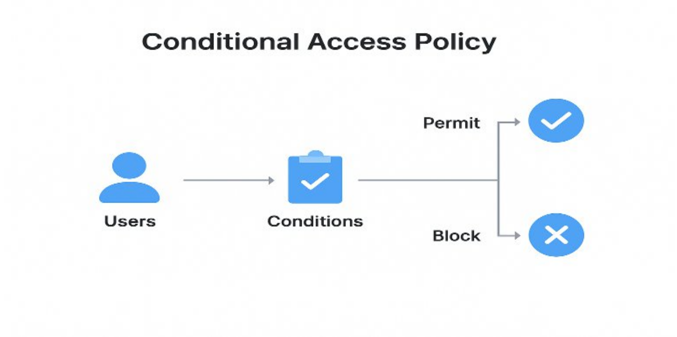
Leonard M. Estos
Cybersecurity Researcher & Technical Author
Edmonton, Alberta, Canada

Conditional Access Policy (Microsoft)

What is Conditional Access Policy: Conditional Access Policy is one of **the most powerful tools in Microsoft 365 security**. It helps organizations protect against password theft, risky sign-ins, and unauthorized device access by enforcing conditions that must be met before granting access to company resources.



Purpose: As part of Cybersecurity protection/mitigation, conditional access acts as part of an organization's cybersecurity defense strategy. Its primary purpose is to protect and prevent access from:

- Password Theft
- Risky Sign-ins
- Unmanaged Devices

See below the baseline for the **company should apply** to their Enterprises/Business.

In simple terms, it functions like a digital security guard, verifying your **identity**, **authenticating** your credentials, and **authorizing** your access before you enter.

Naming Policy Guidelines: To maintain consistency and clarity, apply a structured naming policy when creating Conditional Access policies.

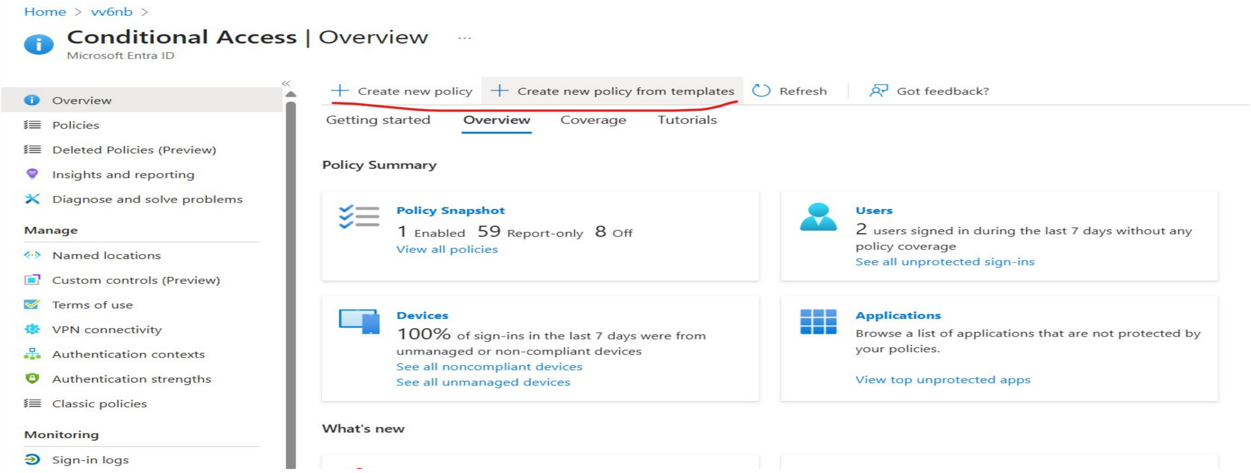
Example naming structure:
- Who: Target users or groups
- What: Condition or app
- Action: Required control

Example: Admins - All Apps - Require MFA

Application/Technical Configuration:

Now for **foundation required all users to grant access and require multifactor Authentication**.

Go to Microsoft 365 Admin Center > Click or Search for Identity (New browser will open for Microsoft 365 Admin Center Identity > Click Conditional Access



Policy Summary

Policy Snapshot
1 Enabled 59 Report-only 8 Off
View all policies

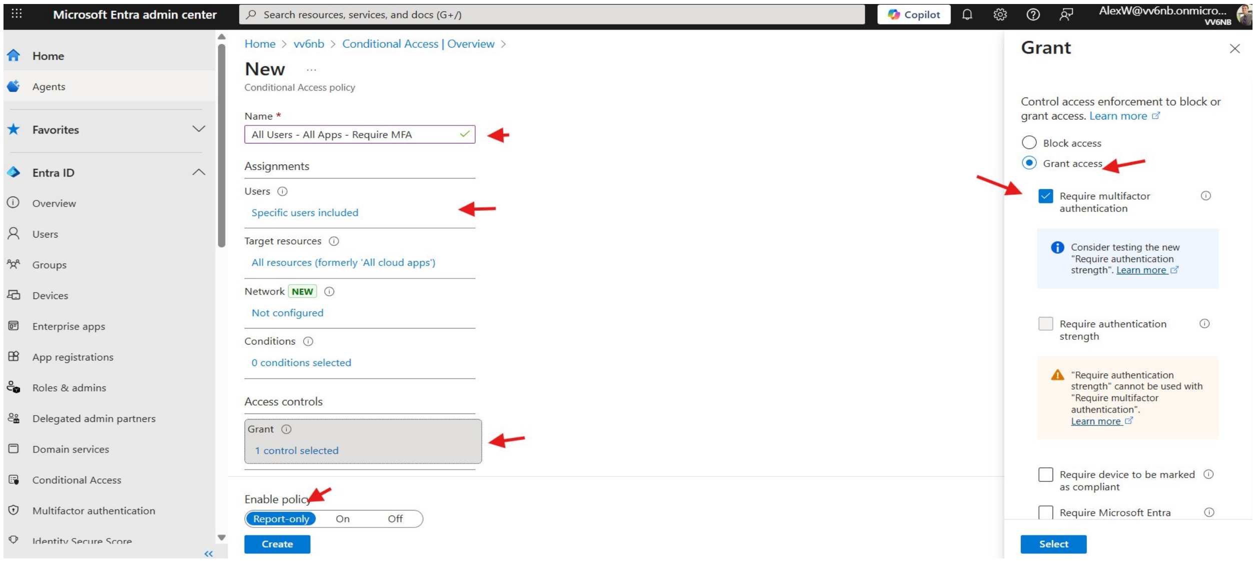
Users
2 users signed in during the last 7 days without any policy coverage
See all unprotected sign-ins

Devices
100% of sign-ins in the last 7 days were from unmanaged or non-compliant devices
See all noncompliant devices
See all unmanaged devices

Applications
Browse a list of applications that are not protected by your policies.
View top unprotected apps

What's new

Now, Click Create new policy and supply the following base on screenshot below > Click Create (Report) Only (If you want to take effect immediately choose on)



New ...
Conditional Access policy

Name *
All Users - All Apps - Require MFA

Assignments

Users
Specific users included

Target resources
All resources (formerly 'All cloud apps')

Network NEW
Not configured

Conditions
0 conditions selected

Access controls

Grant
1 control selected

Enable policy
[✓ Report-only] On Off

Create

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

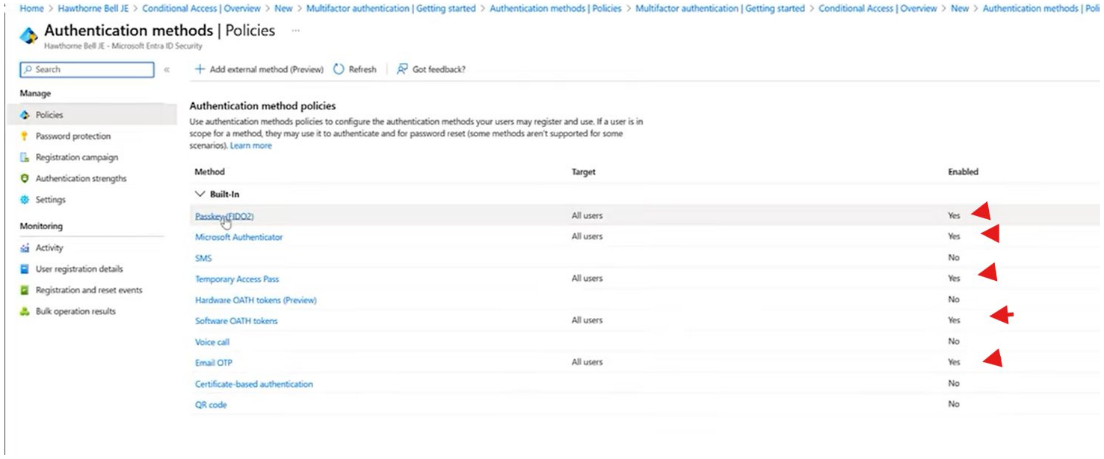
□ Require Microsoft Entra

Select

Five baselines Conditional Access Policies every Company/Business Organization should apply:

Policy 1: Require Strong MFA for all Users

Create a policy to require strong MFA in **All Users - All Apps - Require Strong MFA**. Now to Enable the different Policies MFA, Click in Microsoft 365 Admin Center > **Entra ID > Authentication Method > Policies**



Home > Hawthorne Bell JE > Conditional Access | Overview > New > Multifactor authentication | Getting started > Authentication methods | Policies > Multifactor authentication | Getting started > Conditional Access | Overview > New > Authentication methods | Poli

Authentication methods | Policies

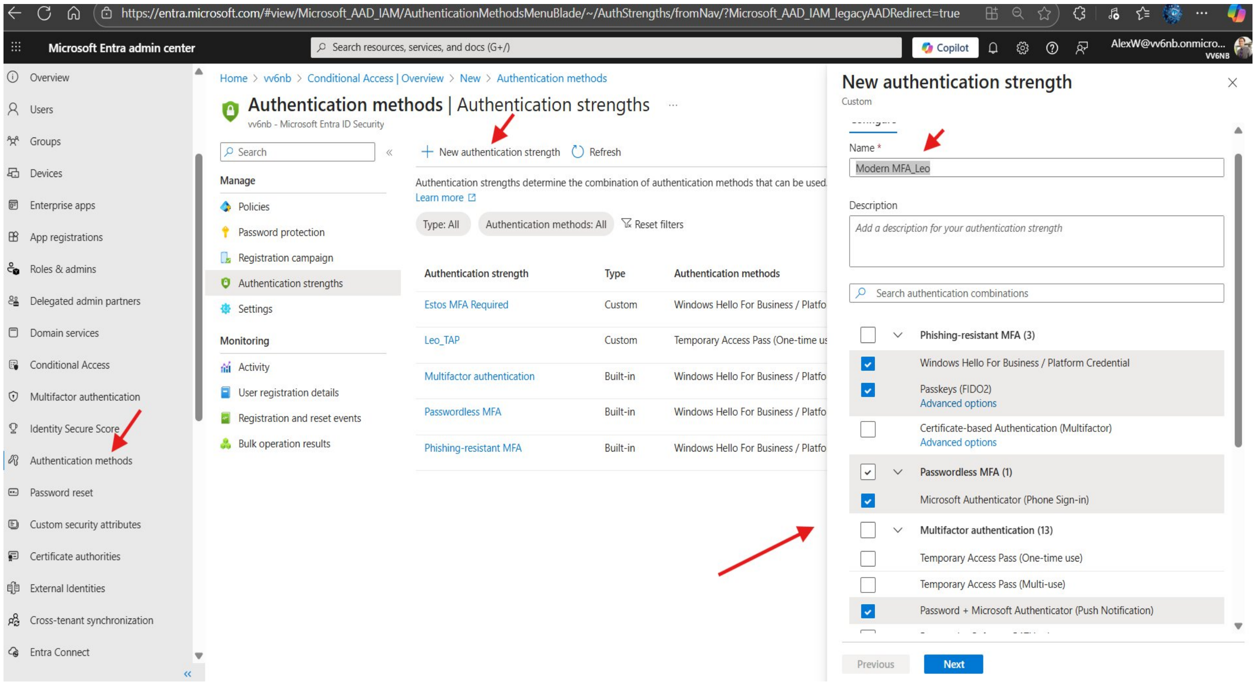
Hawthorne Bell JE - Microsoft Entra ID Security

Authentication method policies

Use authentication methods policies to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenarios). Learn more

Method	Target	Enabled
Built-In		
Passkey (FIDO2)	All users	Yes
Microsoft Authenticator	All users	Yes
SMS		No
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Preview)		No
Software OATH tokens	All users	Yes
Voice call		No
Email OTP	All users	Yes
Certificate-based authentication		No
QR code		No

- To further strengthen your MFA, click in Microsoft 365 Admin Center > Entra ID > Authentication Method > **Policies > Authentication strengths and create the Modern MFA >** Click Next > Review > Create



https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/AuthStrengths/fromNav/?Microsoft_AAD_IAM_legacyAADRedirect=true

Home > vv6nb > Conditional Access | Overview > New > Authentication methods

Authentication methods | Authentication strengths

vv6nb - Microsoft Entra ID Security

Authentication strengths determine the combination of authentication methods that can be used. Learn more

Type: All | Authentication methods: All | Reset filters

Authentication strength	Type	Authentication methods
Estos MFA Required	Custom	Windows Hello For Business / Platfo
Leo_TAP	Custom	Temporary Access Pass (One-time us
Multifactor authentication	Built-in	Windows Hello For Business / Platfo
Passwordless MFA	Built-in	Windows Hello For Business / Platfo
Phishing-resistant MFA	Built-in	Windows Hello For Business / Platfo

New authentication strength

Custom

Name *

Modern MFA_Leo

Description

Add a description for your authentication strength

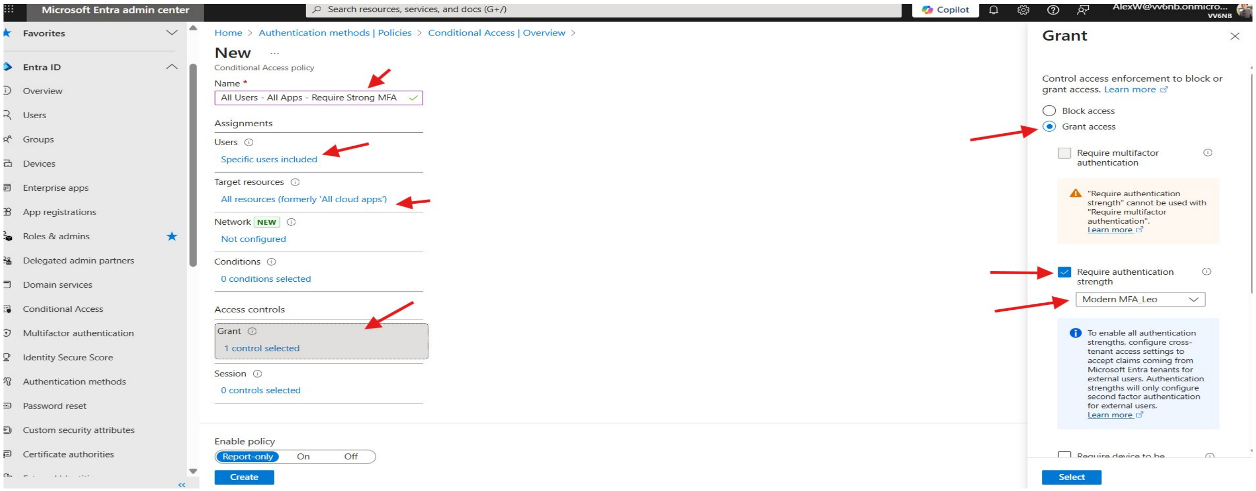
Search authentication combinations

- □ Phishing-resistant MFA (3)
  - ☑ Windows Hello For Business / Platform Credential
  - ☑ Passkeys (FIDO2) Advanced options
  - □ Certificate-based Authentication (Multifactor) Advanced options
- ☑ Passwordless MFA (1)
  - ☑ Microsoft Authenticator (Phone Sign-in)
- □ Multifactor authentication (13)
  - □ Temporary Access Pass (One-time use)
  - □ Temporary Access Pass (Multi-use)
  - ☑ Password + Microsoft Authenticator (Push Notification)

Previous | Next

- Now create a new policy > Microsoft 365 Admin Center Identity > Entra ID> Click Conditional Access > Create New Policy > Naming: All Users - All Apps - Require Strong MFA > Grant **(Required Authentication Strength) and choose (Modern MFA_Leo)** or please see screenshot below for complete implementation of policy.

- In Assignments note to **Include all Users and Group, but Exclude the Administrator Account/s**



New
Conditional Access policy

Name *
All Users - All Apps - Require Strong MFA

Assignments
Users: Specific users included
Target resources: All resources (formerly 'All cloud apps')
Network NEW: Not configured
Conditions: 0 conditions selected

Access controls
Grant: 1 control selected
Session: 0 controls selected

Enable policy: [✓ Report-only] On Off

Grant

Control access enforcement to block or grant access. Learn more

○ Block access
● Grant access

□ Require multifactor authentication

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

☑ Require authentication strength
Modern MFA_Leo

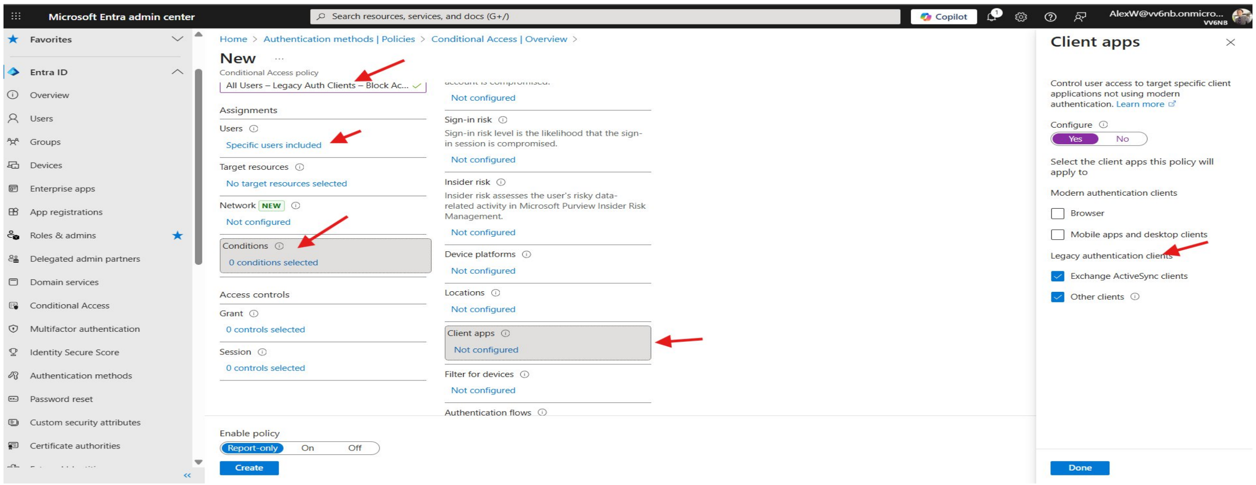
To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users. Learn more

□ Require device to be

Policy 2: Block Legacy Authentication Clients

Create a policy to **All Users – Legacy Auth Clients – Block Access**. The purpose of this policy is to block the legacy authentication protocol like POP, SMTP, and IMAP those protocols don't support MFA this is open to attackers.

- Click in Microsoft 365 Admin Center **> Entra ID > Conditional Access > Create New Policy**



New
Conditional Access policy
All Users – Legacy Auth Clients – Block Ac...

Assignments
Users: Specific users included
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

account is compromised.
Not configured

Sign-in risk
Sign-in risk level is the likelihood that the sign-in session is compromised.
Not configured

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: Not configured
Client apps: Not configured
Filter for devices: Not configured
Authentication flows

Client apps

Control user access to target specific client applications not using modern authentication. Learn more

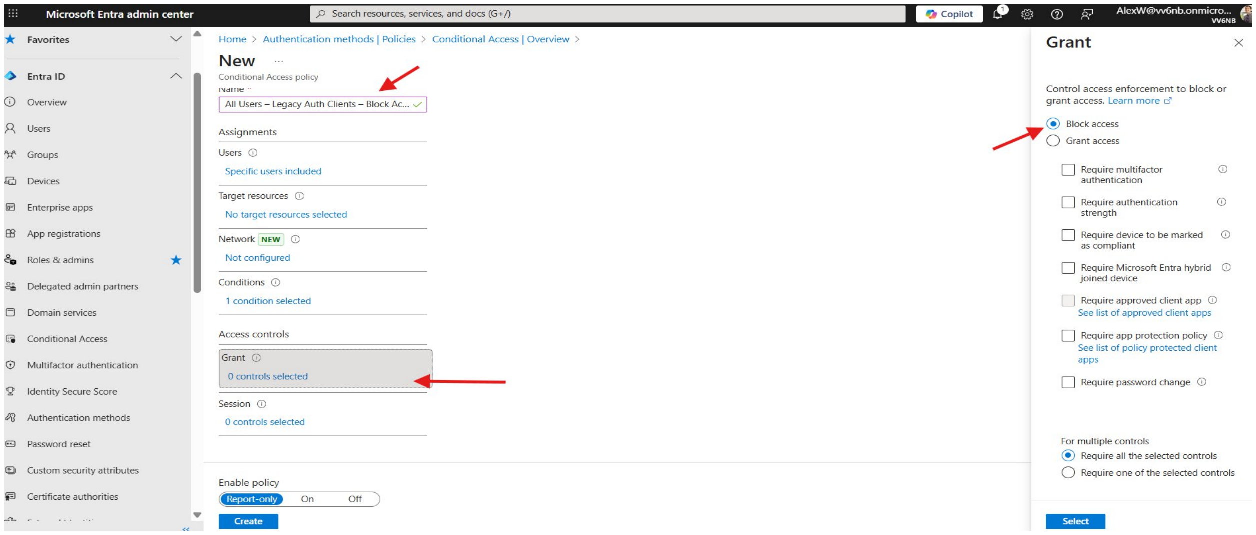
Configure: [✓ Yes] No

Select the client apps this policy will apply to

Modern authentication clients
□ Browser
□ Mobile apps and desktop clients

Legacy authentication clients
☑ Exchange ActiveSync clients
☑ Other clients

- **Grant Control > Block Access > Click Create**



New
Conditional Access policy

Name *
All Users – Legacy Auth Clients – Block Ac... ✓

Assignments

Users
Specific users included

Target resources
No target resources selected

Network NEW
Not configured

Conditions
1 condition selected

Access controls

Grant
0 controls selected

Session
0 controls selected

Enable policy
[✓ Report-only] On Off

Grant

Control access enforcement to block or grant access. Learn more

● Block access
○ Grant access

□ Require multifactor authentication
□ Require authentication strength
□ Require device to be marked as compliant
□ Require Microsoft Entra hybrid joined device
□ Require approved client app
See list of approved client apps
□ Require app protection policy
See list of policy protected client apps
□ Require password change

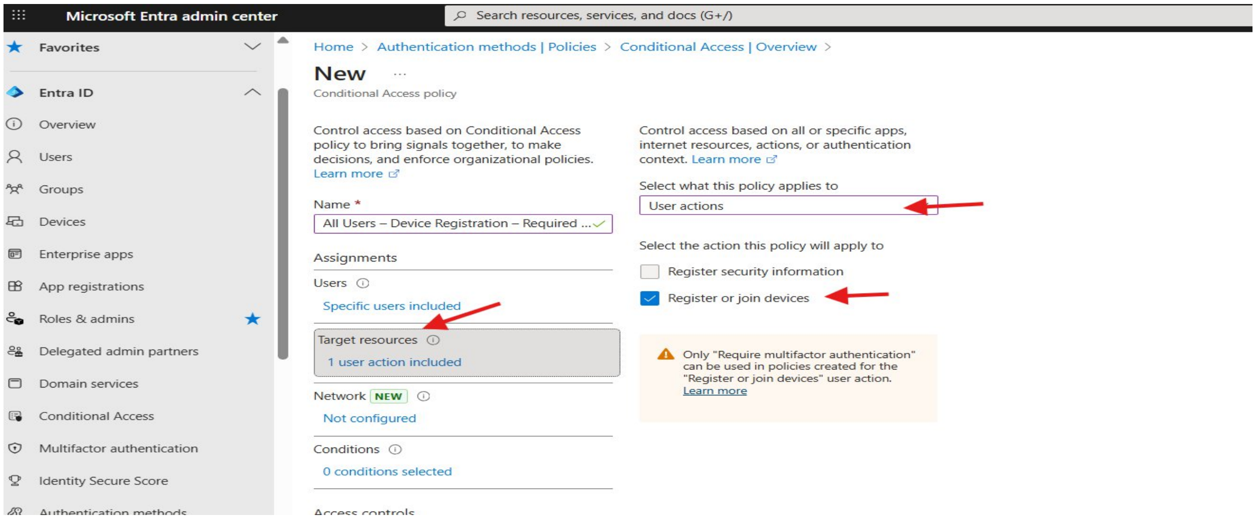
For multiple controls
● Require all the selected controls
○ Require one of the selected controls

Policy 3: Require MFA for Device Registration

Create a policy to **All Users – Device Registration – Required MFA**. The purpose of this policy is to protect the device registration and joining resources in Microsoft 365/Entra, **require an MFA if the device will join**.

- Click in Microsoft 365 Admin Center **> Entra ID > Conditional Access > Create New Policy**

- **Supply the Naming: Users: > Now in Target resources > click User Actions > Register or join devices**



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 *
All Users – Device Registration – Required ... ✓

Assignments

Users
Specific users included

Target resources
1 user action included

Network NEW
Not configured

Conditions
0 conditions selected

Access controls

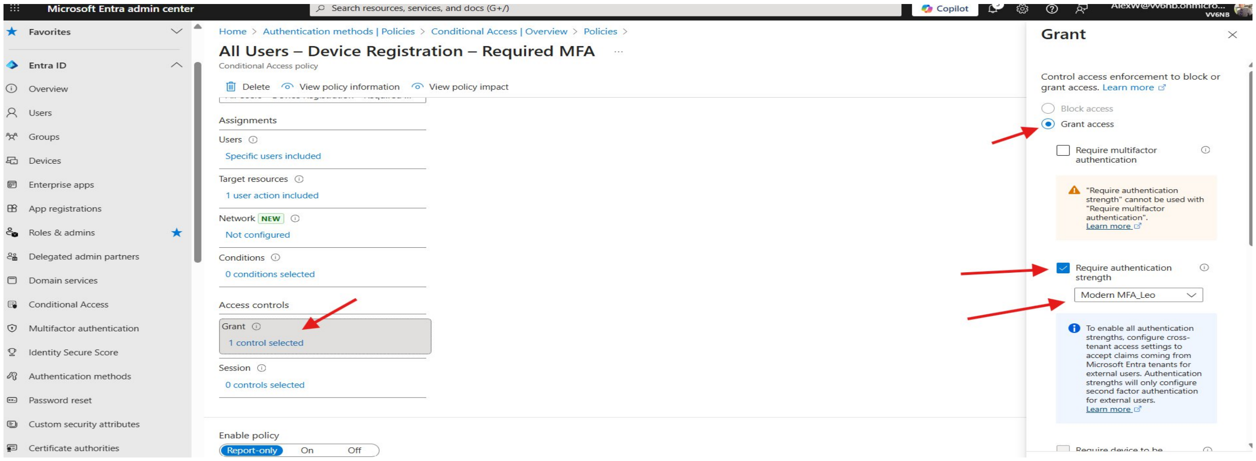
Control access based on all or specific apps, internet resources, actions, or authentication context. Learn more

Select what this policy applies to
User actions

Select the action this policy will apply to
□ Register security information
☑ Register or join devices

Only "Require multifactor authentication" can be used in policies created for the "Register or join devices" user action. Learn more

- **Grant > Grant Access > Required Authentication Strength = Modern MFA_Leo**



Home > Authentication methods | Policies > Conditional Access | Overview > Policies >

All Users – Device Registration – Required MFA

Conditional Access policy

Assignments

Users: Specific users included

Target resources: 1 user action included

Network NEW: Not configured

Conditions: 0 conditions selected

Access controls

Grant: 1 control selected

Session: 0 controls selected

Enable policy: Report-only | On | Off

Grant

Control access enforcement to block or grant access. Learn more

○ Block access

● Grant access

□ Require multifactor authentication

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

☑ Require authentication strength

Modern MFA_Leo

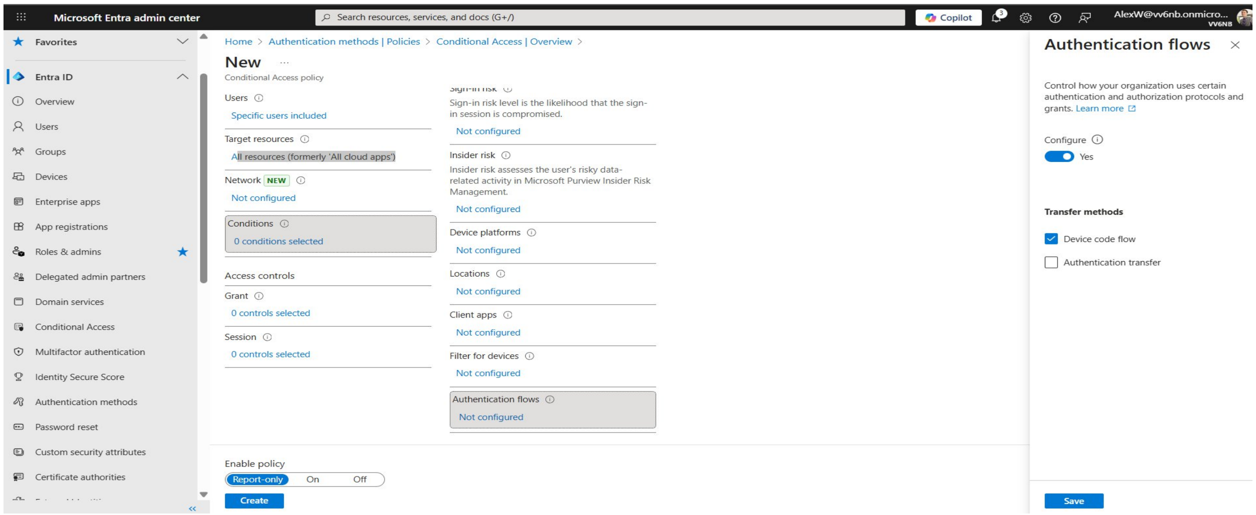
To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users. Learn more

□ Require device to be

Policy 4: Block Device Code Flow Authentication

Create a policy to **All Users – Device Code Flow – Block Access**. The purpose of this policy is to **protect on the device with no proper login page it only says go to website and type in this code, like TV or printer**. The attackers have a threat/attack vector for this.

- Click in Microsoft 365 Admin Center **> Entra ID > Conditional Access > Create New Policy**
- **Supply the Naming: Users: > Now in Target resources > click All resources (formerly 'All cloud apps')**
- **Now, in Conditions > Click Authentication Flow below > Configure = YES > Device code flow > Save**



Home > Authentication methods | Policies > Conditional Access | Overview >

New

Conditional Access policy

Users: Specific users included

Target resources: All resources (formerly 'All cloud apps')

Network NEW: Not configured

Conditions: 0 conditions selected

Access controls

Grant: 0 controls selected

Session: 0 controls selected

Sign-in risk: Sign-in risk level is the likelihood that the sign-in session is compromised. Not configured

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: Not configured

Client apps: Not configured

Filter for devices: Not configured

Authentication flows: Not configured

Enable policy: Report-only | On | Off

Create

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

Save

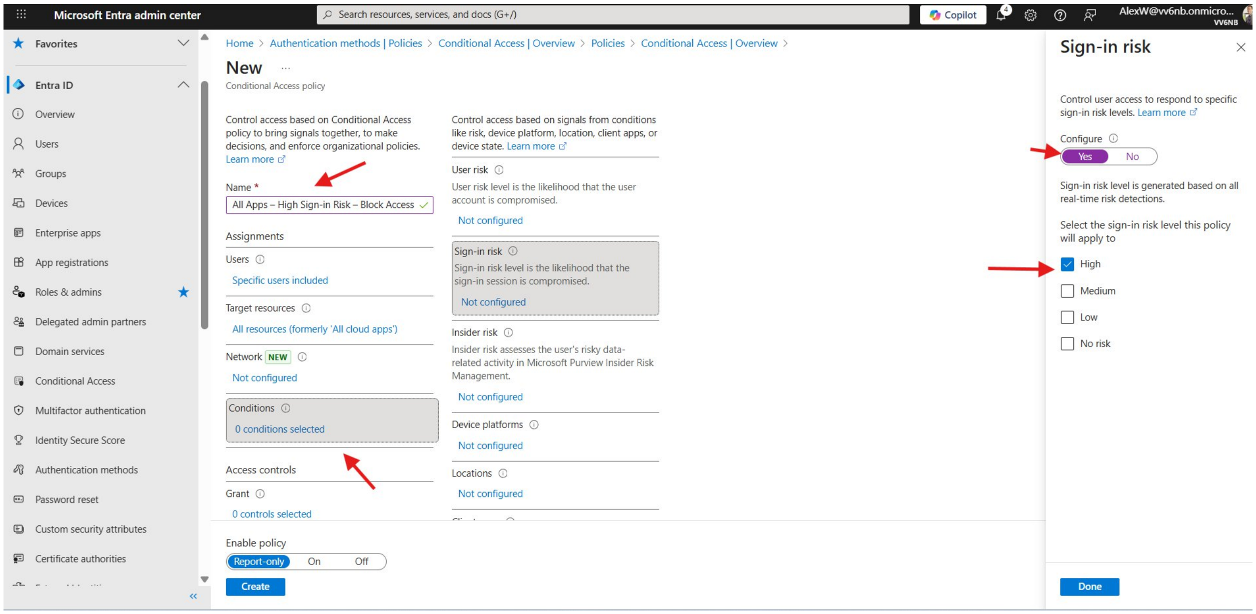
- **Grant Control > Block Access > Click Create**

Policy 5: Block Access for High Sign-in Risk

Create a policy to **All Apps – High Sign-in Risk – Block Access**. The purpose of this policy is to **check every log in real time and score it for a risk or the password is going to breach**

- Click in Microsoft 365 Admin Center **> Entra ID > Conditional Access > Create New Policy**

- **Supply the Naming: Users: > Conditions > Sign-in Risk > Yes > High**



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 *: All Apps – High Sign-in Risk – Block Access ✓

Assignments

Users: Specific users included

Target resources: All resources (formerly 'All cloud apps')

Network NEW: Not configured

Conditions: 0 conditions selected

Access controls

Grant: 0 controls selected

Enable policy: [✓ Report-only] On Off

Create

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. Not configured

Sign-in risk: Sign-in risk level is the likelihood that the sign-in session is compromised. Not configured

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: Not configured

Sign-in risk

Control user access to respond to specific sign-in risk levels. Learn more

Configure: [✓ Yes] No

Sign-in risk level is generated based on all real-time risk detections.

Select the sign-in risk level this policy will apply to

☑ High

☐ Medium

☐ Low

☐ No risk

Done

- **Grant Control > Block Access > Click Create**

Sources:

1. **Advanced Conditional Access for IT Pros | Complete Guide**
https://www.youtube.com/watch?v=5oMaZink7kc

2. **How to Set Up Conditional Access in Microsoft 365 (Step-by-Step) By Jonathan Edwards**
https://www.youtube.com/watch?v=DkCq8wWN9Sc

” When you train Smarter, you defend Stronger”
Leonard Estos