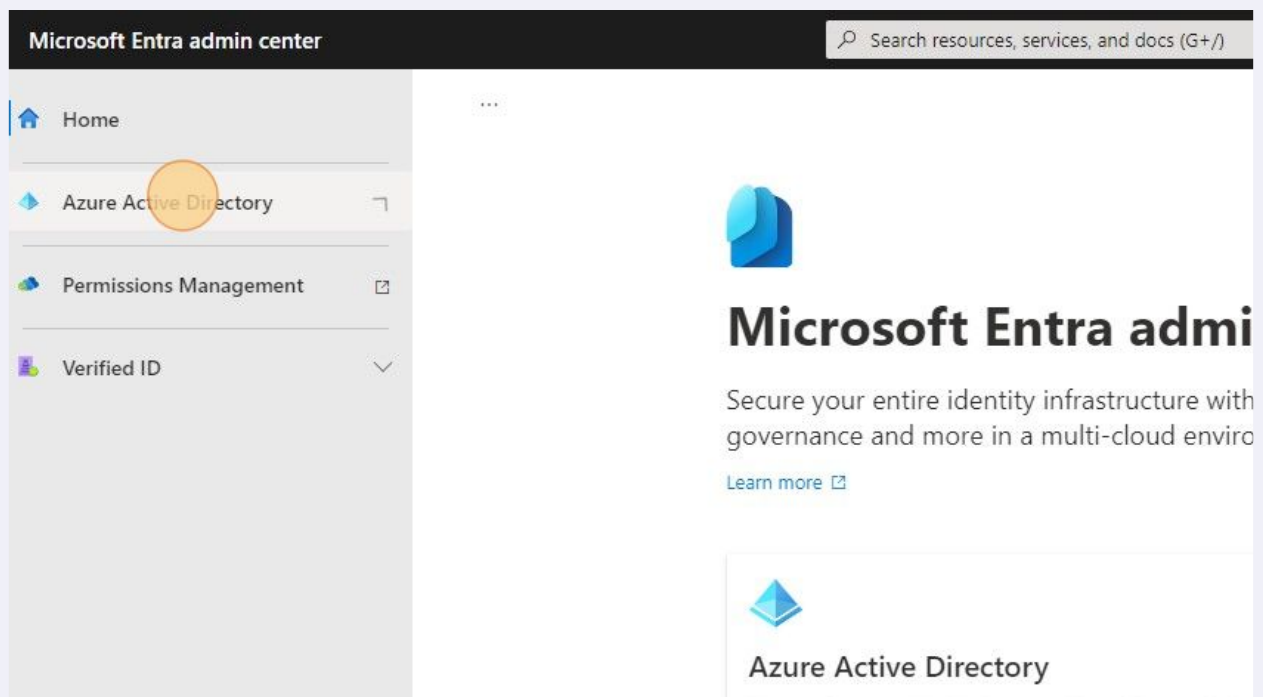


# How to Create a Conditional Access Policy to Block Legacy Authentication

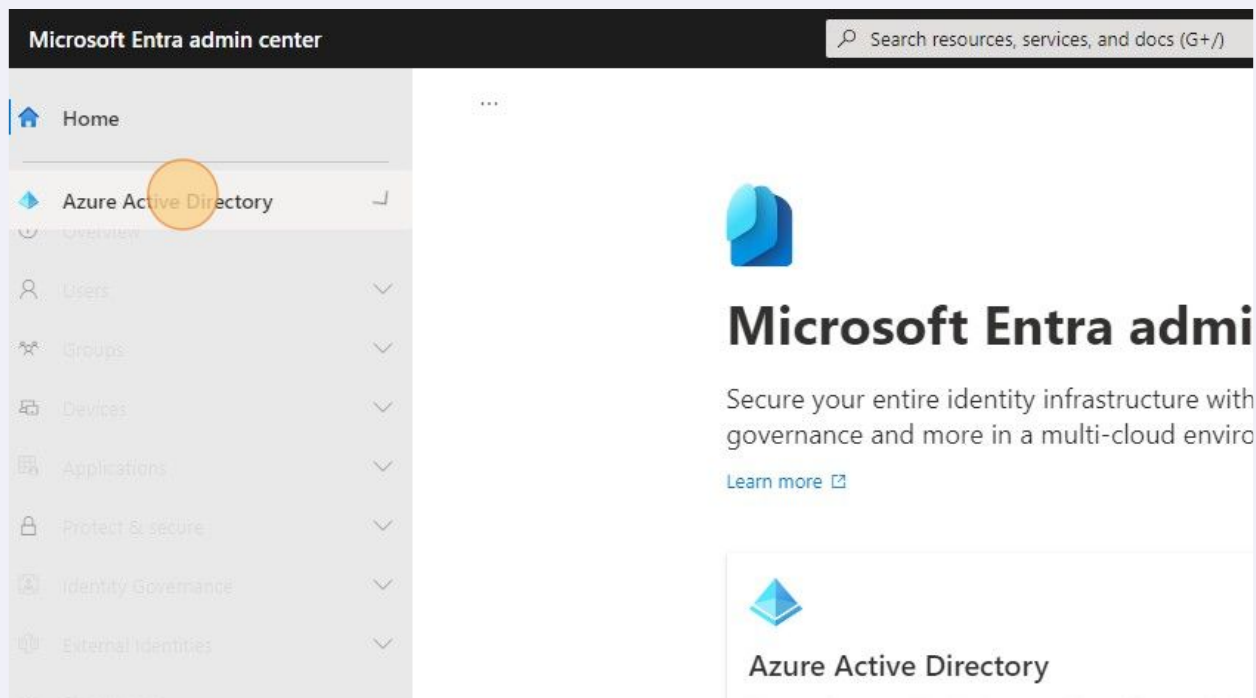
In this guide, we review the template method of deploying a conditional access policy to block legacy authentication.

1 Navigate to [entra.microsoft.com](https://entra.microsoft.com)

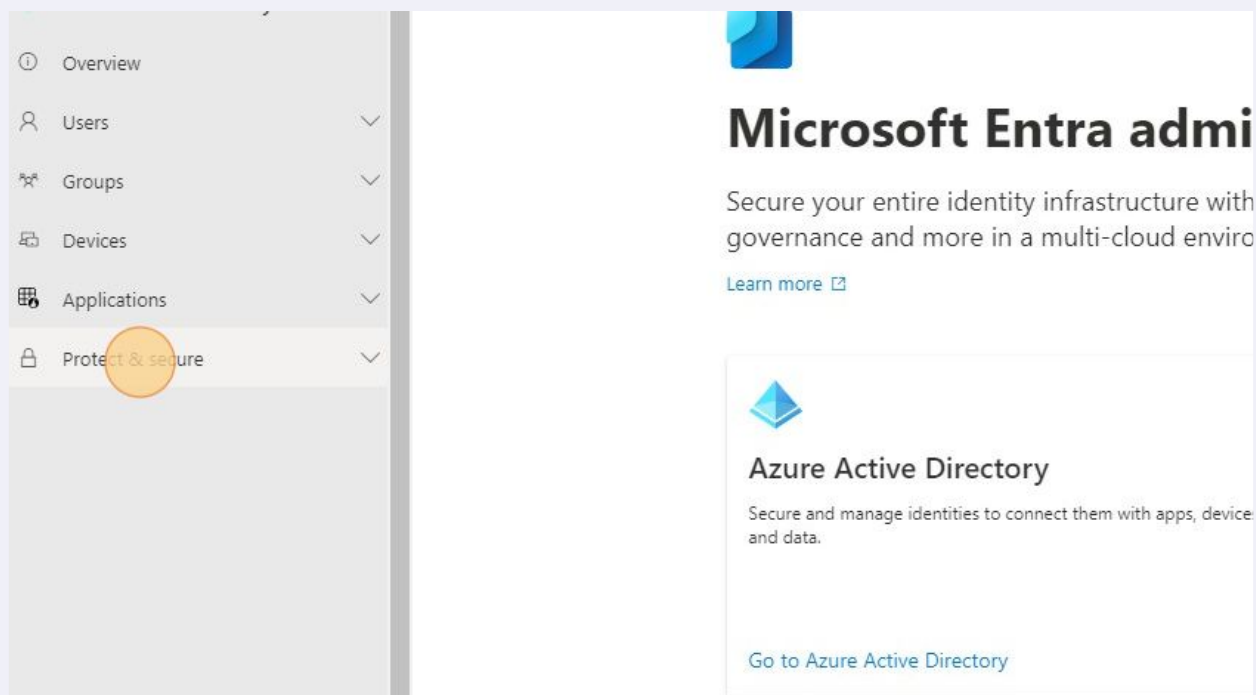
2 Click "Azure Active Directory"



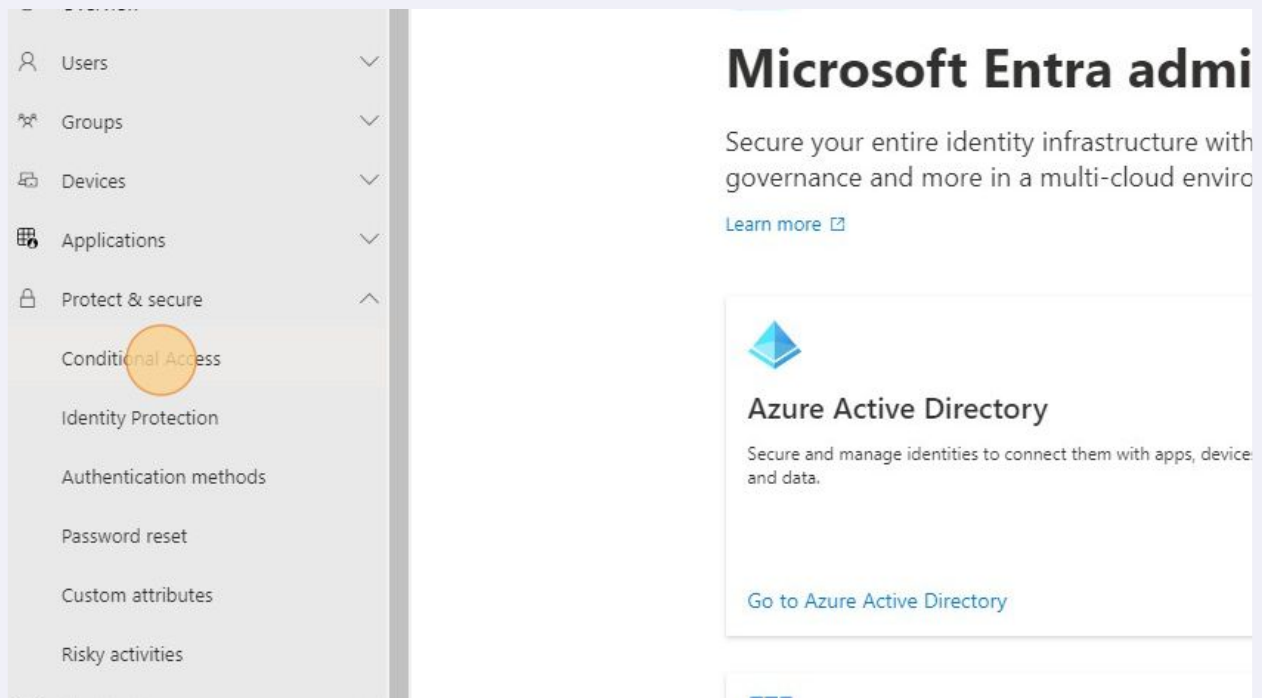
### 3 Click "Azure Active Directory"



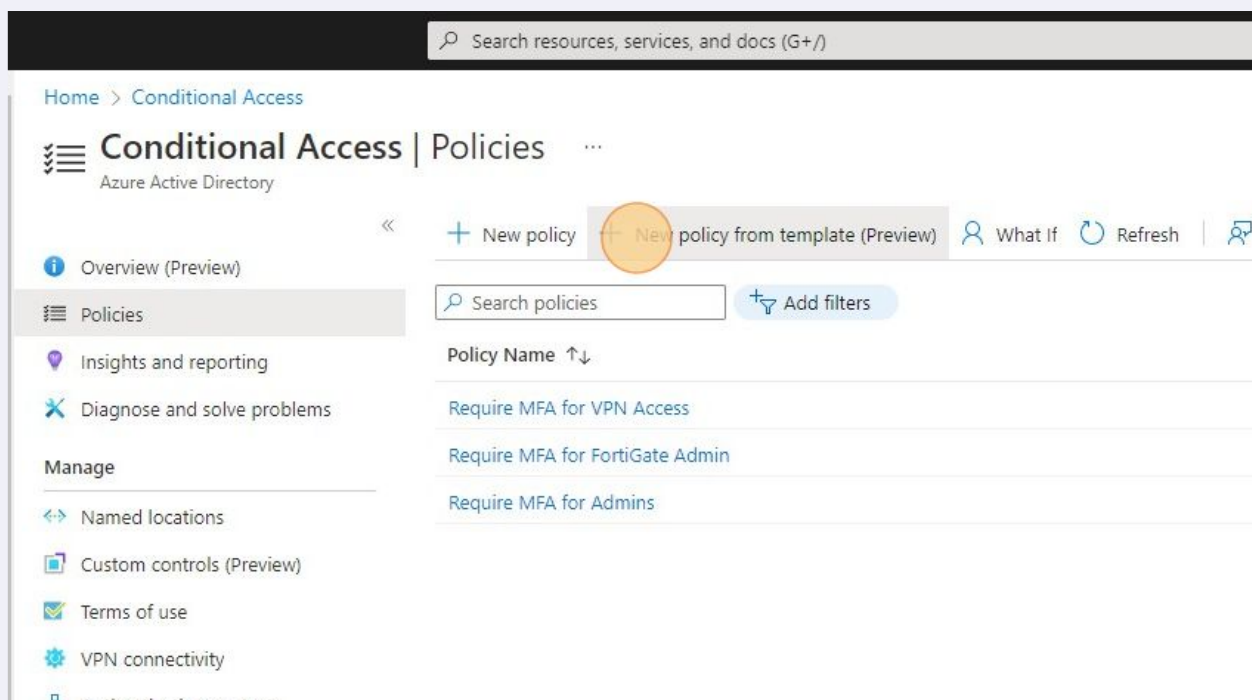
### 4 Click "Protect & secure"



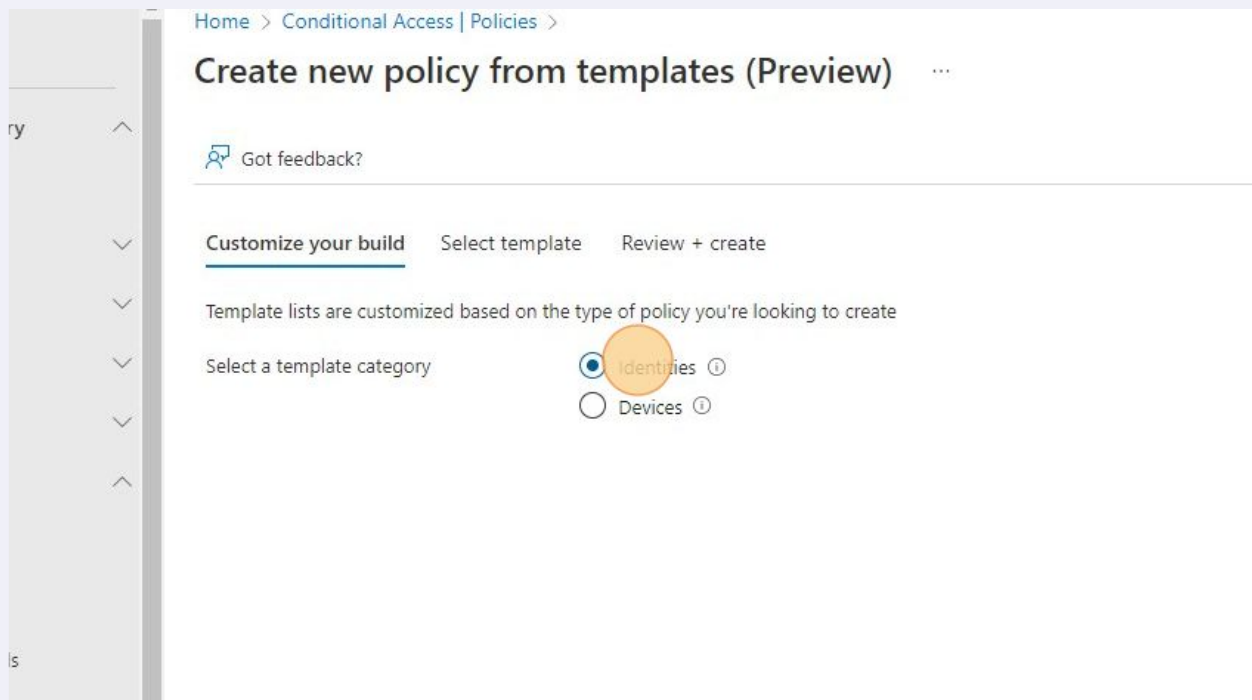
## 5 Click "Conditional Access"



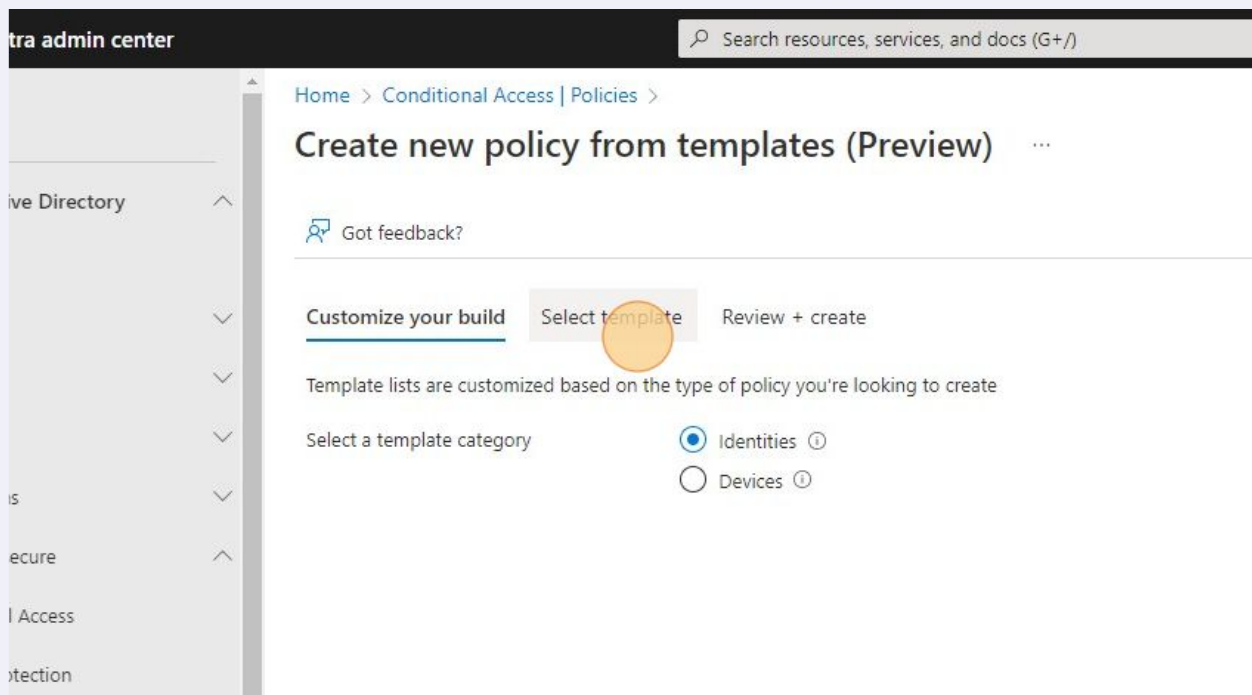
## 6 Click "New policy from template"



## 7 Click "Identities"



## 8 Click "Select template"



## 9 Select "Block legacy authentication"

Conditional Access | Policies >

### Choose a policy from templates (Preview) ...

<?

build Select template Review + create

Choose the following templates based on your response

|   |  |  |  |
|---|--|--|--|
| <input type="radio"/> Multifactor authentication for administrative accounts to reduce the risk of compromise. This policy has the same roles as Security Defaults. | <input type="radio"/> Securing security info registration<br>Secure when and how users register for Azure AD multifactor authentication and self-service password. | <input checked="" type="radio"/> Block legacy authentication<br>Block legacy authentication endpoints that can be used to bypass multifactor authentication. | <input type="radio"/> Require multifactor authentication for all users<br>Require multifactor authentication for all user accounts to reduce the risk of compromise. |
| <a href="#">View policy summary</a>   | <a href="#">View policy summary</a>  | <a href="#">View policy summary</a>  | <a href="#">View policy summary</a>  |
| <input type="radio"/> Multifactor authentication for high-risk users  | <input type="radio"/> Require password change for high-risk users  |  |  |
| <input type="radio"/> Multifactor authentication if the sign-in risk is detected to be medium or high. (Requires an Azure AD Premium 2 License)                     | <input type="radio"/> Require the user to change their password if the user risk is detected to be high. (Requires an Azure AD Premium 2 License)                  |  |  |

## 10 Remove the template string at the beginning of the name.

Authentication methods

Password reset

Custom attributes

Risky activities

Identity Governance

External Identities

Show more

Permissions Management

Verified ID

Support

☐ Require multifactor authentication for risky sign-ins

☐ Require password change for high-risk users

Require multifactor authentication if the sign-in risk is detected to be medium or high. (Requires an Azure AD Premium 2 License)

Require the user to change their password if the user risk is detected to be high. (Requires an Azure AD Premium 2 License)

[View policy summary](#)

[View policy summary](#)

Name your policy

CA003: Block legacy authentication

Policy state

☐ Off ☐ On ☒ Report-only

## 11 Change "Policy state" to "On"

Authentication methods

Password reset

Custom attributes

Risky activities

Identity Governance

External Identities

Show more

Permissions Management

Verified ID

Block support

Require multifactor authentication if the sign-in risk is detected to be medium or high. (Requires an Azure AD Premium 2 License)

View policy summary

Require the user to change their password if the user risk is detected to be high. (Requires an Azure AD Premium 2 License)

View policy summary

Name your policy

Block legacy authentication

Policy state

☐ Off ☒ On ☐ Report-only

Create Policy Previous Next

## 12 Click "Create Policy"

Authentication methods

Password reset

Custom attributes

Risky activities

Identity Governance

External Identities

Show more

Permissions Management

Verified ID

Block support

Excluded users

Cloud apps or actions

Cloud apps

Conditions

Client apps

Legacy authentication clients

Access controls

Block access

Current user

All apps

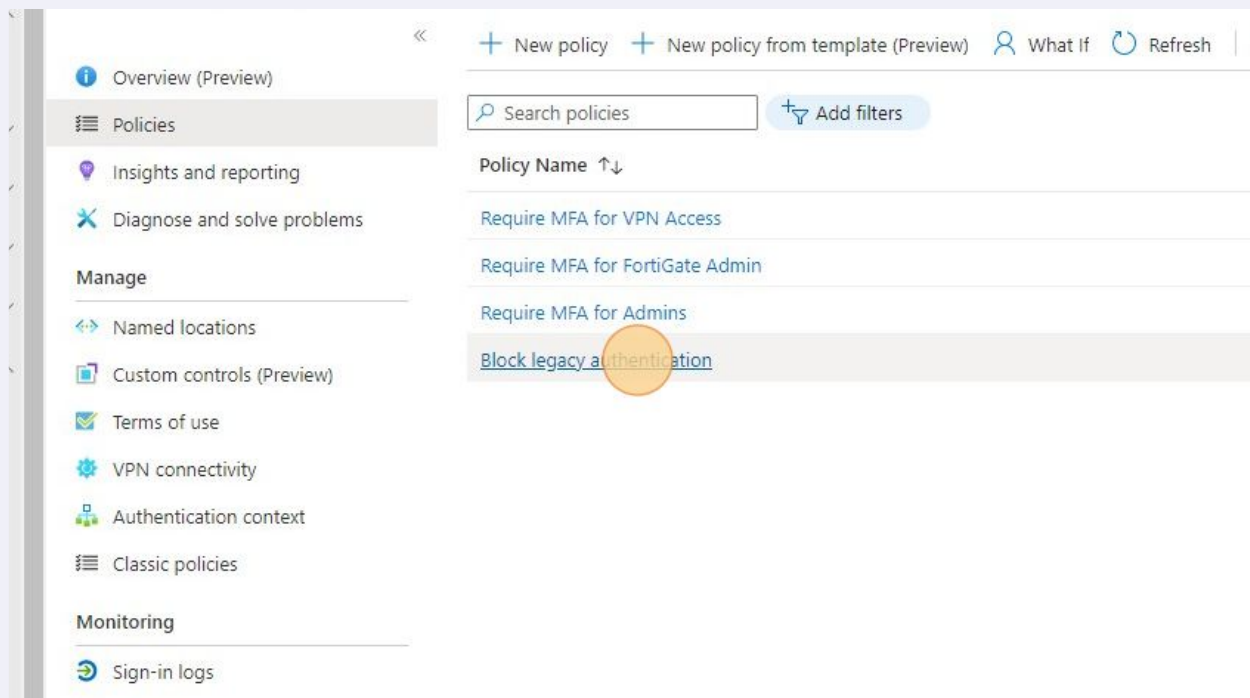
Exchange ActiveSync clients

Other clients

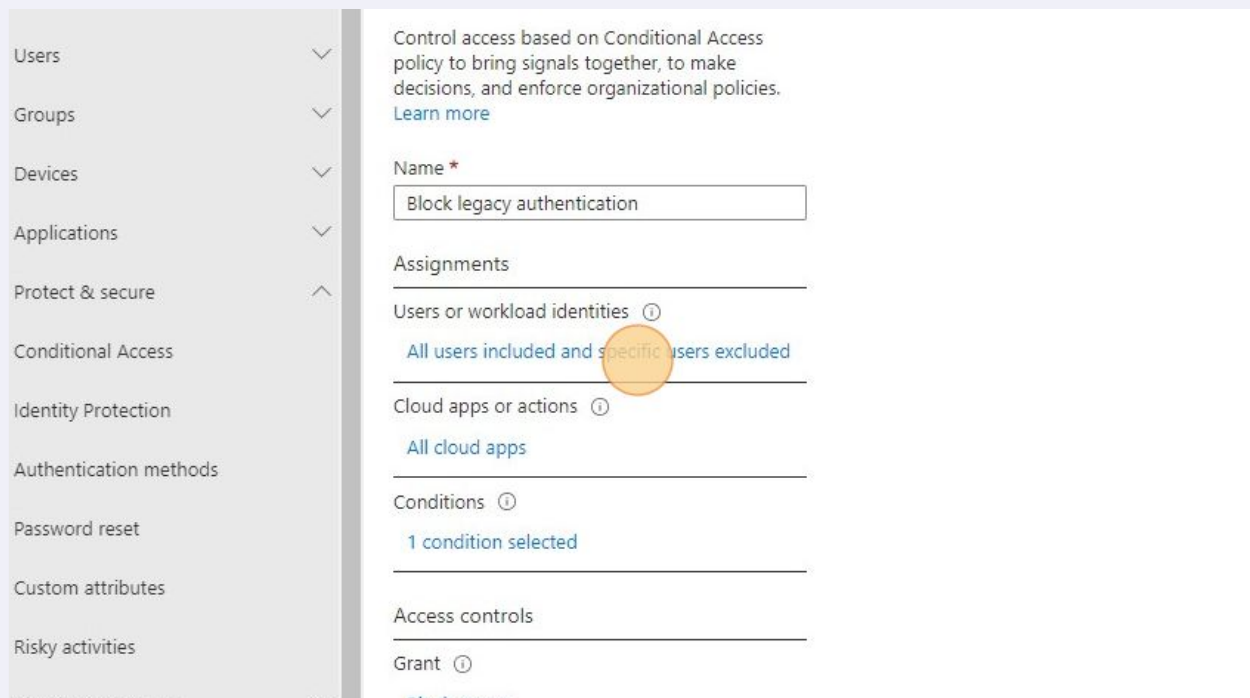
Selected

Create Policy Previous Next

13 Go back into the "Block legacy authentication" policy.




14 Click "All users included and specific users excluded"





## 15 Click "Exclude"

Conditional Access policy

 Delete

---

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

Name \*

Block legacy authentication

Assignments

Users or workload identities ⓘ

All users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

1 condition selected

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

What does this policy apply to?


Users and groups

Include **Exclude**

☐ None

☒ All users

☐ Select users and groups

 Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

## 16 Click "Users and groups"

specific users excluded

the policy



☐ Guest or external users ⓘ

☐ Directory roles ⓘ

☒ Users and groups

Select excluded users and groups

1 user

 Mark Connelly  
Mark@connelly.ventures 



17 Select your break glass admin account to include in the exceptions.

BI

**Selected items**

- AZ Azure.BreakGlass.Admin
- Azure.BreakGlass.Admin@connelly.ventures

We also recommend excluding at least one administrator from this policy.

Select

18 Click "On" to enable the policy.

Authentication methods

- Password reset
- Custom attributes
- Risky activities
- Identity Governance
- External Identities
- Show more

Permissions Management

Verified ID

Support

Access controls

Grant

Block access

Session

0 controls selected

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 to the affected users and apps.

- Exclude current user, Mark@connelly.ventures, from this policy.
- I understand that my account will be impacted by this policy. Proceed anyway.

Save

## 19 Click "Save"

Access controls

Grant ⓘ

Block access

Session ⓘ

0 controls selected

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 impacts the affected users and apps.

☐ Exclude current user, Mark@connelly.ventures, from this policy.

☒ I understand that my account will be impacted by this policy. Proceed anyway.

Save

## 20 You should receive a notification that the policy was successfully updated.

Mark@connelly.ventures  
CONNELLY VENTURES (CONNELLY...)

Got feedback?

Successfully updated Block legacy authentication

Successfully updated Block legacy authentication. Policy will be enabled in a few minutes if you have "Enable policy" set to "On".

4 out of 4 policies found

| State ↑↓ | Creation Date ↑↓       | Modified Date ↑↓          |
|----------|------------------------|---------------------------|
| On       | 2/6/2022, 11:39:39 AM  | 2/6/2022, 11:39:59 AM ... |
| On       | 2/6/2022, 11:51:57 AM  | ...                       |
| On       | 12/18/2022, 8:12:24 PM | ...                       |
| On       |                        | ...                       |