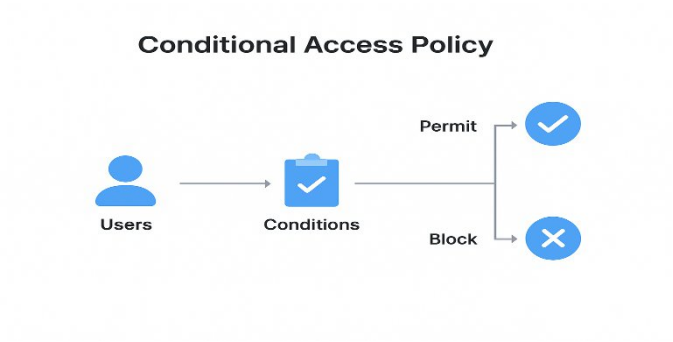
Leonard M. Estos
Cybersecurity Researcher & Technical Author
Edmonton, Alberta, Canada

Conditional Access Policy (Microsoft)

What is Conditional Access Policy: Conditional Access Policy is one of **the most powerful tools i 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

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

What is **Persona baseline**? In Conditional Access policies are a framework that defines minimum access controls for different **user groups, or personas, like internal staff, external vendors, or developers**.

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

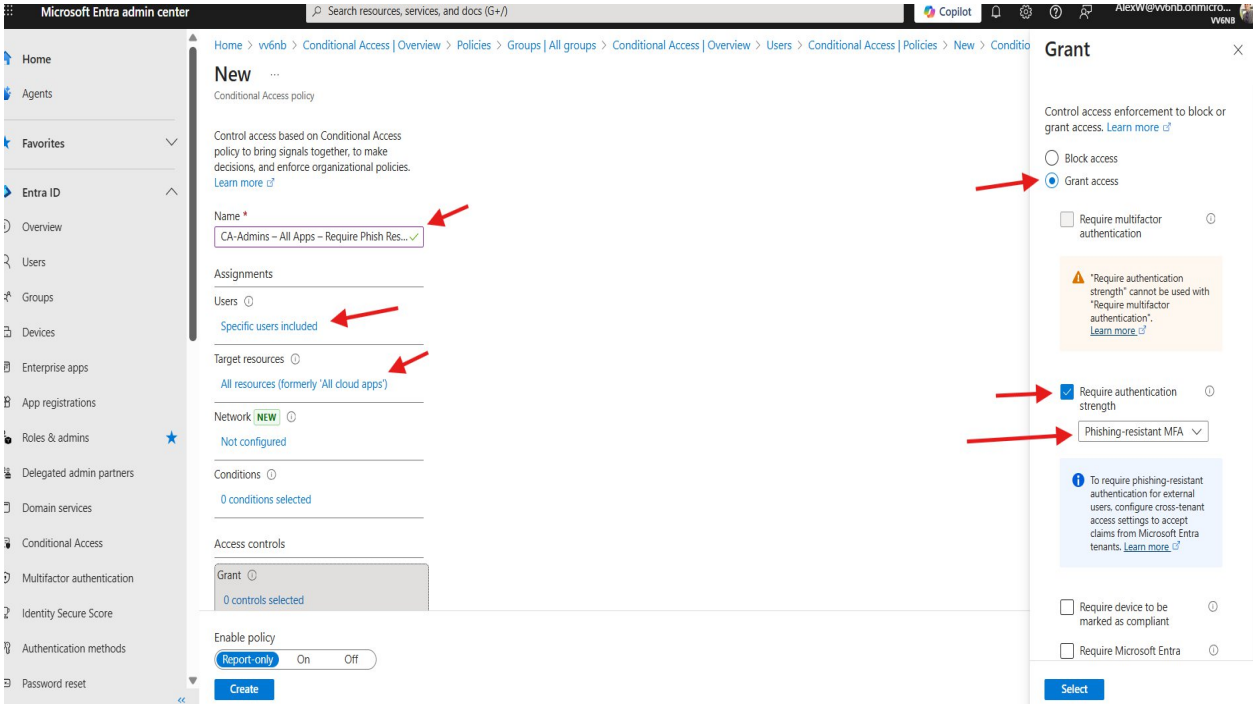
Example naming structure:
• Who: Target users or groups
• What: Condition or app
• Action: Required control
Example: Admins - All Apps - Require MFA

Application/Technical Configuration:

Policy 1: CA-Admins – All Apps – Require Phish Resistant MFA

Create a policy to **CA-Admins – All Apps – Require Phish Resistant MFA**. Click in Microsoft 365 Admin Center > **Conditional Access > Policies > New Policy**

- Select User > Select Users and Group > Select the Group of Users which is CA - Admins Group.
- Target Resources > All resources (Formerly “All cloud apps)
- Grant > Grant Access > Require Authentication Strength > Phishing-resistant MFA > Click Create



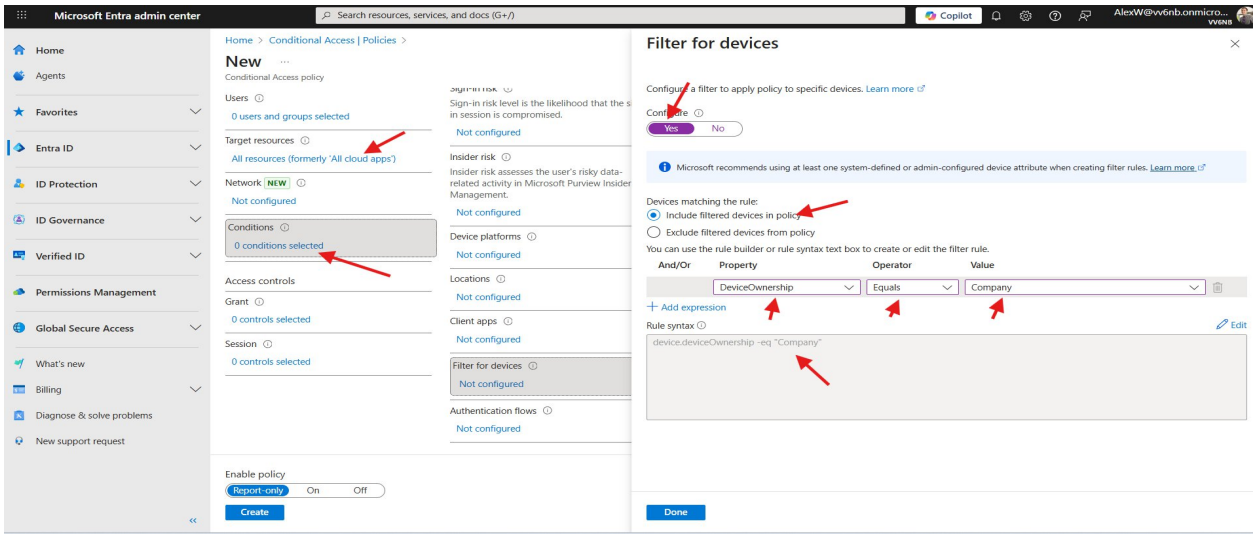
- The purpose of this policy is specifically for the **admins**, while regular staff can use the **Required strong MFA**.

Policy 2: CA-Admins – All Apps – Require Company/Compliant Device

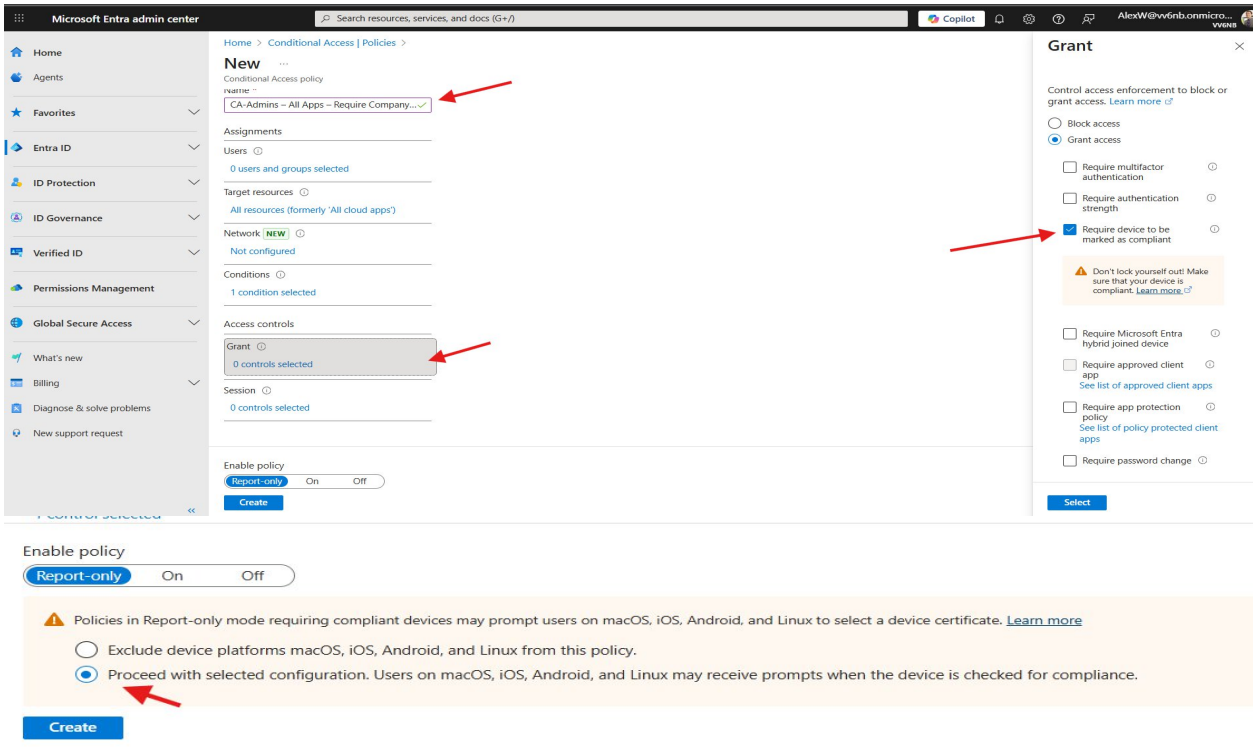
Create a policy to **CA-Admins – All Apps – Require Phish Resistant MFA**. Click in Microsoft 365 Admin Center > **Conditional Access > Policies > New Policy**

- Select User > Select Users and Group > Select the Group of Users which is CA - Admins Group.
- Target Resources > All resources (Formerly “All cloud apps)
- Conditions > Filter for Devices > Configure = Yes > Devices matching the rule = Include filtered devices in policy

- Property = DeviceOwnership, Operator = Equal, Value = Company > Click Done



- Grant Control > Grant Access > Require device to be marked as compliant > click Select > click

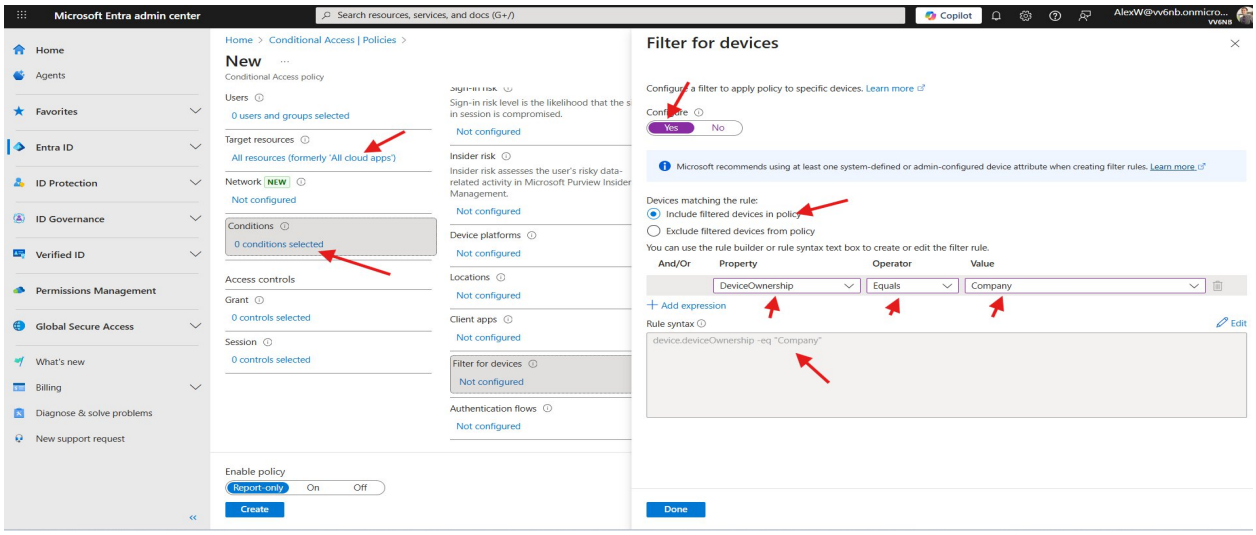


click Create

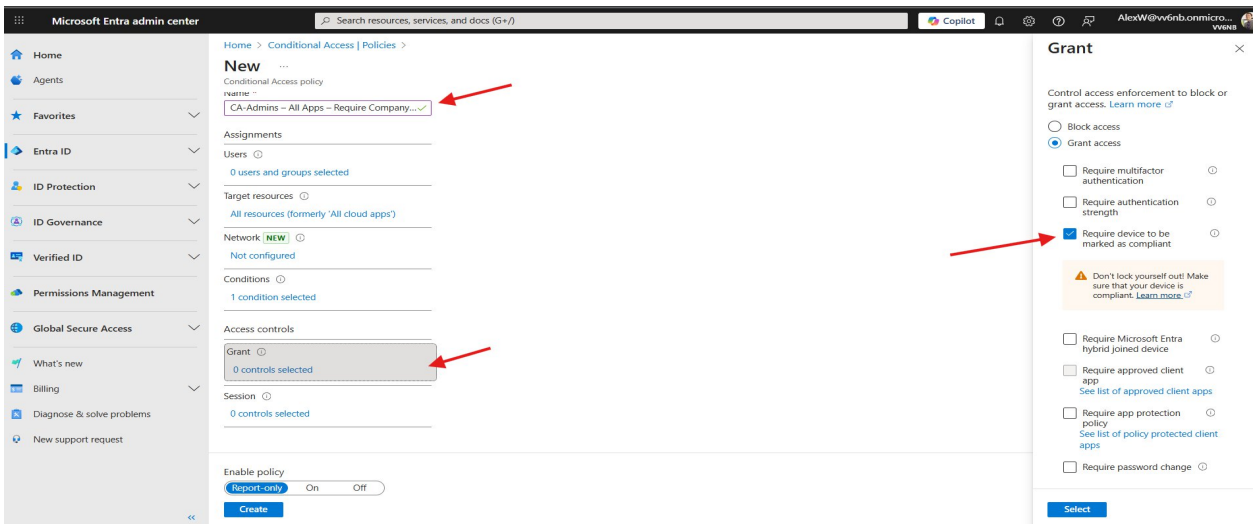
Policy 3: CA-Staff – All Apps – Require Company/Compliant Device

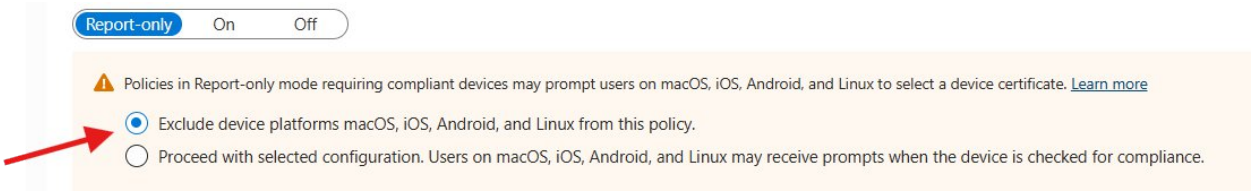
Create a policy to **CA-Admins – All Apps – Require Phish Resistant MFA**. Click in Microsoft 365 Admin Center > **Conditional Access > Policies > New Policy**

- Select User > Select Users and Group > Select the Group of Users which is CA - Staff Group.
- Target Resources > All resources (Formerly “All cloud apps)
- Conditions > Filter for Devices > Configure = Yes > Devices matching the rule = Include filtered devices in policy
- Property = DeviceOwnership, Operator = Equal, Value = Company > Click Done



- Grant Control > Grant Access > Require device to be marked as compliant > click Select > click



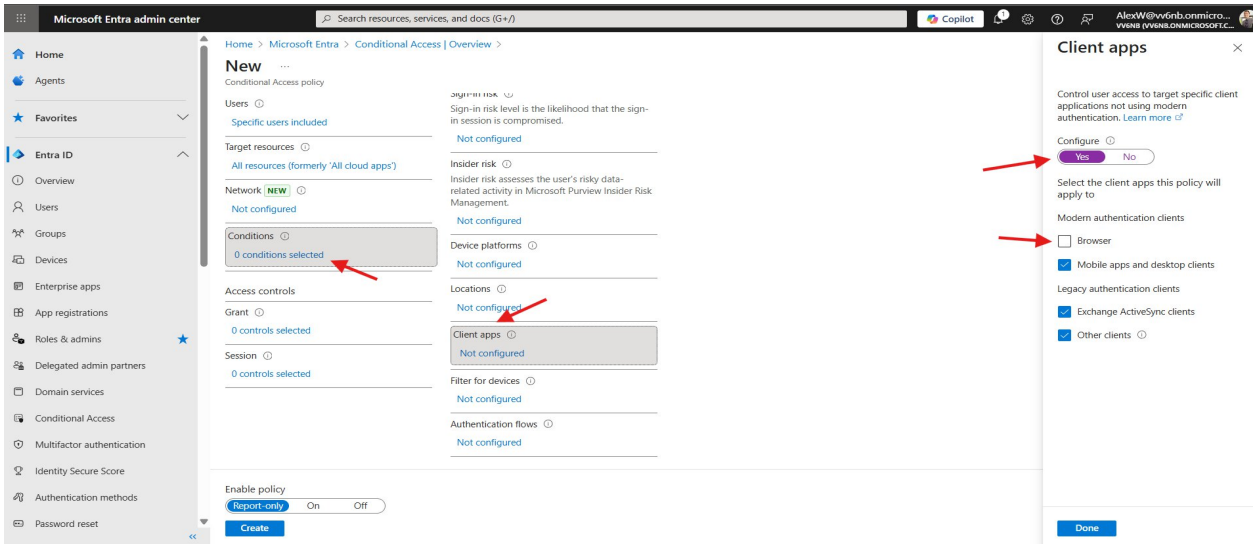


click Create

Policy 3: CA-Guest – All Apps – Block Mobile and Desktop Apps

Create a policy to **CA-Guest – All Apps – Block Mobile and Desktop Apps**. Click in Microsoft 365 Admin Center > **Conditional Access > Policies > New Policy**

- Select User > Select Users and Group > Select the Group of Users which is CA - Guest Group.
- Target Resources > All resources (Formerly “All cloud apps)
- Conditions > Client apps > Configure Yes > Uncheck the browser > Click Done

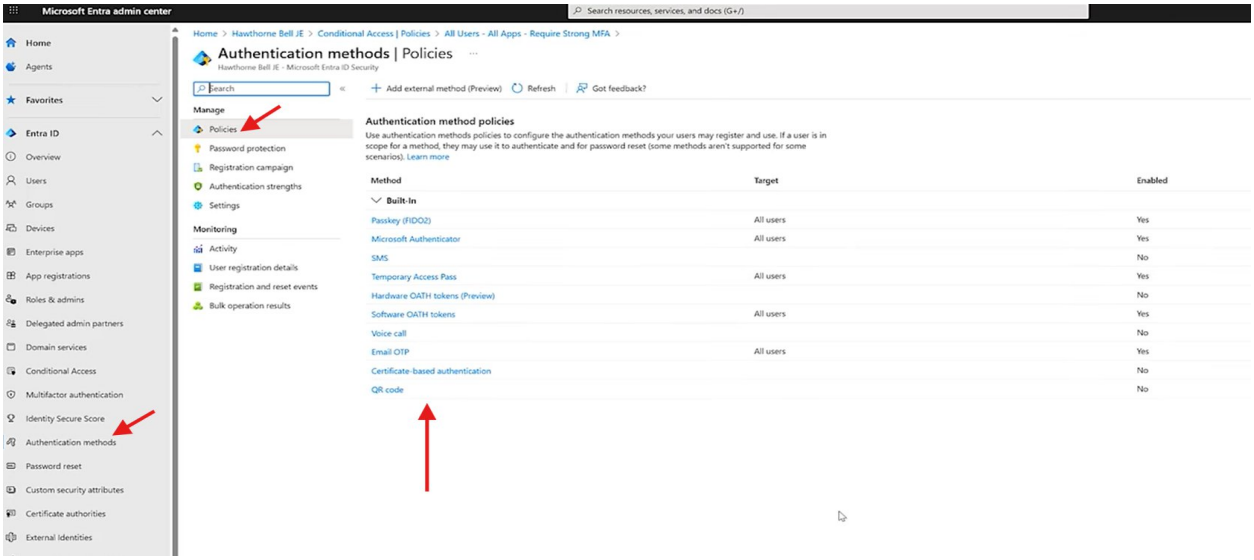


- Click Grant > Click Block > Create

Scenario:

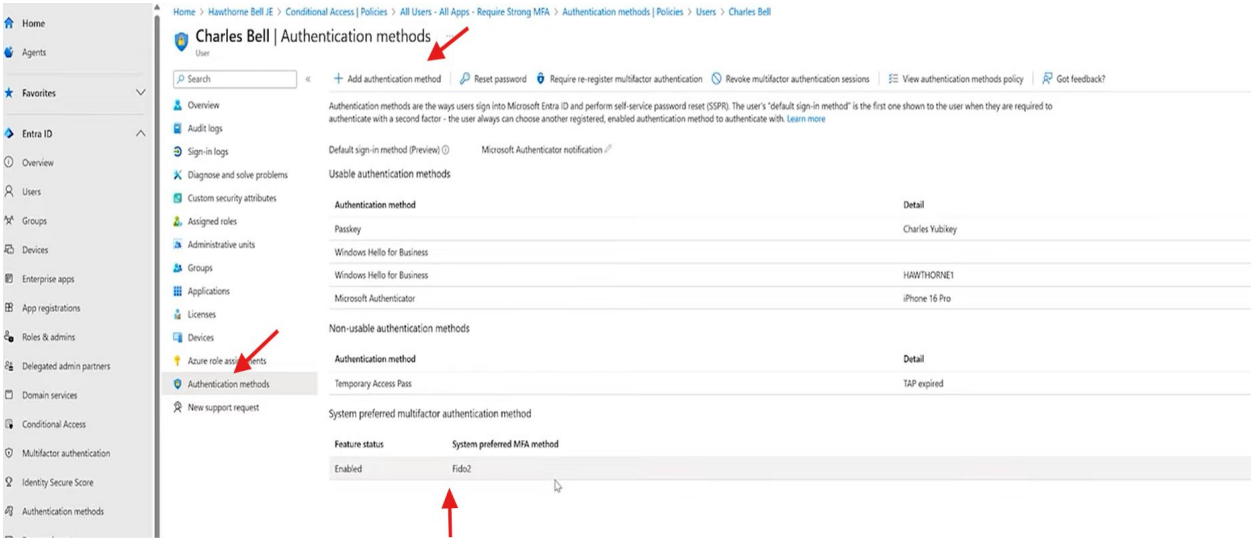
In real life, situations may arise such as someone losing their phone, experiencing laptop failure or corruption, or requesting temporary access from a different device. In these cases, we will implement the exclusion command to allow secure, time-bound access while maintaining policy integrity. Also, we will implement the **TAP (Temporary Access Password).**

To check your Microsoft Entra Admin Authentication Method, this is where we implement the **MFA something you have, something you know and something you are.**
Click > Authentication Methods > Policies



Policy 4: Provide TAP (Temporary Access Password) To the Executive or Administrative Users

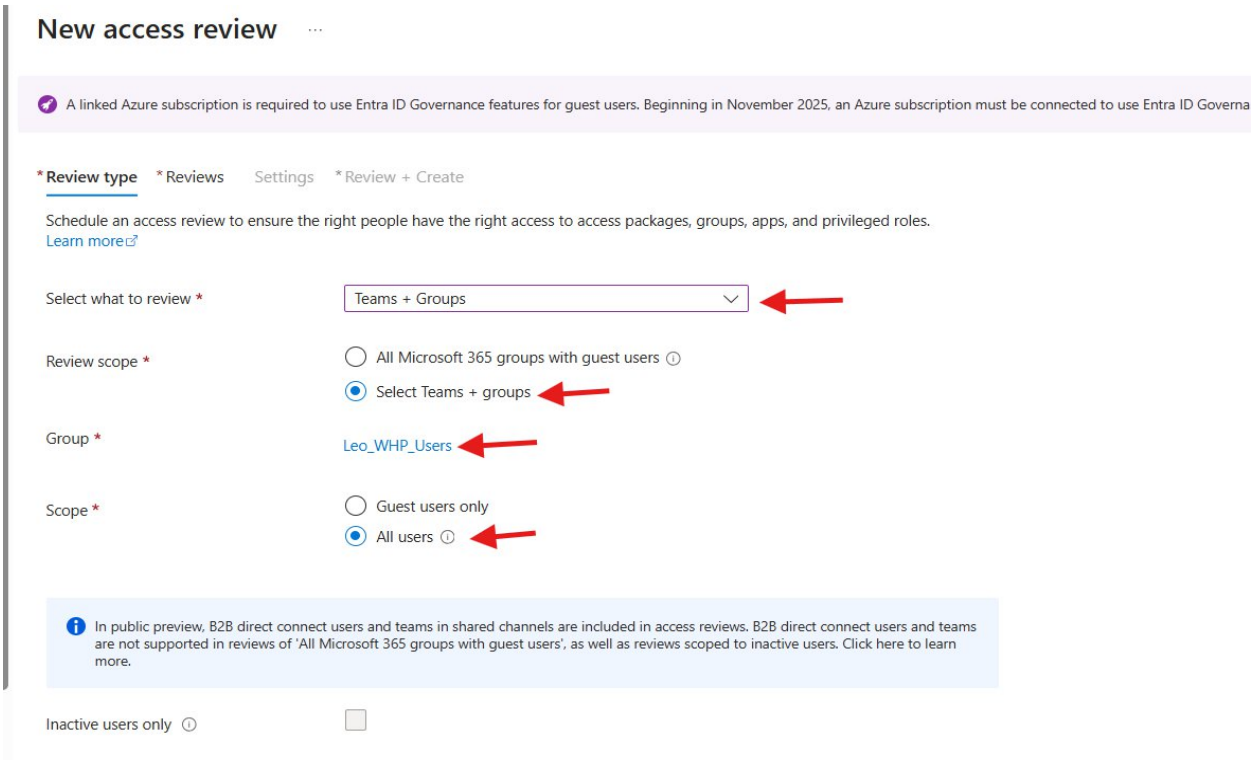
- Click Users > All Users > Click the Username > **Click Authentication Method > Add Authentication Method > Choose Method and Choose Temporary Access Pass > Click One-Time use > Click Yes > Click Add**



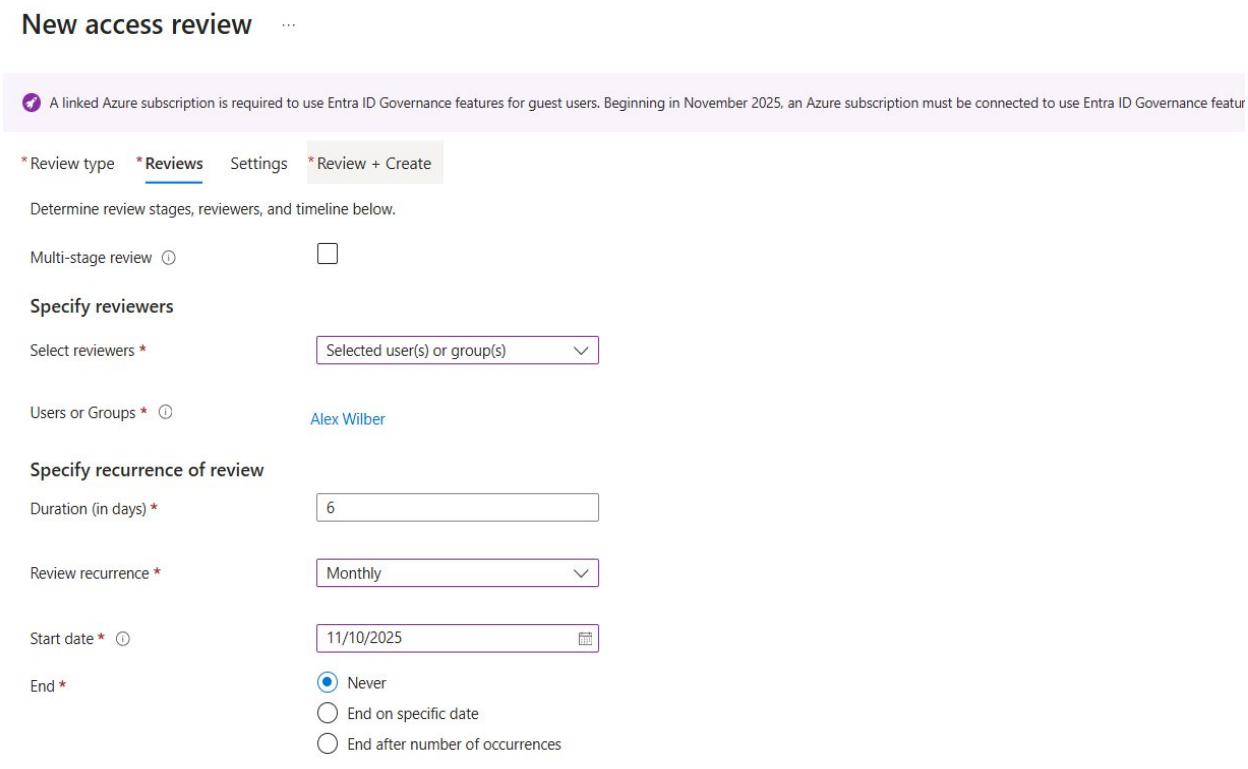
Policy 5: Another way is the **ID Governance**, **Access Reviews.**

- Click **ID Governance > Click Access Review > Click New Access Review**

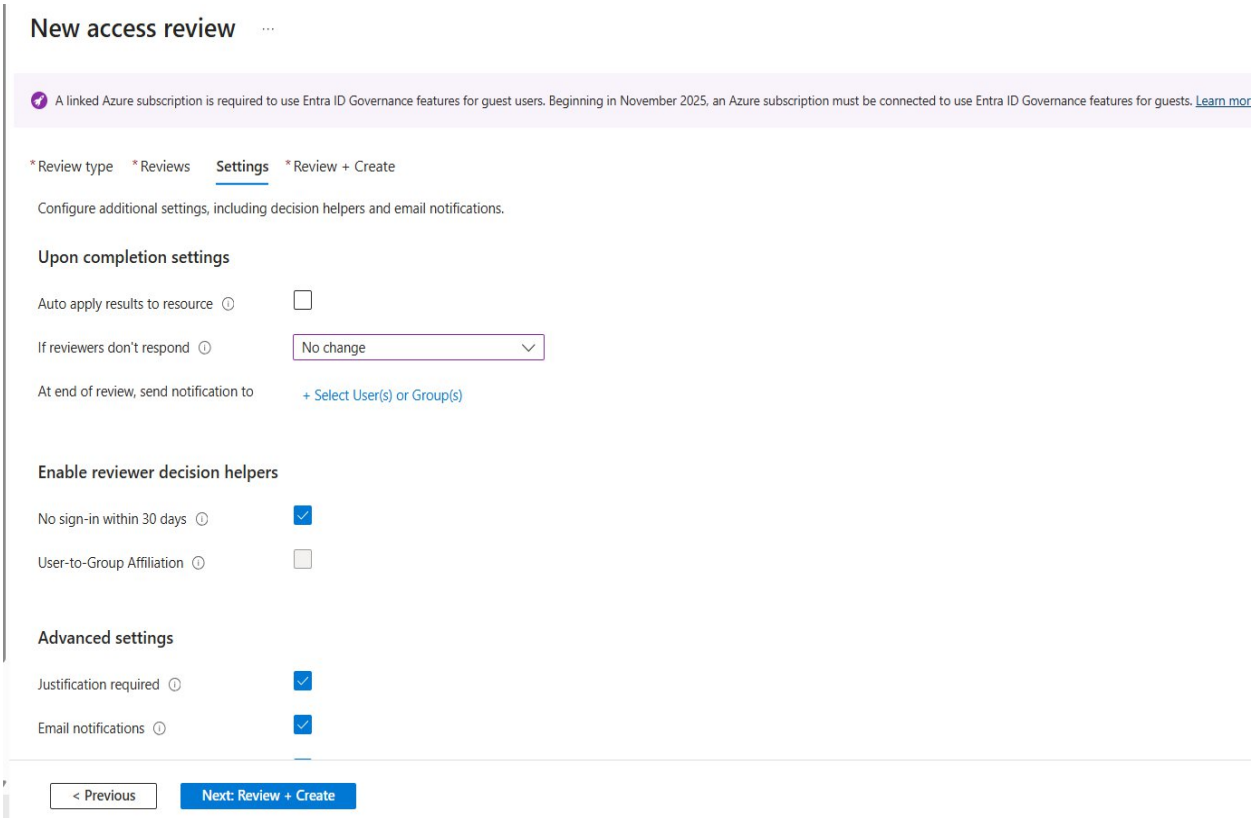
- See below information to review

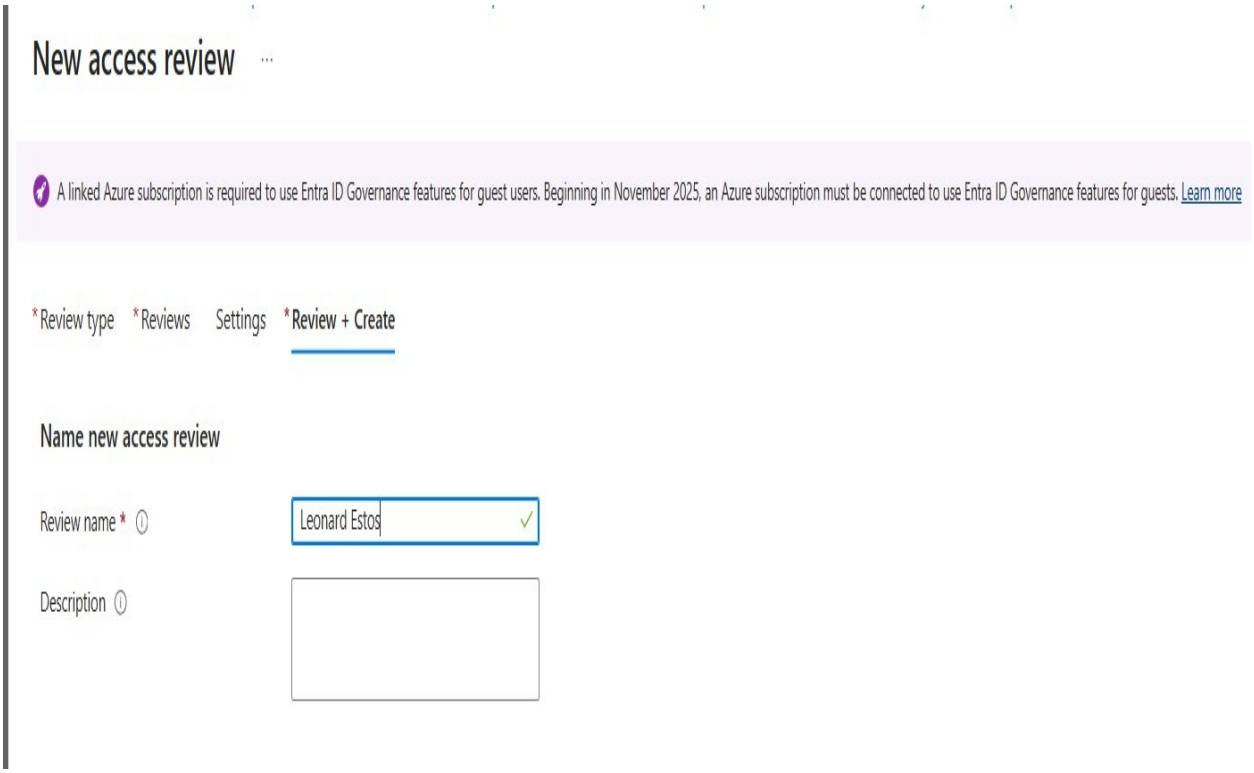


- Click > Next >

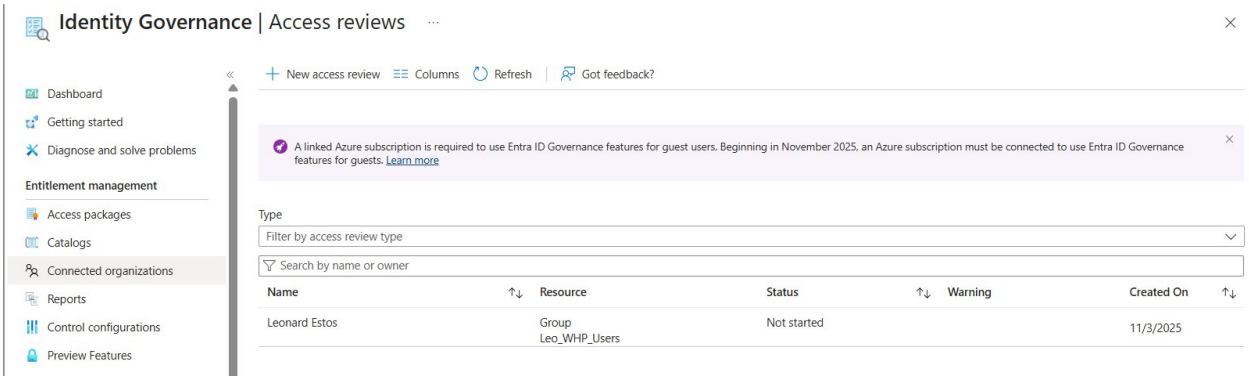


- Click > Settings >





- **Click > Create**
- Now, verify your creation.



Sources:

1. **Advanced Conditional Access for IT Pros | Complete Guide**
https://www.youtube.com/watch?v=DkCq8wWN9Sc

2. **How to Set Up Conditional Access in Microsoft 365 (Step-by-Step) By Jonathan Edwards**
https://www.youtube.com/watch?v=5oMaZink7kc

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