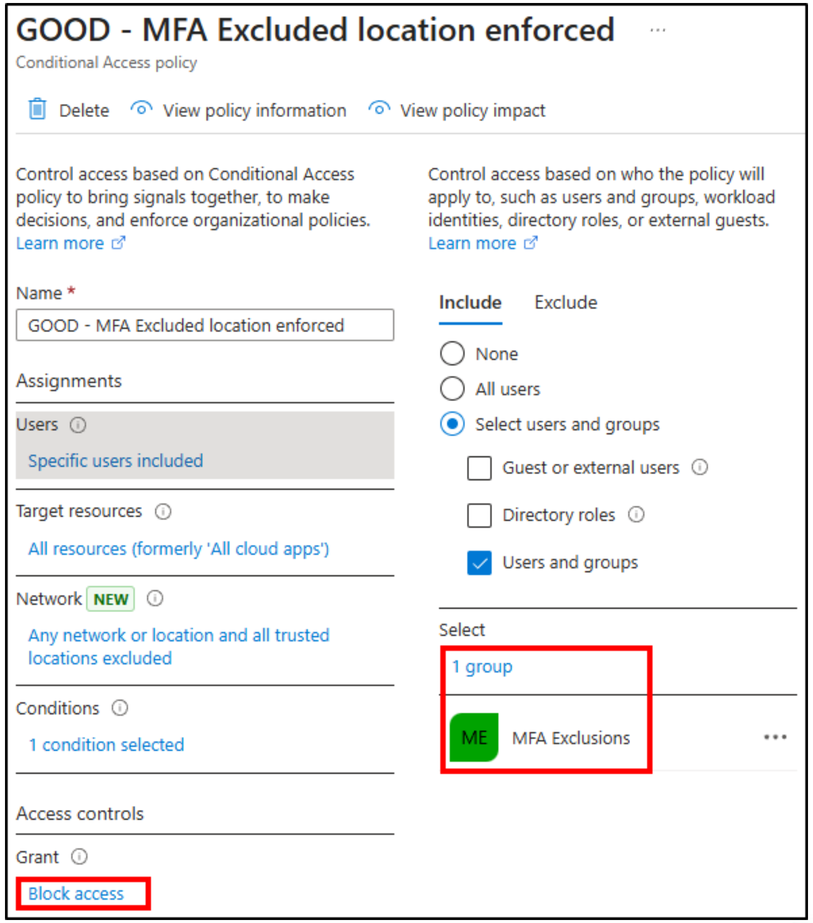
# Location(Network) Based Conditions

- Named Locations
  - IP range configuration
  - Regular Maintenance



# Location(Network) Based Conditions

- Named Locations
  - IP range configuration
  - Regular Maintenance
  - Used for exclusions <u>not</u> the exception



GOOD - MFA Excluded location enforced ···

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

GOOD - MFA Excluded location enforced

Assignments

Users ⓘ

Specific users included

Target resources ⓘ

All resources (formerly 'All cloud apps')

Network NEW ⓘ

Any network or location and all trusted locations excluded

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

Block access

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more

Include Exclude

○ None

○ All users

● Select users and groups

□ Guest or external users ⓘ

□ Directory roles ⓘ

☑ Users and groups

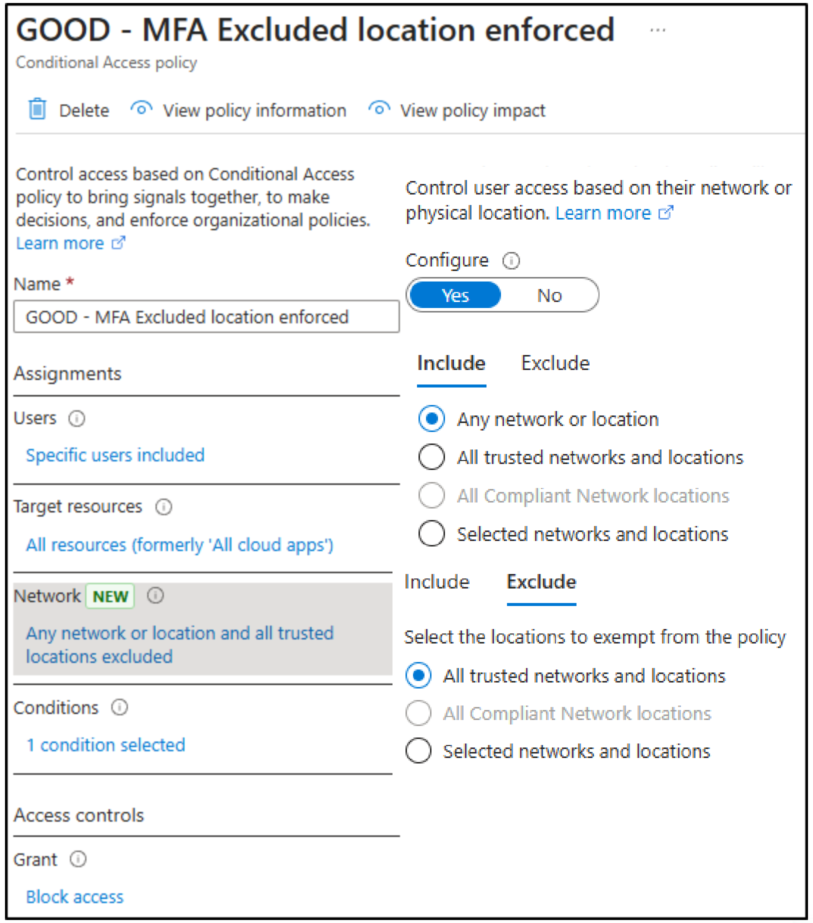
Select

1 group

ME MFA Exclusions ···

# Location(Network) Based Conditions

- Named Locations
  - IP range configuration
  - Regular Maintenance
  - Used for exclusions not the exception



GOOD - MFA Excluded location enforced ···

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

GOOD - MFA Excluded location enforced

Assignments

Users ⓘ

Specific users included

Target resources ⓘ

All resources (formerly 'All cloud apps')

Network NEW ⓘ

Any network or location and all trusted locations excluded

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

Block access

Control user access based on their network or physical location. Learn more

Configure ⓘ

[✓ Yes] No

**Include** Exclude

● Any network or location

○ All trusted networks and locations

○ All Compliant Network locations

○ Selected networks and locations

Include **Exclude**

Select the locations to exempt from the policy

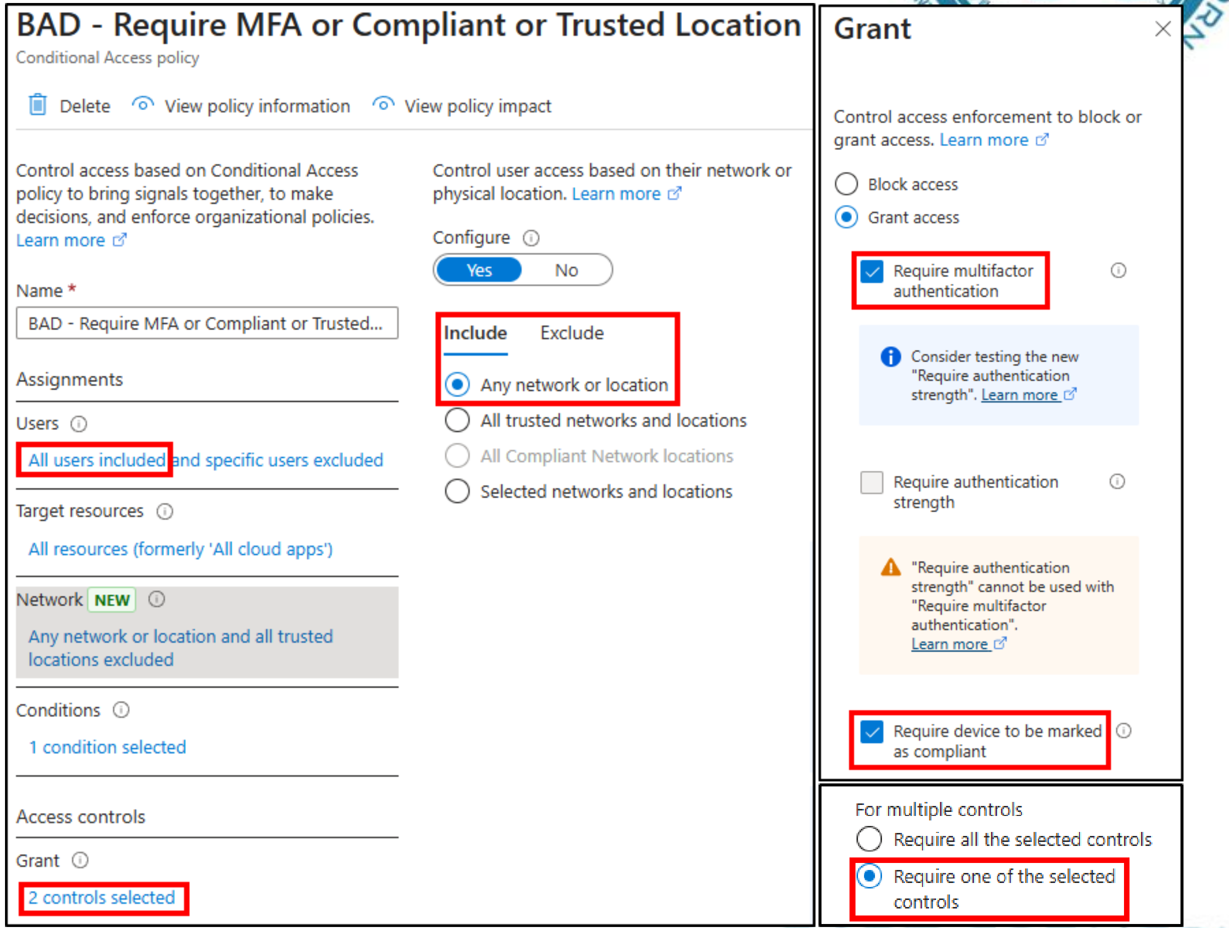
● All trusted networks and locations

○ All Compliant Network locations

○ Selected networks and locations

# Location(Network) Based Conditions

- Named Locations
  - IP range configuration
  - Regular Maintenance
  - Used for exclusions not the exception



**BAD - Require MFA or Compliant or Trusted Location**

Conditional Access policy

Delete | View policy information | View policy impact

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

BAD - Require MFA or Compliant or Trusted...

Assignments

Users ⓘ

All users included and specific users excluded

Target resources ⓘ

All resources (formerly 'All cloud apps')

Network NEW ⓘ

Any network or location and all trusted locations excluded

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

2 controls selected

Control user access based on their network or physical location. Learn more

Configure ⓘ

[✓ Yes] No

Include | Exclude

● Any network or location

○ All trusted networks and locations

○ All Compliant Network locations

○ Selected networks and locations

**Grant**

Control access enforcement to block or grant access. Learn more

○ Block access

● Grant access

☑ Require multifactor authentication ⓘ

Consider testing the new "Require authentication strength". Learn more

□ Require authentication strength ⓘ

"Require authentication strength" cannot be used with "Require multifactor authentication". Learn more

☑ Require device to be marked as compliant ⓘ

For multiple controls

○ Require all the selected controls

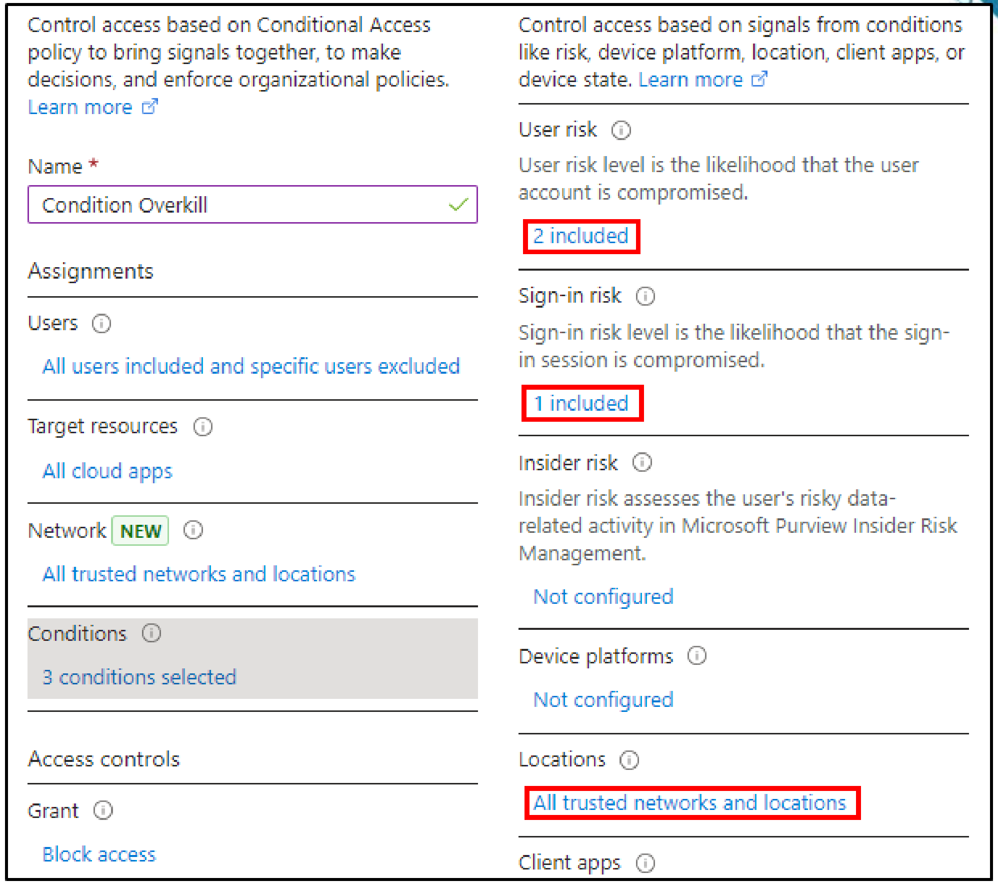
● Require one of the selected controls

# Multiple Conditions

SIGN-IN RISK
AND
USER RISK
AND
TRUSTED LOCATION
AND
imgflip.com

# Multiple Conditions

- Block access:
  - High/Medium User Risk
  - High Sign-in risk
  - Dangerous Countries



Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Condition Overkill

Assignments

Users

All users included and specific users excluded

Target resources

All cloud apps

Network NEW

All trusted networks and locations

Conditions

3 conditions selected

Access controls

Grant

Block access

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk

User risk level is the likelihood that the user account is compromised.

2 included

Sign-in risk

Sign-in risk level is the likelihood that the sign-in session is compromised.

1 included

Insider risk

Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management.

Not configured

Device platforms

Not configured

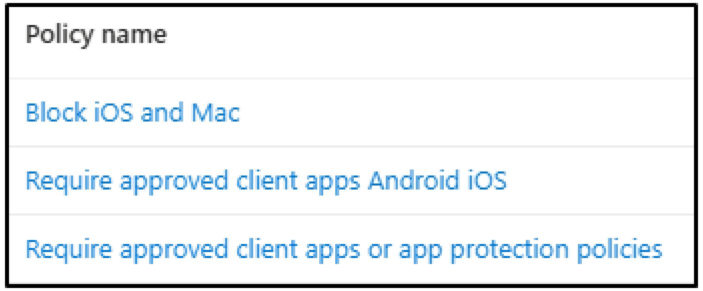
Locations

All trusted networks and locations

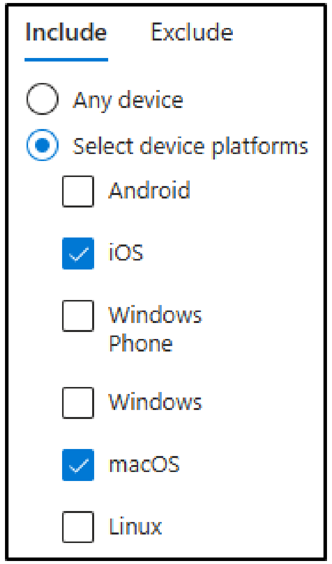
Client apps

# Multiple Conditions

- Device Platforms



| Policy name |
|---|
| Block iOS and Mac |
| Require approved client apps Android iOS |
| Require approved client apps or app protection policies |



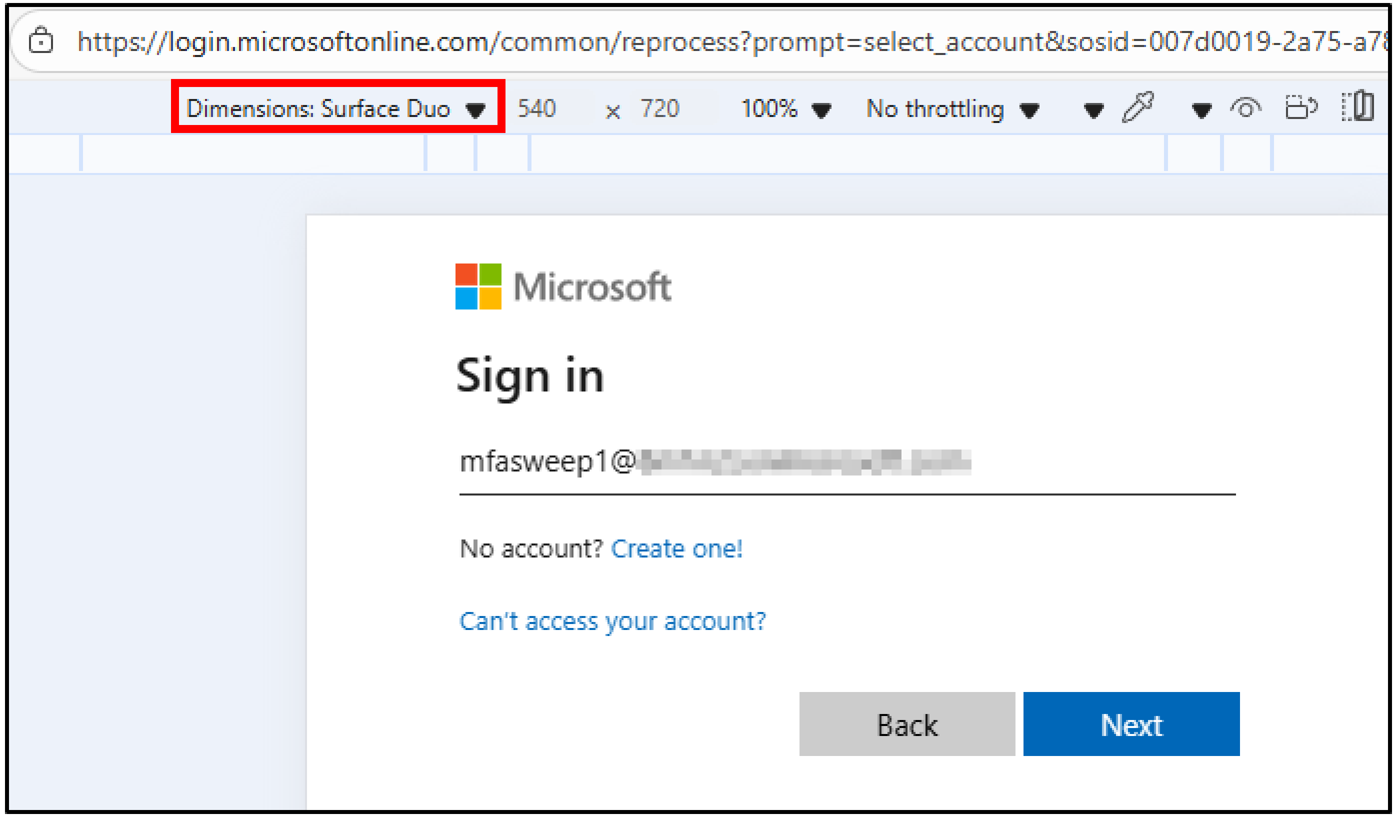
**Include** Exclude

○ Any device

● Select device platforms

- □ Android
- ☑ iOS
- □ Windows Phone
- □ Windows
- ☑ macOS
- □ Linux

# User-Agent Attack Demo:



https://login.microsoftonline.com/common/reprocess?prompt=select_account&sosid=007d0019-2a75-a78

Dimensions: Surface Duo 540 × 720 100% No throttling

Microsoft

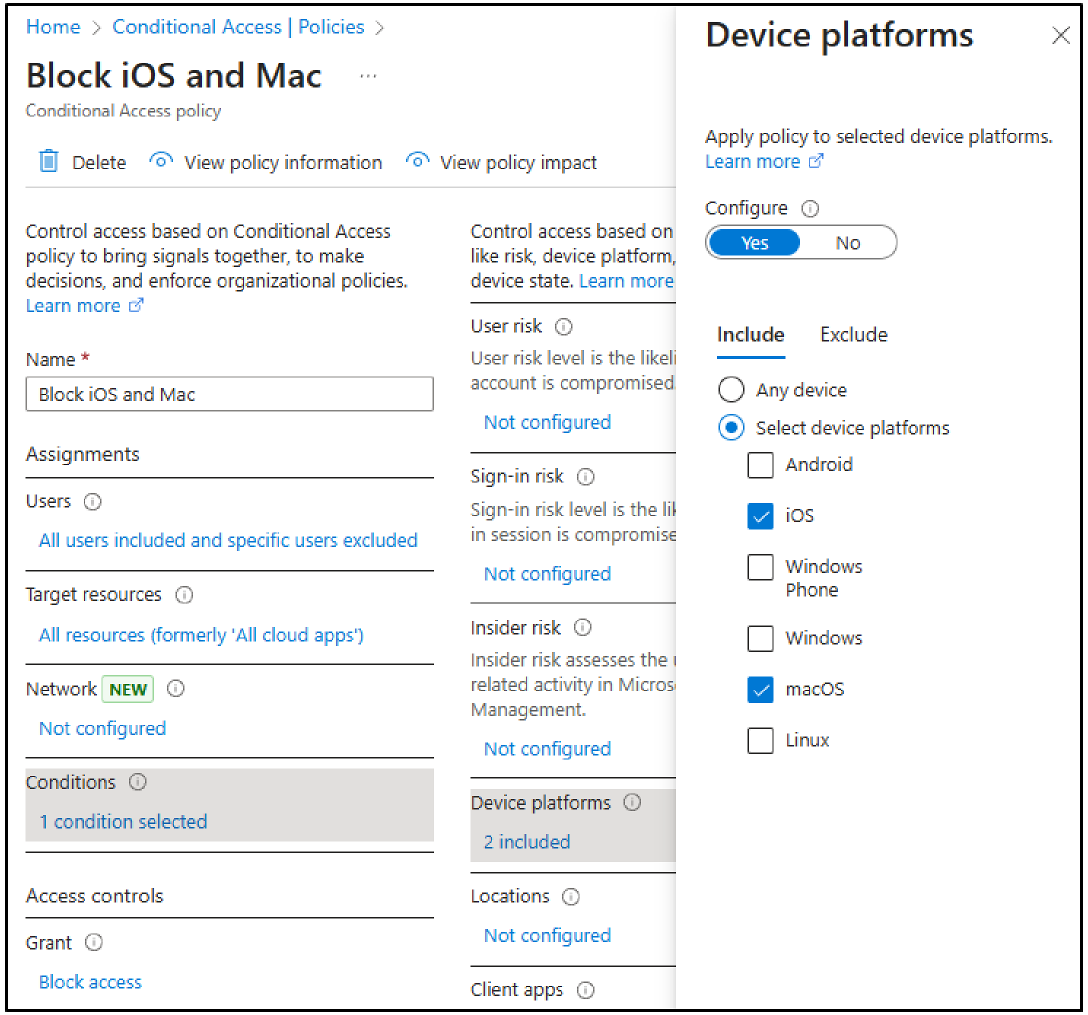
Sign in

mfasweep1@[redacted]

No account? Create one!

Can't access your account?

# User-Agent Attack Demo:



Home > Conditional Access | Policies >

Block iOS and Mac ...

Conditional Access policy

Delete View policy information View policy impact

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Block iOS and Mac

Assignments

Users ⓘ

All users included and specific users excluded

Target resources ⓘ

All resources (formerly 'All cloud apps')

Network NEW ⓘ

Not configured

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

Block access

Control access based on like risk, device platform, device state. Learn more

User risk ⓘ

User risk level is the likeli account is compromised

Not configured

Sign-in risk ⓘ

Sign-in risk level is the lik in session is compromise

Not configured

Insider risk ⓘ

Insider risk assesses the related activity in Micros Management.

Not configured

Device platforms ⓘ

2 included

Locations ⓘ

Not configured

Client apps ⓘ

## Device platforms

Apply policy to selected device platforms. Learn more

Configure ⓘ

[✓ Yes] No

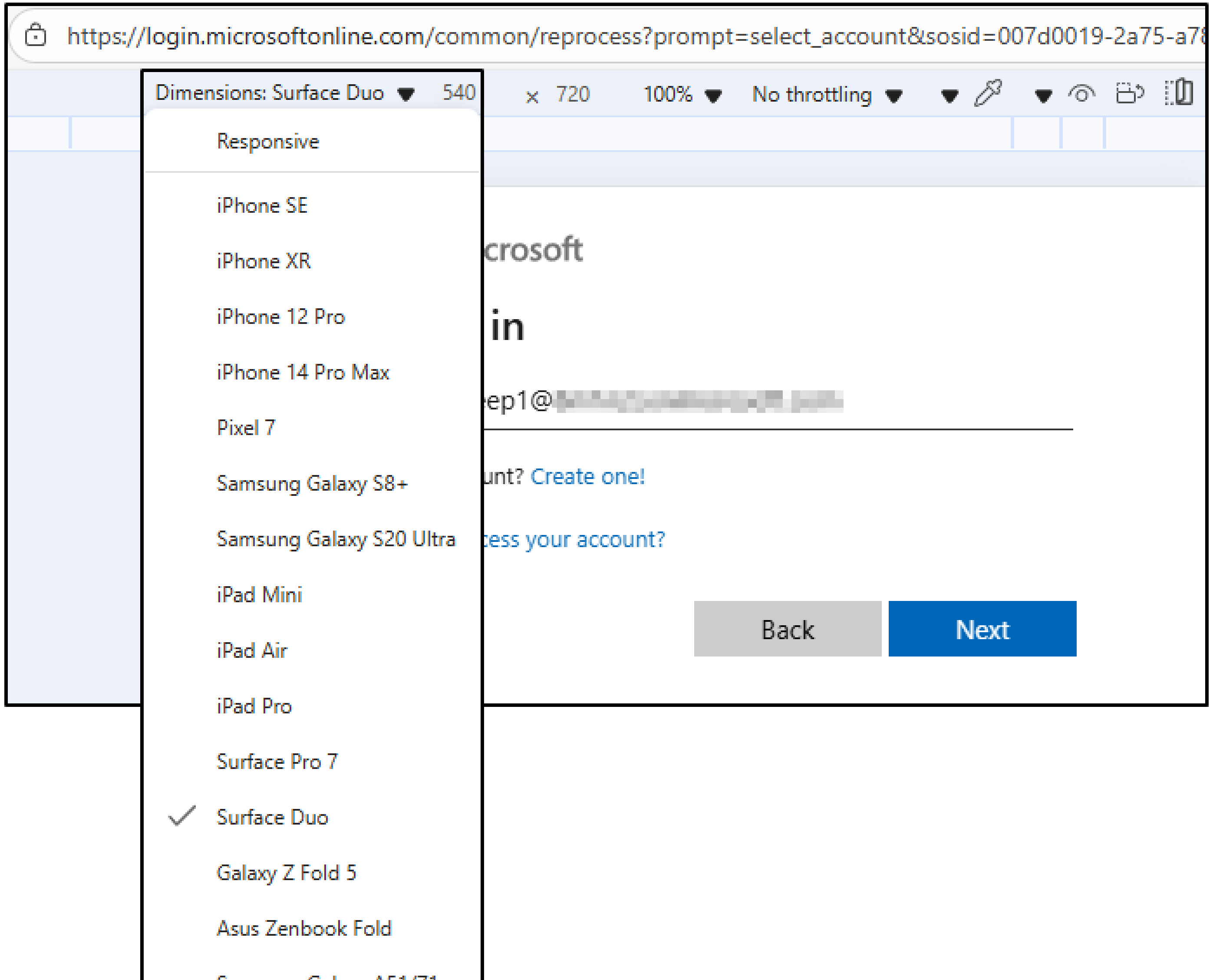
Include Exclude

○ Any device

● Select device platforms

- □ Android
- ☑ iOS
- □ Windows Phone
- □ Windows
- ☑ macOS
- □ Linux

# User-Agent Attack Demo:



https://login.microsoftonline.com/common/reprocess?prompt=select_account&sosid=007d0019-2a75-a78

Dimensions: Surface Duo 540 × 720 100% No throttling

crosoft

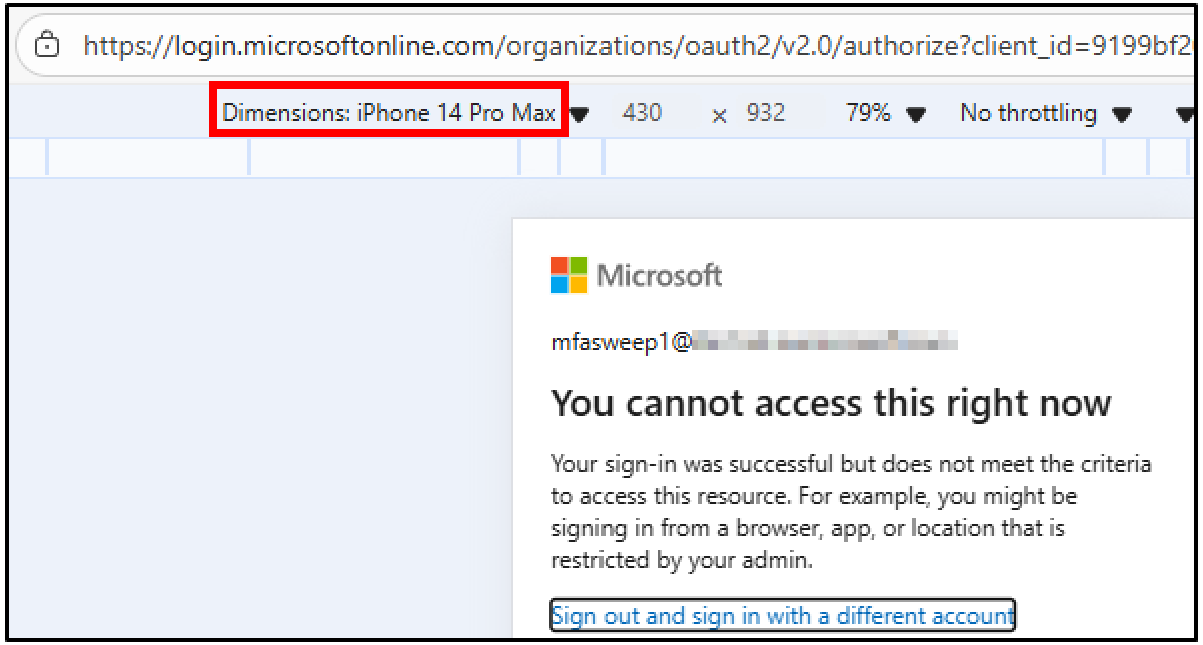
in

ep1@[redacted]

unt? Create one!

cess your account?

# User-Agent Attack Demo:



https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize?client_id=9199bf2

Dimensions: iPhone 14 Pro Max 430 × 932 79% No throttling

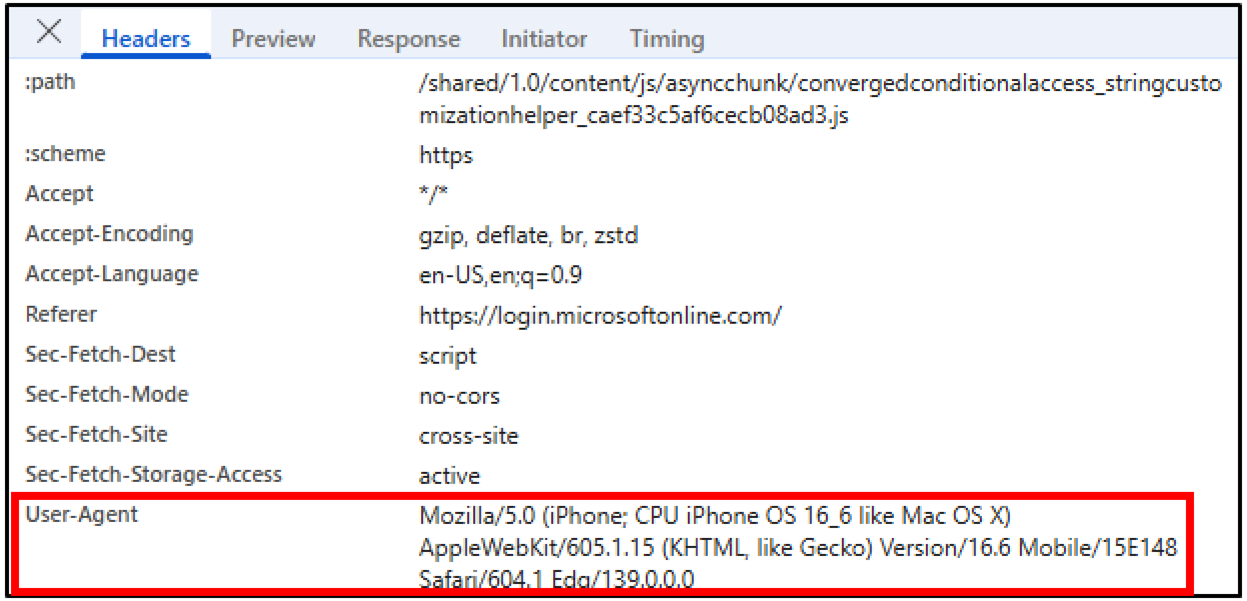
Microsoft

mfasweep1@[redacted]

**You cannot access this right now**

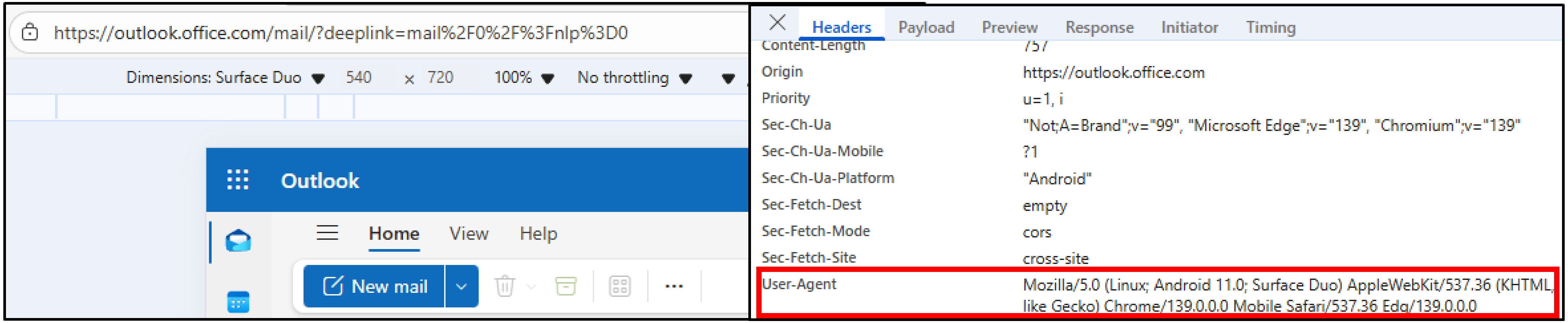
Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.

Sign out and sign in with a different account



| | |
|---|---|
| :path | /shared/1.0/content/js/asyncchunk/convergedconditionalaccess_stringcustomizationhelper_caef33c5af6cecb08ad3.js |
| :scheme | https |
| Accept | */* |
| Accept-Encoding | gzip, deflate, br, zstd |
| Accept-Language | en-US,en;q=0.9 |
| Referer | https://login.microsoftonline.com/ |
| Sec-Fetch-Dest | script |
| Sec-Fetch-Mode | no-cors |
| Sec-Fetch-Site | cross-site |
| Sec-Fetch-Storage-Access | active |
| User-Agent | Mozilla/5.0 (iPhone; CPU iPhone OS 16_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.6 Mobile/15E148 Safari/604.1 Edg/139.0.0.0 |

# User-Agent Attack Demo:



https://outlook.office.com/mail/?deeplink=mail%2F0%2F%3Fnlp%3D0

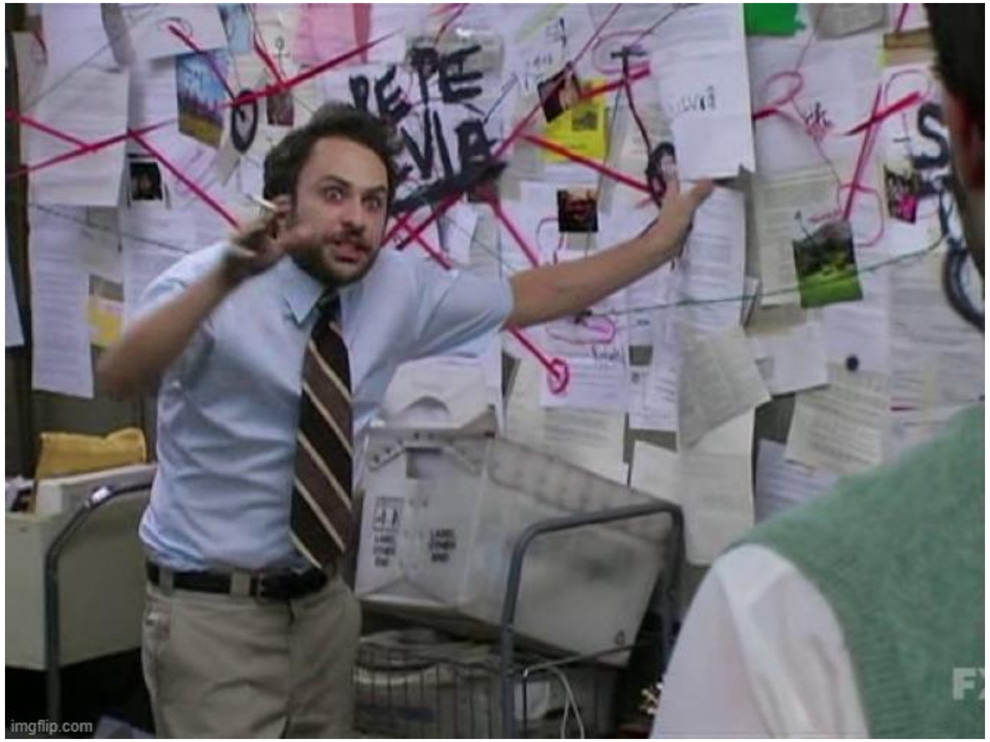
Dimensions: Surface Duo ▾ 540 × 720 100% ▾ No throttling ▾

| | |
|---|---|
| Content-Length | 757 |
| Origin | https://outlook.office.com |
| Priority | u=1, i |
| Sec-Ch-Ua | "Not;A=Brand";v="99", "Microsoft Edge";v="139", "Chromium";v="139" |
| Sec-Ch-Ua-Mobile | ?1 |
| Sec-Ch-Ua-Platform | "Android" |
| Sec-Fetch-Dest | empty |
| Sec-Fetch-Mode | cors |
| Sec-Fetch-Site | cross-site |
| User-Agent | Mozilla/5.0 (Linux; Android 11.0; Surface Duo) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Mobile Safari/537.36 Edg/139.0.0.0 |

# Common Misconfigurations

- Large Number of Policies
- Require MFA for Admins
- Location Conditions
- Multiple Conditions
- Device Platforms

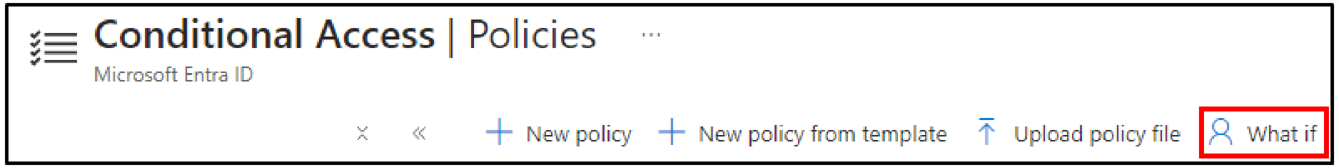
# Finding Holes



# Finding Holes

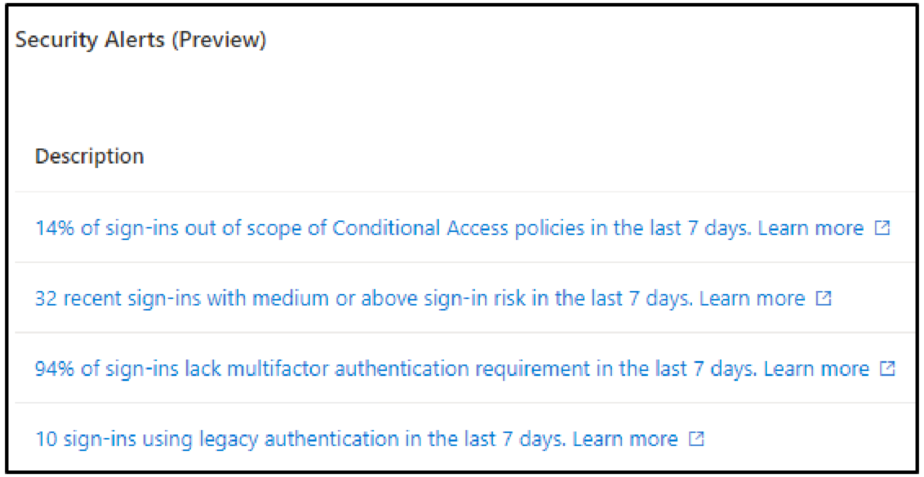
# Finding Holes

- Built In Tools
  - What If
  - Security Alerts
  - Coverage



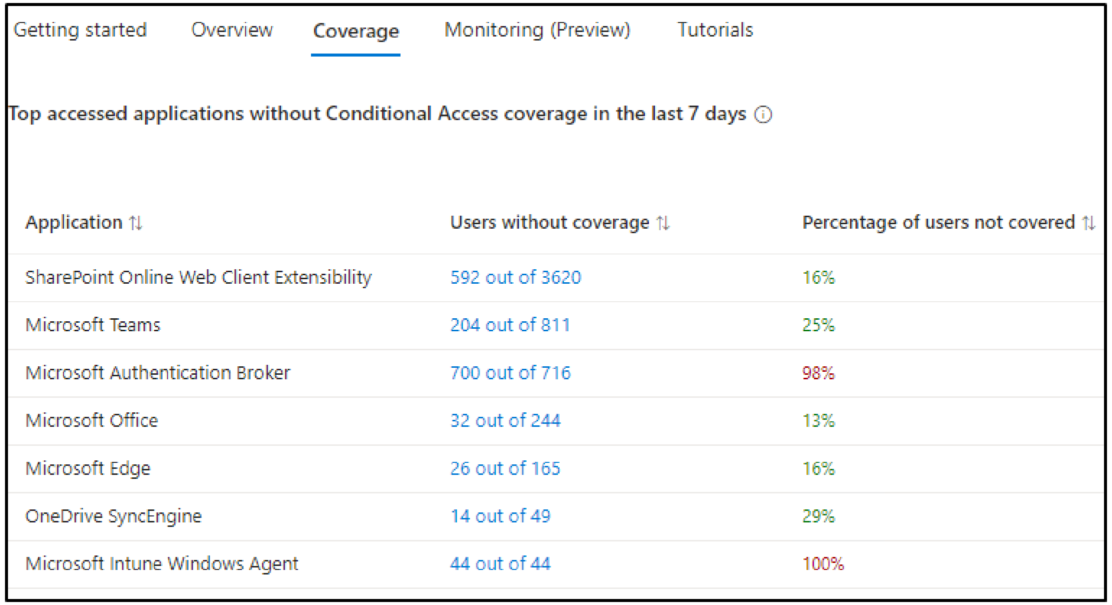
Conditional Access | Policies ···

Microsoft Entra ID



Security Alerts (Preview)

| Description |
|---|
| 14% of sign-ins out of scope of Conditional Access policies in the last 7 days. Learn more |
| 32 recent sign-ins with medium or above sign-in risk in the last 7 days. Learn more |
| 94% of sign-ins lack multifactor authentication requirement in the last 7 days. Learn more |
| 10 sign-ins using legacy authentication in the last 7 days. Learn more |



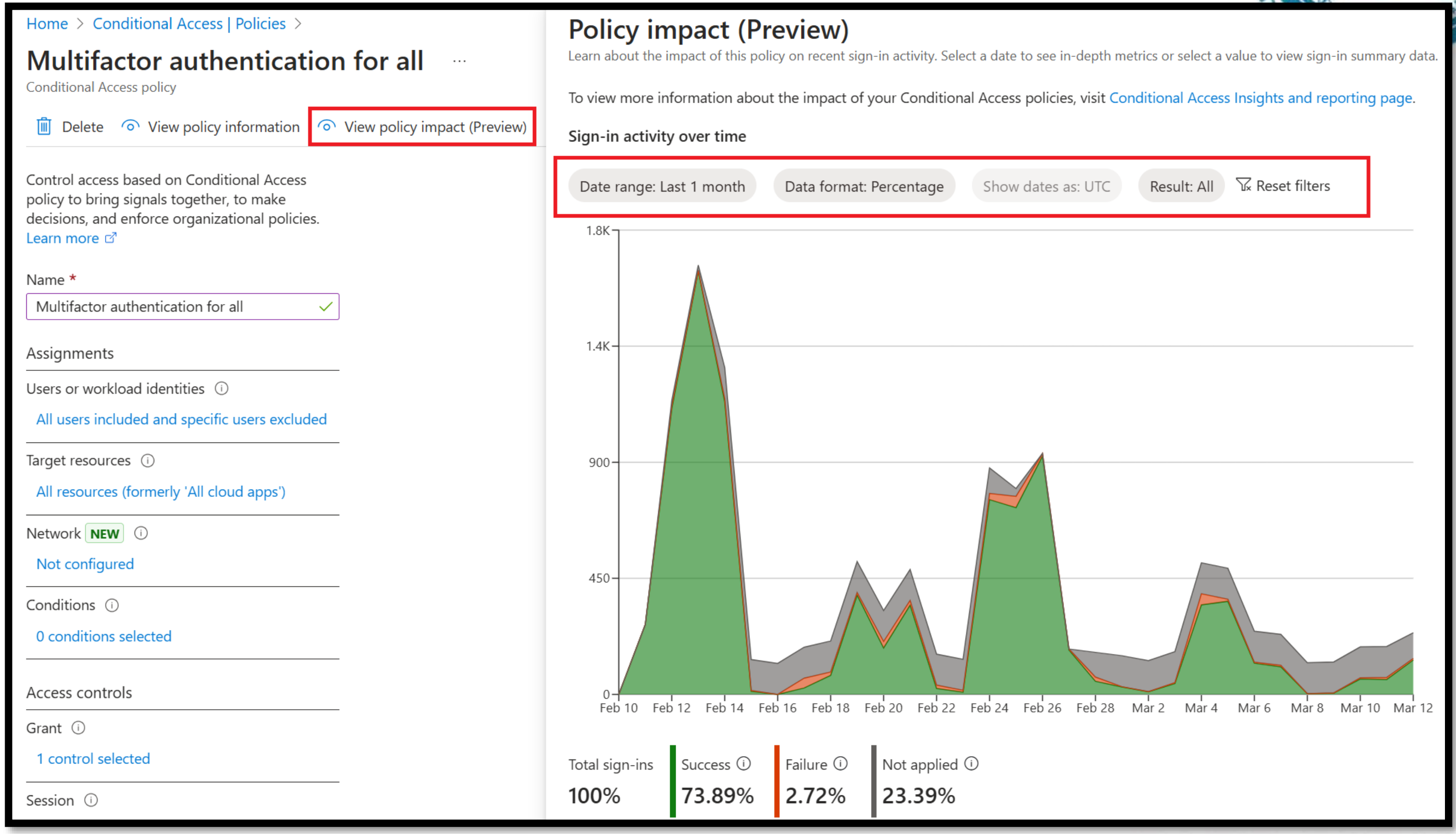
Top accessed applications without Conditional Access coverage in the last 7 days

| Application | Users without coverage | Percentage of users not covered |
|---|---|---|
| SharePoint Online Web Client Extensibility | 592 out of 3620 | 16% |
| Microsoft Teams | 204 out of 811 | 25% |
| Microsoft Authentication Broker | 700 out of 716 | 98% |
| Microsoft Office | 32 out of 244 | 13% |
| Microsoft Edge | 26 out of 165 | 16% |
| OneDrive SyncEngine | 14 out of 49 | 29% |
| Microsoft Intune Windows Agent | 44 out of 44 | 100% |

#CORNCON

# Finding Holes

- Built In Tools
  - Policy Impact



Home > Conditional Access | Policies >

Multifactor authentication for all ...

Conditional Access policy

Delete | View policy information | View policy impact (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Multifactor authentication for all ✓

Assignments

Users or workload identities ⓘ

All users included and specific users excluded

Target resources ⓘ

All resources (formerly 'All cloud apps')

Network NEW ⓘ

Not configured

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

Policy impact (Preview)

Learn about the impact of this policy on recent sign-in activity. Select a date to see in-depth metrics or select a value to view sign-in summary data.

To view more information about the impact of your Conditional Access policies, visit Conditional Access Insights and reporting page.

Sign-in activity over time

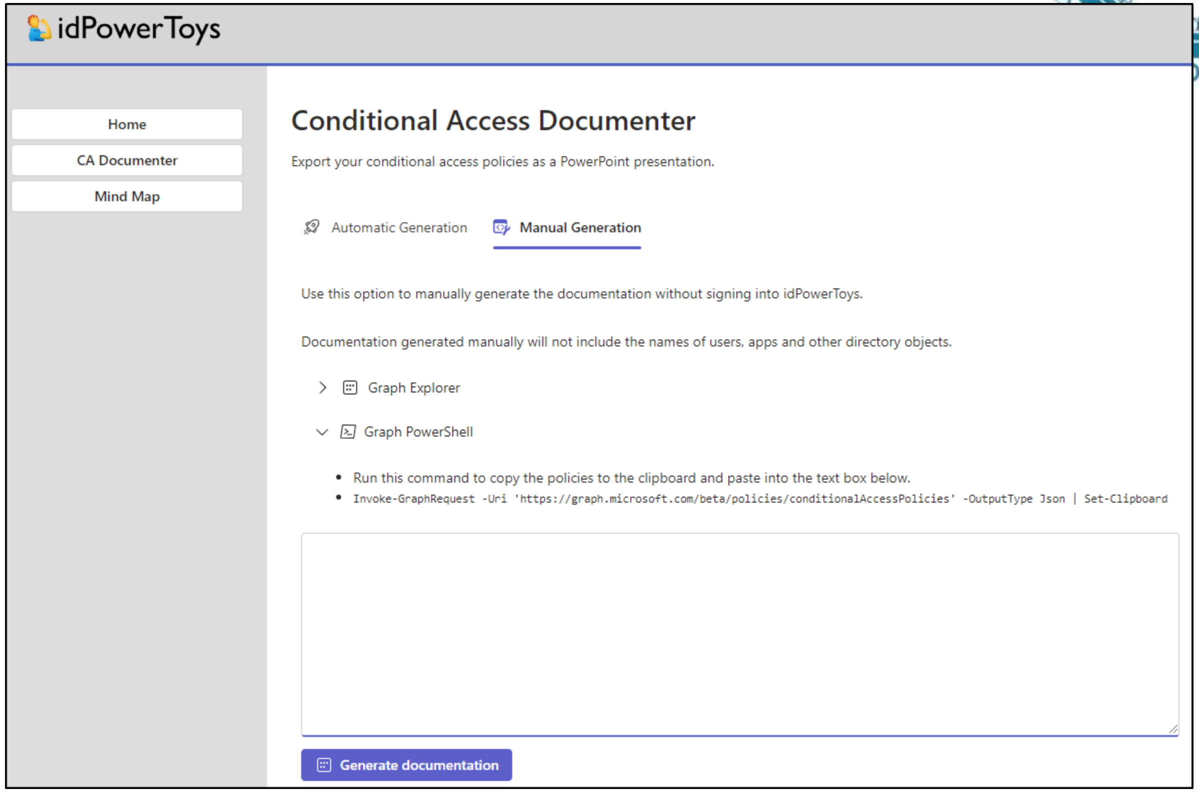
Date range: Last 1 month | Data format: Percentage | Show dates as: UTC | Result: All | Reset filters

| Total sign-ins | Success ⓘ | Failure ⓘ | Not applied ⓘ |
|---|---|---|---|
| 100% | 73.89% | 2.72% | 23.39% |

2025 CORNCON
CYBERSECURITY
CONFERENCE

# Finding Holes

- idPowerToys
  - Conditional Access Documenter



Conditional Access Documenter

Export your conditional access policies as a PowerPoint presentation.

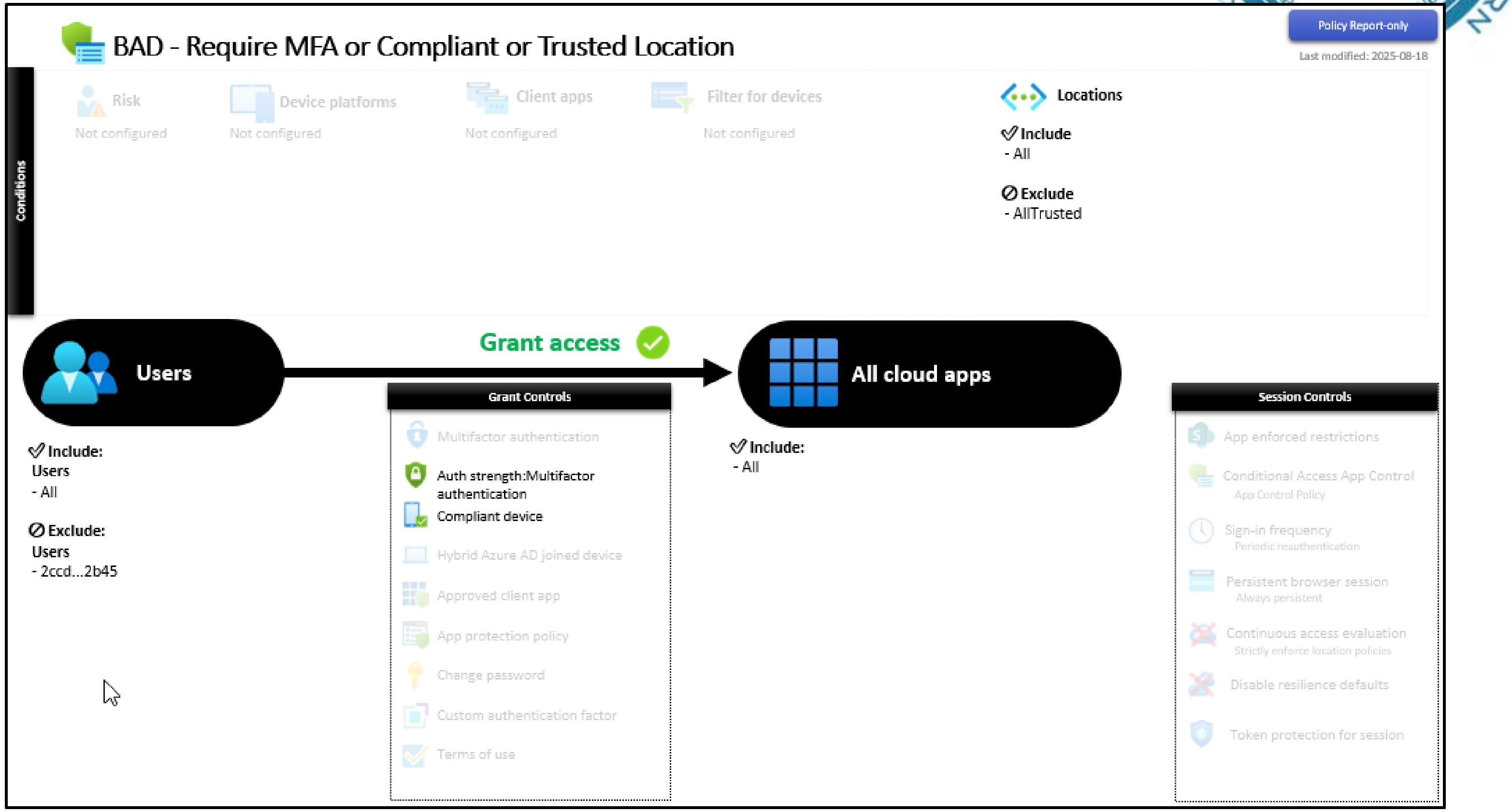
Use this option to manually generate the documentation without signing into idPowerToys.

Documentation generated manually will not include the names of users, apps and other directory objects.

- Run this command to copy the policies to the clipboard and paste into the text box below.
- `Invoke-GraphRequest -Uri 'https://graph.microsoft.com/beta/policies/conditionalAccessPolicies' -OutputType Json | Set-Clipboard`

# Finding Holes

- idPowerToys
  - Conditional Access Documenter



BAD - Require MFA or Compliant or Trusted Location

Policy Report-only

Last modified: 2025-08-18

Conditions

Risk
Not configured

Device platforms
Not configured

Client apps
Not configured

Filter for devices
Not configured

Locations
✓ Include
- All

Exclude
- AllTrusted

Users

✓ Include:
Users
- All

Exclude:
Users
- 2ccd...2b45

Grant access ✓

Grant Controls

- Multifactor authentication
- Auth strength:Multifactor authentication
- Compliant device
- Hybrid Azure AD joined device
- Approved client app
- App protection policy
- Change password
- Custom authentication factor
- Terms of use

All cloud apps

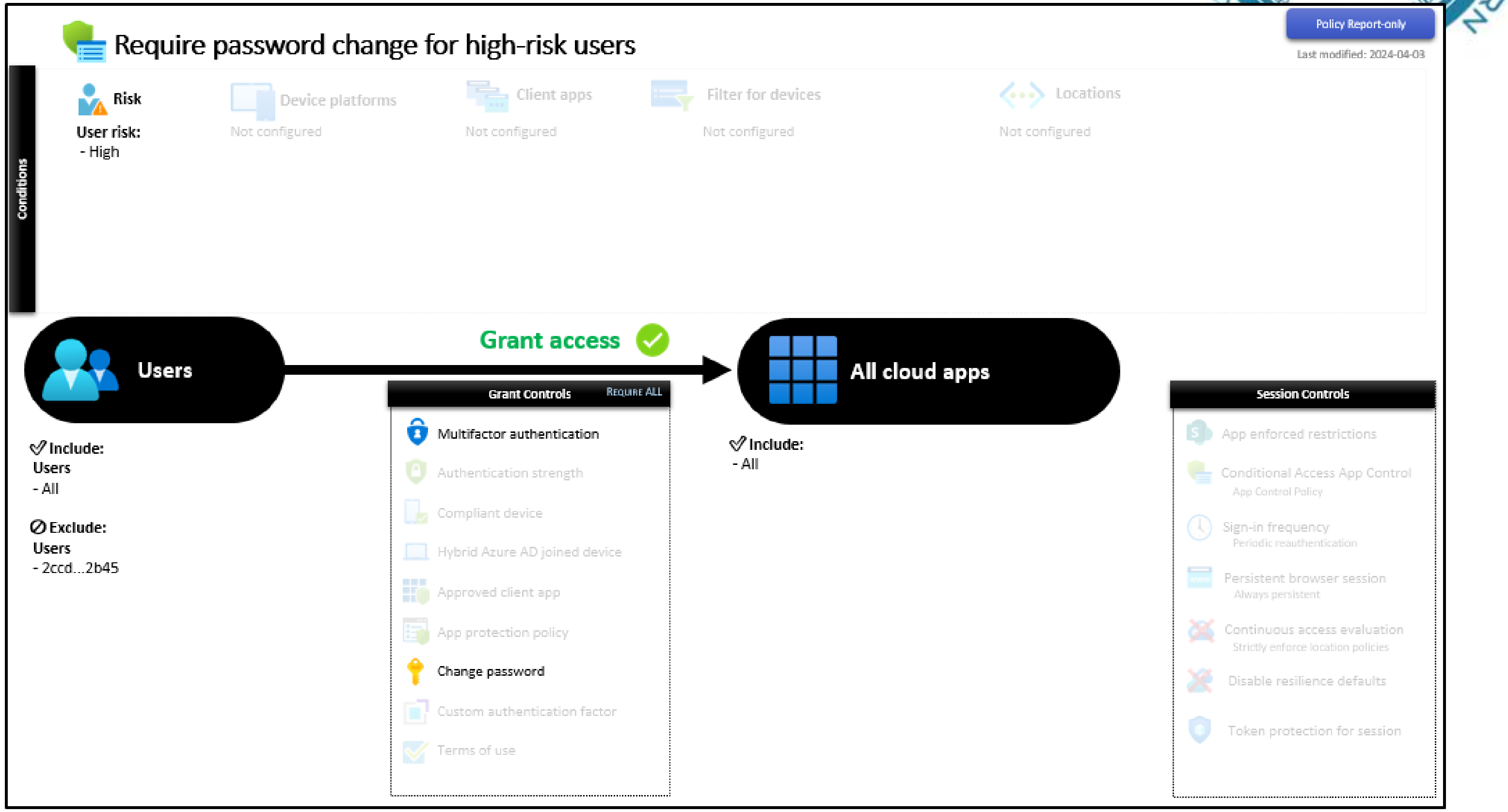
✓ Include:
- All

Session Controls

- App enforced restrictions
- Conditional Access App Control
  App Control Policy
- Sign-in frequency
  Periodic reauthentication
- Persistent browser session
  Always persistent
- Continuous access evaluation
  Strictly enforce location policies
- Disable resilience defaults
- Token protection for session

# Finding Holes

- idPowerToys
  - Conditional Access Documenter



Require password change for high-risk users

Policy Report-only

Last modified: 2024-04-03

Conditions

Risk
User risk:
- High

Device platforms
Not configured

Client apps
Not configured

Filter for devices
Not configured

Locations
Not configured

Users

✓ Include:
Users
- All

⊘ Exclude:
Users
- 2ccd...2b45

Grant access ✓

All cloud apps

✓ Include:
- All

Grant Controls — Require ALL

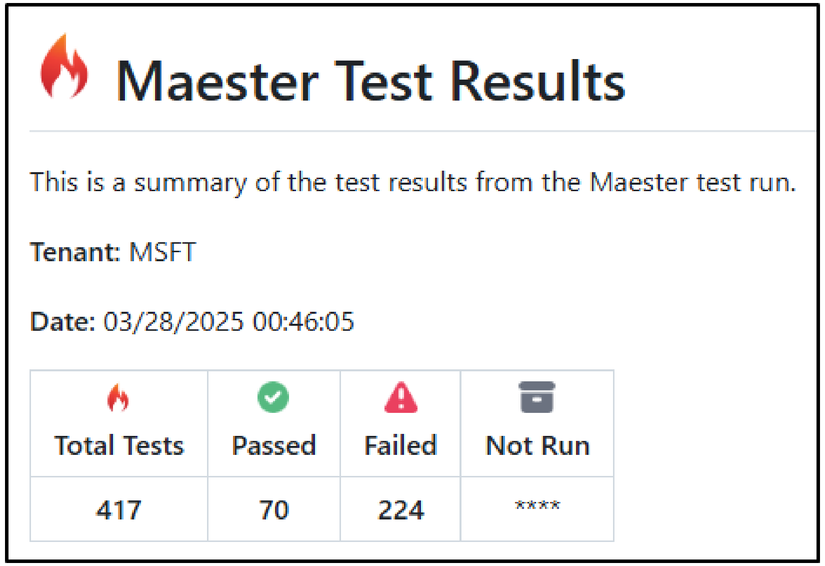
- Multifactor authentication
- Authentication strength
- Compliant device
- Hybrid Azure AD joined device
- Approved client app
- App protection policy
- Change password
- Custom authentication factor
- Terms of use

Session Controls

- App enforced restrictions
- Conditional Access App Control
  App Control Policy
- Sign-in frequency
  Periodic reauthentication
- Persistent browser session
  Always persistent
- Continuous access evaluation
  Strictly enforce location policies
- Disable resilience defaults
- Token protection for session

# Finding Holes

- Maester
  - Full Framework
  - 417+ checks
  - 24 CAP checks



## Maester Test Results

This is a summary of the test results from the Maester test run.

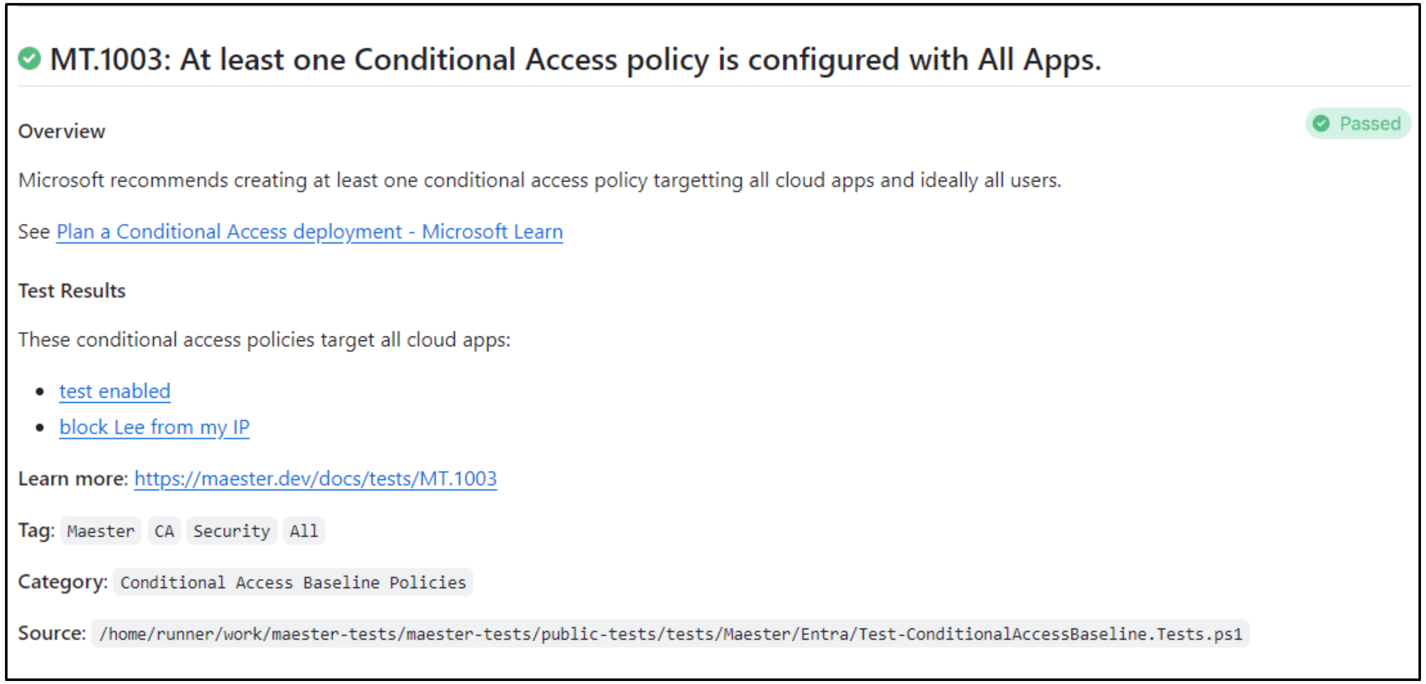
**Tenant:** MSFT

**Date:** 03/28/2025 00:46:05

| Total Tests | Passed | Failed | Not Run |
|---|---|---|---|
| 417 | 70 | 224 | **** |

# Finding Holes

- Maester



### MT.1003: At least one Conditional Access policy is configured with All Apps.

Passed

**Overview**

Microsoft recommends creating at least one conditional access policy targetting all cloud apps and ideally all users.

See Plan a Conditional Access deployment - Microsoft Learn

**Test Results**

These conditional access policies target all cloud apps:

- test enabled
- block Lee from my IP

**Learn more:** https://maester.dev/docs/tests/MT.1003

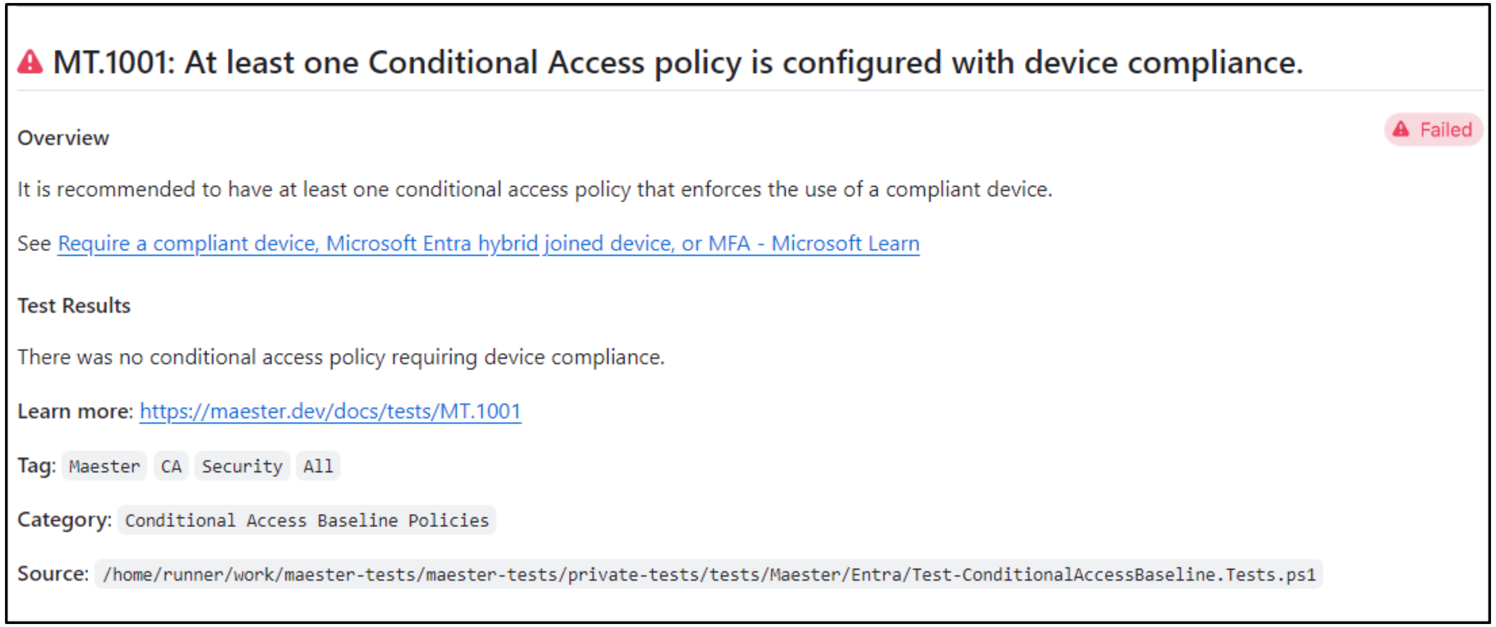
**Tag:** `Maester` `CA` `Security` `All`

**Category:** `Conditional Access Baseline Policies`

**Source:** `/home/runner/work/maester-tests/maester-tests/public-tests/tests/Maester/Entra/Test-ConditionalAccessBaseline.Tests.ps1`

# Finding Holes

- Maester



⚠ MT.1001: At least one Conditional Access policy is configured with device compliance.

Overview ⚠ Failed

It is recommended to have at least one conditional access policy that enforces the use of a compliant device.

See Require a compliant device, Microsoft Entra hybrid joined device, or MFA - Microsoft Learn

Test Results

There was no conditional access policy requiring device compliance.

**Learn more:** https://maester.dev/docs/tests/MT.1001

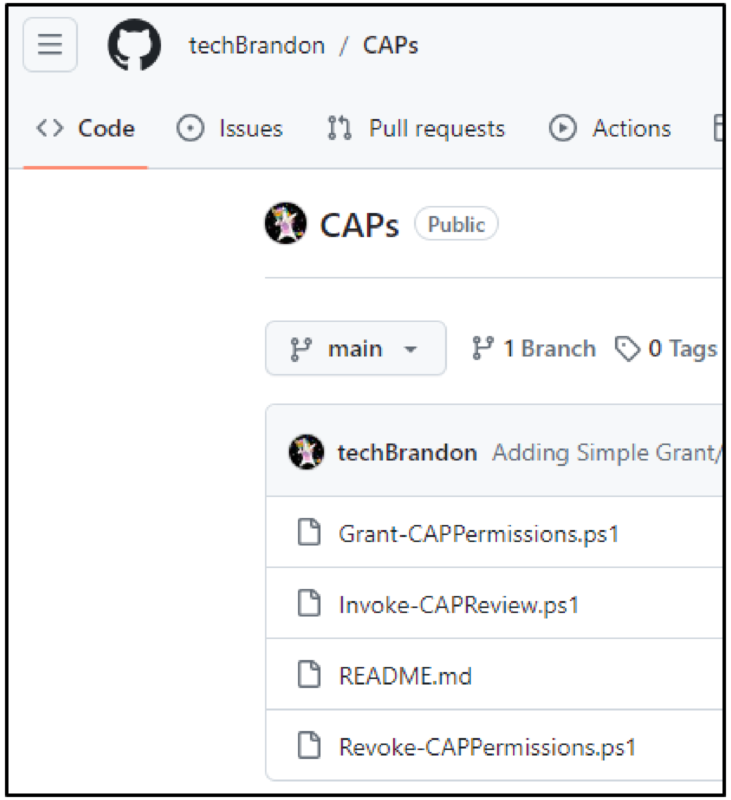
**Tag:** `Maester` `CA` `Security` `All`

**Category:** `Conditional Access Baseline Policies`

**Source:** `/home/runner/work/maester-tests/maester-tests/private-tests/tests/Maester/Entra/Test-ConditionalAccessBaseline.Tests.ps1`

# Finding Holes

- Invoke-CAPReview
  - https://github.com/techBrandon/CAPs



techBrandon / CAPs

Code Issues Pull requests Actions

CAPs Public

main 1 Branch 0 Tags

techBrandon Adding Simple Grant/

Grant-CAPPermissions.ps1

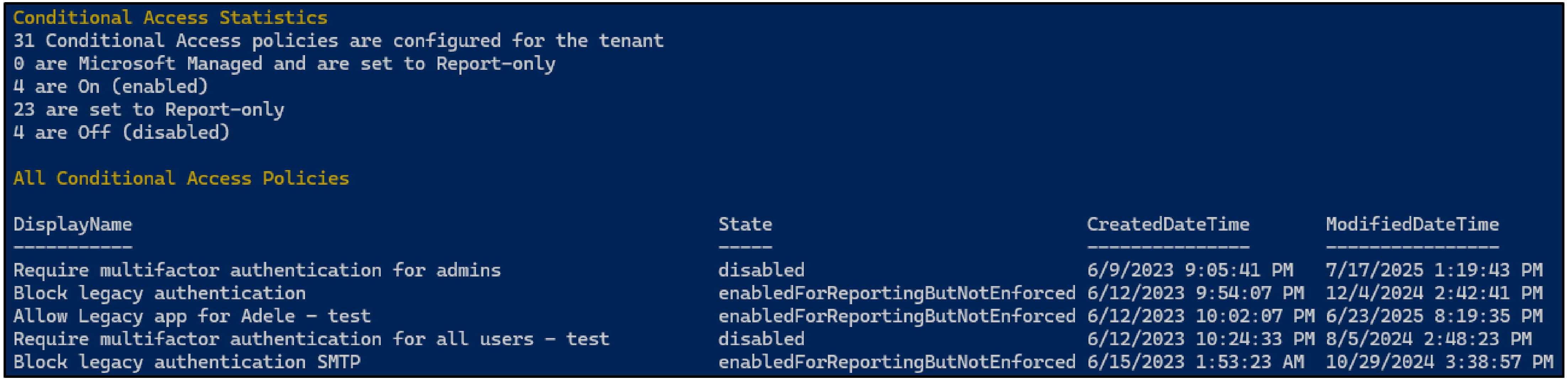
Invoke-CAPReview.ps1

README.md

Revoke-CAPPermissions.ps1

# Finding Holes

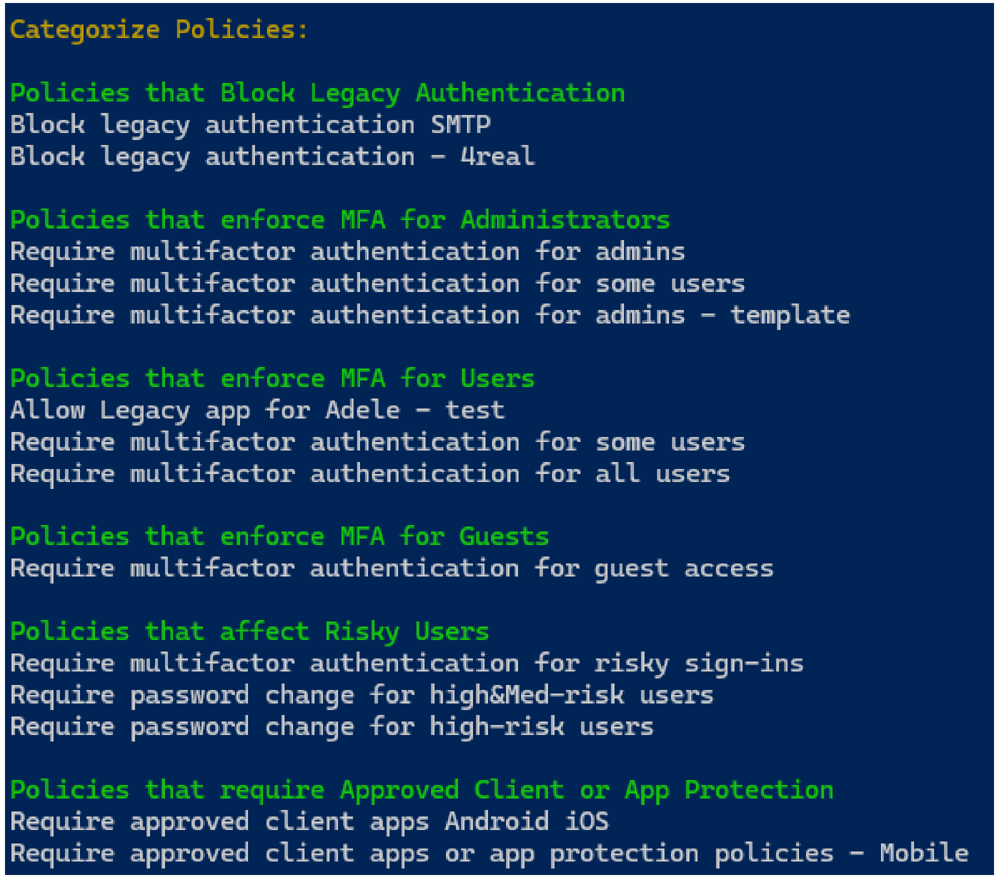
- Invoke-CAPReview



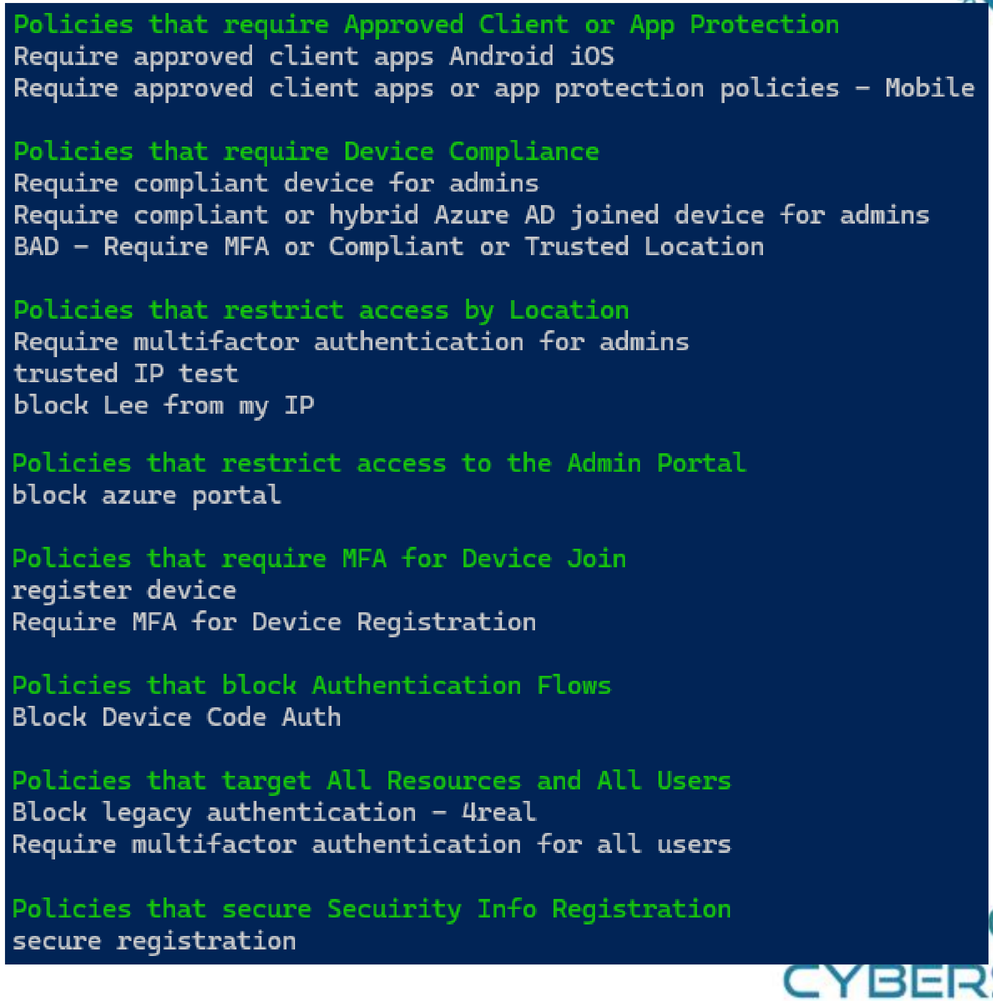
```
Conditional Access Statistics
31 Conditional Access policies are configured for the tenant
0 are Microsoft Managed and are set to Report-only
4 are On (enabled)
23 are set to Report-only
4 are Off (disabled)

All Conditional Access Policies

DisplayName                                                      State                             CreatedDateTime       ModifiedDateTime
-----------                                                      -----                             ---------------       ----------------
Require multifactor authentication for admins                    disabled                          6/9/2023 9:05:41 PM   7/17/2025 1:19:43 PM
Block legacy authentication                                      enabledForReportingButNotEnforced 6/12/2023 9:54:07 PM  12/4/2024 2:42:41 PM
Allow Legacy app for Adele - test                                enabledForReportingButNotEnforced 6/12/2023 10:02:07 PM 6/23/2025 8:19:35 PM
Require multifactor authentication for all users - test          disabled                          6/12/2023 10:24:33 PM 8/5/2024 2:48:23 PM
Block legacy authentication SMTP                                 enabledForReportingButNotEnforced 6/15/2023 1:53:23 AM  10/29/2024 3:38:57 PM
```

# Finding Holes

- Invoke-CAPReview



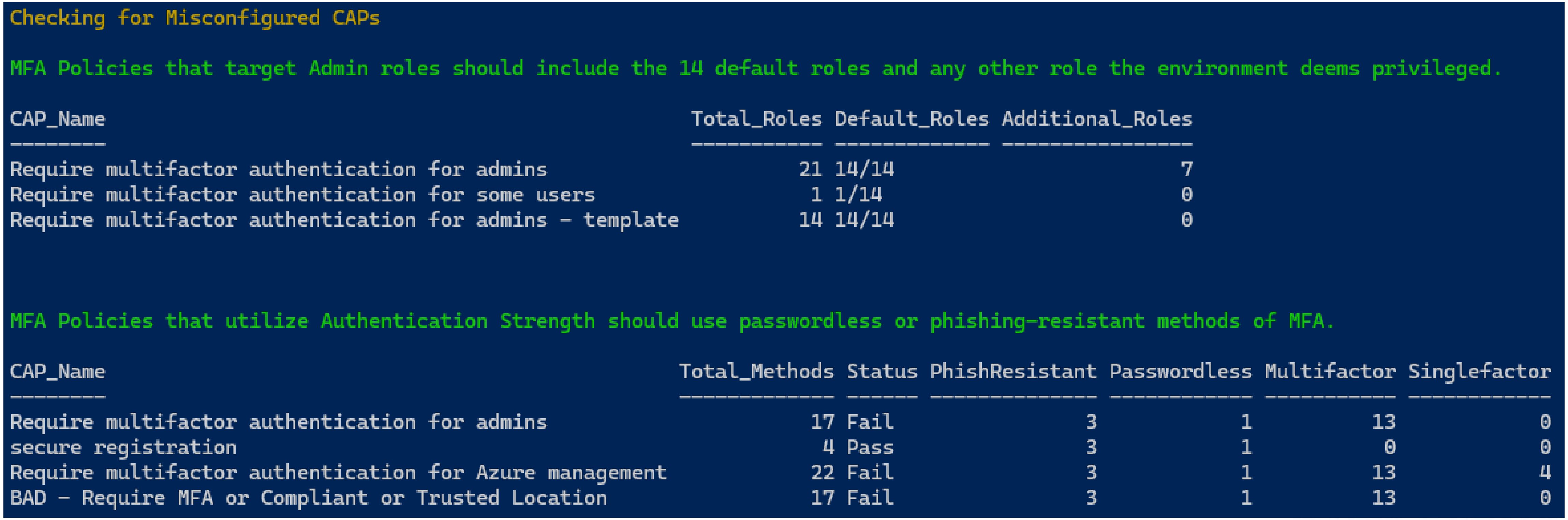
```
Categorize Policies:

Policies that Block Legacy Authentication
Block legacy authentication SMTP
Block legacy authentication - 4real

Policies that enforce MFA for Administrators
Require multifactor authentication for admins
Require multifactor authentication for some users
Require multifactor authentication for admins - template

Policies that enforce MFA for Users
Allow Legacy app for Adele - test
Require multifactor authentication for some users
Require multifactor authentication for all users

Policies that enforce MFA for Guests
Require multifactor authentication for guest access

Policies that affect Risky Users
Require multifactor authentication for risky sign-ins
Require password change for high&Med-risk users
Require password change for high-risk users

Policies that require Approved Client or App Protection
Require approved client apps Android iOS
Require approved client apps or app protection policies - Mobile
```



```
Policies that require Approved Client or App Protection
Require approved client apps Android iOS
Require approved client apps or app protection policies - Mobile

Policies that require Device Compliance
Require compliant device for admins
Require compliant or hybrid Azure AD joined device for admins
BAD - Require MFA or Compliant or Trusted Location

Policies that restrict access by Location
Require multifactor authentication for admins
trusted IP test
block Lee from my IP

Policies that restrict access to the Admin Portal
block azure portal

Policies that require MFA for Device Join
register device
Require MFA for Device Registration

Policies that block Authentication Flows
Block Device Code Auth

Policies that target All Resources and All Users
Block legacy authentication - 4real
Require multifactor authentication for all users

Policies that secure Security Info Registration
secure registration
```

# Finding Holes

- Invoke-CAPReview

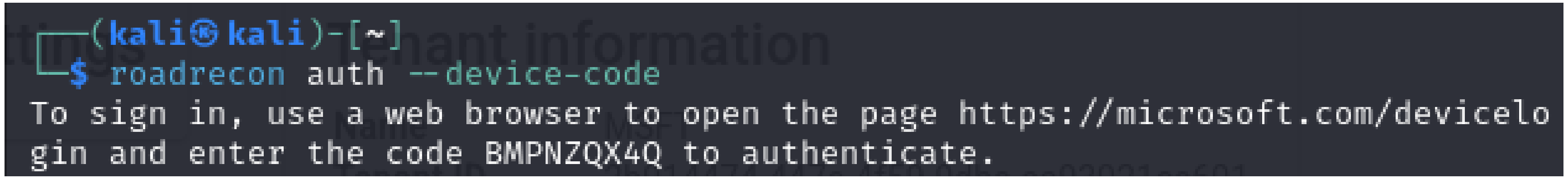


```
Checking for Misconfigured CAPs

MFA Policies that target Admin roles should include the 14 default roles and any other role the environment deems privileged.

CAP_Name                                                 Total_Roles Default_Roles Additional_Roles
--------                                                 ----------- ------------- ----------------
Require multifactor authentication for admins                     21 14/14                        7
Require multifactor authentication for some users                  1 1/14                         0
Require multifactor authentication for admins - template          14 14/14                        0



MFA Policies that utilize Authentication Strength should use passwordless or phishing-resistant methods of MFA.

CAP_Name                                                Total_Methods Status PhishResistant Passwordless Multifactor Singlefactor
--------                                                ------------- ------ -------------- ------------ ----------- ------------
Require multifactor authentication for admins                      17 Fail                3            1          13            0
secure registration                                                 4 Pass                3            1           0            0
Require multifactor authentication for Azure management            22 Fail                3            1          13            4
BAD - Require MFA or Compliant or Trusted Location                 17 Fail                3            1          13            0
```

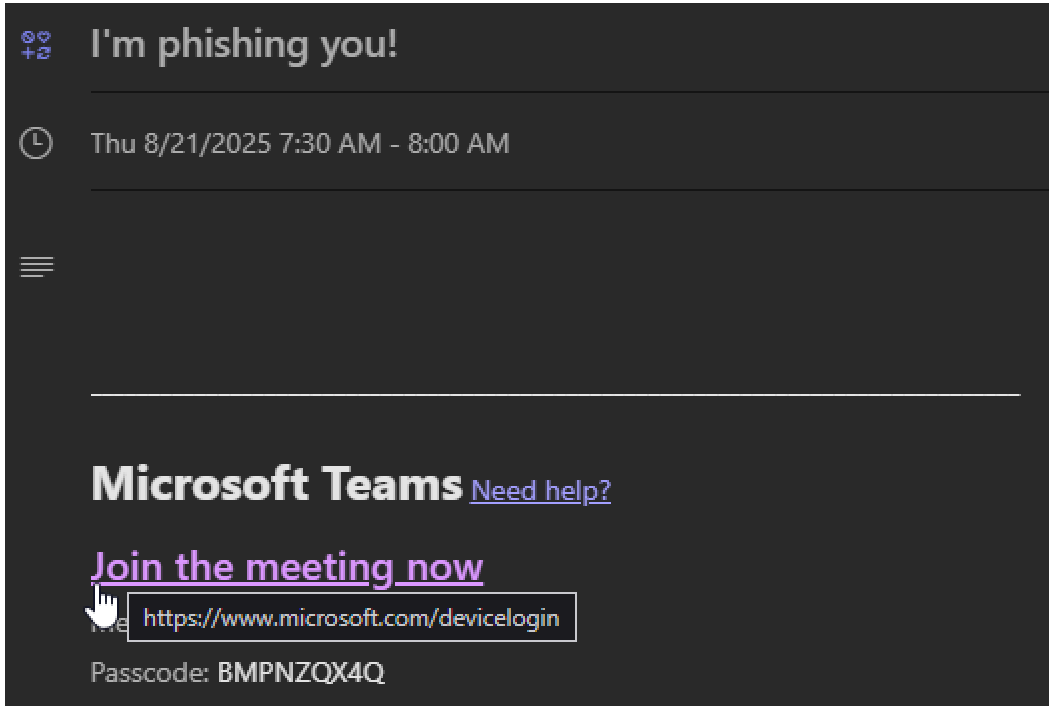
# Finding Holes

- ROADtools
  - Device Code Flow
  - Reconnaissance
  - Conditional Access Enumeration

# Device Code Flow



```
┌──(kali㉿kali)-[~]
└─$ roadrecon auth --device-code
To sign in, use a web browser to open the page https://microsoft.com/devicelo
gin and enter the code BMPNZQX4Q to authenticate.
```



I'm phishing you!

Thu 8/21/2025 7:30 AM - 8:00 AM

**Microsoft Teams** Need help?

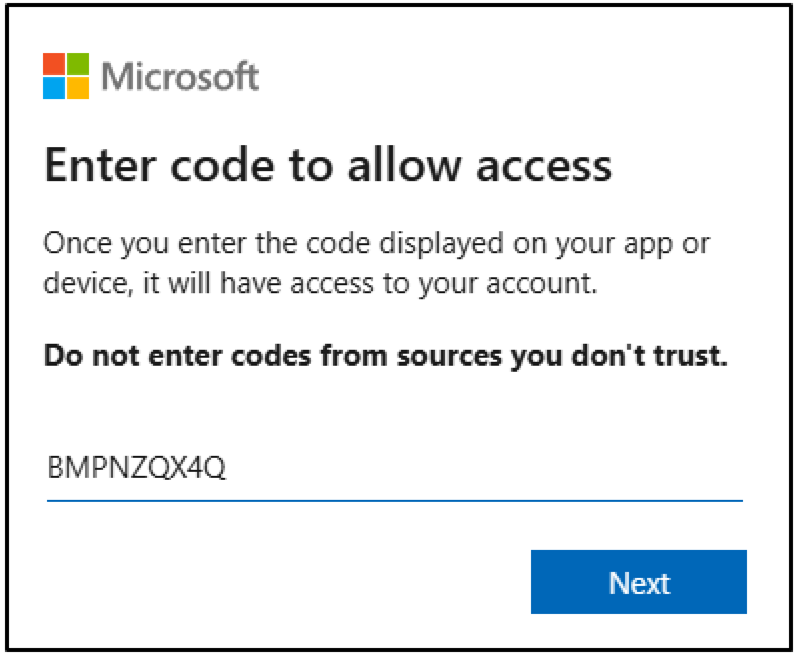
Join the meeting now

https://www.microsoft.com/devicelogin

Passcode: BMPNZQX4Q

# Device Code Flow

- https://www.microsoft.com/devicelogin



Microsoft

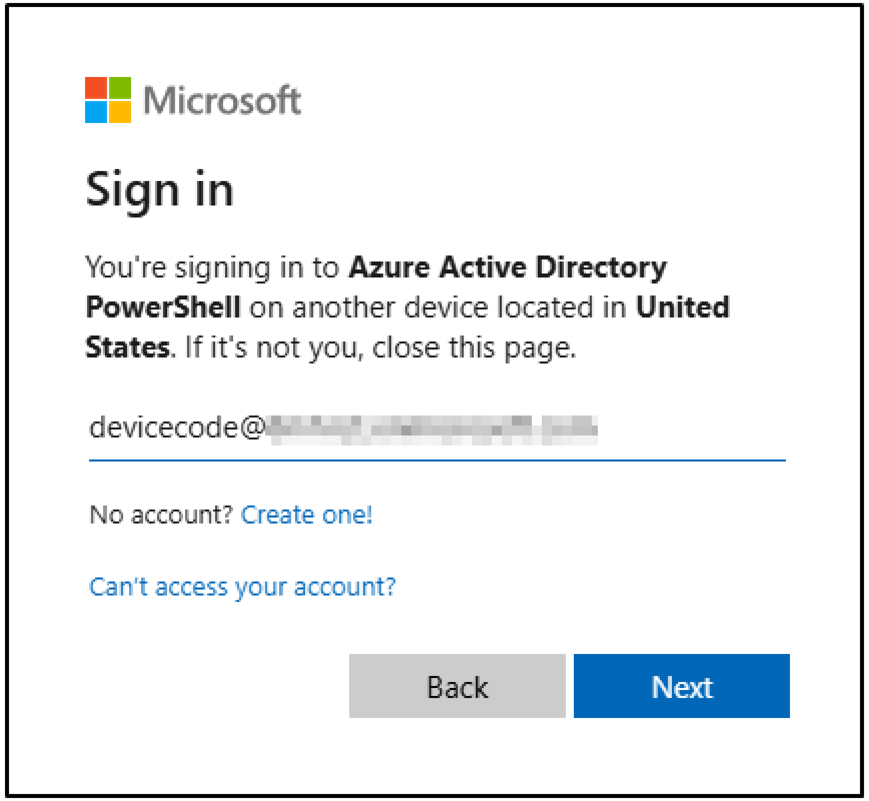
Enter code to allow access

Once you enter the code displayed on your app or device, it will have access to your account.

**Do not enter codes from sources you don't trust.**

BMPNZQX4Q

# Device Code Flow



Microsoft

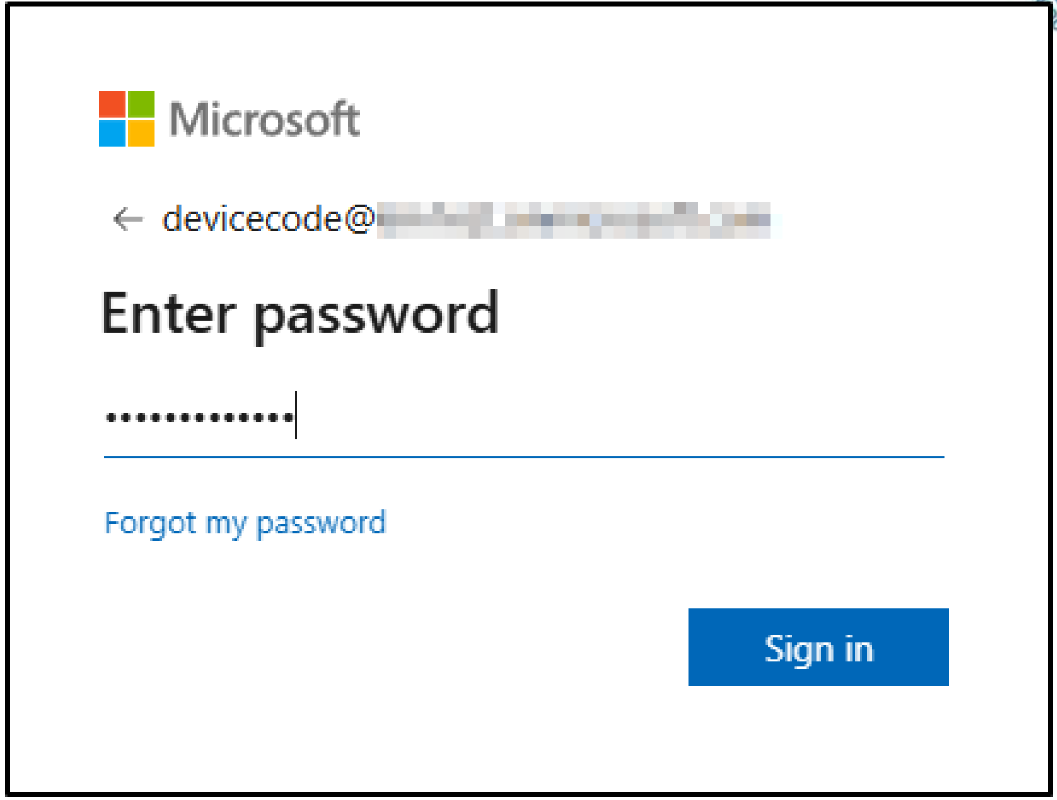
Sign in

You're signing in to **Azure Active Directory PowerShell** on another device located in **United States**. If it's not you, close this page.

devicecode@[redacted]

No account? Create one!

Can't access your account?



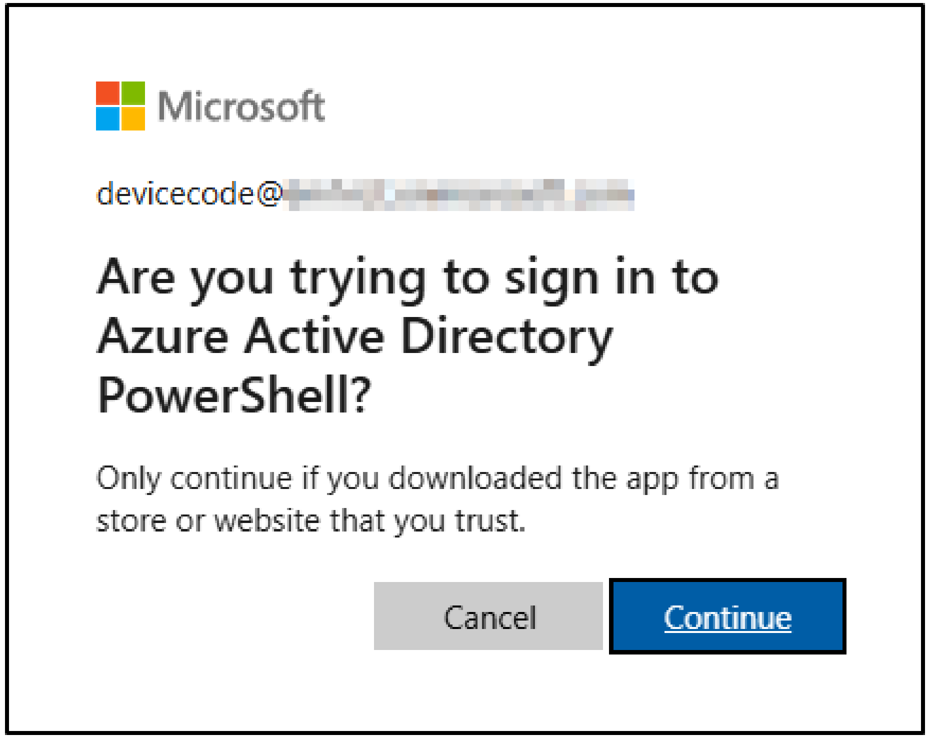
Microsoft

← devicecode@[redacted]

Enter password

•••••••••••••

# Device Code Flow

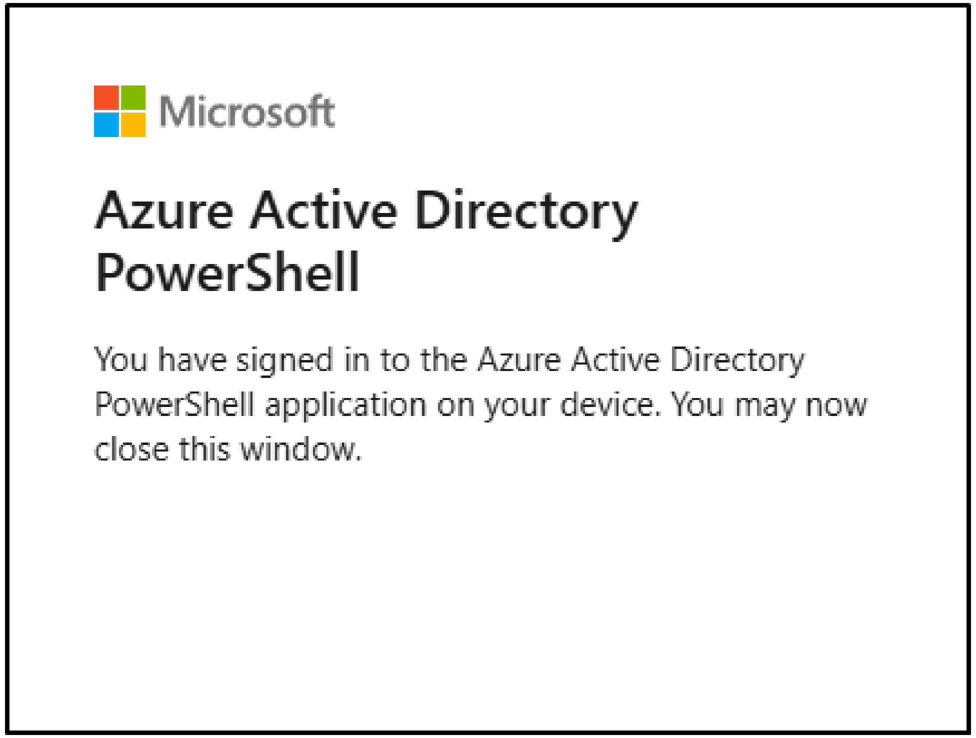


Microsoft

devicecode@[redacted]

Are you trying to sign in to Azure Active Directory PowerShell?

Only continue if you downloaded the app from a store or website that you trust.

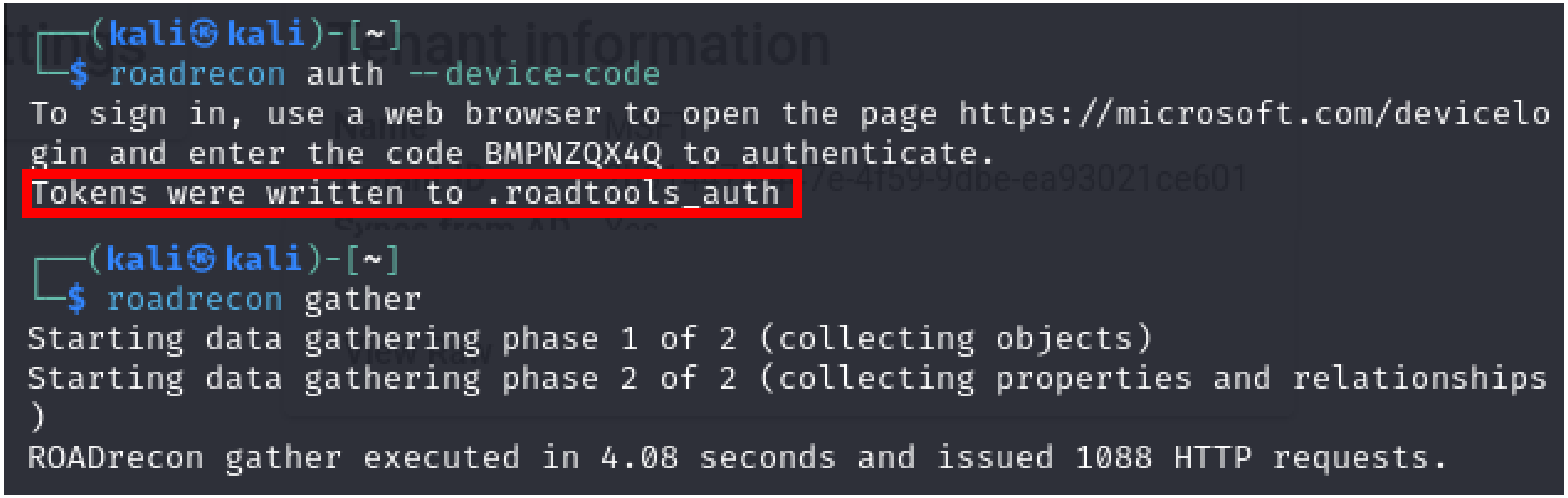


Microsoft

Azure Active Directory PowerShell

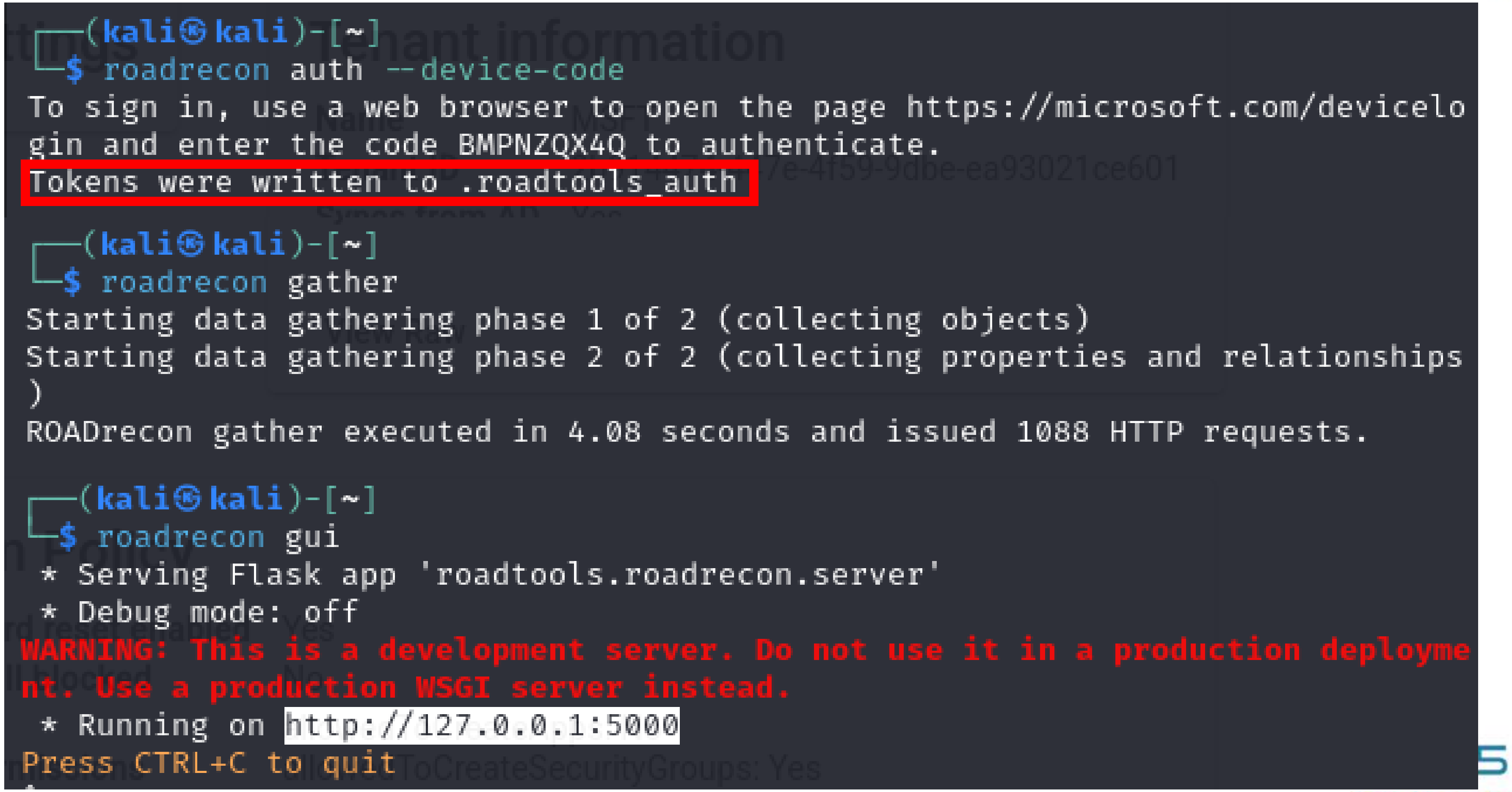
You have signed in to the Azure Active Directory PowerShell application on your device. You may now close this window.

# Device Code Flow



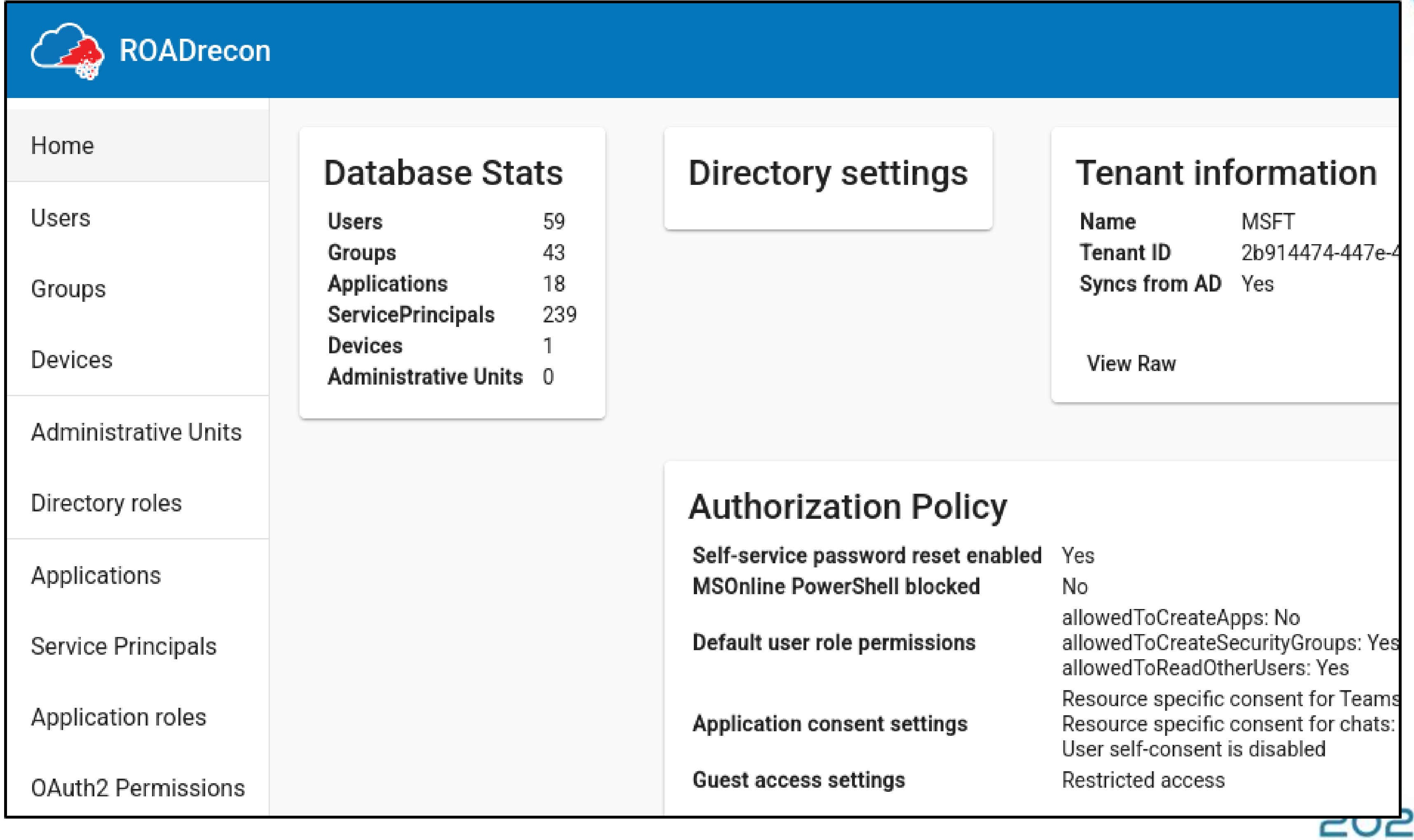
```
┌──(kali㉿kali)-[~]
└─$ roadrecon auth --device-code
To sign in, use a web browser to open the page https://microsoft.com/devicelo
gin and enter the code BMPNZQX4Q to authenticate.
Tokens were written to .roadtools_auth

┌──(kali㉿kali)-[~]
└─$ roadrecon gather
Starting data gathering phase 1 of 2 (collecting objects)
Starting data gathering phase 2 of 2 (collecting properties and relationships
)
ROADrecon gather executed in 4.08 seconds and issued 1088 HTTP requests.
```

# Device Code Flow



```
┌──(kali㉿kali)-[~]
└─$ roadrecon auth --device-code
To sign in, use a web browser to open the page https://microsoft.com/devicelo
gin and enter the code BMPNZQX4Q to authenticate.
Tokens were written to .roadtools_auth

┌──(kali㉿kali)-[~]
└─$ roadrecon gather
Starting data gathering phase 1 of 2 (collecting objects)
Starting data gathering phase 2 of 2 (collecting properties and relationships
)
ROADrecon gather executed in 4.08 seconds and issued 1088 HTTP requests.

┌──(kali㉿kali)-[~]
└─$ roadrecon gui
 * Serving Flask app 'roadtools.roadrecon.server'
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployme
nt. Use a production WSGI server instead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
```

# Reconnaissance



## Database Stats

| | |
|---|---|
| Users | 59 |
| Groups | 43 |
| Applications | 18 |
| ServicePrincipals | 239 |
| Devices | 1 |
| Administrative Units | 0 |

## Directory settings

## Tenant information

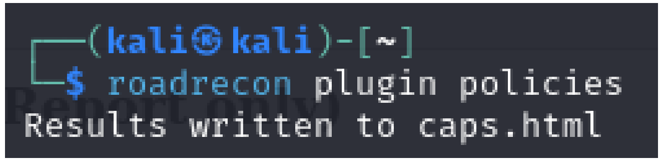
| | |
|---|---|
| Name | MSFT |
| Tenant ID | 2b914474-447e-4 |
| Syncs from AD | Yes |

View Raw

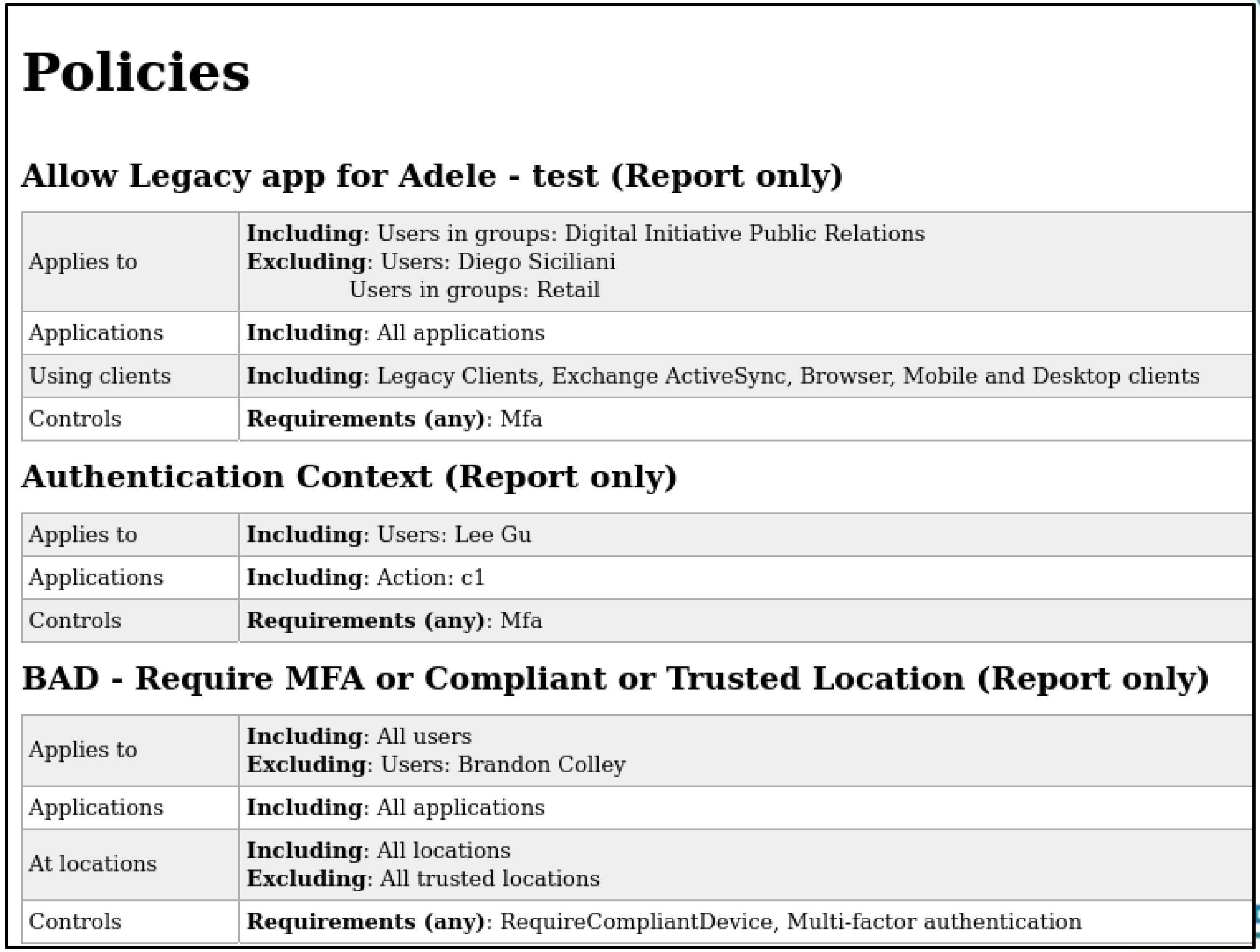
## Authorization Policy

| | |
|---|---|
| Self-service password reset enabled | Yes |
| MSOnline PowerShell blocked | No |
| Default user role permissions | allowedToCreateApps: No<br>allowedToCreateSecurityGroups: Yes<br>allowedToReadOtherUsers: Yes |
| Application consent settings | Resource specific consent for Teams<br>Resource specific consent for chats:<br>User self-consent is disabled |
| Guest access settings | Restricted access |

# Conditional Access Enumeration



```
┌──(kali㉿kali)-[~]
└─$ roadrecon plugin policies
Results written to caps.html
```



# Policies

### Allow Legacy app for Adele - test (Report only)

| | |
|---|---|
| Applies to | **Including**: Users in groups: Digital Initiative Public Relations<br>**Excluding**: Users: Diego Siciliani<br>Users in groups: Retail |
| Applications | **Including**: All applications |
| Using clients | **Including**: Legacy Clients, Exchange ActiveSync, Browser, Mobile and Desktop clients |
| Controls | **Requirements (any)**: Mfa |

### Authentication Context (Report only)

| | |
|---|---|
| Applies to | **Including**: Users: Lee Gu |
| Applications | **Including**: Action: c1 |
| Controls | **Requirements (any)**: Mfa |

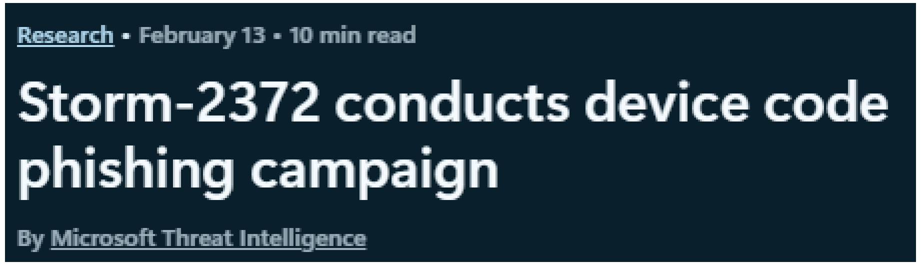
### BAD - Require MFA or Compliant or Trusted Location (Report only)

| | |
|---|---|
| Applies to | **Including**: All users<br>**Excluding**: Users: Brandon Colley |
| Applications | **Including**: All applications |
| At locations | **Including**: All locations<br>**Excluding**: All trusted locations |
| Controls | **Requirements (any)**: RequireCompliantDevice, Multi-factor authentication |

# Finding Holes

- ROADtools
  - Device Code Flow
  - Reconnaissance
  - Conditional Access Enumeration

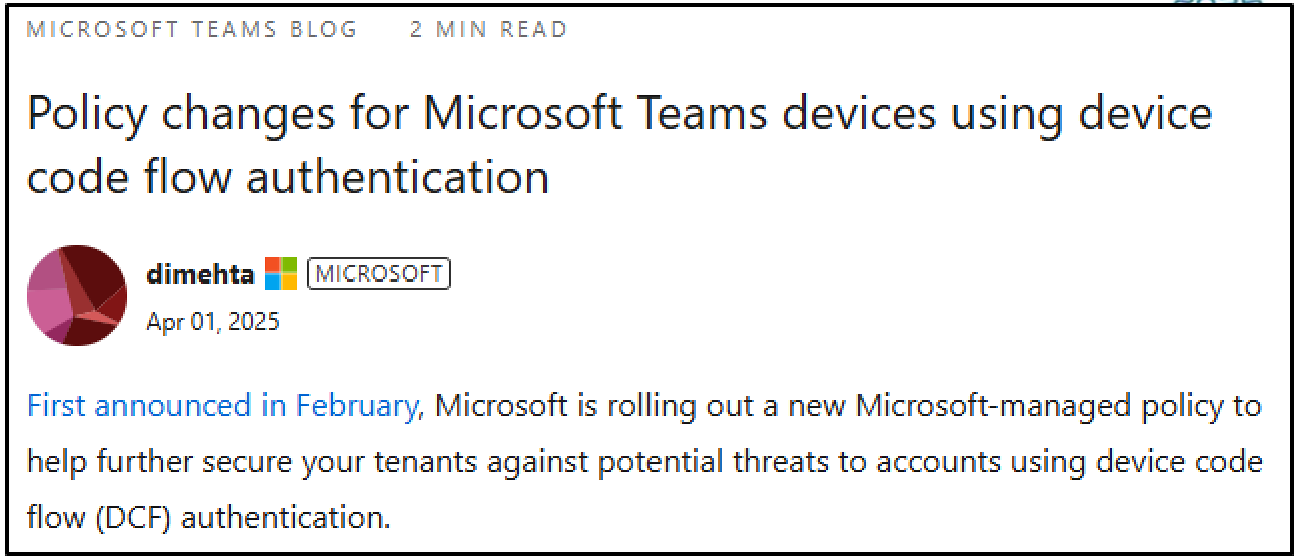
# Device Code Flow



Research • February 13 • 10 min read

Storm-2372 conducts device code phishing campaign

By Microsoft Threat Intelligence



MICROSOFT TEAMS BLOG 2 MIN READ

Policy changes for Microsoft Teams devices using device code flow authentication

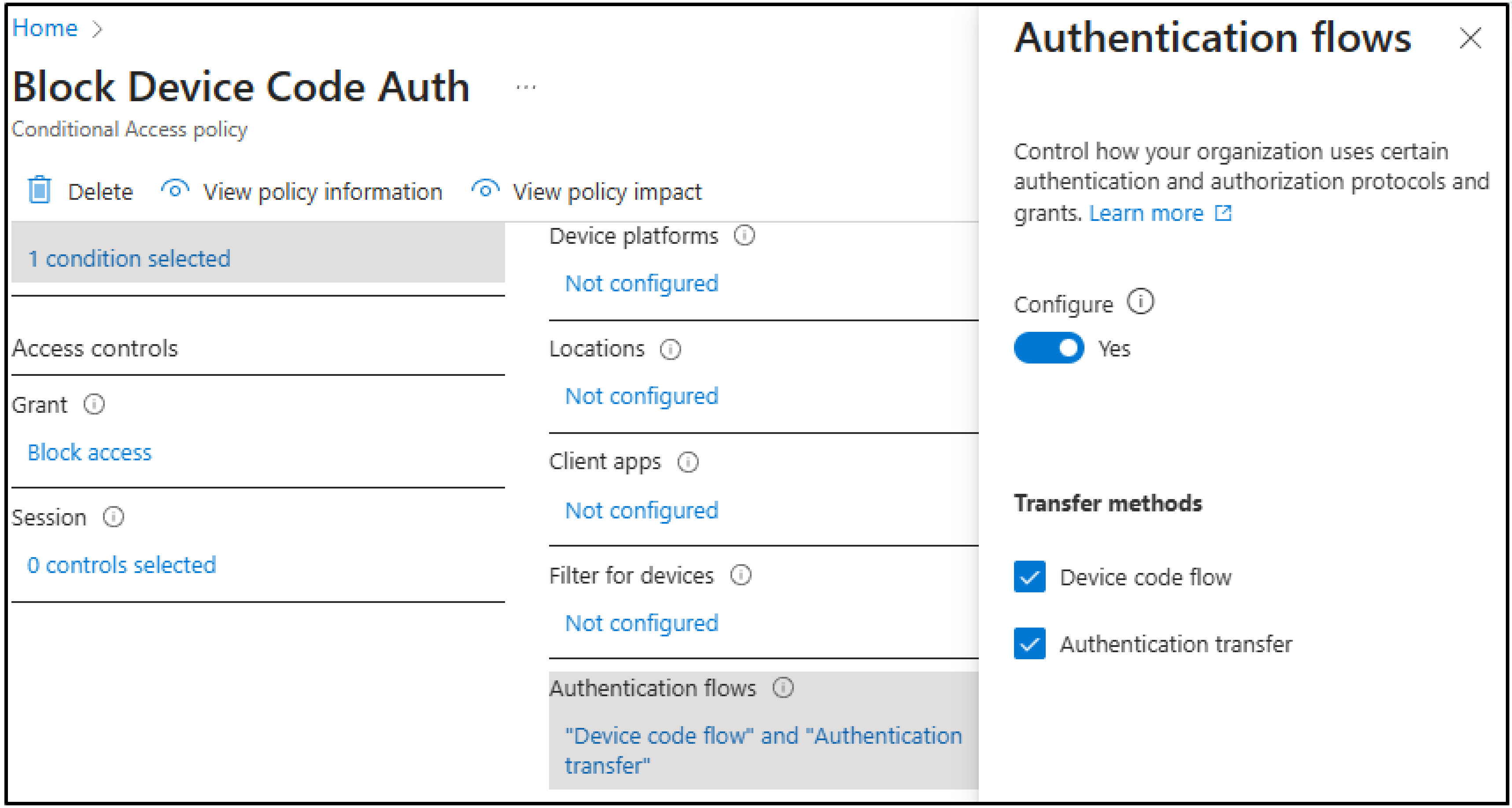
dimehta MICROSOFT

Apr 01, 2025

First announced in February, Microsoft is rolling out a new Microsoft-managed policy to help further secure your tenants against potential threats to accounts using device code flow (DCF) authentication.

https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/#Update-February-14
https://techcommunity.microsoft.com/blog/microsoftteamsblog/policy-changes-for-microsoft-teams-devices-using-device-code-flow-authentication/4399337
https://youtu.be/Y8SSYLEq15Q?si=_e3OFAv7BOJQ1Ide

# Device Code Flow



Home >

Block Device Code Auth ...

Conditional Access policy

Delete | View policy information | View policy impact

1 condition selected

Access controls

Grant ⓘ

Block access

Session ⓘ

0 controls selected

Device platforms ⓘ

Not configured

Locations ⓘ

Not configured

Client apps ⓘ

Not configured

Filter for devices ⓘ

Not configured

Authentication flows ⓘ

"Device code flow" and "Authentication transfer"

Authentication flows

Control how your organization uses certain authentication and authorization protocols and grants. Learn more

Configure ⓘ

Yes

**Transfer methods**

☑ Device code flow

☑ Authentication transfer

https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-authentication-flows

# Takeaways

- Did you have fun?
- Learn something exciting?
- Logic flaws and defaults
- New tools
- Understand the adversary

# Thank you!

- https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Overview
- https://learn.microsoft.com/en-us/entra/identity/conditional-access/what-if-tool
- https://idpowertoys.merill.net/ca
- https://maester.dev/
- https://github.com/techBrandon/CAPs
- https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-admin-mfa
- https://techcommunity.microsoft.com/t5/microsoft-entra-blog/introducing-the-microsoft-entra-powershell-module/ba-p/4173546
- https://learn.microsoft.com/en-us/azure/architecture/guide/security/conditional-access-framework
- https://github.com/dafthack/MFASweep
- https://github.com/dirkjanm/ROADtools

# Questions?

@techBrandon

contact@bnrconsulting.net