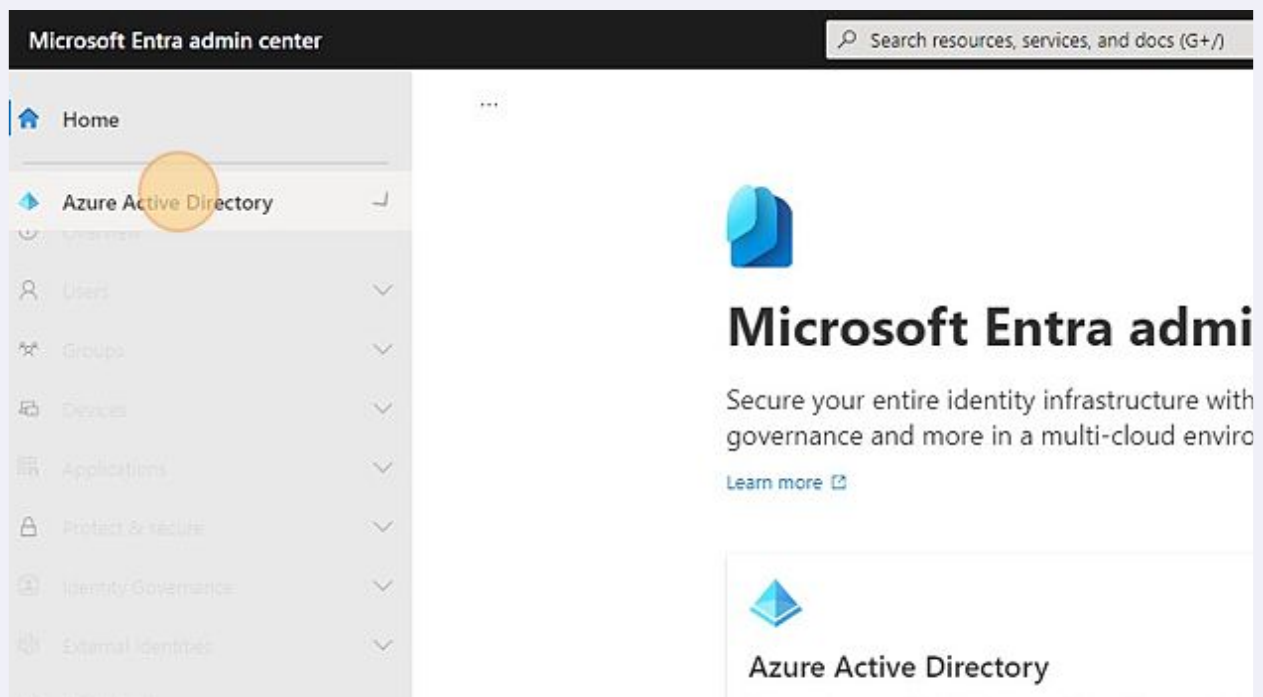


How to Create a Conditional Access Policy to Block Legacy Authentication

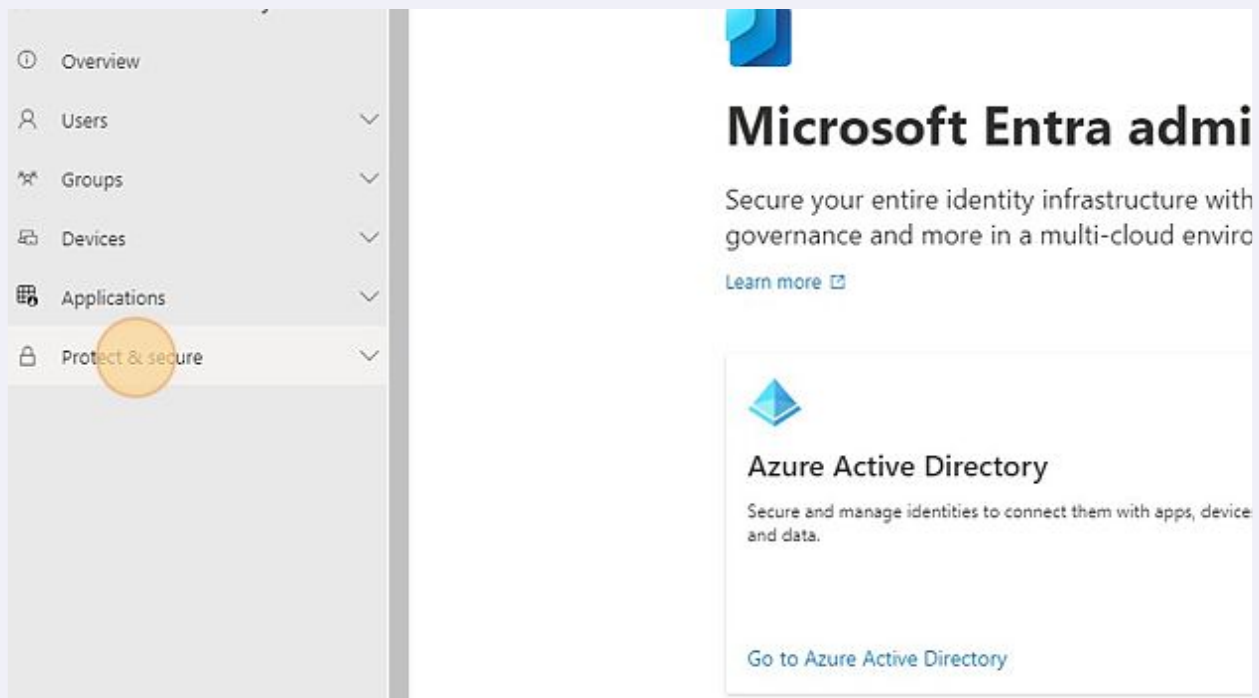
In this guide, we review the template method of deploying a conditional access policy to block legacy authentication.

1 Navigate to entra.microsoft.com

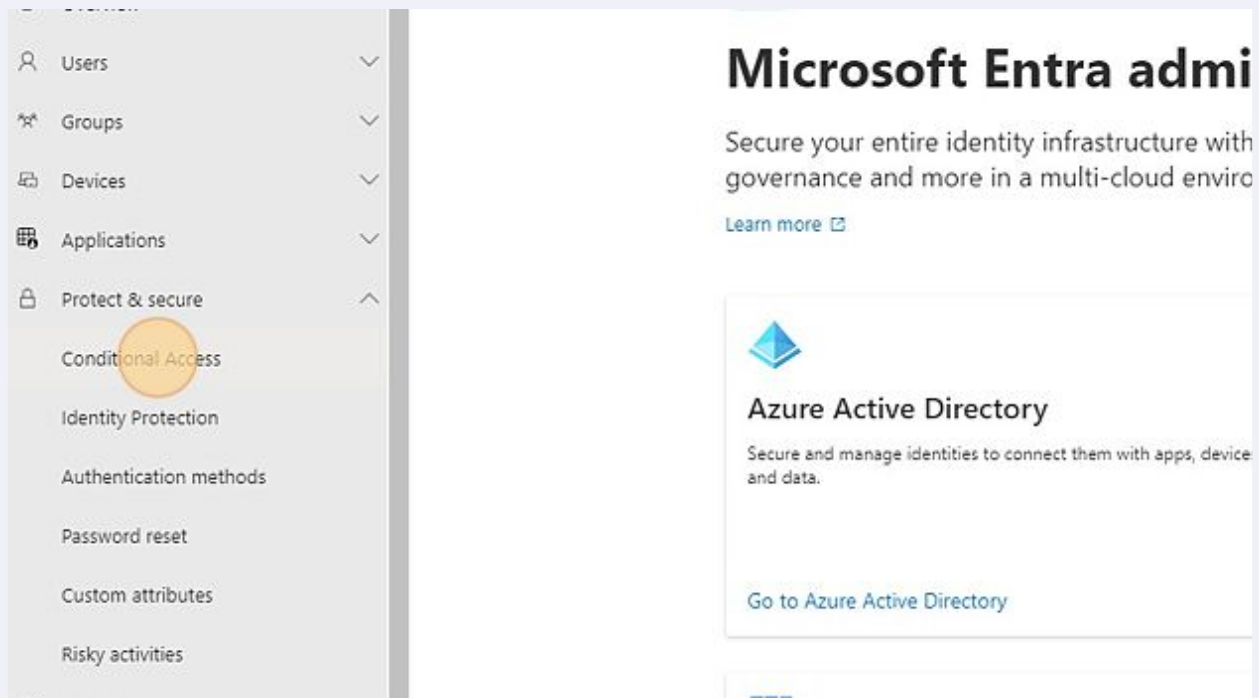
2 Click "Azure Active Directory"



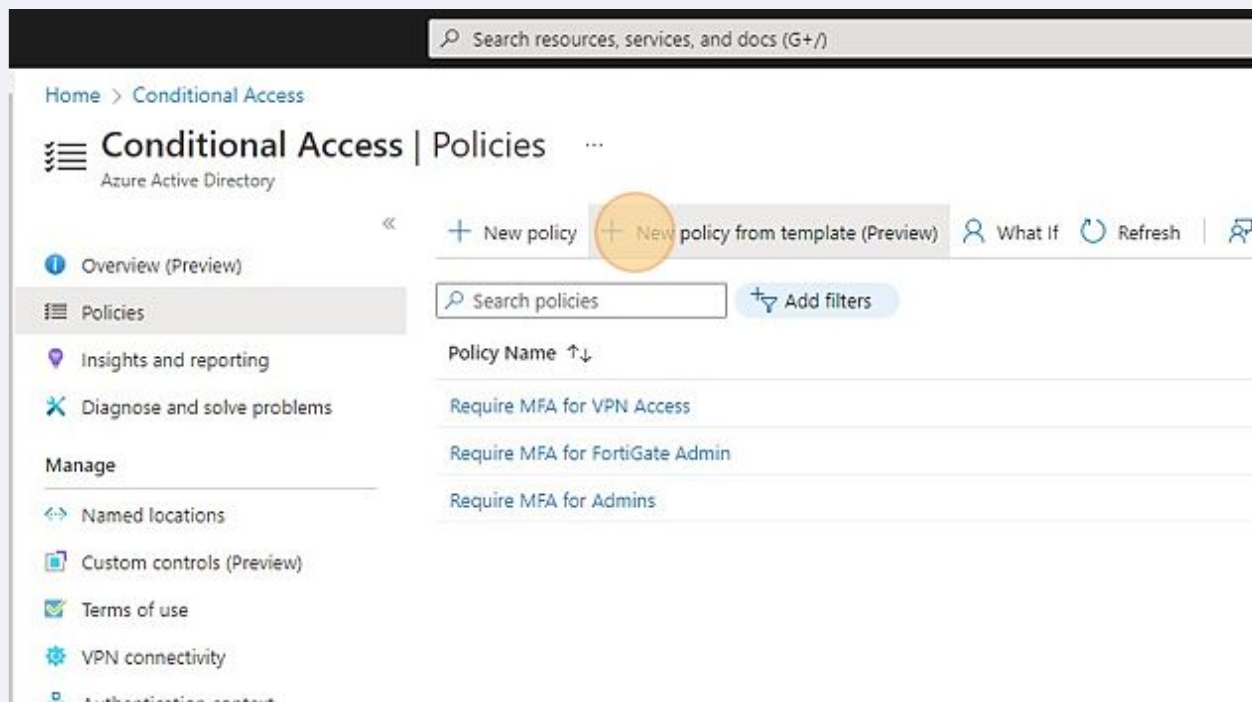
3 Click "Protect & secure"



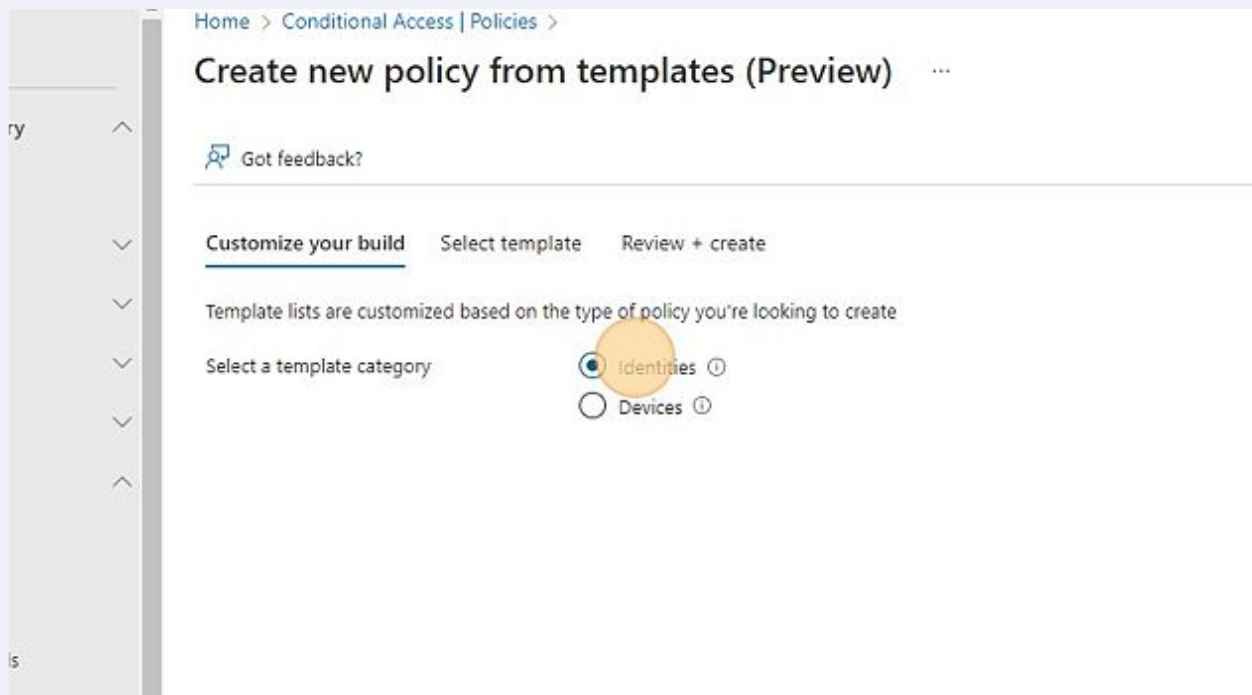
4 Click "Conditional Access"



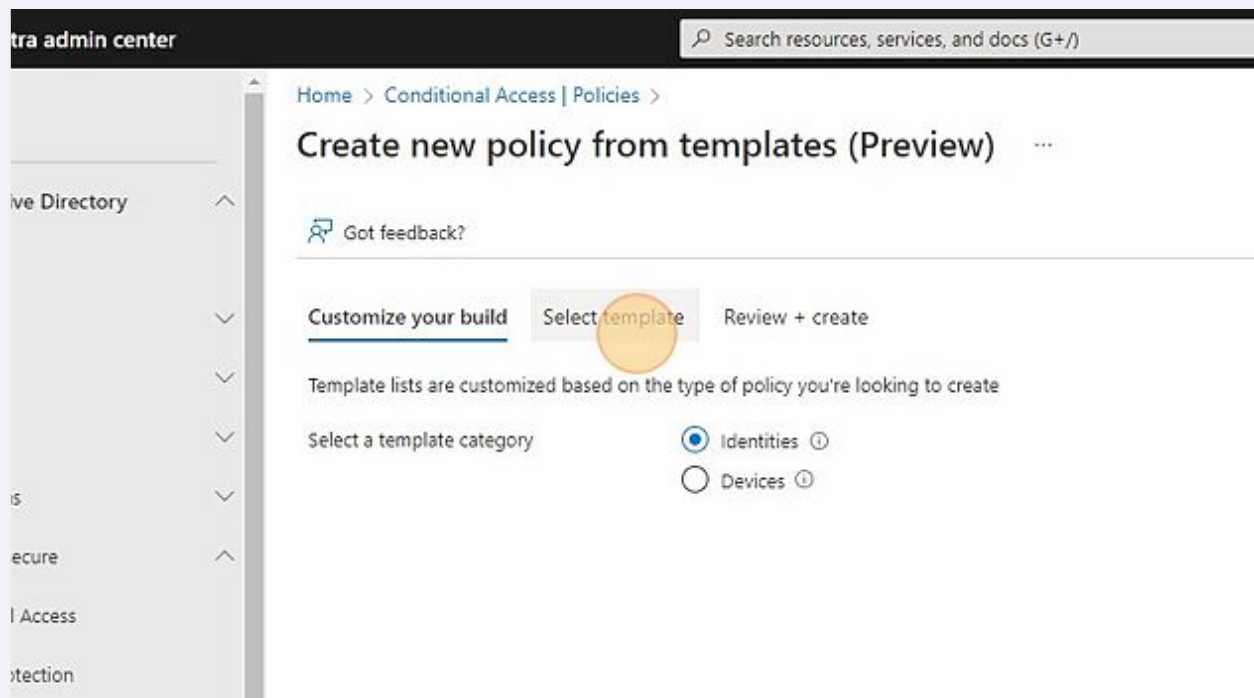
5 Click "New policy from template"



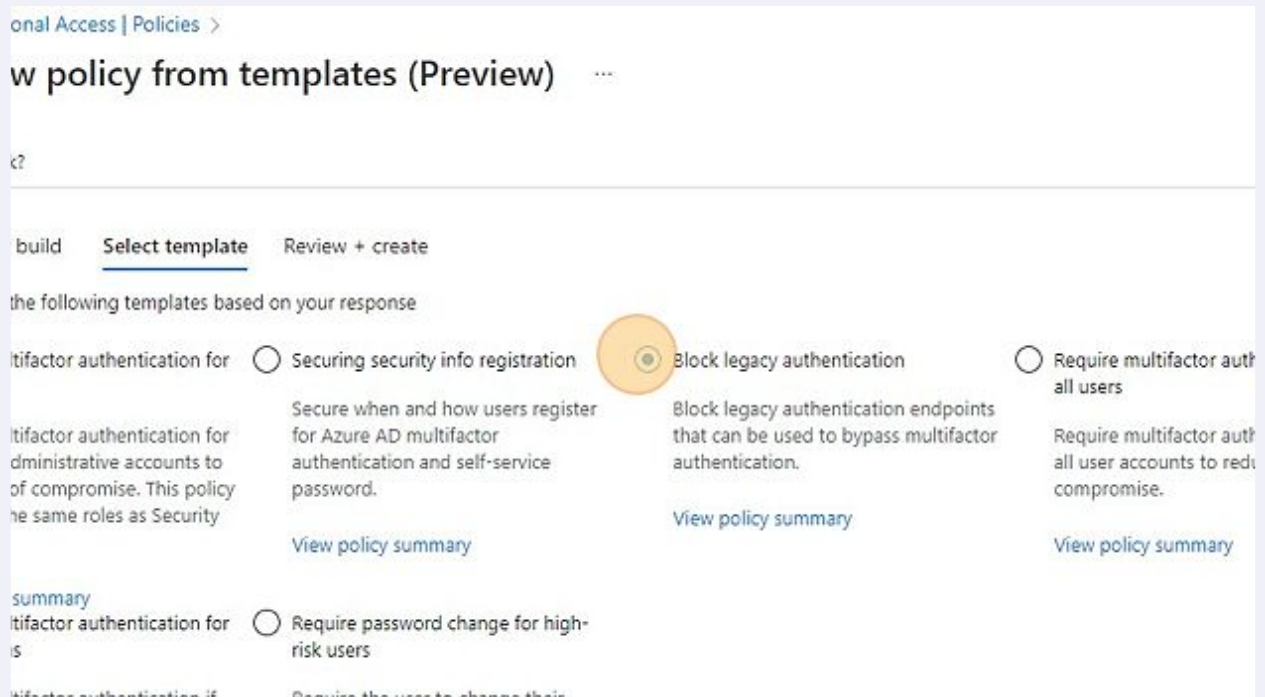
6 Click "Identities"



7 Click "Select template"



8 Select "Block legacy authentication"



9 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 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 password change for high-risk users

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

CA003: Block legacy authentication

Policy state

☐ Off ☐ On ☒ Report-only

10 Change "Policy state" to "On"

Authentication methods

Password reset

Custom attributes

Risky activities

Identity Governance

External Identities

Show more

Permissions Management

Verified ID

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

11 Click "Create Policy"

Authentication methods

- Password reset
- Custom attributes
- Risky activities
- Identity Governance
- External Identities
- Show more
- Permissions Management
- Verified ID
- Support

Excluded users

Cloud apps or actions

Cloud apps

Conditions

Client apps

Legacy authentication clients

Exchange ActiveSync clients

Other clients

Access controls

Block access

Selected

Create Policy Previous Next

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

Overview (Preview)

Policies

Insights and reporting

Diagnose and solve problems

Manage

- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Authentication context
- Classic policies

Monitoring

- Sign-in logs

New policy New policy from template (Preview) What if Refresh

Search policies Add filters

Policy Name ↑↓

- Require MFA for VPN Access
- Require MFA for FortiGate Admin
- Require MFA for Admins
- Block legacy authentication

13 Click "All users included and specific users excluded"

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 ①

All users included and specific users excluded

Cloud apps or actions ①

All cloud apps

Conditions ①

1 condition selected

Access controls

Grant ①

Block access

14 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 ①

All users included and specific users excluded

Cloud apps or actions ①

All cloud apps

Conditions ①

1 condition selected

What does this policy apply to?

Users and groups

Include Exclude

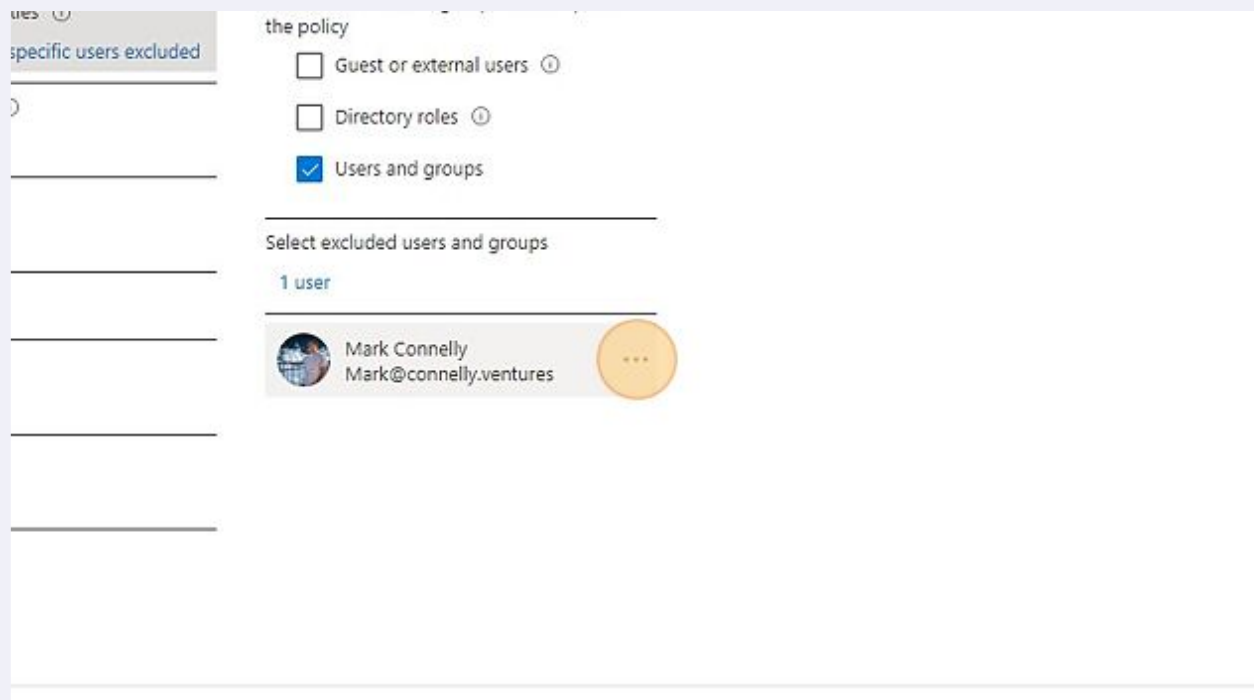
☐ None

☒ All users

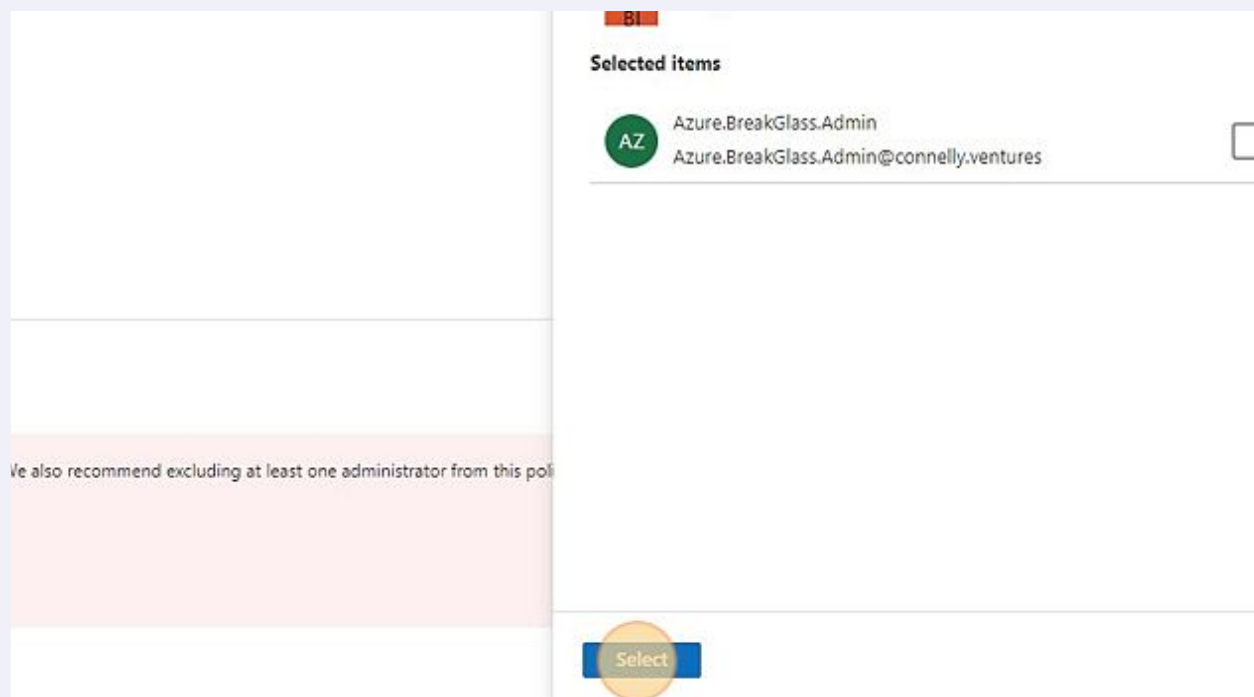
☐ Select users and groups

⚠ 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.

15 Click "Users and groups"



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



17 Click "On" to enable the policy.

The screenshot shows the Azure AD policy configuration interface. On the left, a navigation pane lists various identity management options. The main content area is titled 'Access controls' and includes sections for 'Grant', 'Block access', 'Session', and '0 controls selected'. Below this, the 'Enable policy' section features a toggle switch set to 'On'. A warning message is displayed, and the 'Save' button is highlighted.

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

18 Click "Save"

The screenshot shows the Azure AD policy configuration interface. On the left, a navigation pane lists various identity management options. The main content area is titled 'Access controls' and includes sections for 'Grant', 'Block access', 'Session', and '0 controls selected'. Below this, the 'Enable policy' section features a toggle switch set to 'On'. A warning message is displayed, and the 'Save' button is highlighted.

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

The screenshot shows the Microsoft 365 admin center interface. At the top, a notification banner reads: "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'." Below the notification, there is a "Got feedback?" link. The main content area displays a table of policies, with the header "4 out of 4 policies found". The table has three columns: "State", "Creation Date", and "Modified Date". The "State" column is sorted in descending order. The table contains four rows, all with the state "On". The first row has a creation date of "2/6/2022, 11:39:39 AM" and a modified date of "2/6/2022, 11:39:59 AM". The second row has a creation date of "2/6/2022, 11:51:57 AM". The third row has a creation date of "12/18/2022, 8:12:24 PM". The fourth row is highlighted in grey and has a creation date of "On".

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		