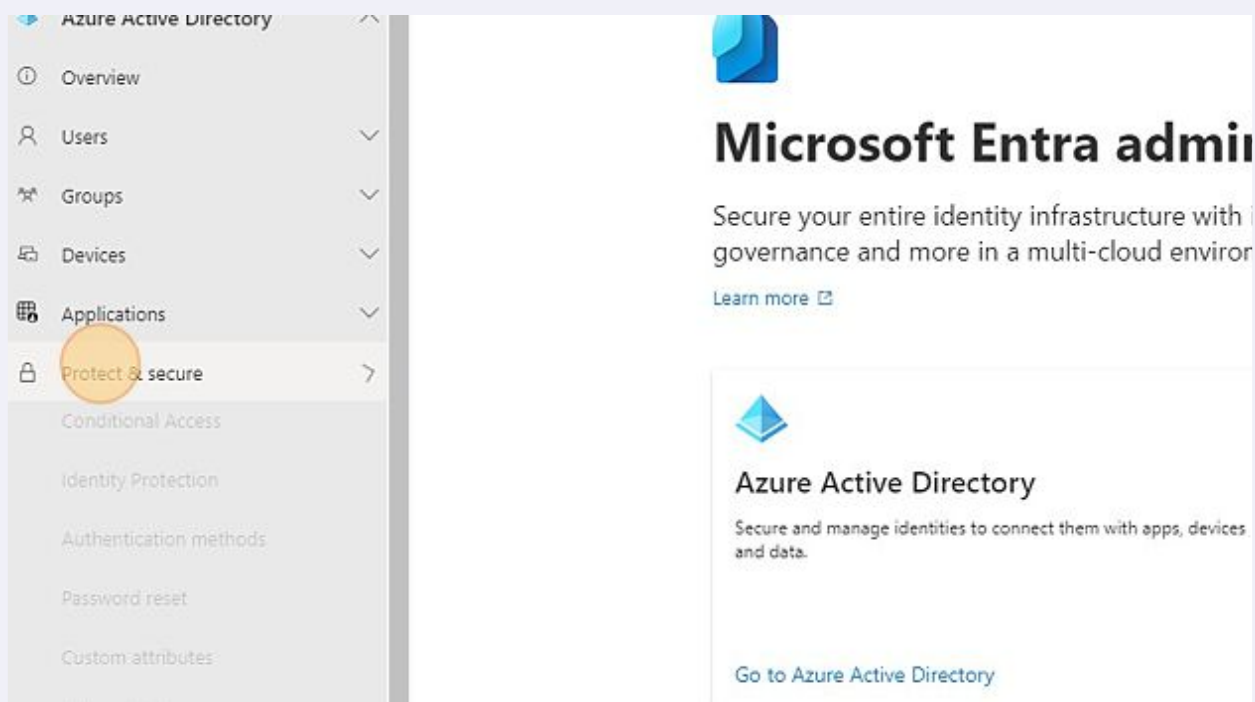


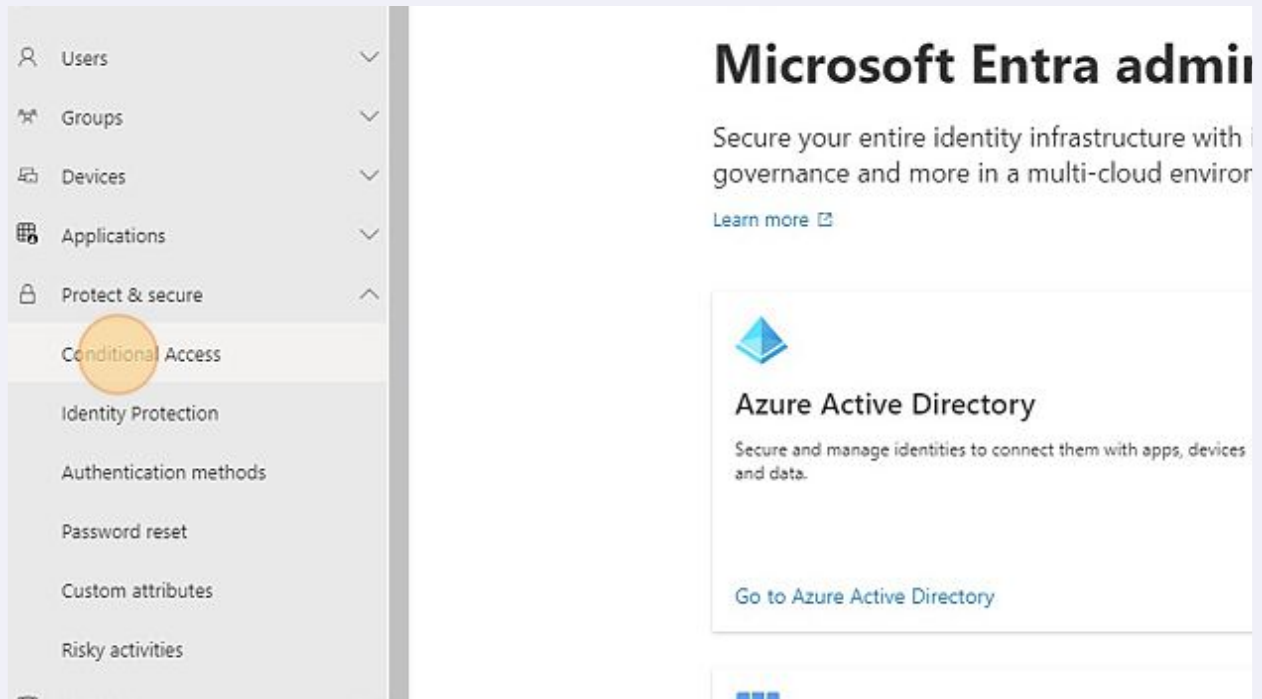
How to Configure "Require MFA Off-Net" Conditional Access Policy

1 Navigate to entra.microsoft.com

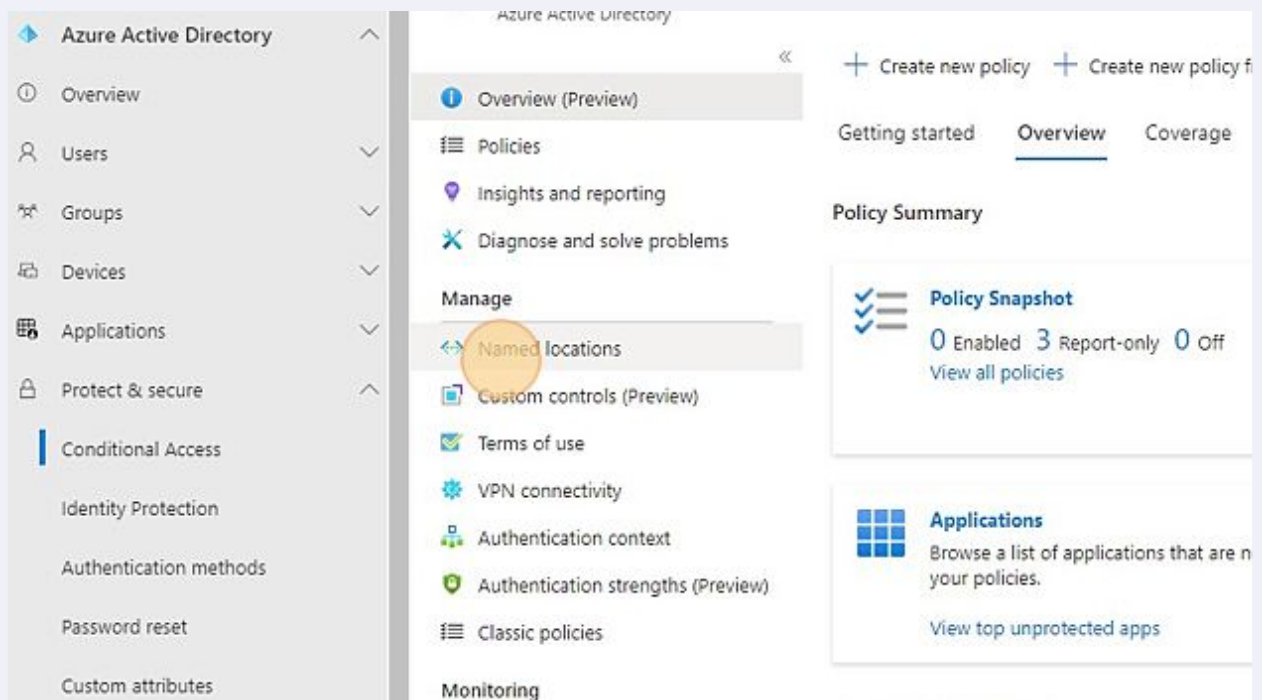
2 Click "Protect & secure"



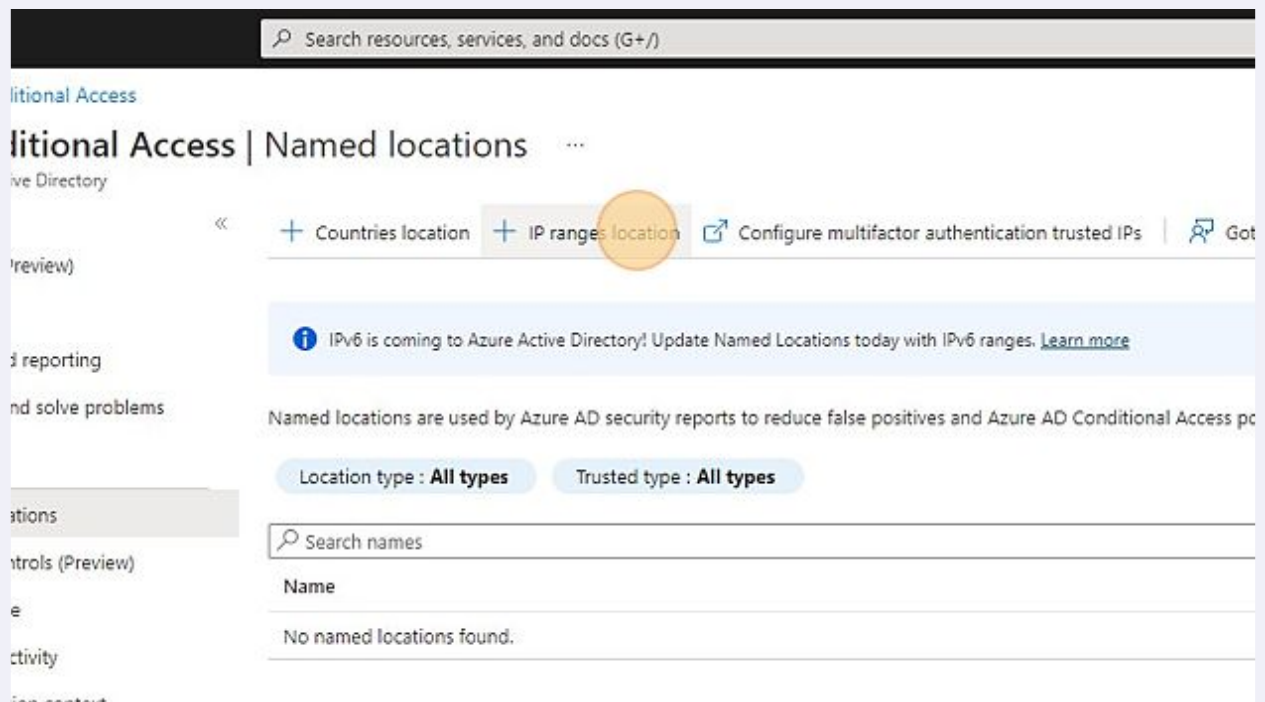
3 Click "Conditional Access"



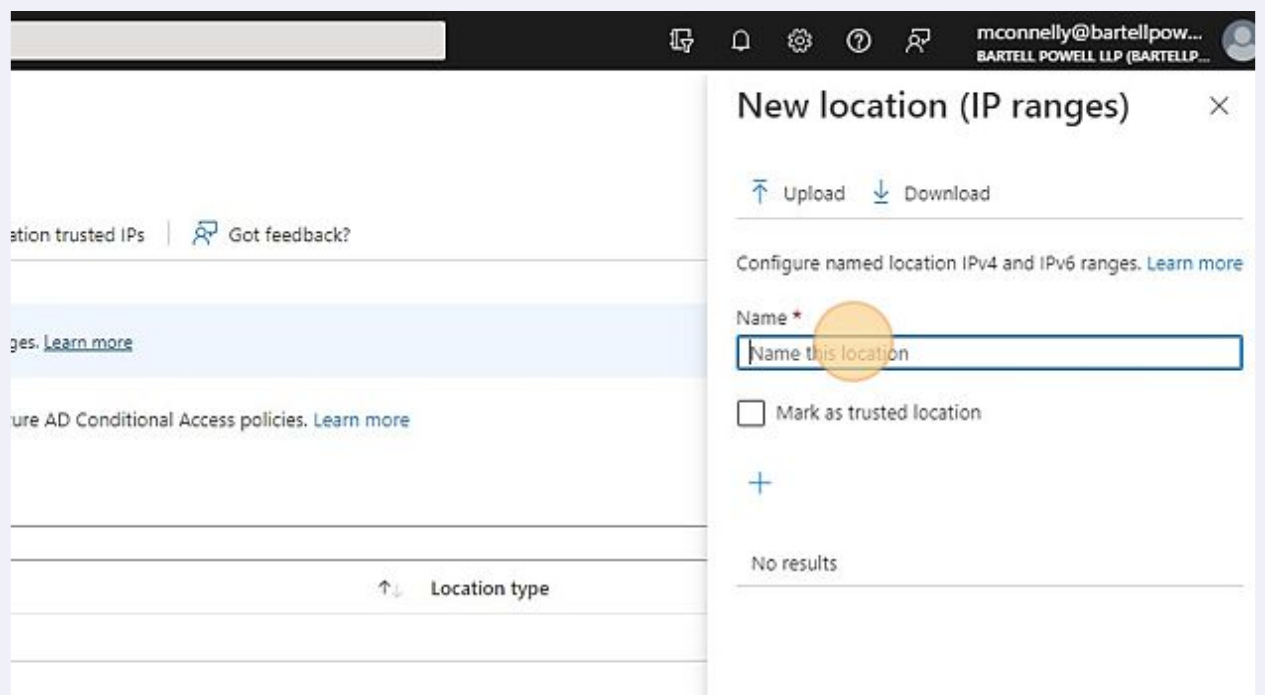
4 Click "Named locations"



5 Click here.



6 Enter "HQ Office" in the "Name" field.



7 Mark this location as a "Trust Location"

The screenshot shows the 'New location (IP ranges)' dialog box. The 'Name' field is set to 'HQ Office'. The checkbox 'Mark as trusted location' is checked and highlighted with an orange circle. The background shows a table with a 'Location type' header and a 'Got feedback?' link.

ation trusted IPs | [Got feedback?](#)

ges. [Learn more](#)

ure AD Conditional Access policies. [Learn more](#)

Location type

New location (IP ranges) ×

[↑](#) Upload [↓](#) Download

Configure named location IPv4 and IPv6 ranges. [Learn more](#)

Name *
HQ Office ✓

☒ Mark as trusted location

+

No results

8 Click the "+" icon to add an IP address

The screenshot shows the 'New location (IP ranges)' dialog box. The 'Name' field is set to 'HQ Office'. The checkbox 'Mark as trusted location' is checked. The '+' icon is highlighted with an orange circle. The background shows a table with a 'Location type' header and a 'Got feedback?' link.

ation trusted IPs | [Got feedback?](#)

ges. [Learn more](#)

ure AD Conditional Access policies. [Learn more](#)

Location type

New location (IP ranges) ×

[↑](#) Upload [↓](#) Download

Configure named location IPv4 and IPv6 ranges. [Learn more](#)

Name *
HQ Office ✓

☒ Mark as trusted location

+

No results

9 Enter the WAN IP address of your office.

The screenshot shows the Azure portal interface for configuring a named location. On the left, a table lists existing locations with columns for Name, Location type, and a plus icon for adding more. The right-hand pane is titled "Configure named location IPv4 and IPv6 ranges. [Learn more](#)". It contains a "Name" field with the value "HQ Office" and a checkmark icon. Below this is a checkbox labeled "Mark as trusted location" which is checked. A plus icon is visible below the checkbox. A modal dialog titled "Enter a new IPv4 or IPv6 range" is open, showing a text input field with the example "ex: 40.77.182.32/27 or 2a01:111::/32" and two buttons: "Add" and "Cancel".

Name	Location type	
		+

Configure named location IPv4 and IPv6 ranges. [Learn more](#)

Name *
HQ Office ✓

☒ Mark as trusted location

+

Enter a new IPv4 or IPv6 range

ex: 40.77.182.32/27 or 2a01:111::/32

Add Cancel



Alert!

Be very specific in scoping your WAN IP address. If your WAN is on DHCP, you may need to include a broad range, like a /24. If you have a static public IP address, you can enter it as a /32.

10 Click "Add"

ions today with IPv6 ranges. [Learn more](#)

false positives and Azure AD Conditional Access policies. [Learn more](#)

Location type

Enter a new IPv4 or IPv6

/32

Add

Cancel

11 Click "Create"

Create

12 Click "Policies"

The screenshot shows the Microsoft Entra admin center interface. The left-hand navigation pane is expanded, showing the 'Conditional Access' section. The 'Policies' link is highlighted with a yellow circle. The main content area displays the 'Conditional Access | Named locations' page, which includes a search bar, a list of named locations, and a 'Manage' section with links to 'Named locations', 'Custom controls (Preview)', 'Terms of use', and 'VPN connectivity'.

13 Click "New Policy"

The screenshot shows the Microsoft Entra admin center interface. The left-hand navigation pane is expanded, showing the 'Conditional Access' section. The 'Policies' link is highlighted. The main content area displays the 'Conditional Access | Policies' page, which includes a search bar, a list of policies, and a 'Manage' section with links to 'Named locations', 'Custom controls (Preview)', 'Terms of use', and 'VPN connectivity'. The 'New policy' button is highlighted with a yellow circle.

14 Enter "Require MFA Off-Net" in the "Name" field.

Home > Conditional Access | Policies >

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 *

Example: 'Device compliance app policy'

Assignments

Users ⓘ

0 users and groups selected

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

15 Select "Users"

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

Name *

Require MFA Off-Net ✓

Assignments

Users ⓘ

0 users and groups selected

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

16 Click "Select users and groups"

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 Off-Net ✓

Assignments

Users ⓘ

0 users and groups selected

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

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

Include Exclude

☒ None

☐ All users

☒ Select users and groups

17 Click "All Users"

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 Off-Net ✓

Assignments

Users ⓘ

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

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

Include Exclude

☐ None

☒ All users

☒ Select users and groups

☐ Guest or external users ⓘ

☐ Directory roles ⓘ

☐ Users and groups

18 Click "Exclude"

Home > Conditional Access | Policies >

New

Conditional Access policy

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

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

Name *

Require MFA Off-Net ✓

Assignments

Users ⓘ

All users

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

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. [Learn more](#)

19 Exclude your Break Glass Admin account.

Search

3H

AD

AU All Users

AZ Azure.BreakGlass.Admin
Azure.BreakGlass.Admin@

AZ Azure.MFA.Excluded

BP

Selected items

No items selected

20 Click "Cloud apps"

Name *

Require MFA Off-Net ✓

Assignments

Users ⓘ

All users included and specific users excluded

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

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. [Learn more](#)

21 Click "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 Off-Net ✓

Assignments

Users ⓘ

All users included and specific users excluded

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

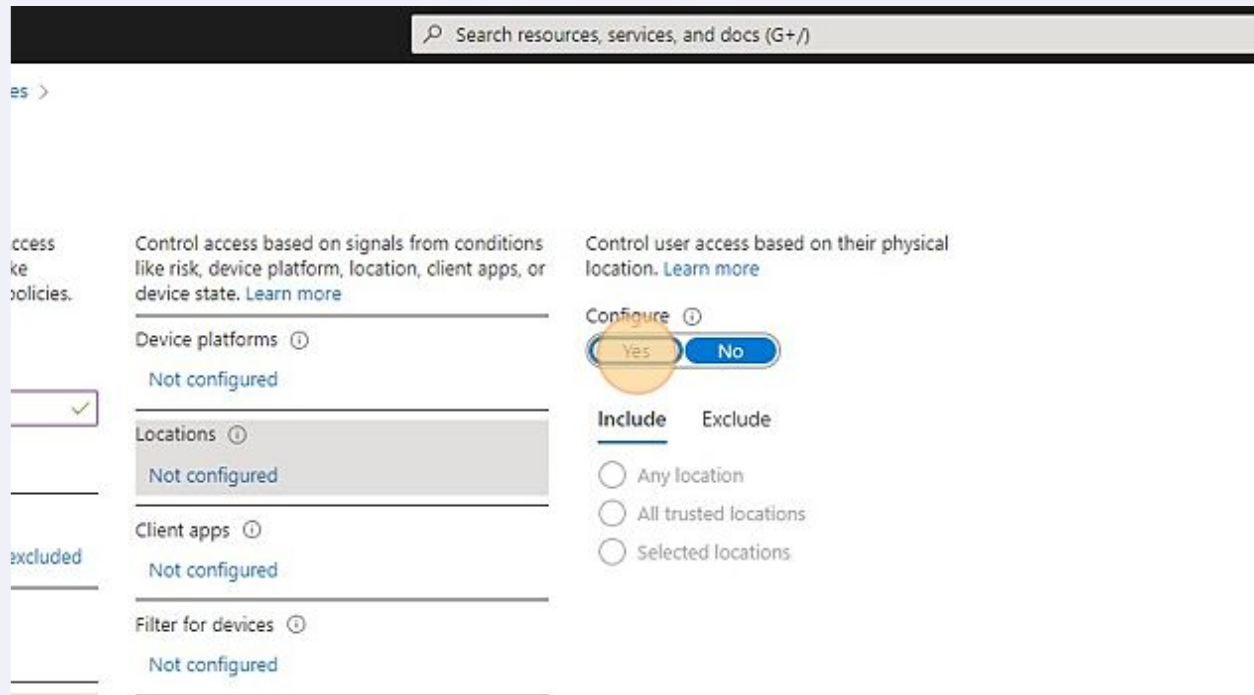
☒ All cloud apps

☐ Select apps

22

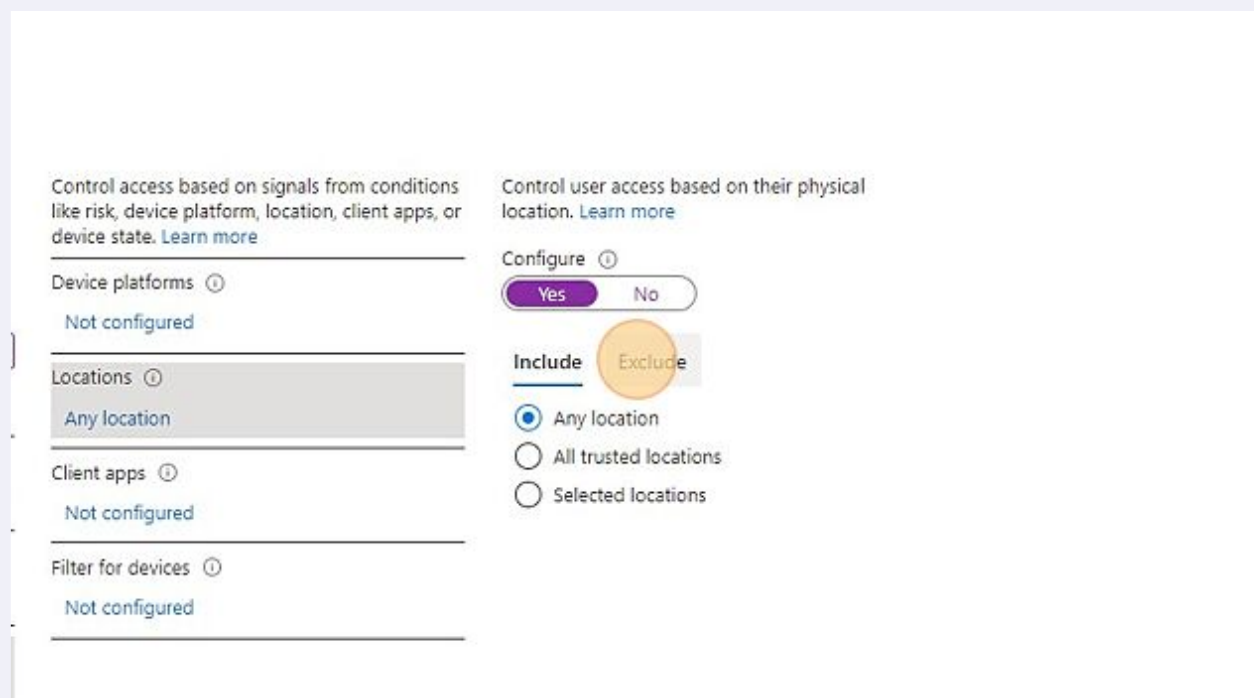
Click "Conditions" > "Locations"

Include "All Locations"



23

Click "Exclude"



24 Click "Select" to choose a location to exclude.

The screenshot shows a 'Configure' dialog box with several sections. On the left, there are four sections: 'Device platforms' (Not configured), 'Locations' (Any location), 'Client apps' (Not configured), and 'Filter for devices' (Not configured). The 'Locations' section is highlighted. On the right, there are two tabs: 'Include' and 'Exclude', with 'Exclude' selected. Below the tabs, there is a text input field with the placeholder 'Select' and a dropdown menu showing 'None'. A yellow circle highlights the 'Select' text.

25 Select "HQ Office"

The screenshot shows a 'Select' dialog box for 'Locations'. It has two tabs: 'Location type : All types' and 'Trusted type : All types'. Below the tabs is a search bar with the placeholder 'Search names'. Below the search bar is a table with the following columns: 'Name', 'Location type', and 'Trusted type'. The table contains two rows: 'Multifactor authentication trusted IPs' and 'HQ Office'. The 'HQ Office' row is highlighted. A yellow circle highlights the 'HQ Office' row.

Name	Location type	Trusted type
Multifactor authentication trusted IPs	IP ranges	Yes
HQ Office	IP ranges	Yes

26 Click "Grant"

Name *

Require MFA Off-Net ✓

Assignments

Users ⓘ

All users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

27 Click "Require MFA"

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](#)

28 Click "Select"

⚠ "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

- ☐ 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](#)

Select

29 Save the policy and verify it creates successfully.

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

Got feedback?

4 out of 4 policies found

State ↑↓	Creation Date ↑↓	Modified Date ↑↓	
Report-only	2/6/2023, 9:22:04 PM		...
Report-only	2/6/2023, 9:23:39 PM	2/6/2023, 9:24:35 PM	...
Report-only	2/6/2023, 9:59:44 PM		...
Report-only	2/6/2023, 10:21:02 PM		...