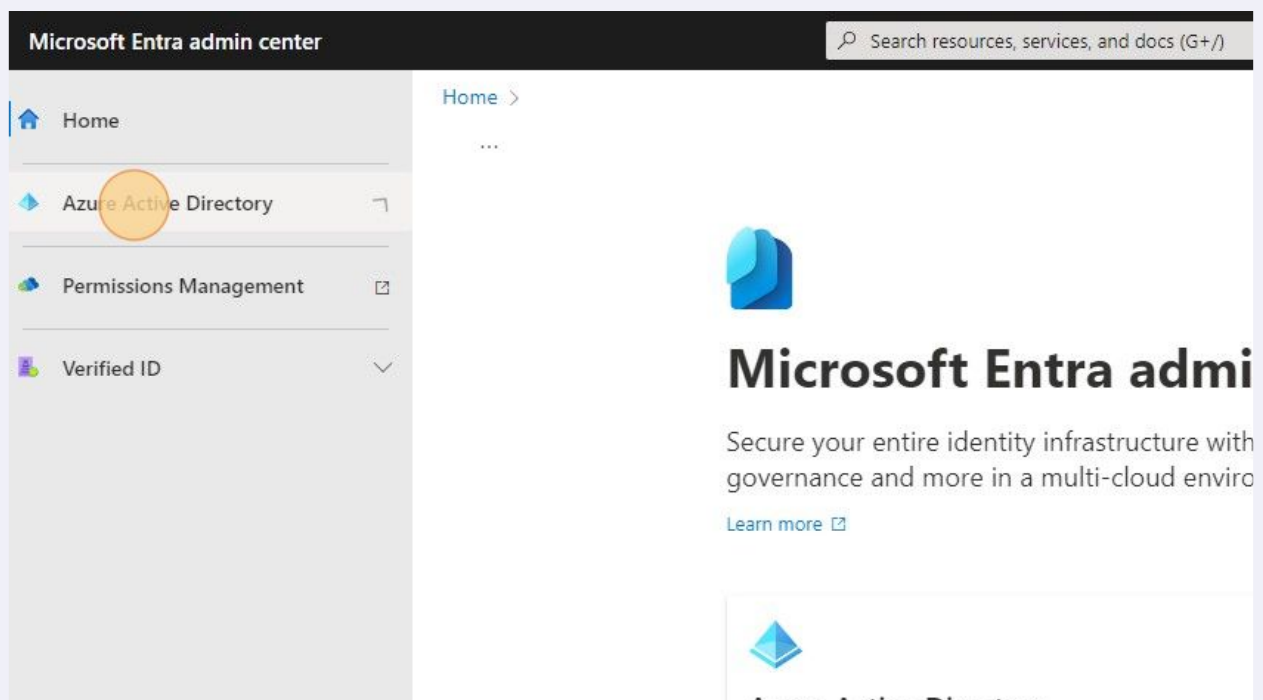


How to Create a Conditional Access Policy to Block Guest Users

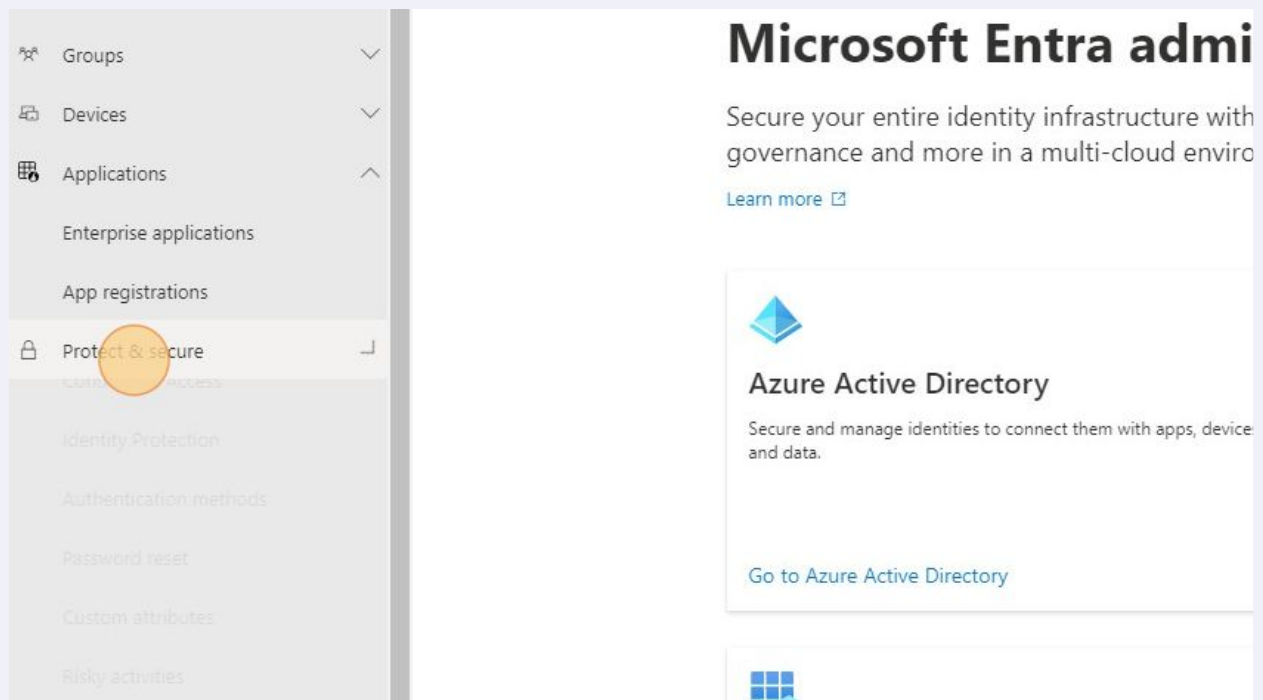
In this guide, we walk through how to block guest access via conditional access policy.

1 Navigate to entra.microsoft.com

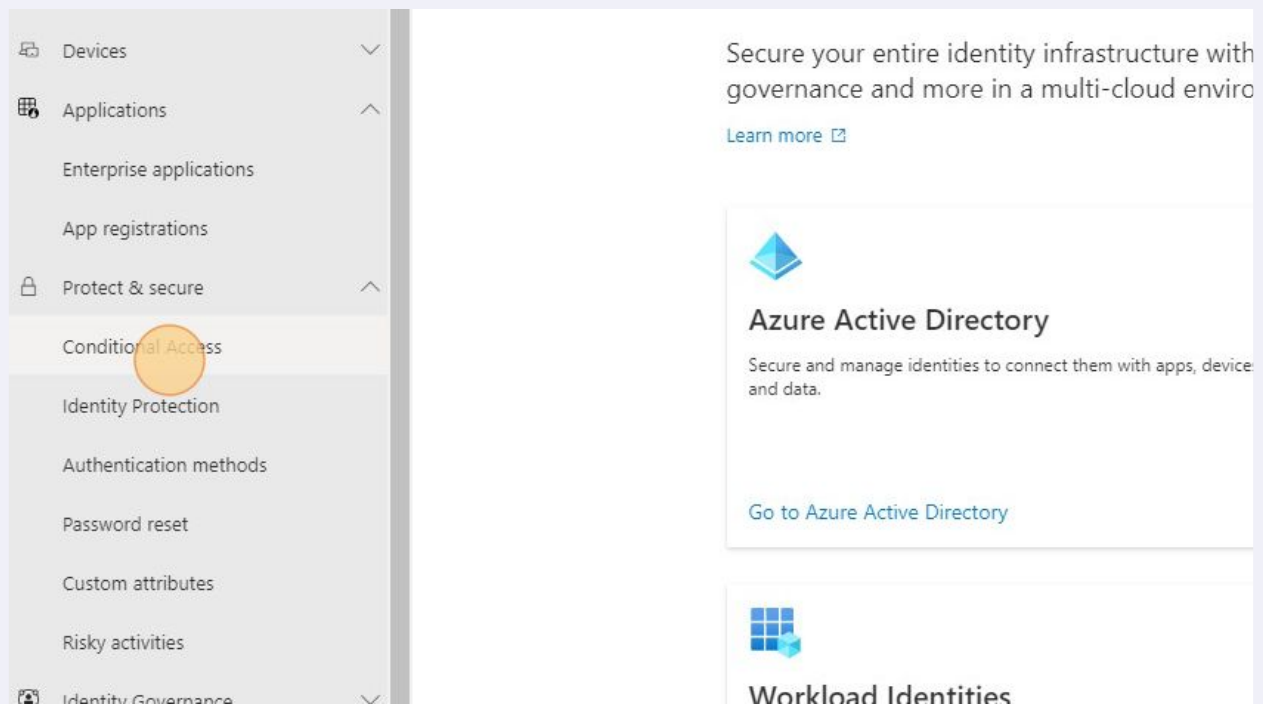
2 Click "Azure Active Directory"



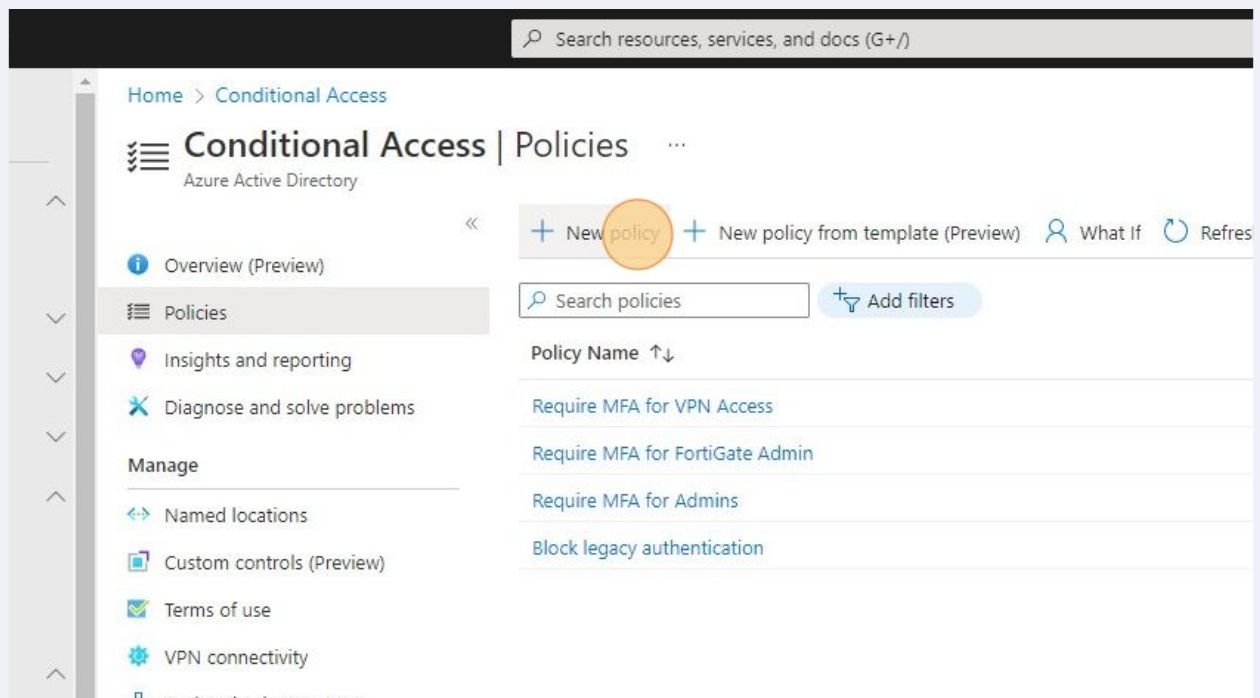
3 Click "Protect & secure"



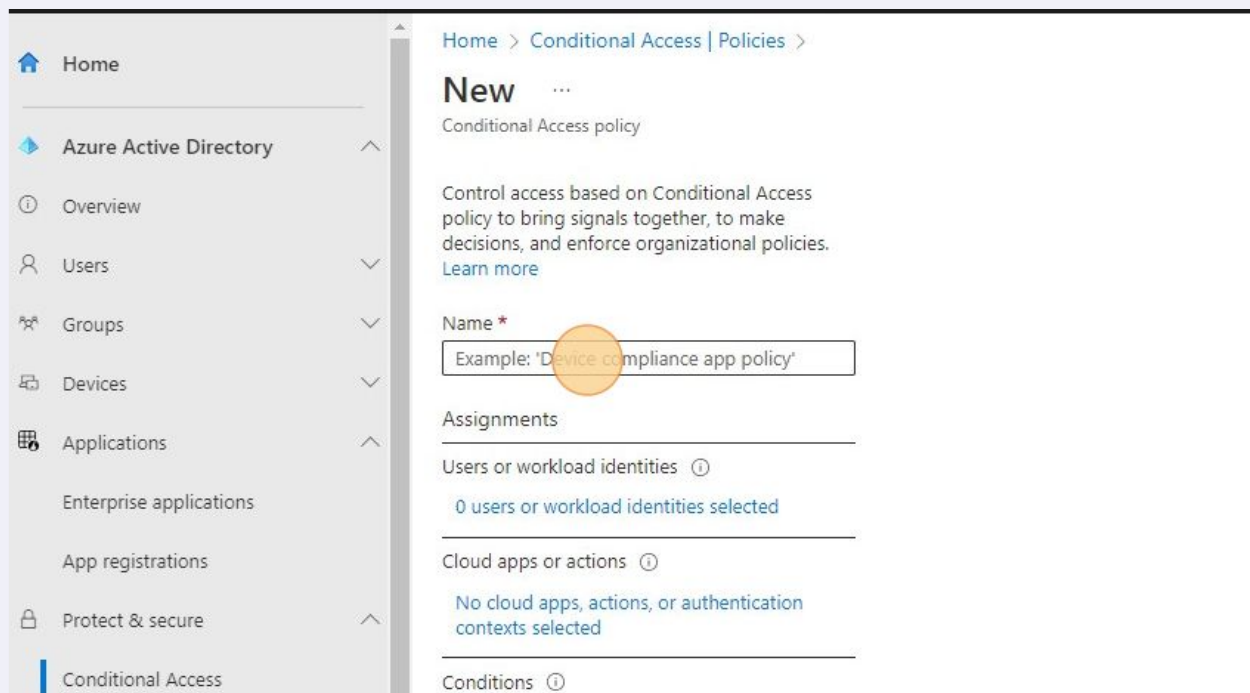
4 Click "Conditional Access"



5 Click "New Policy"



6 Set the "Name" to "Block Guest Access"



7 For "Users", target "Guest or external users"

decisions, and enforce organizational policies. [Learn more](#)

Name *
Block Guest Accounts ✓

What does this policy apply to?
Users and groups

Assignments

Users or workload identities ⓘ
[Specific users included](#)

✗ "Select users and groups" must be configured

Cloud apps or actions ⓘ
[No cloud apps, actions, or authentication contexts selected](#)

Conditions ⓘ
[0 conditions selected](#)

Access controls

Grant ⓘ

Include Exclude

☐ None

☐ All users

☒ Select users and groups

☒ Guest or external users ⓘ

☐ Directory roles ⓘ

☐ Users and groups

8 Select the types of "Guests" that you would like to block.

Cloud apps or actions ⓘ
[No cloud apps, actions, or authentication contexts selected](#)

Conditions ⓘ
[0 conditions selected](#)

Access controls

Grant ⓘ
[0 controls selected](#)

Session ⓘ
[0 controls selected](#)

Guest or external users ⓘ

3 selected

☒ B2B collaboration guest users (preview)

☐ B2B collaboration member users (preview)

☐ B2B direct connect users (preview)

☒ Local guest users (preview)

☒ Service provider users (preview)

☒ Other external users (preview)

Enable policy



Alert!
Remember to exclude your break glass admin

9 For "Cloud apps", target "All cloud apps"

The screenshot shows the 'Conditional Access policy' configuration page in the Microsoft Entra admin center. The policy is named 'Block Guest Accounts'. Under the 'Assignments' section, 'Users or workload identities' is expanded, showing 'Specific users included'. The 'Cloud apps or actions' section is expanded, showing 'No cloud apps, actions, or authentication contexts selected'. The 'Conditions' section shows '0 conditions selected'. The 'Access controls' section is partially visible. On the right side, the 'Select what this policy applies to' dropdown is set to 'Cloud apps'. Under the 'Include' tab, the 'All cloud apps' radio button is selected, while 'None' and 'Select apps' are unselected. The 'Exclude' tab is also visible.

Conditional Access policy

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

Name *

Block Guest Accounts ✓

Assignments

Users or workload identities ⓘ

[Specific users included](#)

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps

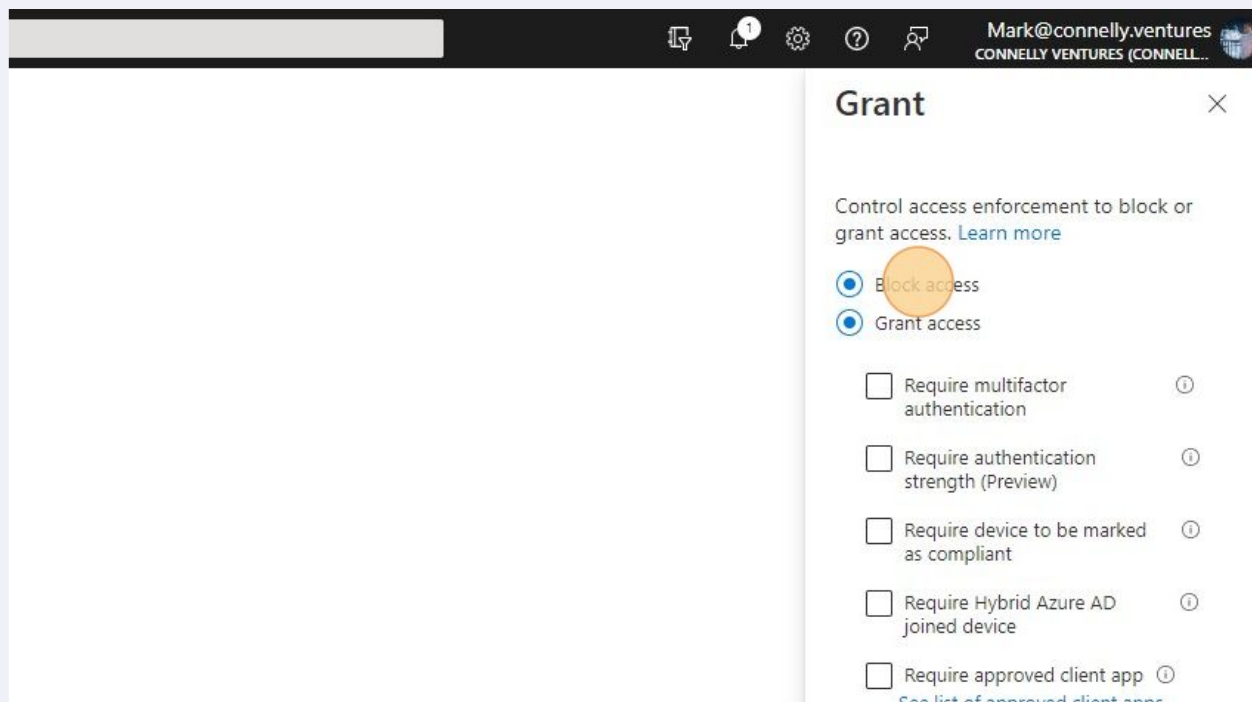
Include Exclude

☒ None

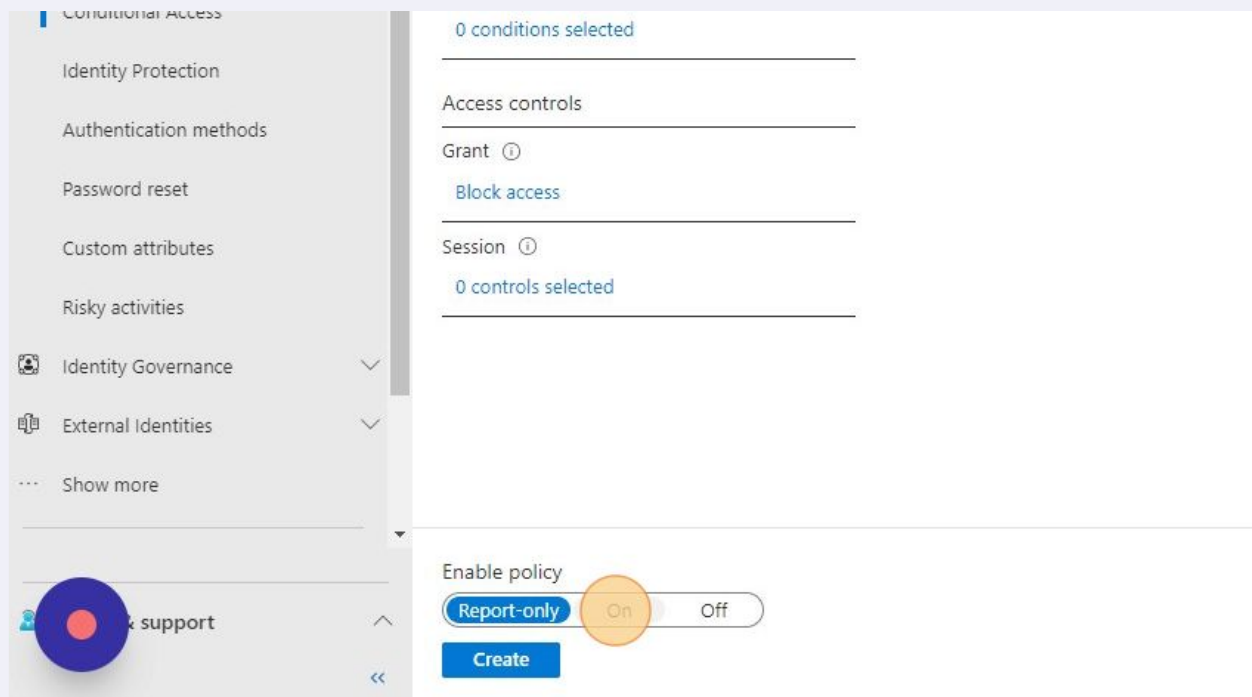
☒ All cloud apps

☐ Select apps

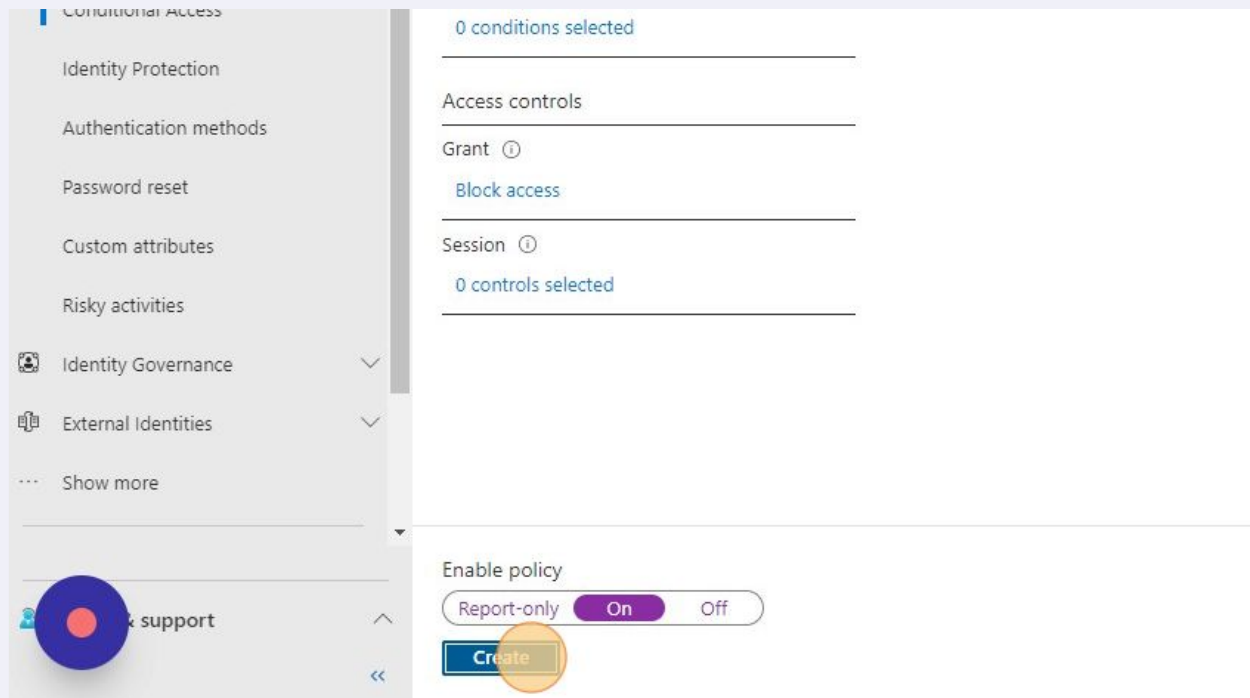
10 Set "Grant" to "Block access"



11 Click "On" to enforce the policy immediately.



12 Click "Create"



13 You should receive a notification letting you know that the policy was created successfully.

