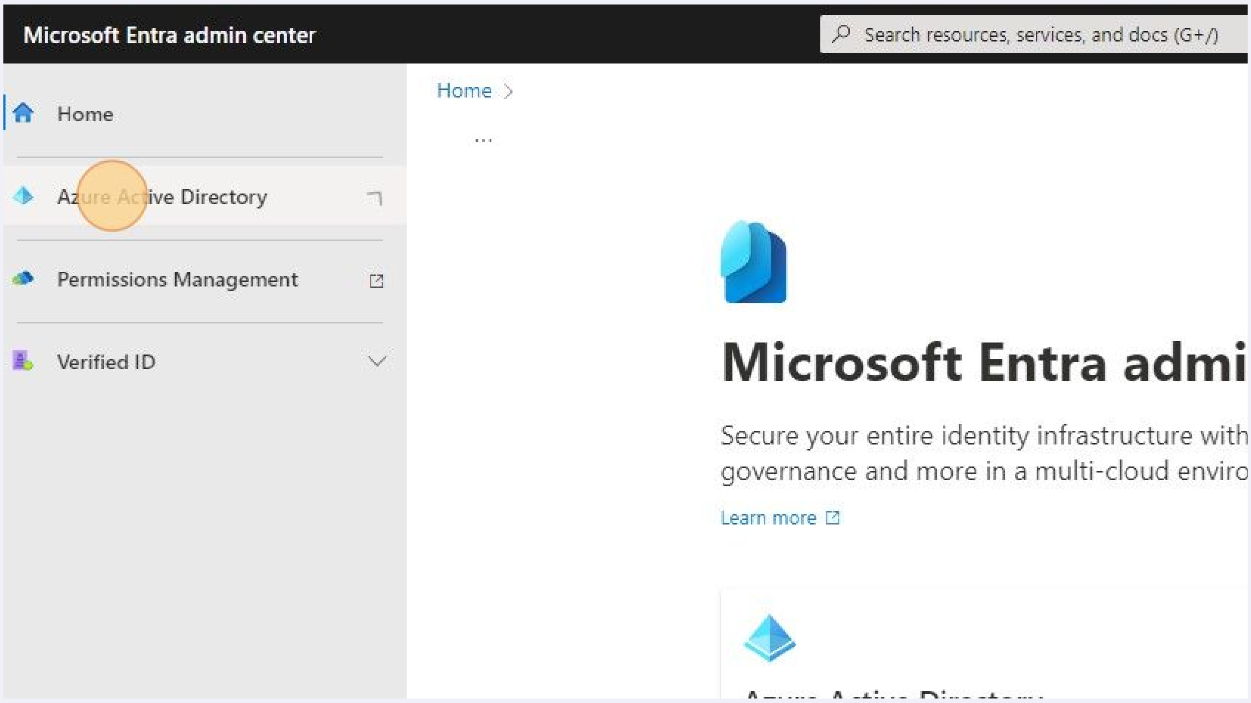
# How to Create a Conditional Access Policy to Require MFA for Administrators

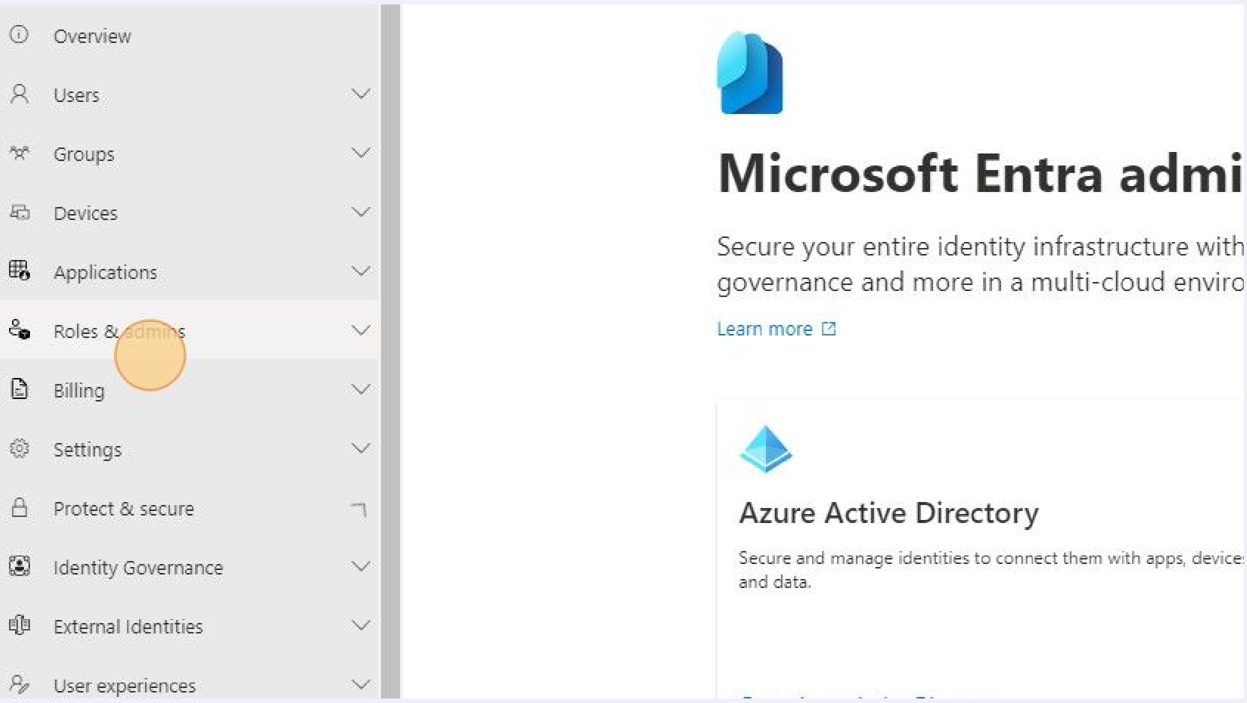
In this guide, we walk through the process of creating a conditional access policy, specifically targeted at administrative roles, to require MFA for all applications.

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

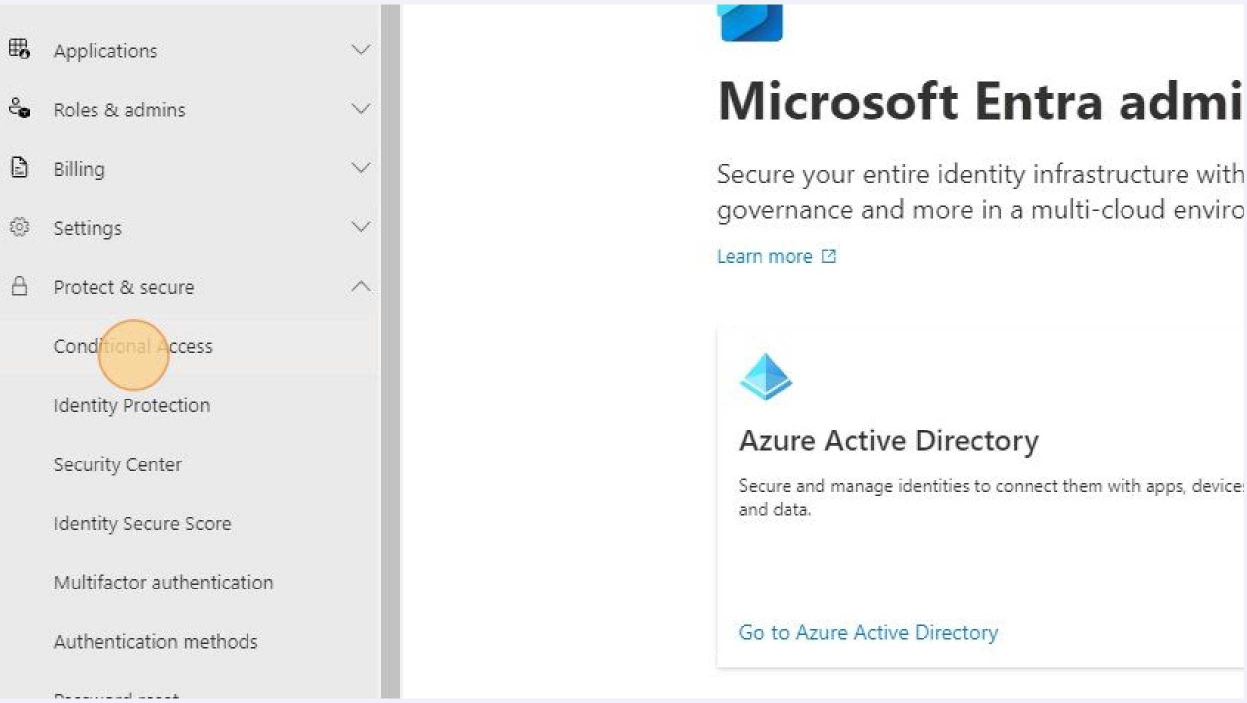
2 Click "Azure Active Directory"


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Home
Azure Active Directory
Permissions Management
Verified ID
Home >
...
Microsoft Entra admi
Secure your entire identity infrastructure with
governance and more in a multi-cloud enviro
Learn more
Azure Active Directory

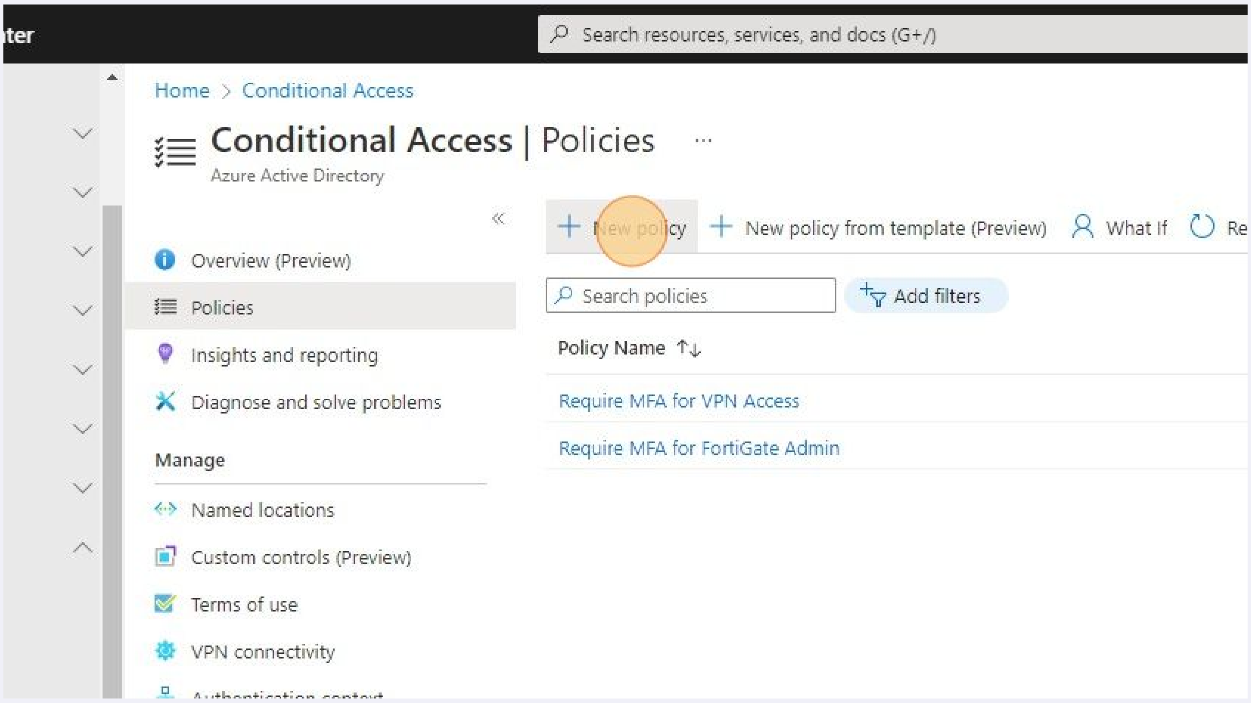
3 Click "Protect & secure"



4 Click "Conditional Access"



5 Click "New Policy"



ter

Search resources, services, and docs (G+/)

Home > Conditional Access

## Conditional Access | Policies ...

Azure Active Directory

- Overview (Preview)
- Policies
- Insights and reporting
- Diagnose and solve problems

Manage

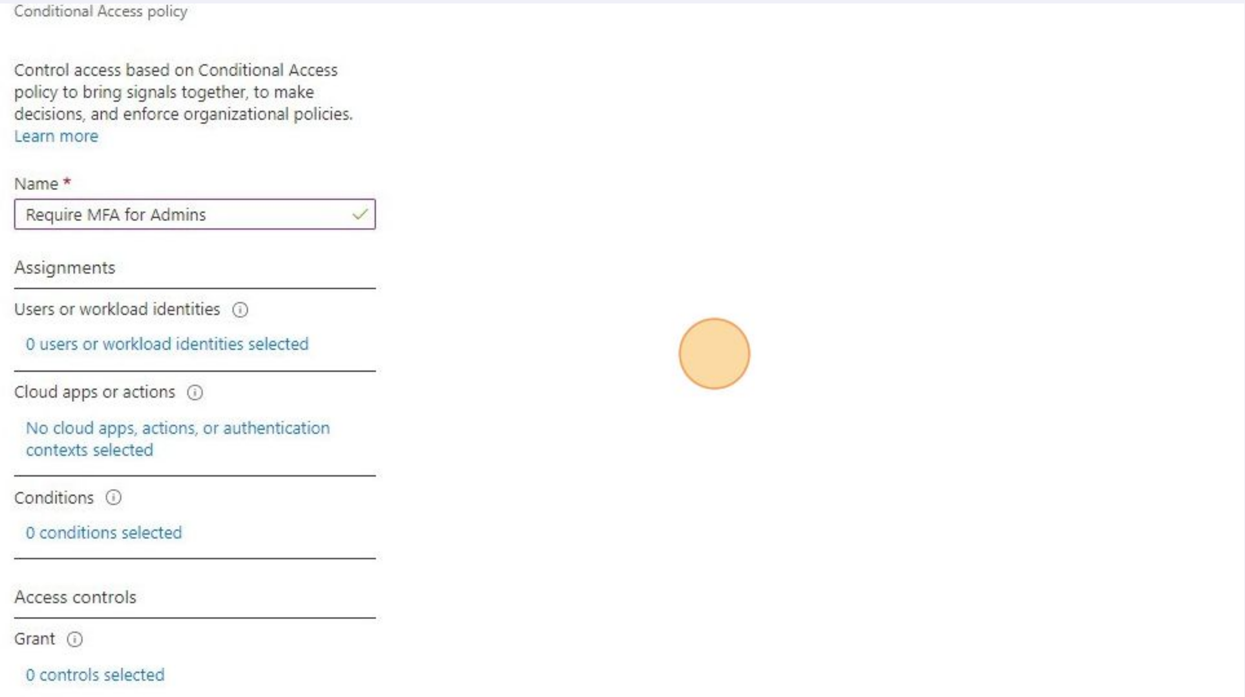
- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Authentication context

+ New policy   + New policy from template (Preview)   What If   Re

Search policies   Add filters

| Policy Name ↑↓ |
|---|
| Require MFA for VPN Access |
| Require MFA for FortiGate Admin |

6 Set "Name" to "Require MFA for Admins"



Conditional Access policy

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

Name *
Require MFA for Admins ✓

Assignments

Users or workload identities ⓘ
0 users or workload identities selected

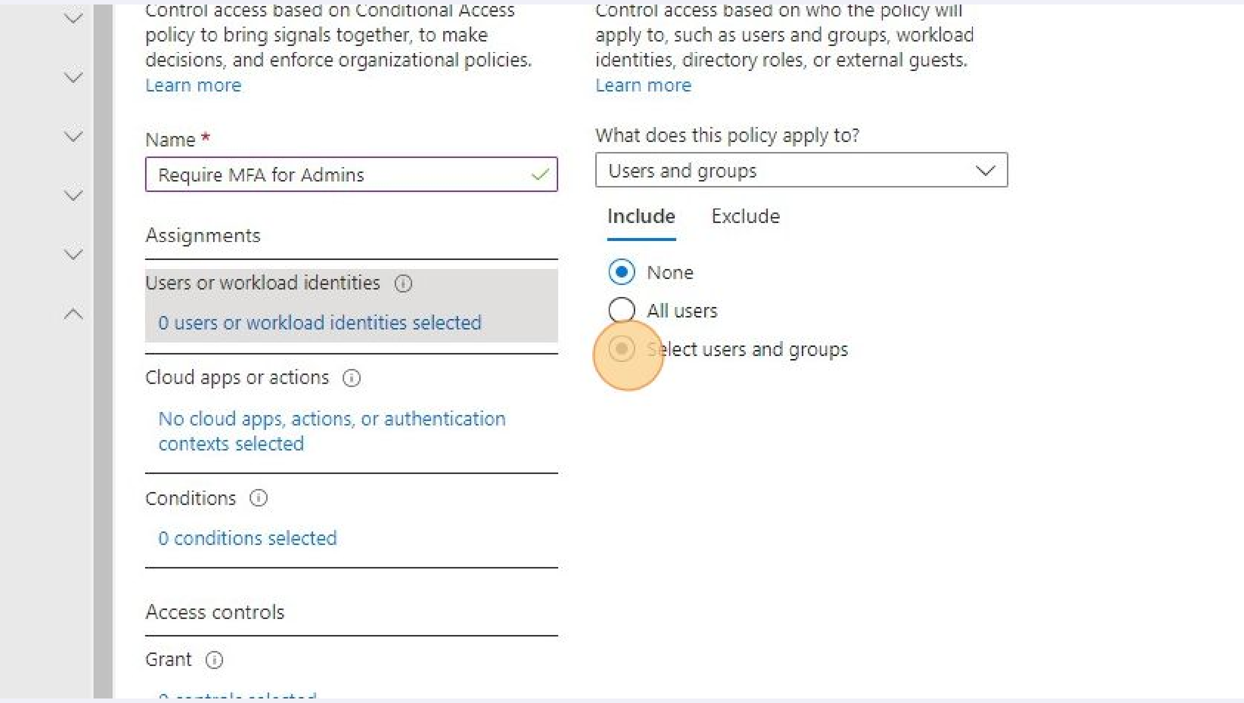
Cloud apps or actions ⓘ
No cloud apps, actions, or authentication contexts selected

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
0 controls selected

## 7 Target "Select users and groups"



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

Name *

Require MFA for Admins

Assignments

Users or workload identities ⓘ

0 users or workload identities selected

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

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

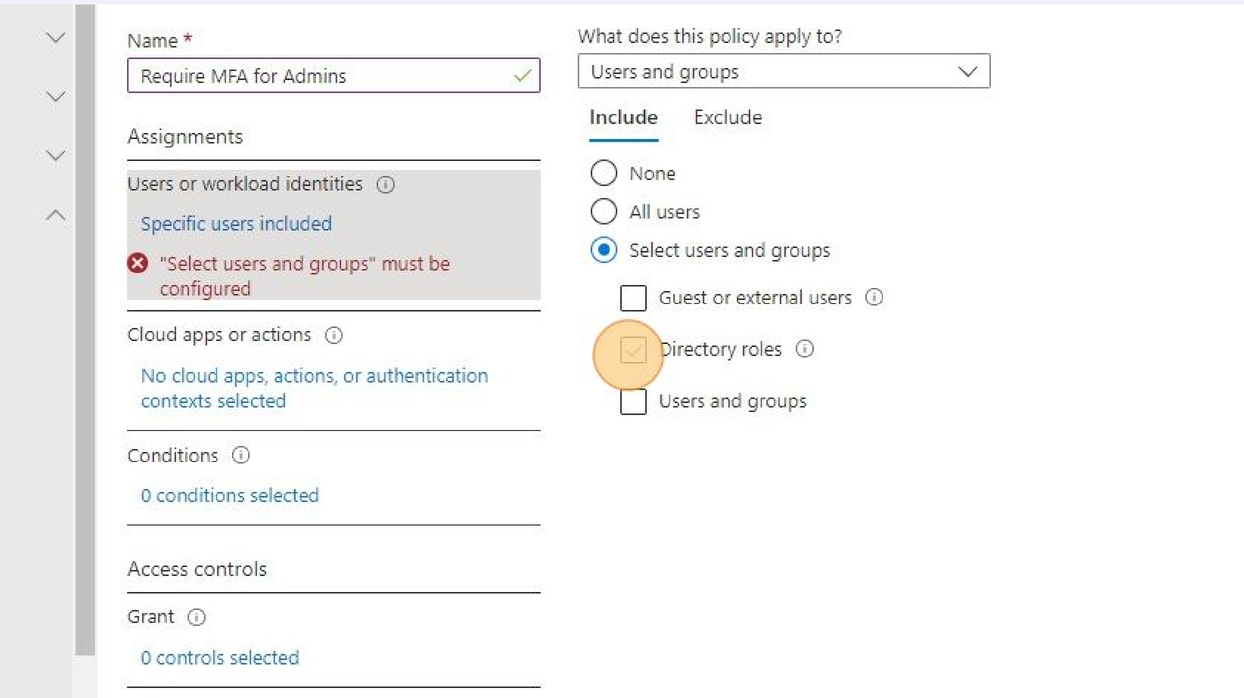
Include Exclude

● None

○ All users

○ Select users and groups

## 8 Under "Users", target "Directory roles"



Name *

Require MFA for Admins

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 ⓘ

0 controls selected

What does this policy apply to?

Users and groups

Include Exclude

○ None

○ All users

● Select users and groups

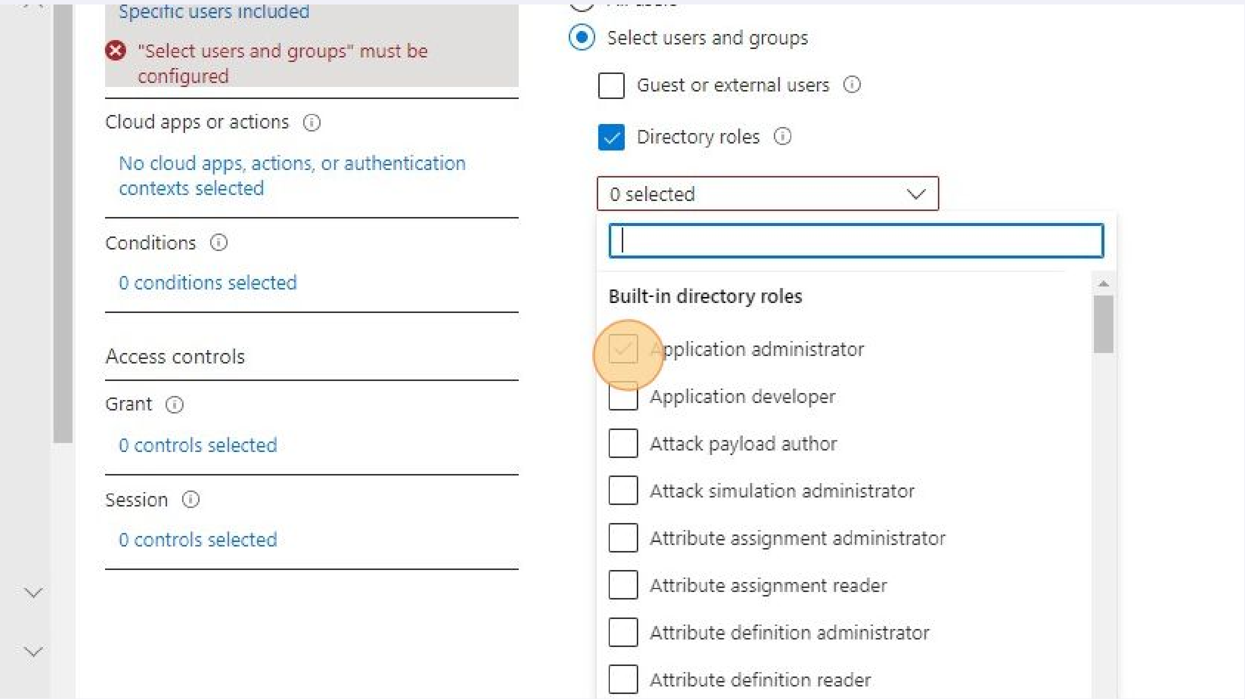
□ Guest or external users ⓘ

□ Directory roles ⓘ

□ Users and groups

9

Include:
Global Administrator
Application administrator
Authentication Administrator
Billing administrator
Cloud application administrator
Conditional Access Administrator
Exchange administrator
Helpdesk administrator
Password administrator
Privileged authentication administrator
Privileged Role Administrator
Security administrator
SharePoint administrator
User administrator



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

0 controls selected

Session

0 controls selected

● Select users and groups

□ Guest or external users

☑ Directory roles

0 selected

Built-in directory roles

□ Application administrator

□ Application developer

□ Attack payload author

□ Attack simulation administrator

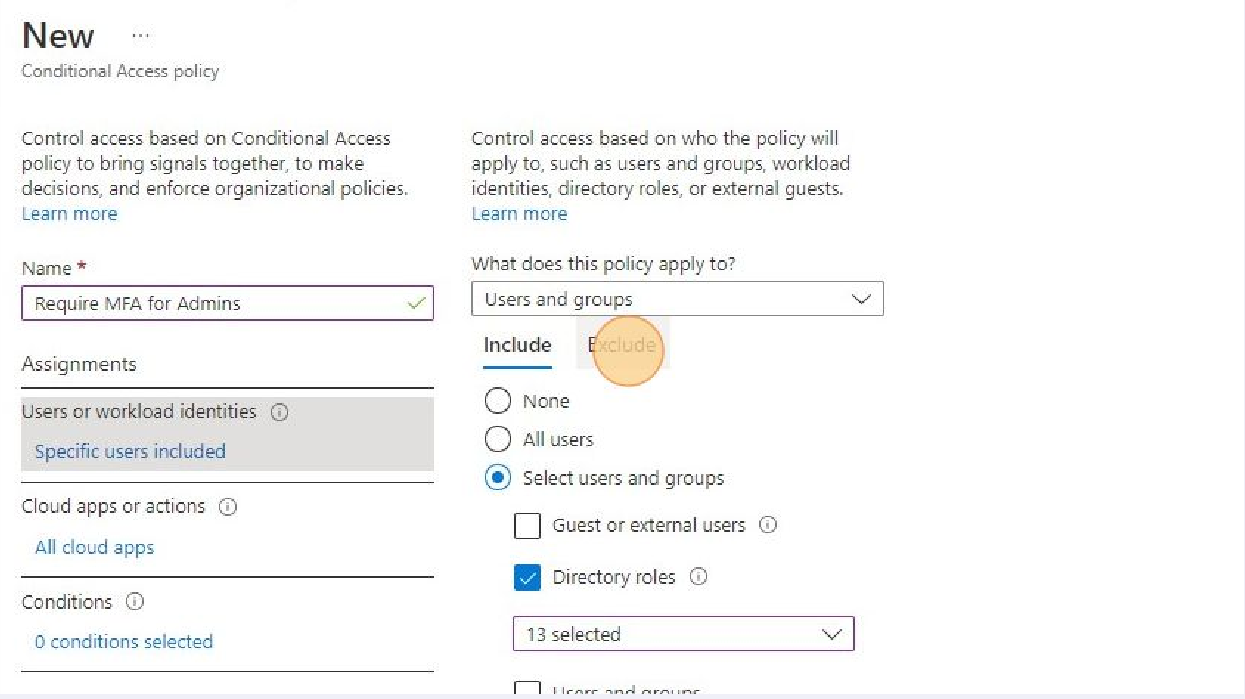
□ Attribute assignment administrator

□ Attribute assignment reader

□ Attribute definition administrator

□ Attribute definition reader

10 Click "Exclude"



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 *

Require MFA for Admins

Assignments

Users or workload identities

Specific users included

Cloud apps or actions

All cloud apps

Conditions

0 conditions 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

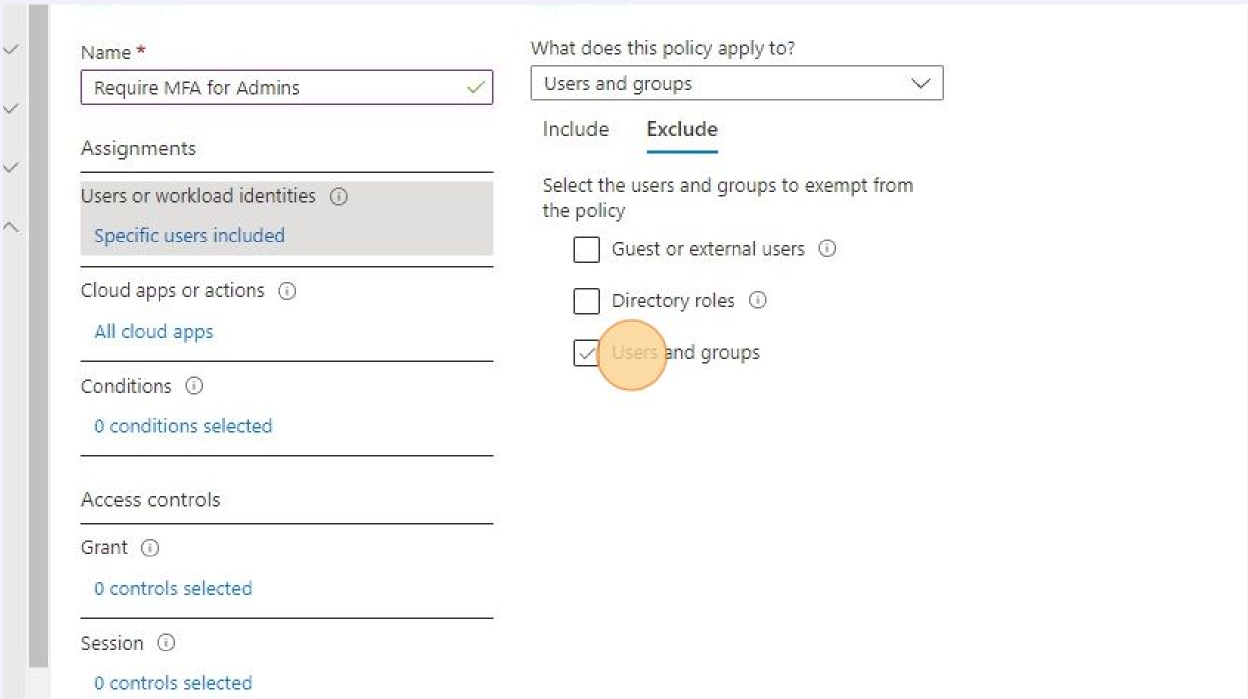
□ Guest or external users

☑ Directory roles

13 selected

□ Users and groups

11 Click "Users and groups"



Name *

Require MFA for Admins

Assignments

Users or workload identities

Specific users included

Cloud apps or actions

All cloud apps

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Session

0 controls selected

What does this policy apply to?

Users and groups

Include Exclude

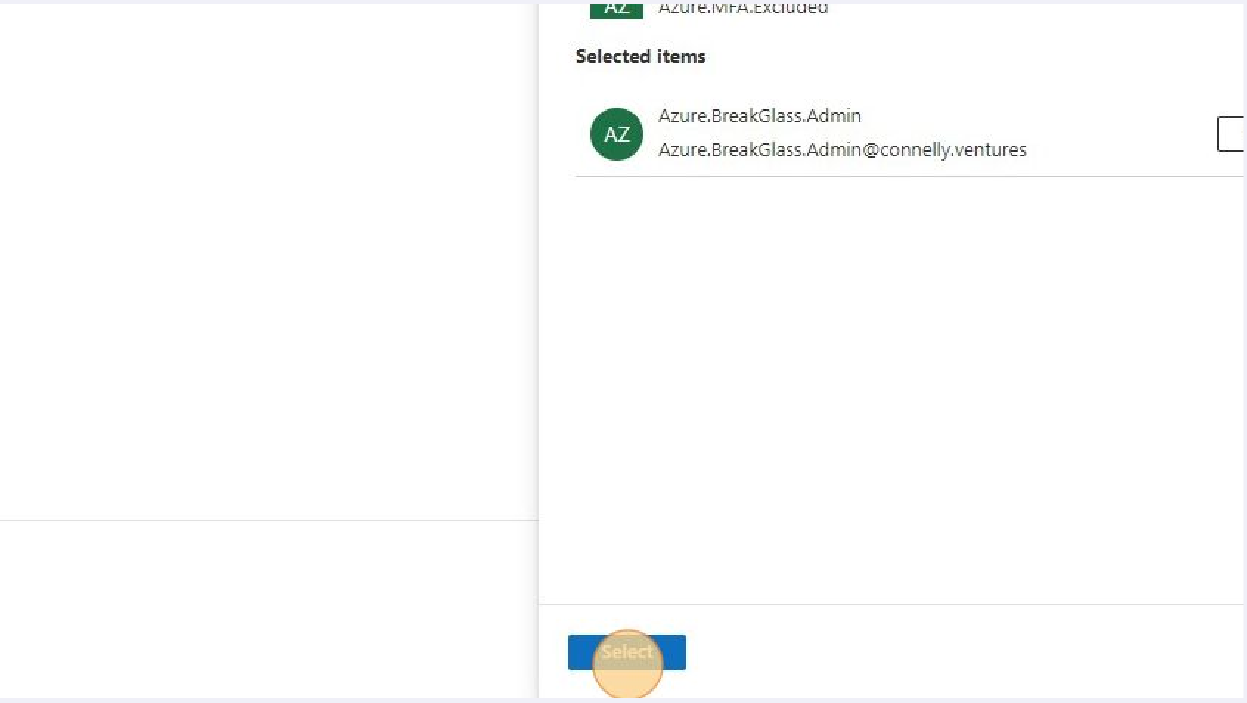
Select the users and groups to exempt from the policy

□ Guest or external users

□ Directory roles

☑ Users and groups

12 Exclude your break glass account and save it.

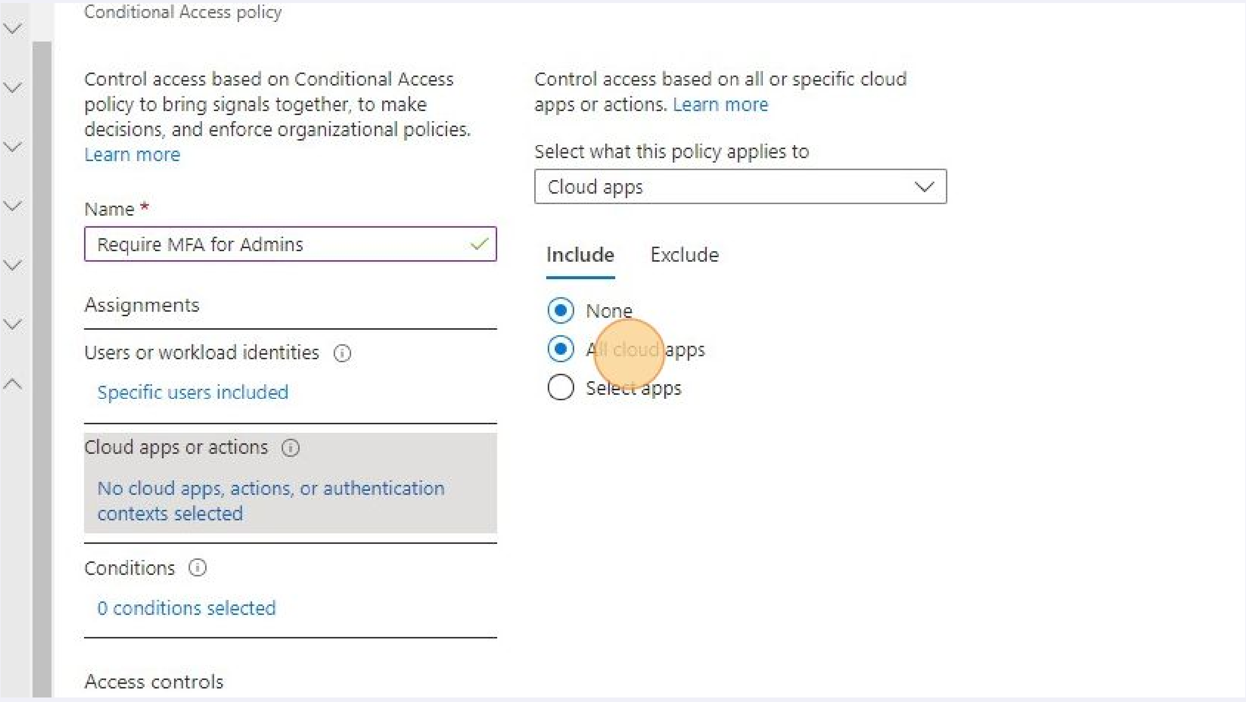


AZ Azure.MFA.Excluded

Selected items

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

13 Under "Cloud Apps", target "All cloud apps"



Conditional Access policy

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

Name *

Require MFA for Admins

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

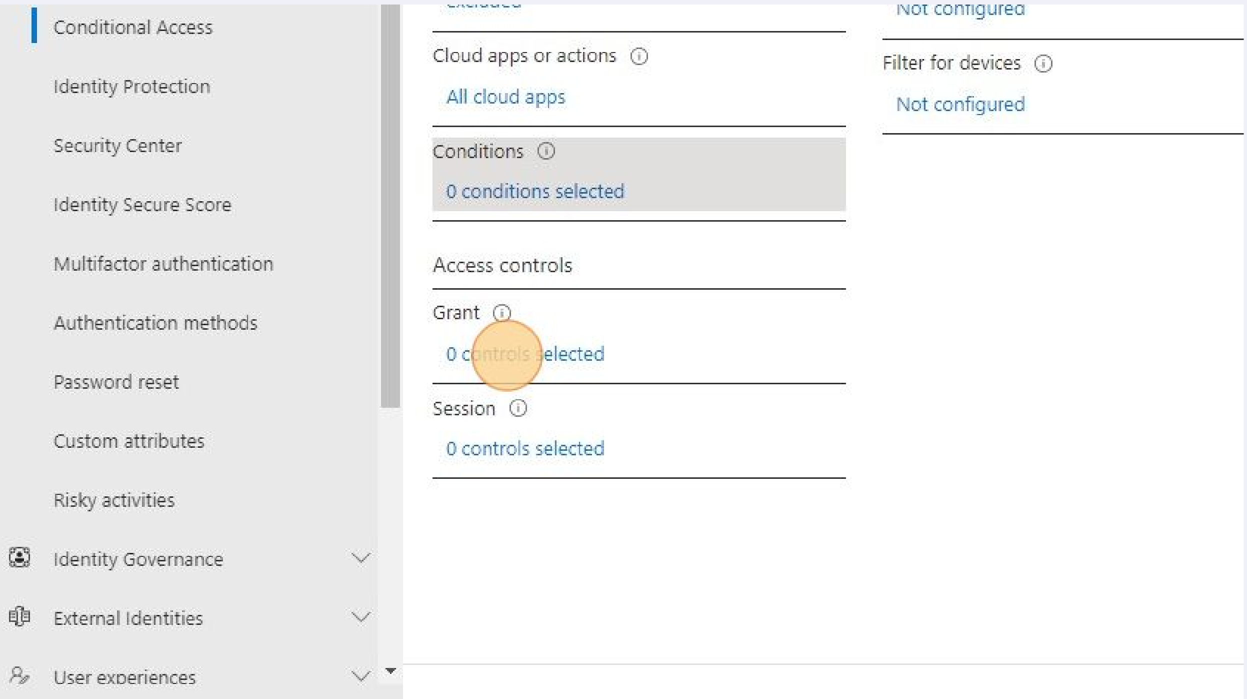
Select what this policy applies to

Cloud apps

Include Exclude

● None
● All cloud apps
○ Select apps

14 Click the link under "Grant"



Conditional Access
Identity Protection
Security Center
Identity Secure Score
Multifactor authentication
Authentication methods
Password reset
Custom attributes
Risky activities
Identity Governance
External Identities
User experiences

excluded

Cloud apps or actions
All cloud apps

Conditions
0 conditions selected

Access controls

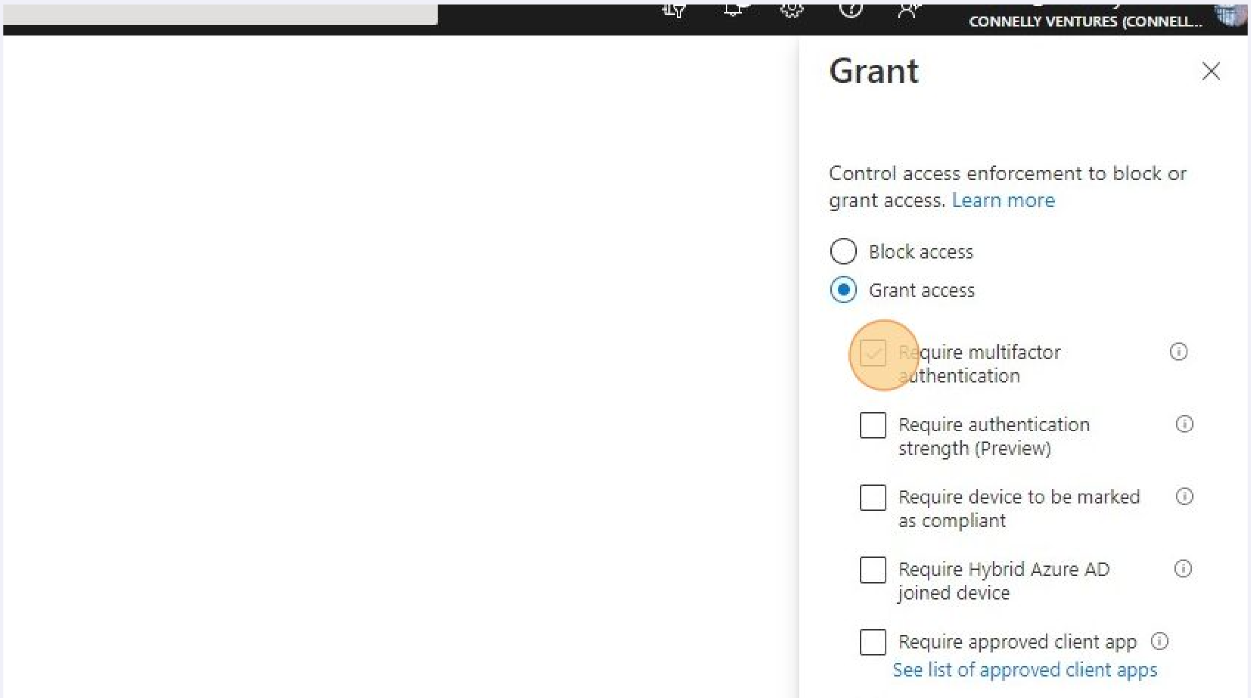
Grant
0 controls selected

Session
0 controls selected

Not configured

Filter for devices
Not configured

15 Click "Require multifactor authentication"



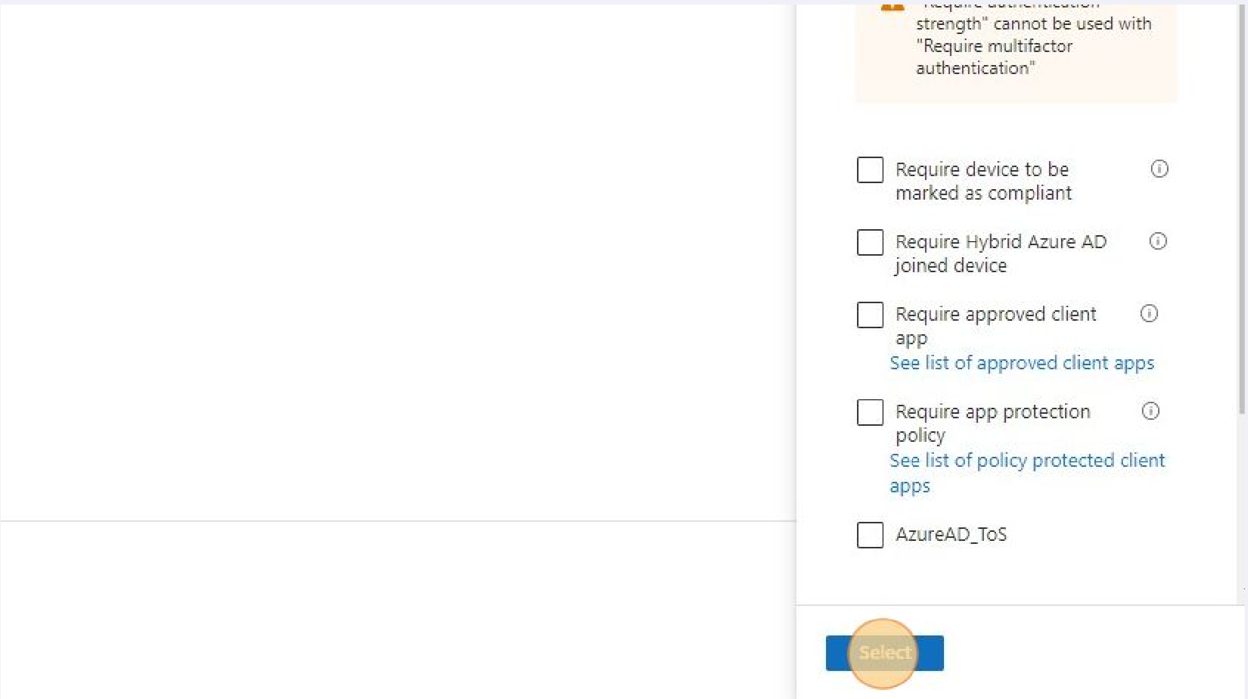
Grant

Control access enforcement to block or grant access. Learn more

○ Block access
● Grant access

□ Require multifactor authentication
□ Require authentication strength (Preview)
□ Require device to be marked as compliant
□ Require Hybrid Azure AD joined device
□ Require approved client app
See list of approved client apps

16 Click "Select"



"Require authentication strength" cannot be used with "Require multifactor authentication"

□ Require device to be marked as compliant

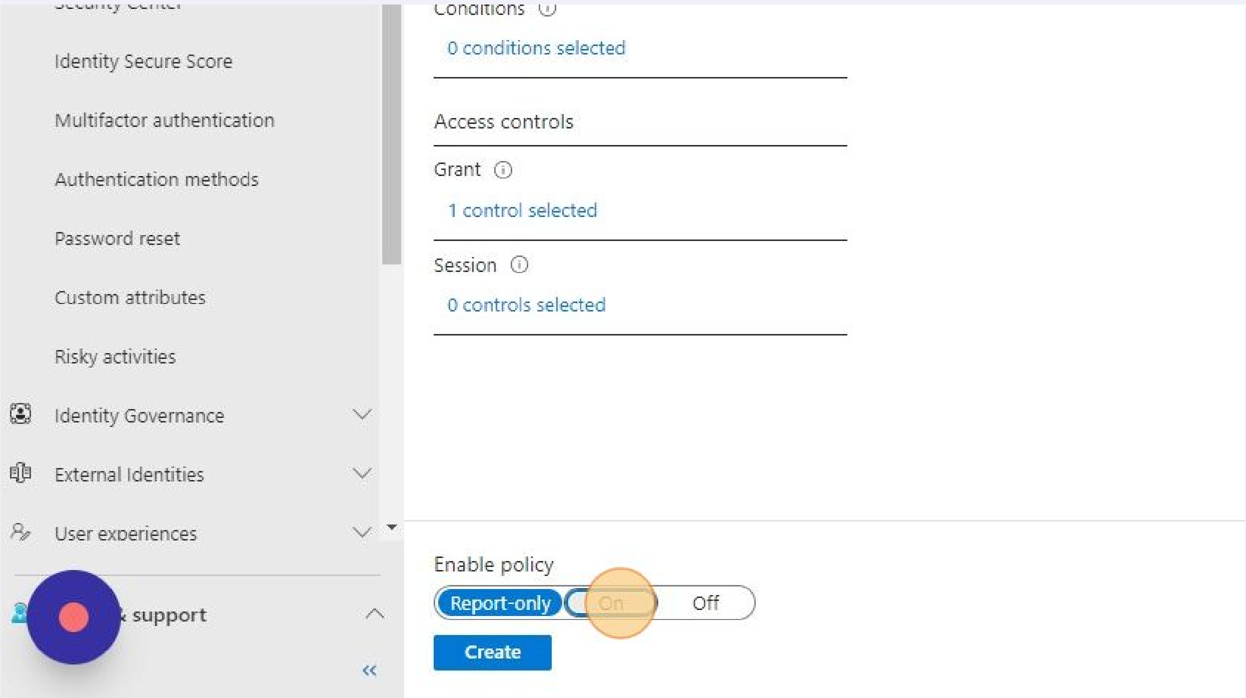
□ Require Hybrid Azure AD joined device

□ Require approved client app
See list of approved client apps

□ Require app protection policy
See list of policy protected client apps

□ AzureAD_ToS

17 Select "On" to enable the policy immediately.



Conditions
0 conditions selected

Access controls

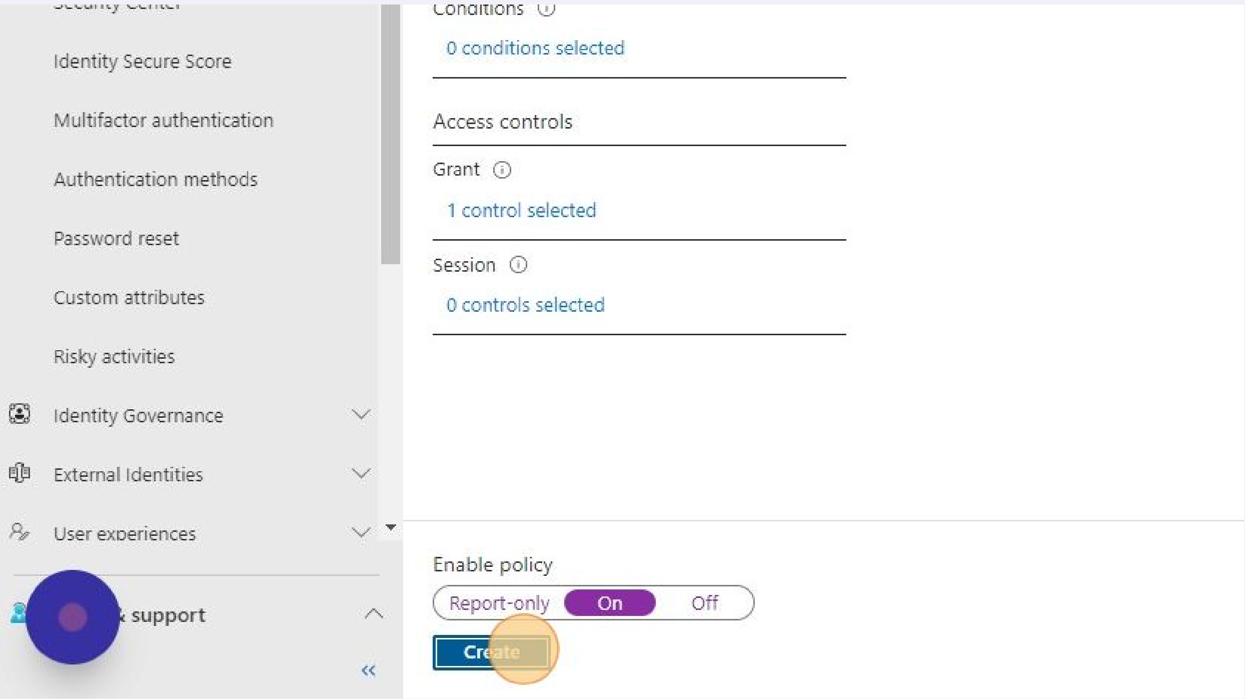
Grant
1 control selected

Session
0 controls selected

Enable policy
Report-only | On | Off

Alert!
If you want to see how a rule would perform before enforcing it, choose "Report-only"

**18** Click "Create" to finish creating the policy.



Conditions

0 conditions selected

Access controls

Grant

1 control selected

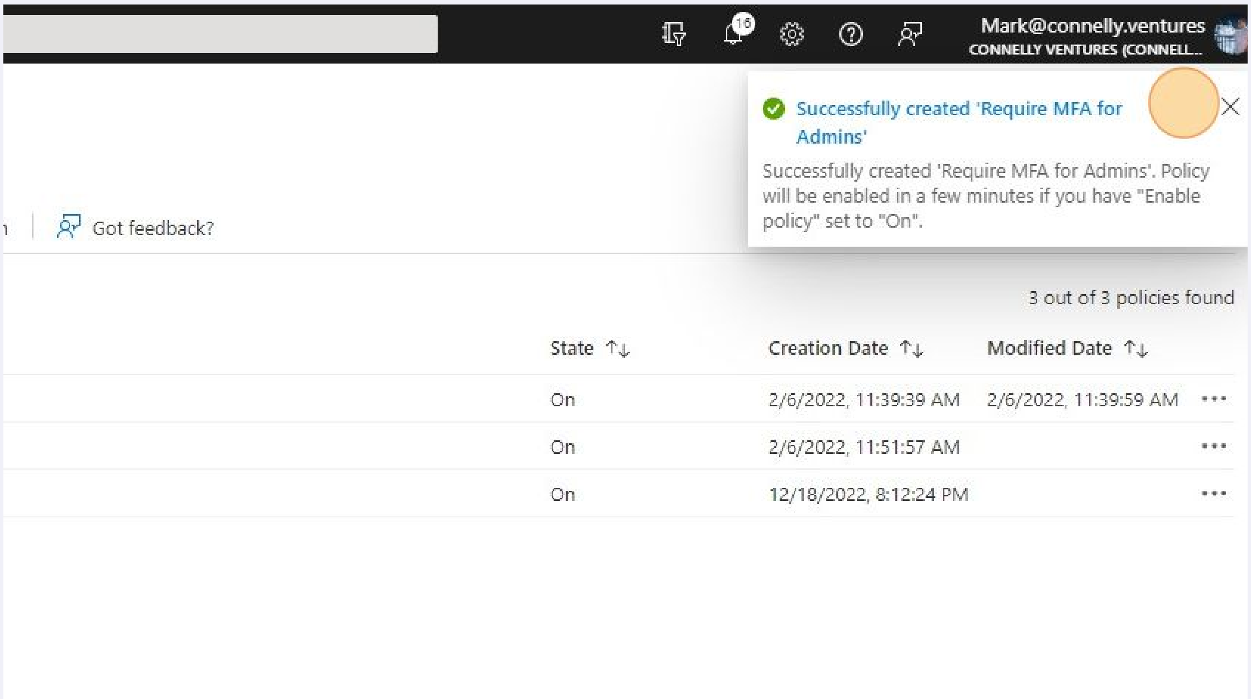
Session

0 controls selected

Enable policy

Report-only | On | Off

19 You should see a notification that the policy was created successfully.



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

Successfully created 'Require MFA for Admins'

Successfully created 'Require MFA for Admins'. Policy will be enabled in a few minutes if you have "Enable policy" set to "On".

Got feedback?

3 out of 3 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 | | ••• |