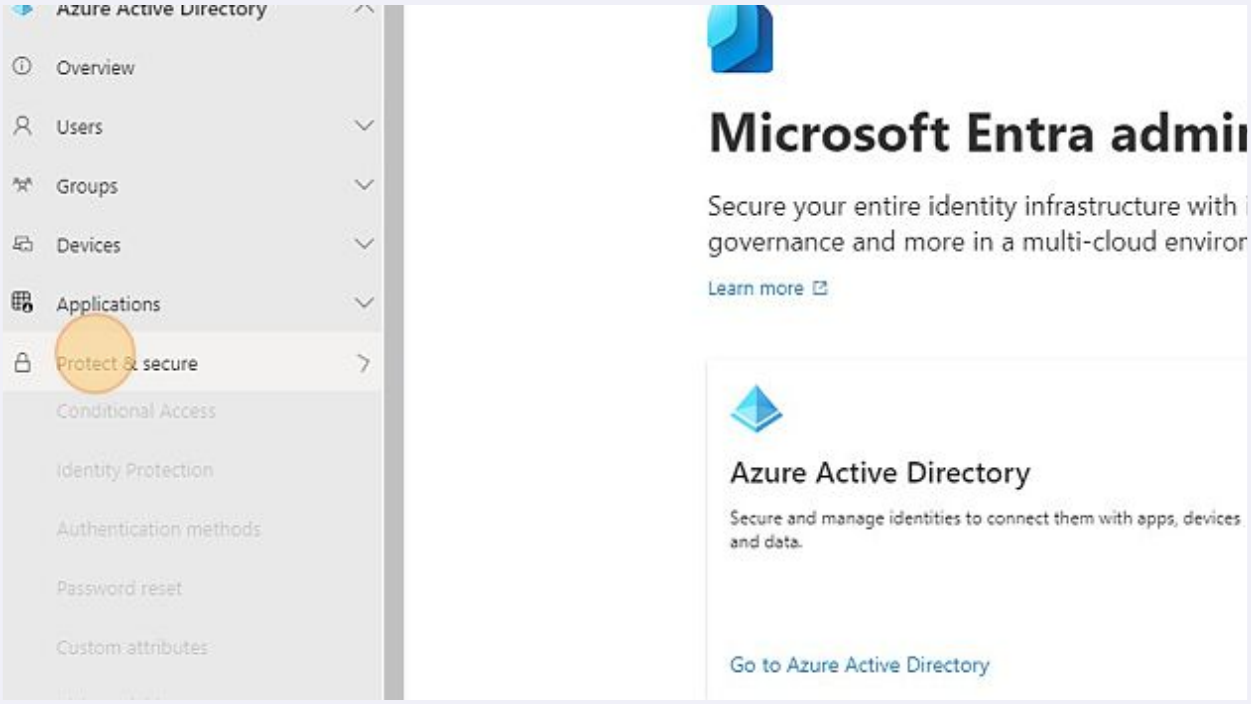
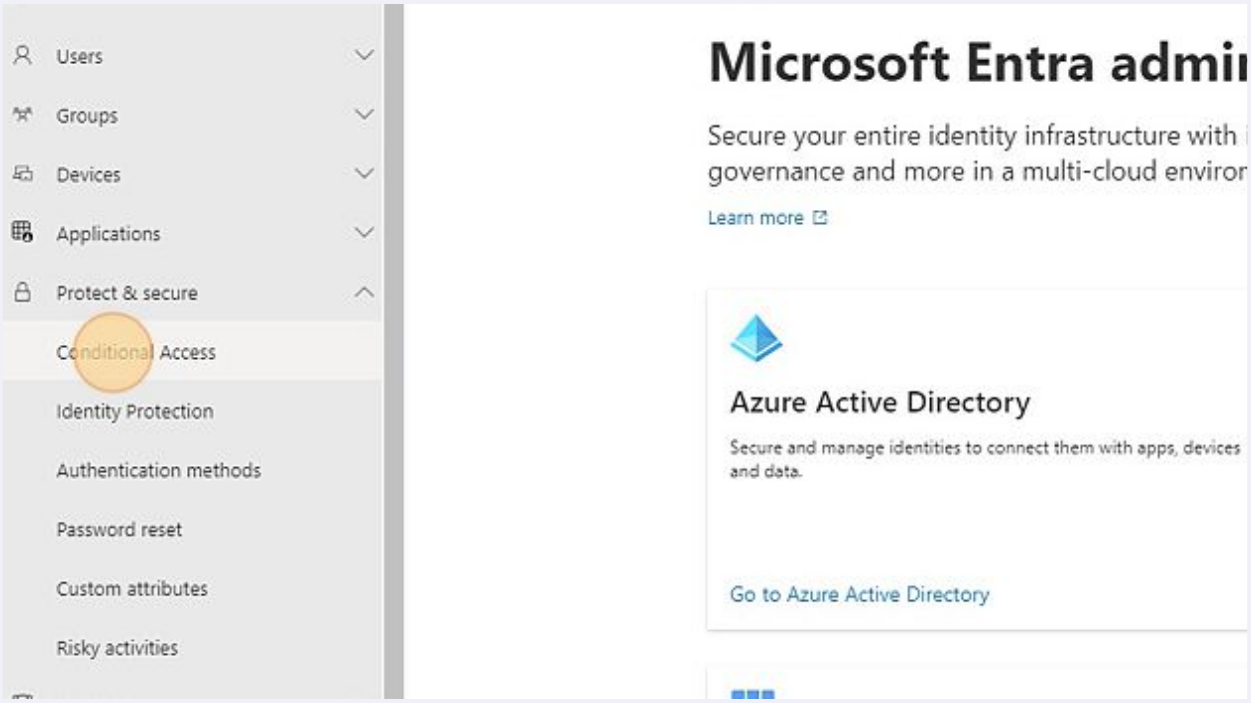
How to Configure "Require MFA Off-Net" Conditional Access Policy

1 Navigate to entra.microsoft.com

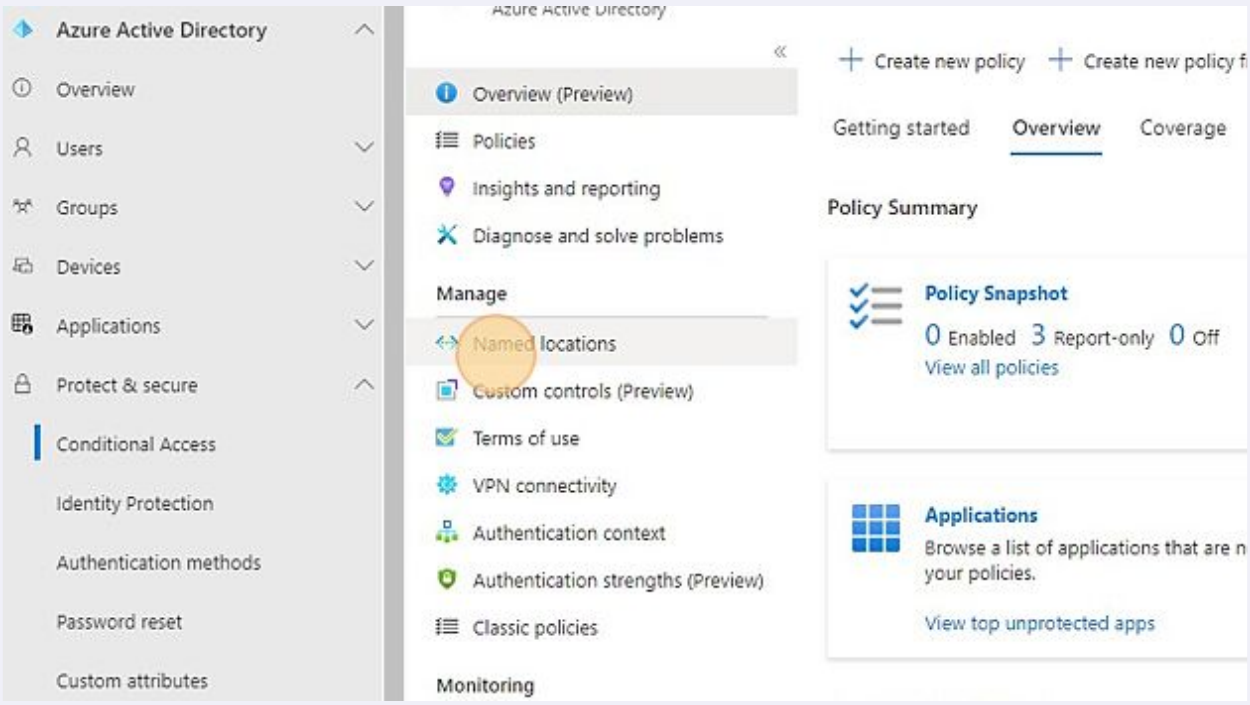
2 Click "Protect & secure"



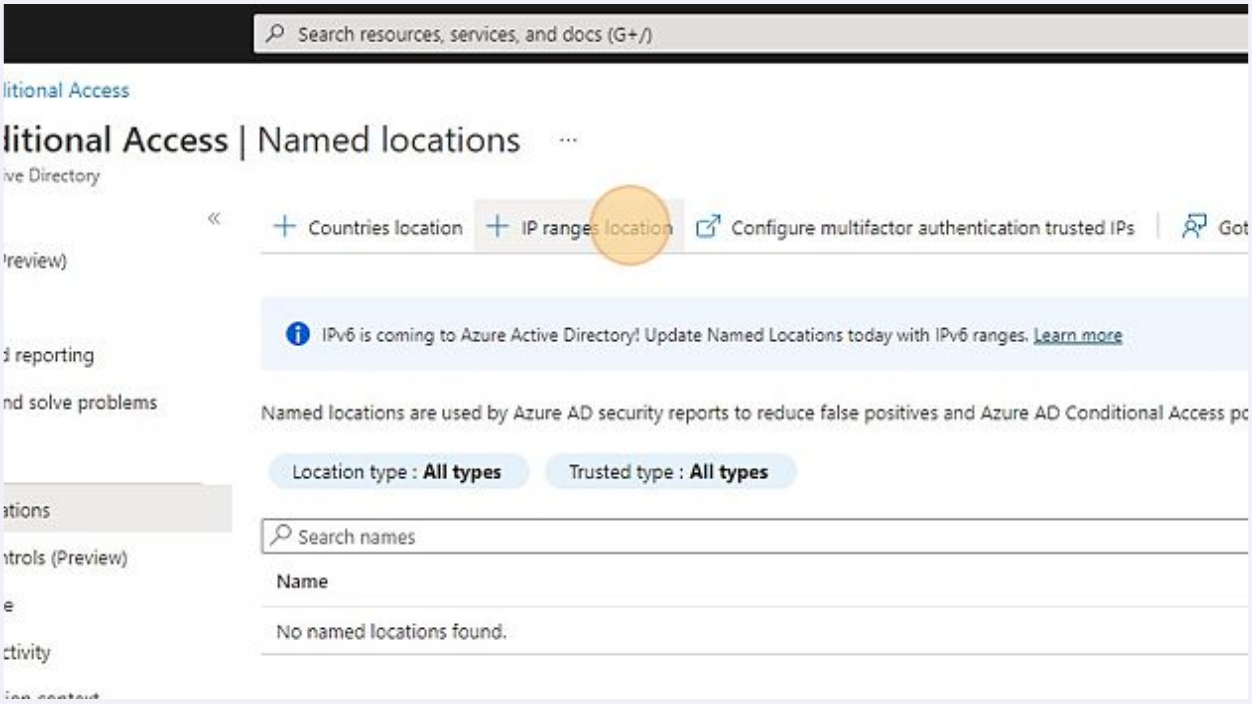
3 Click "Conditional Access"



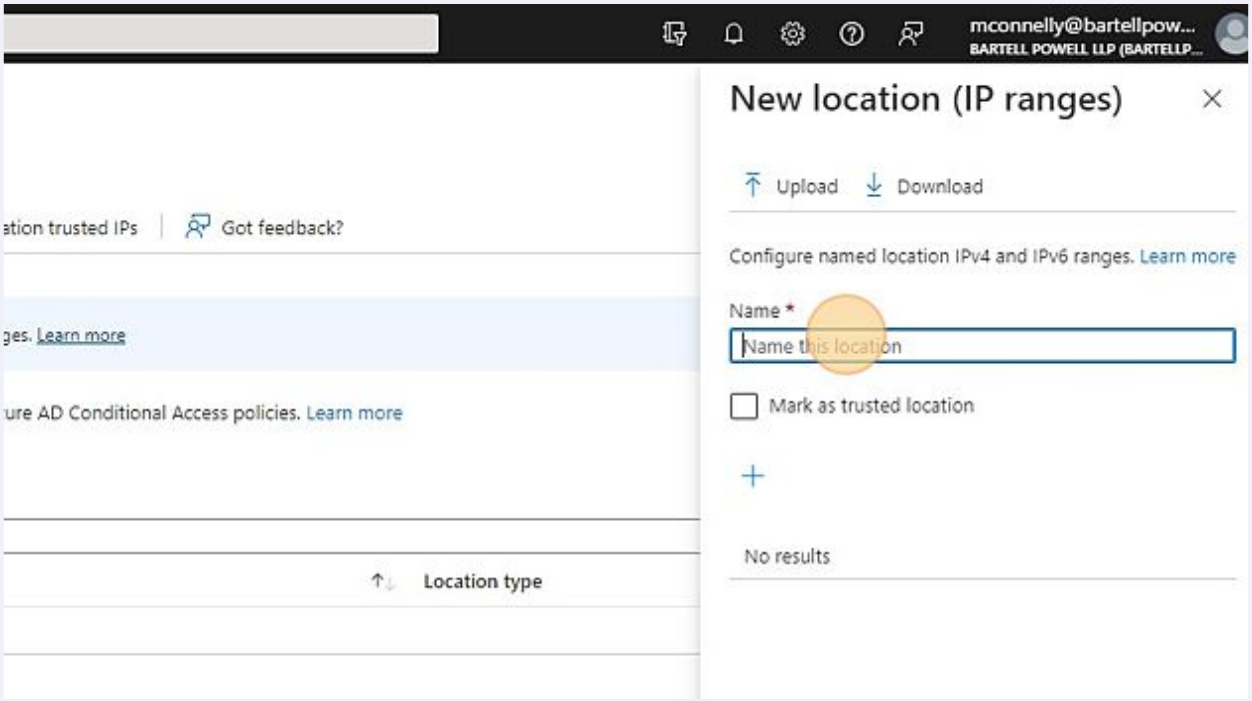
4 Click "Named locations"



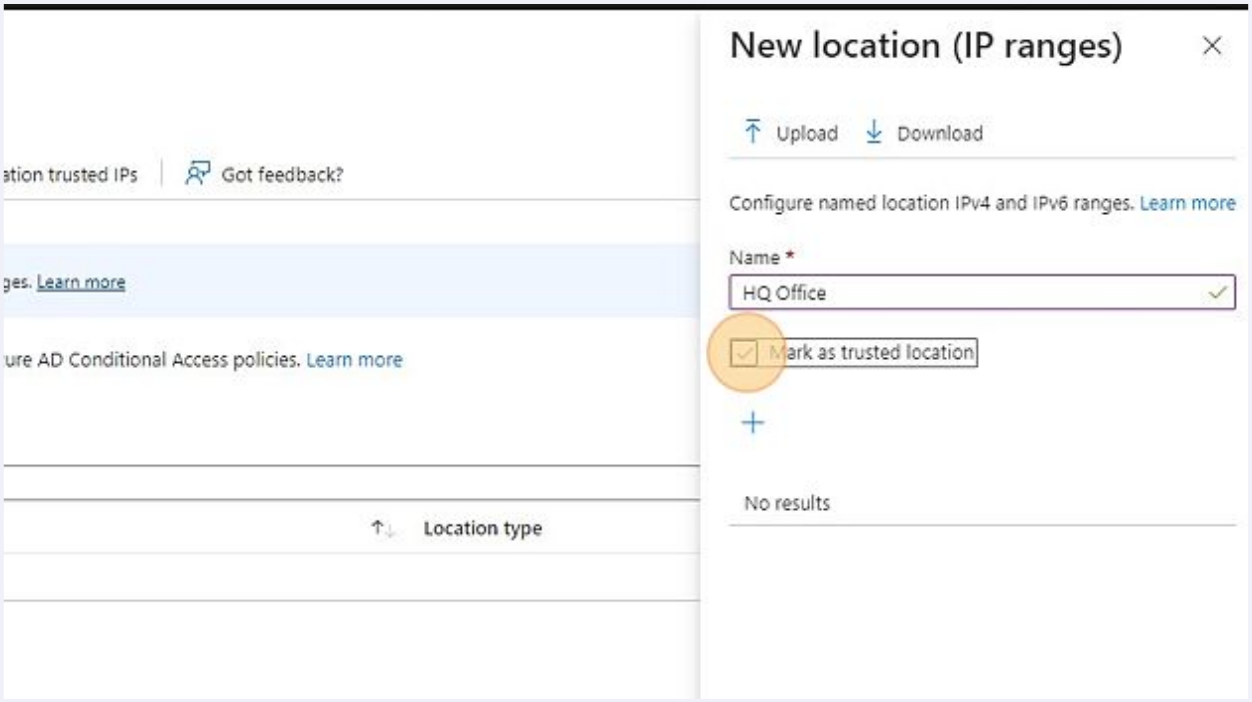
5 Click here.



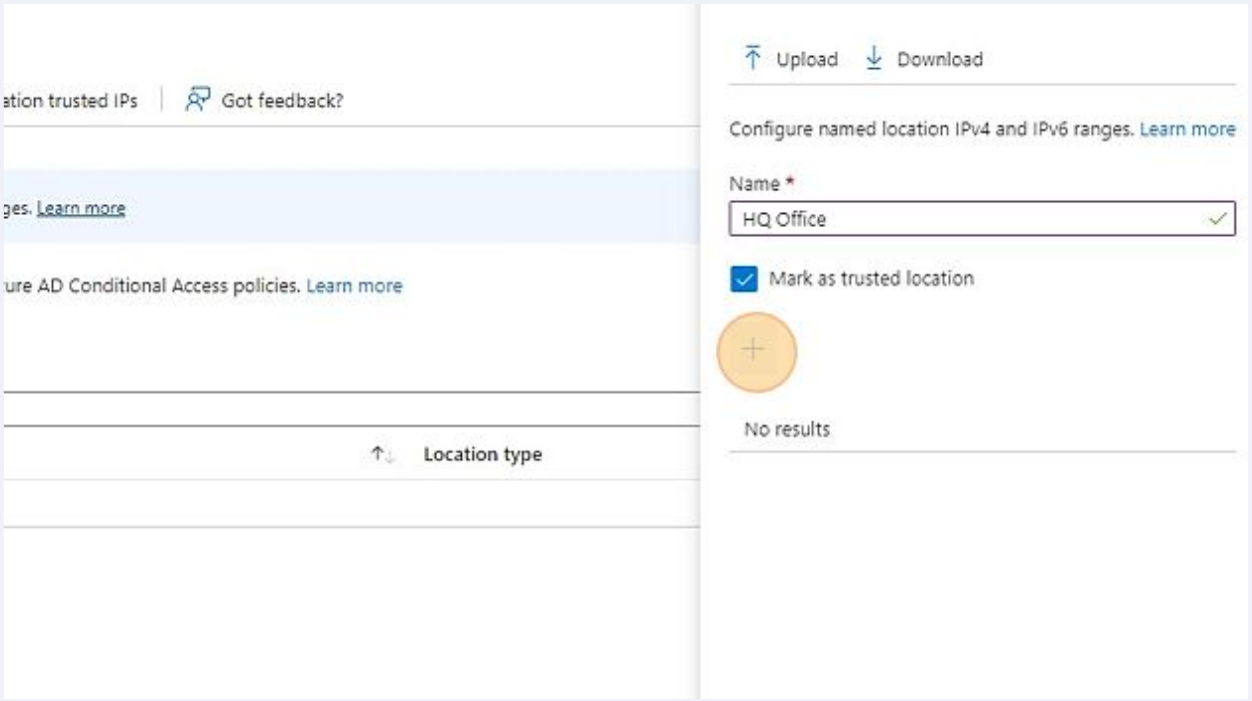
6 Enter "HQ Office" in the "Name" field.



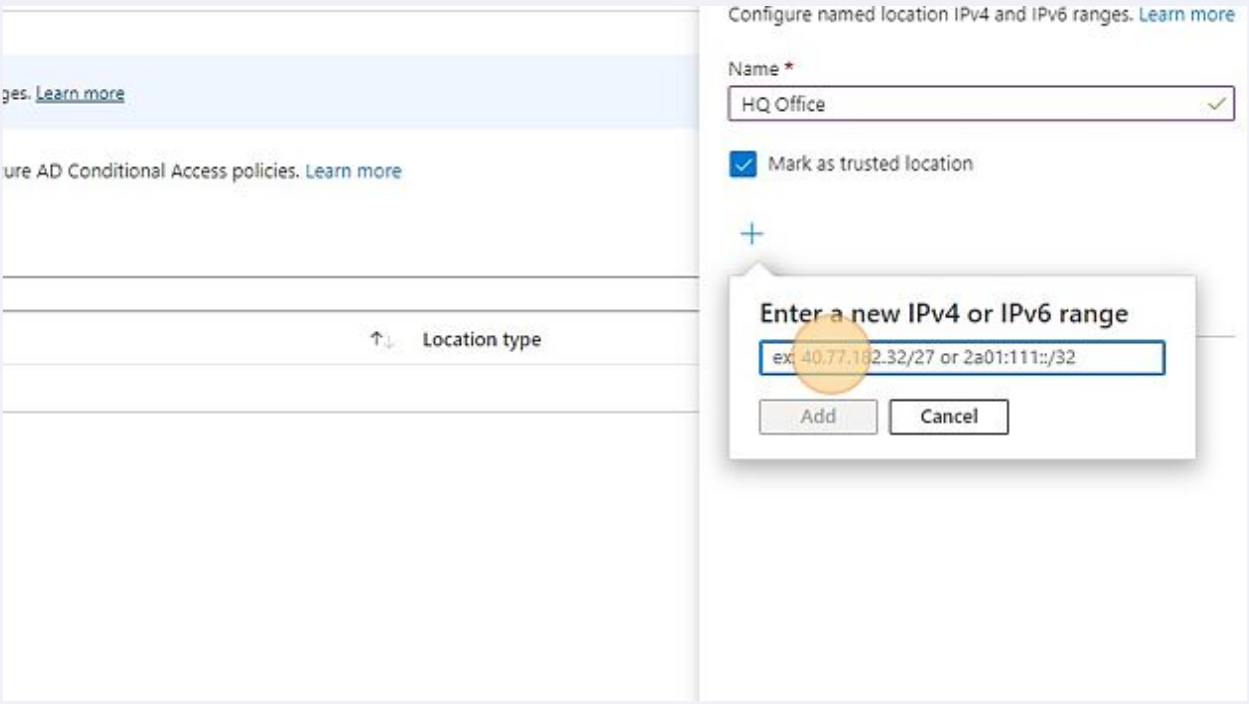
7 Mark this location as a "Trust Location"



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

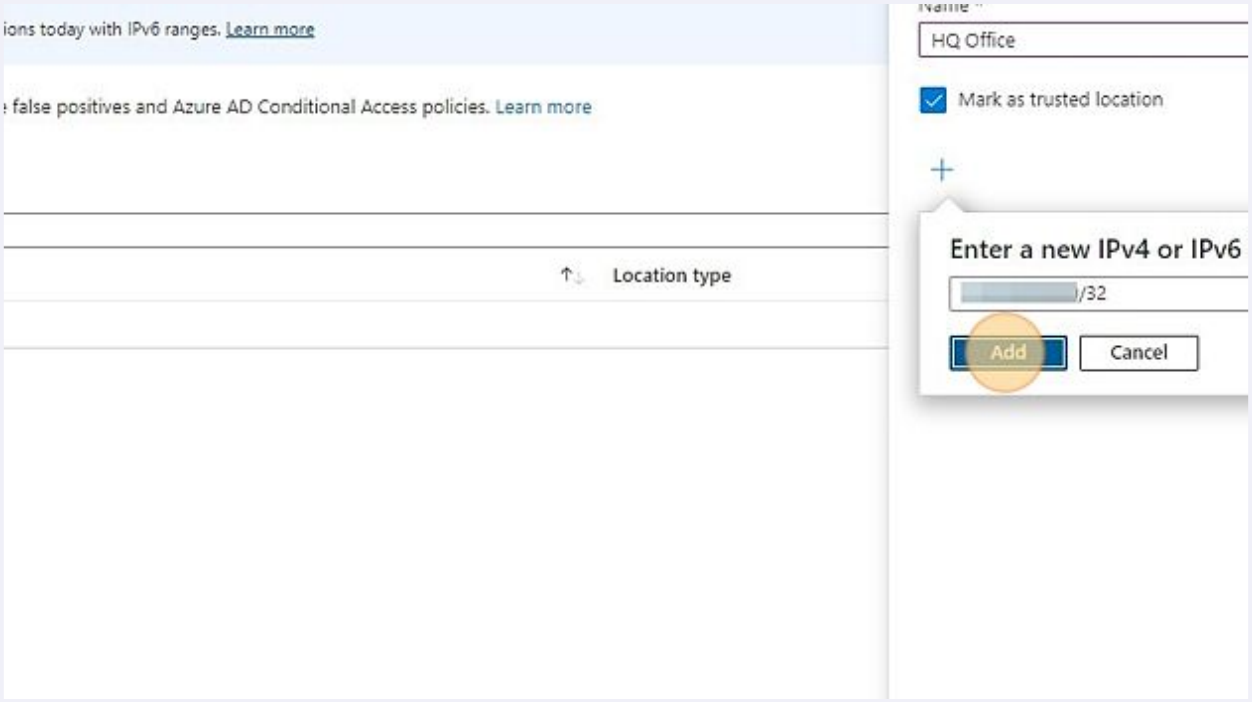


9 Enter the WAN IP address of your office.

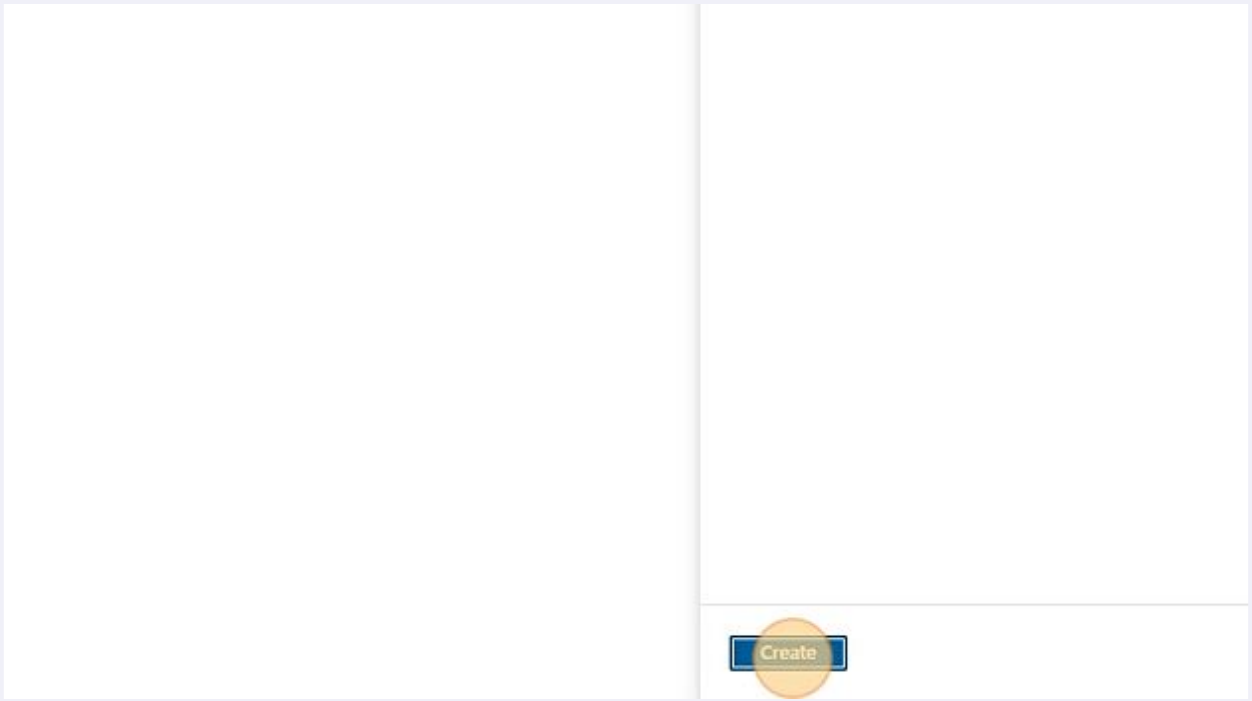


⚠ Alert!
Be very specific in scoping your WAN IP address. If your WAN is on DHCP, you may need to include a broad range, like a /24. If you have a static public IP address, you can enter it as a /32.

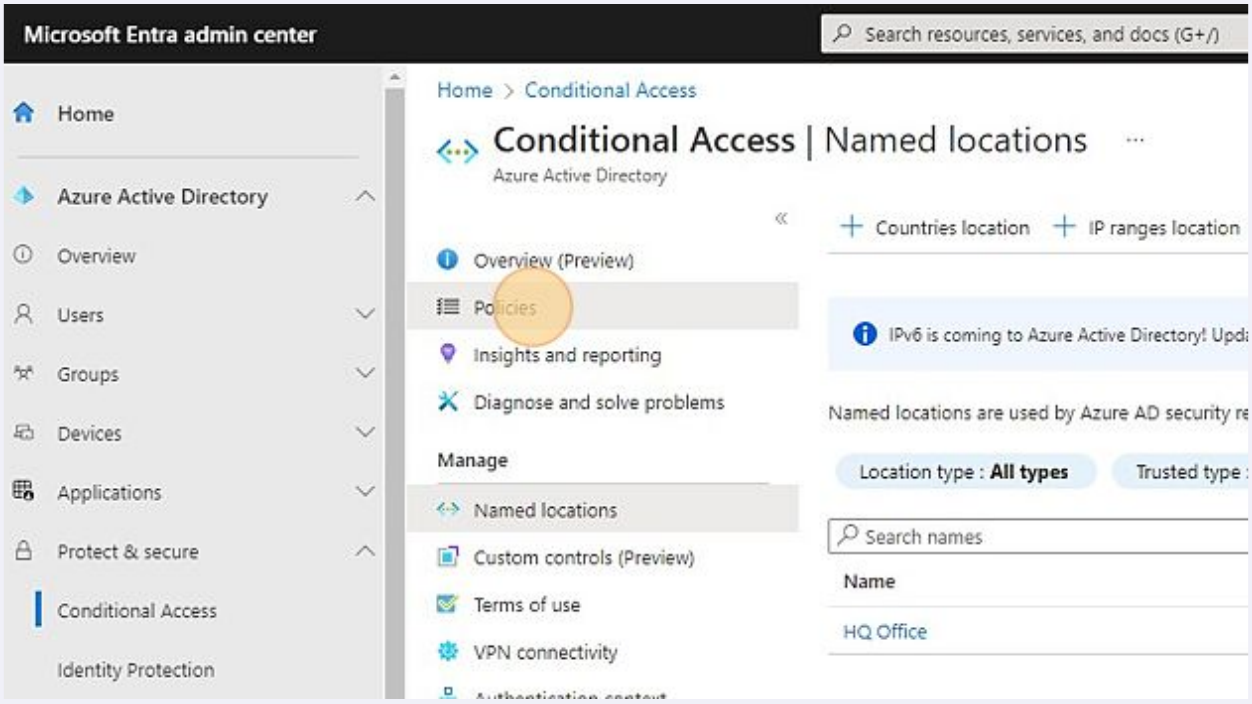
10 Click "Add"



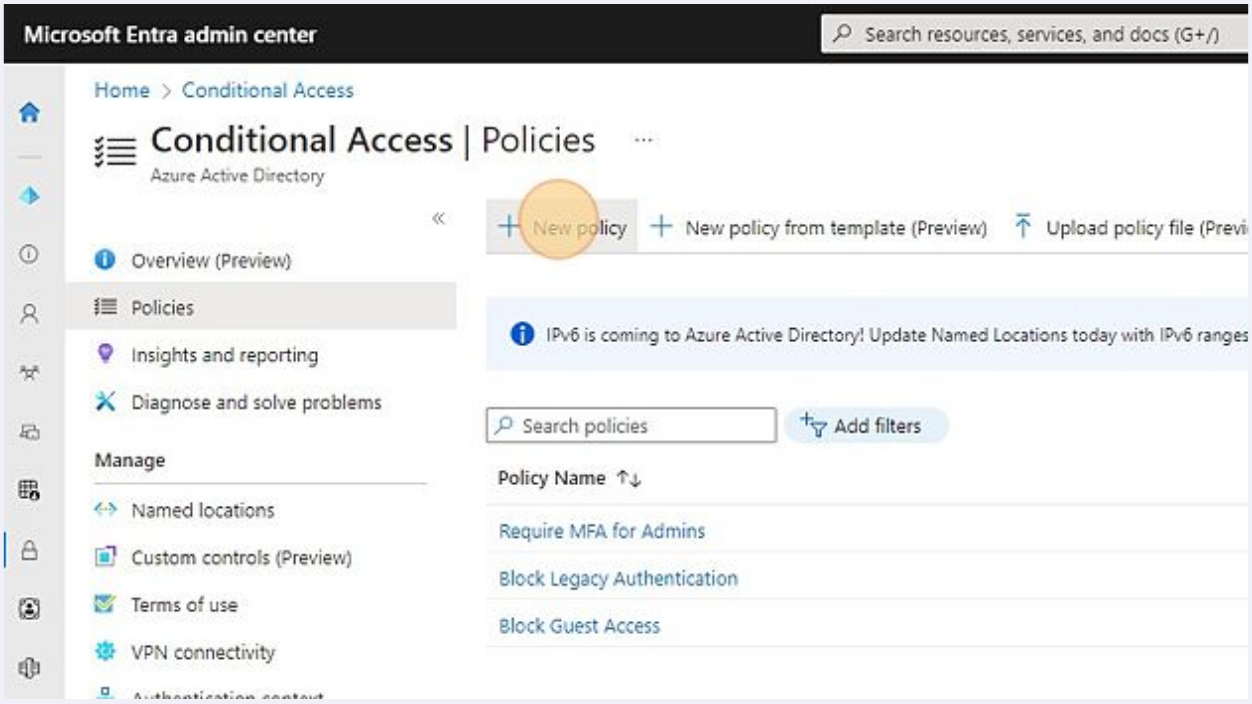
11 Click "Create"



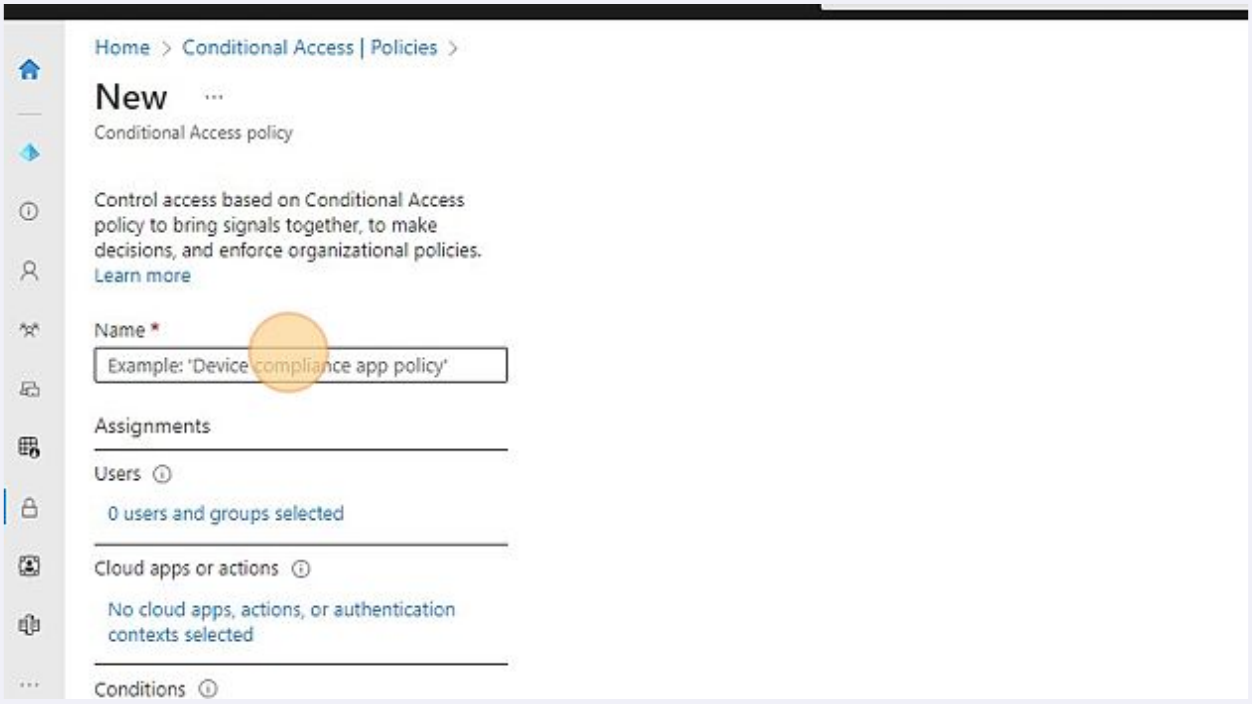
12 Click "Policies"



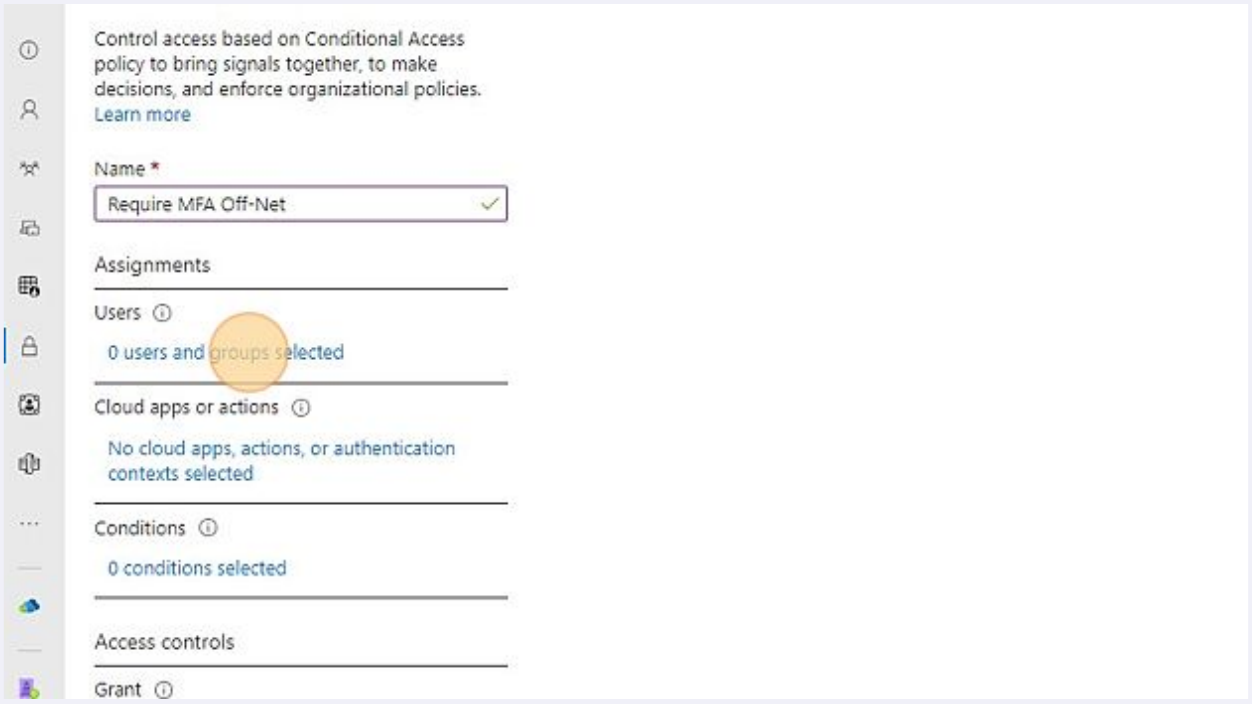
13 Click "New Policy"



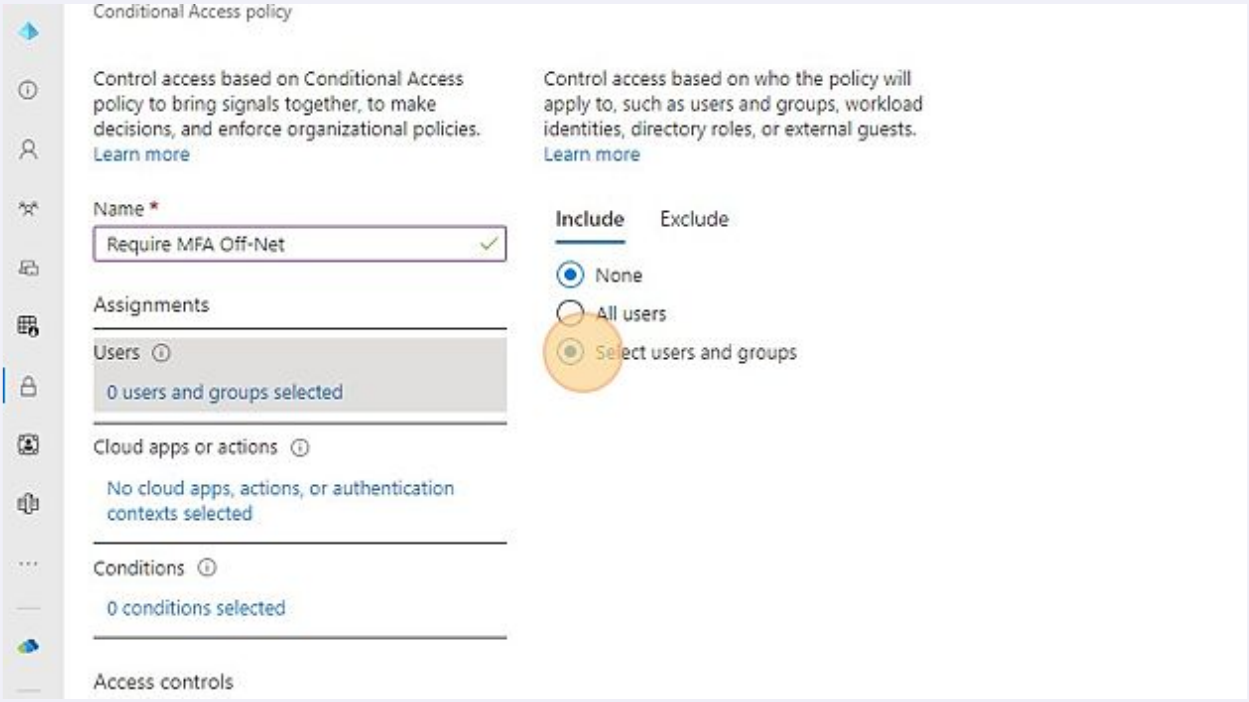
14 Enter "Require MFA Off-Net" in the "Name" field.



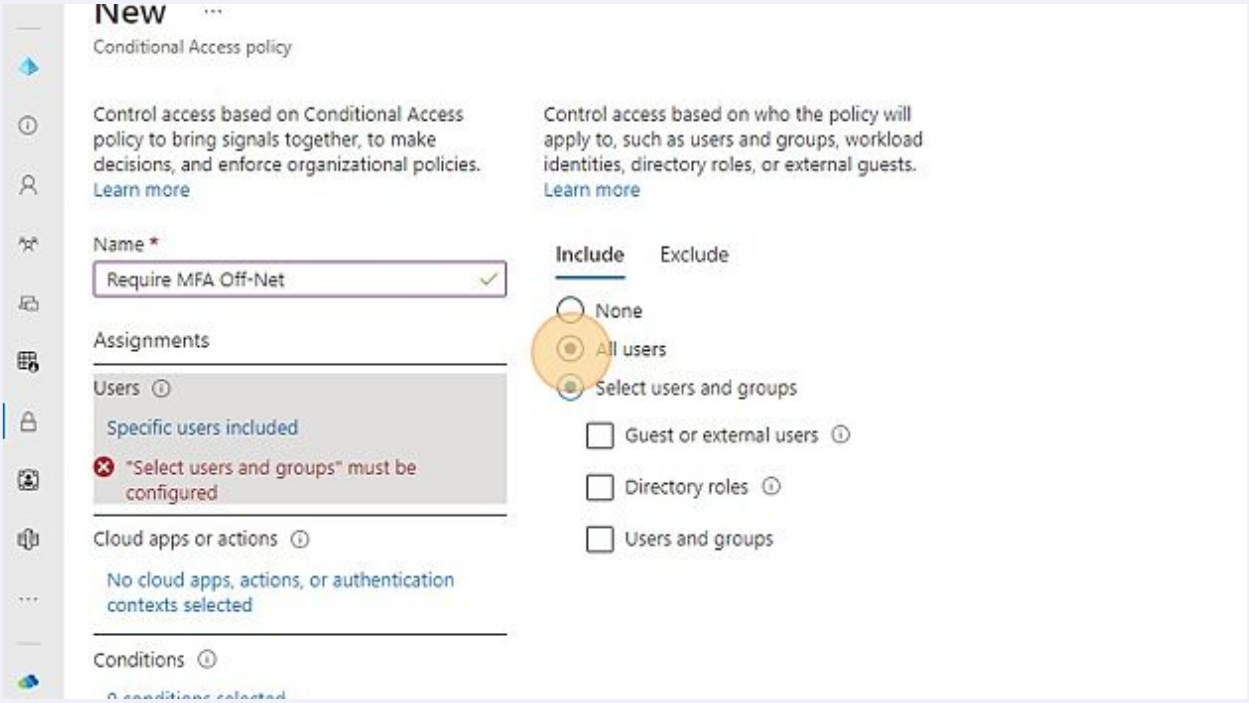
15 Select "Users"



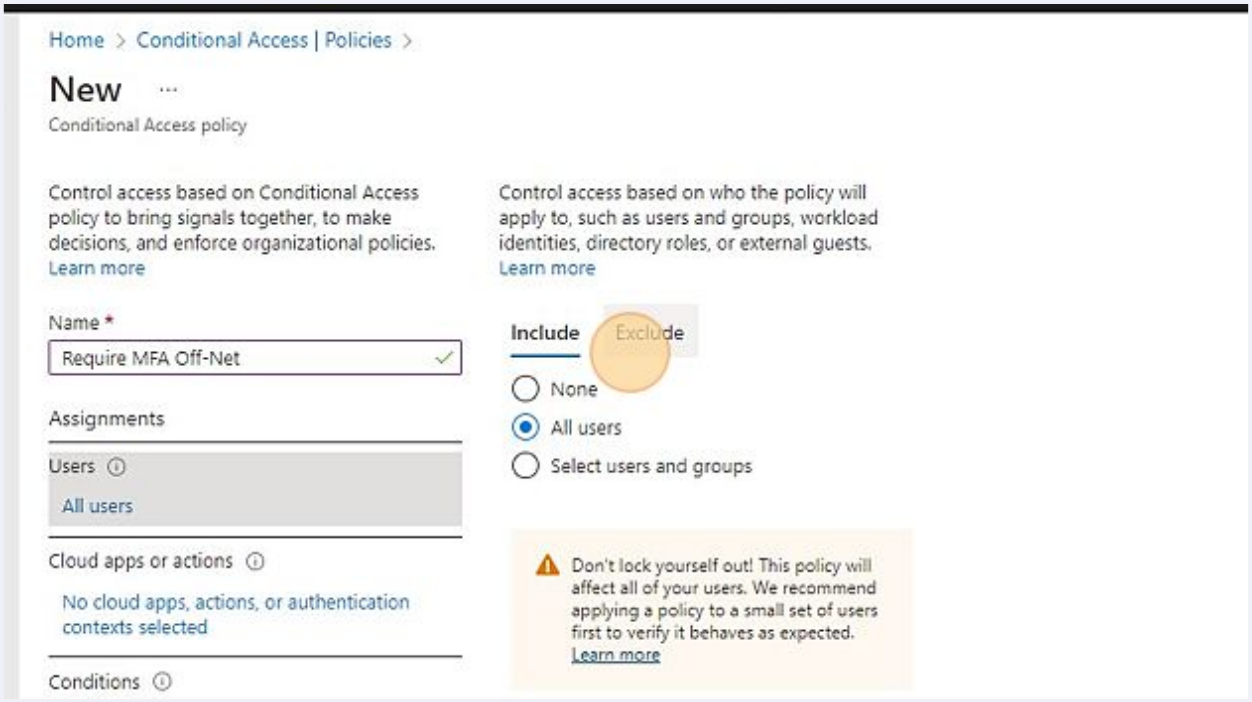
16 Click "Select users and groups"



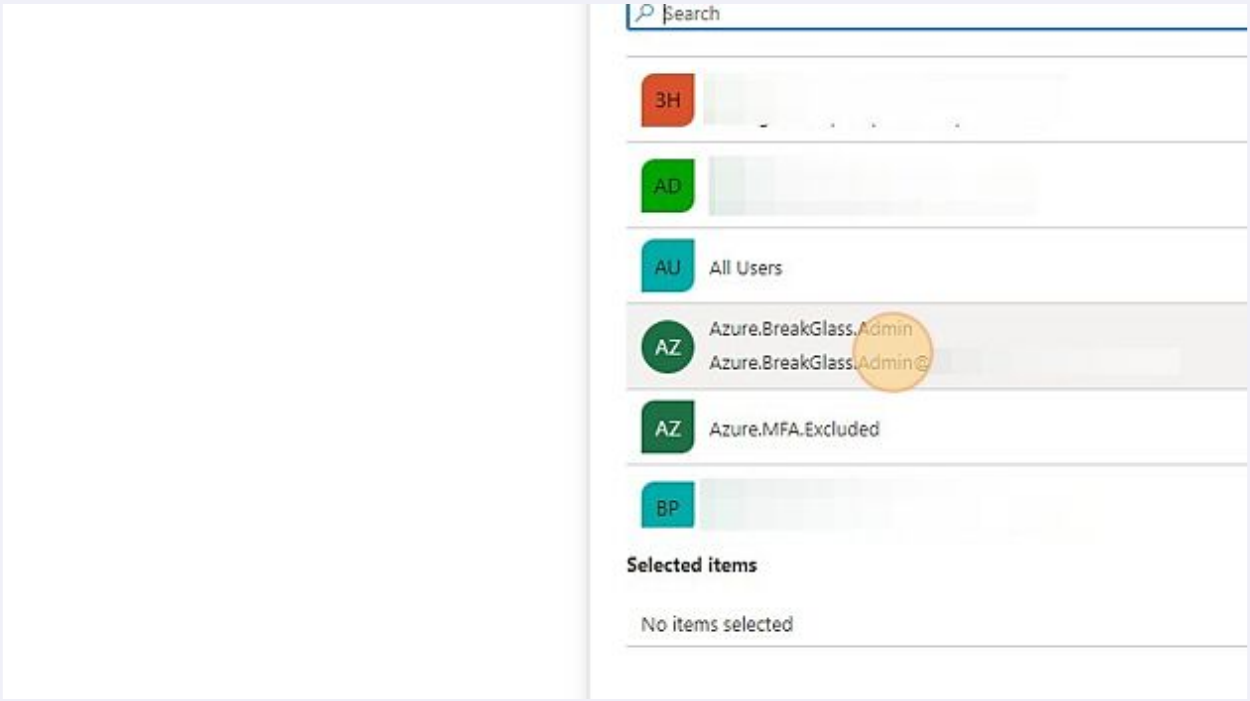
17 Click "All Users"



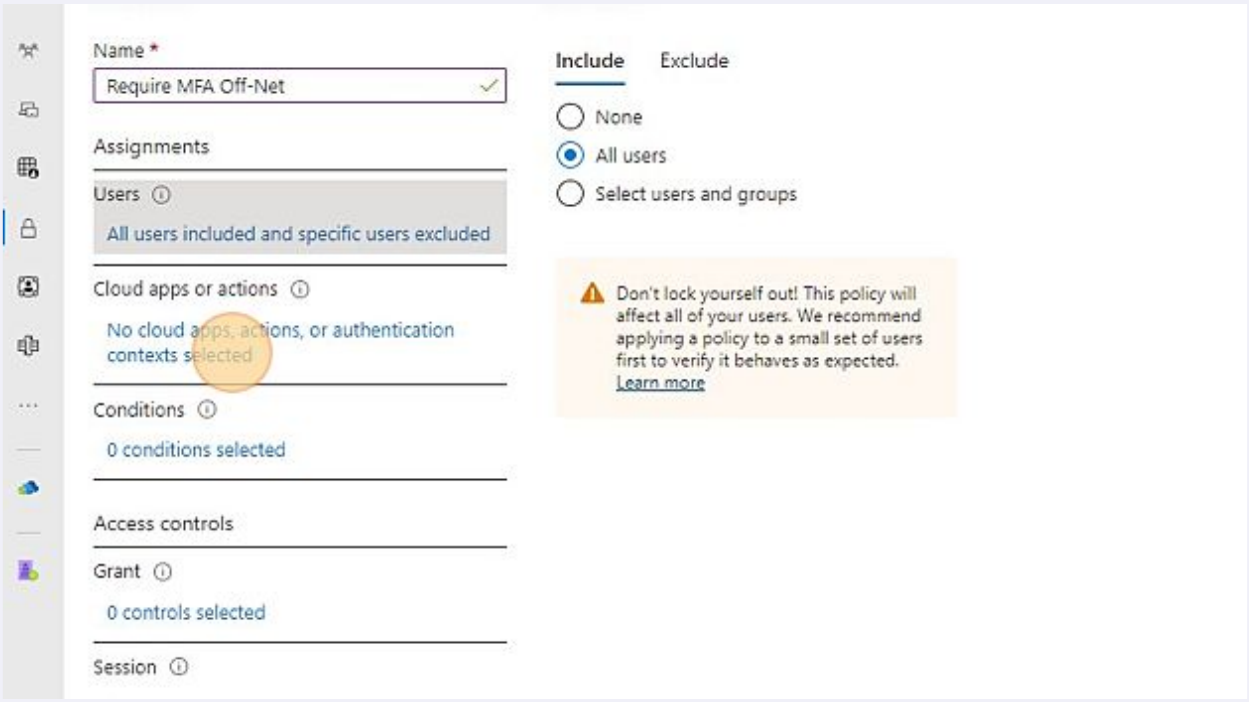
18 Click "Exclude"



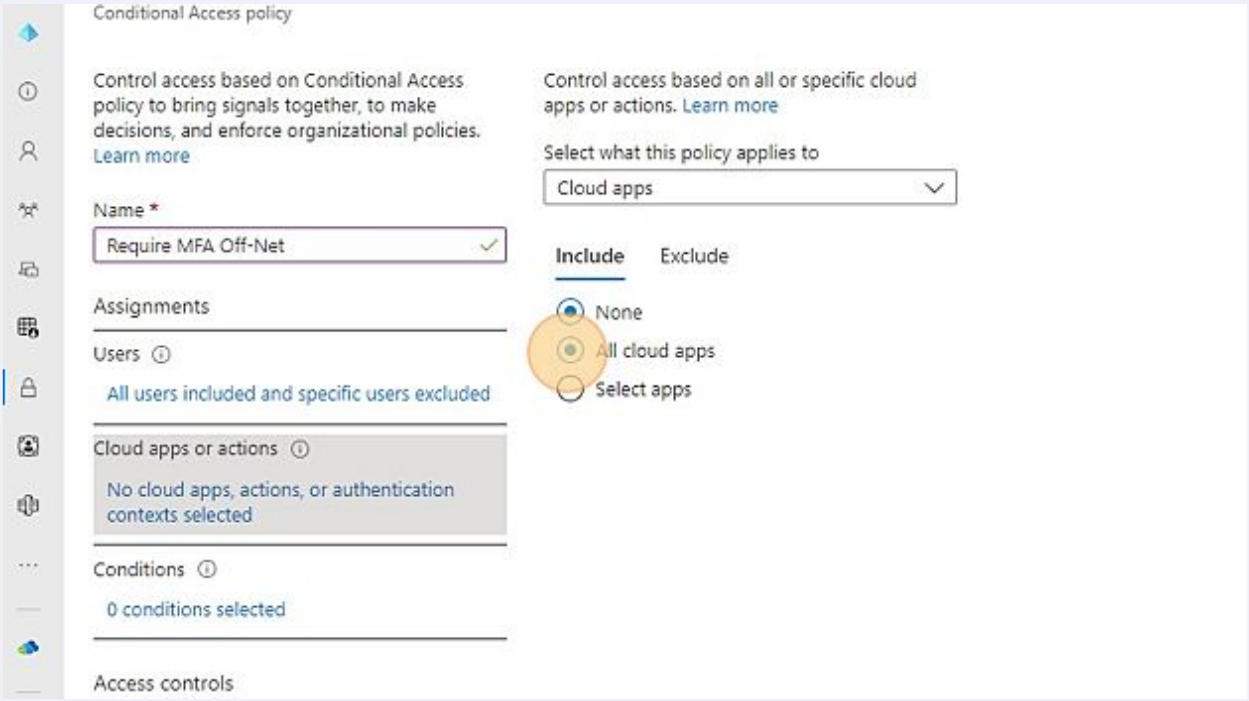
19 Exclude your Break Glass Admin account.



20 Click "Cloud apps"

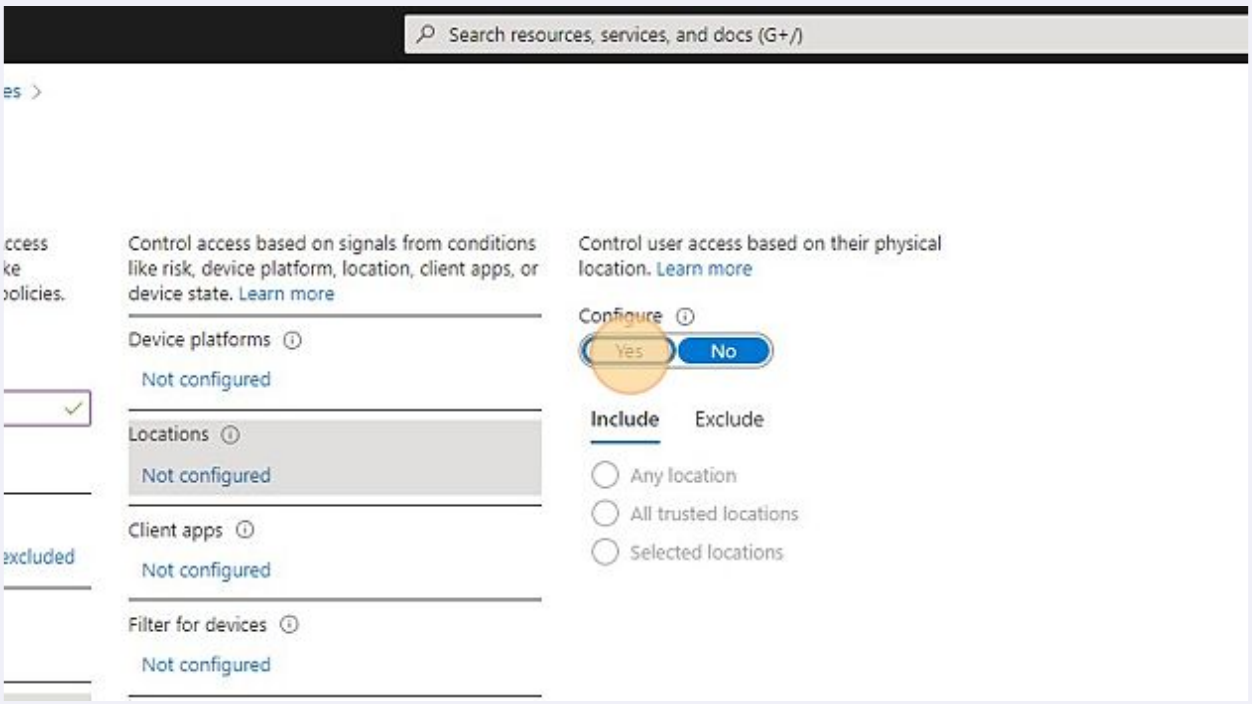


21 Click "All Cloud Apps"

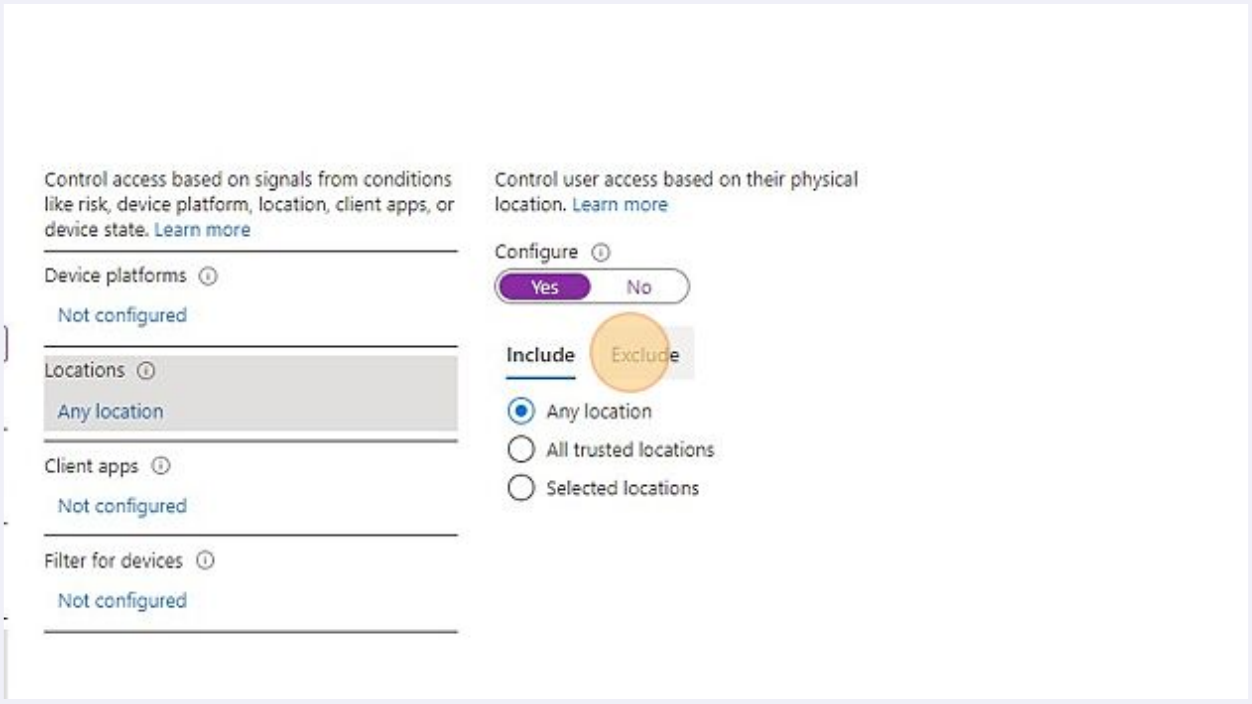


22 Click "Conditions" > "Locations"

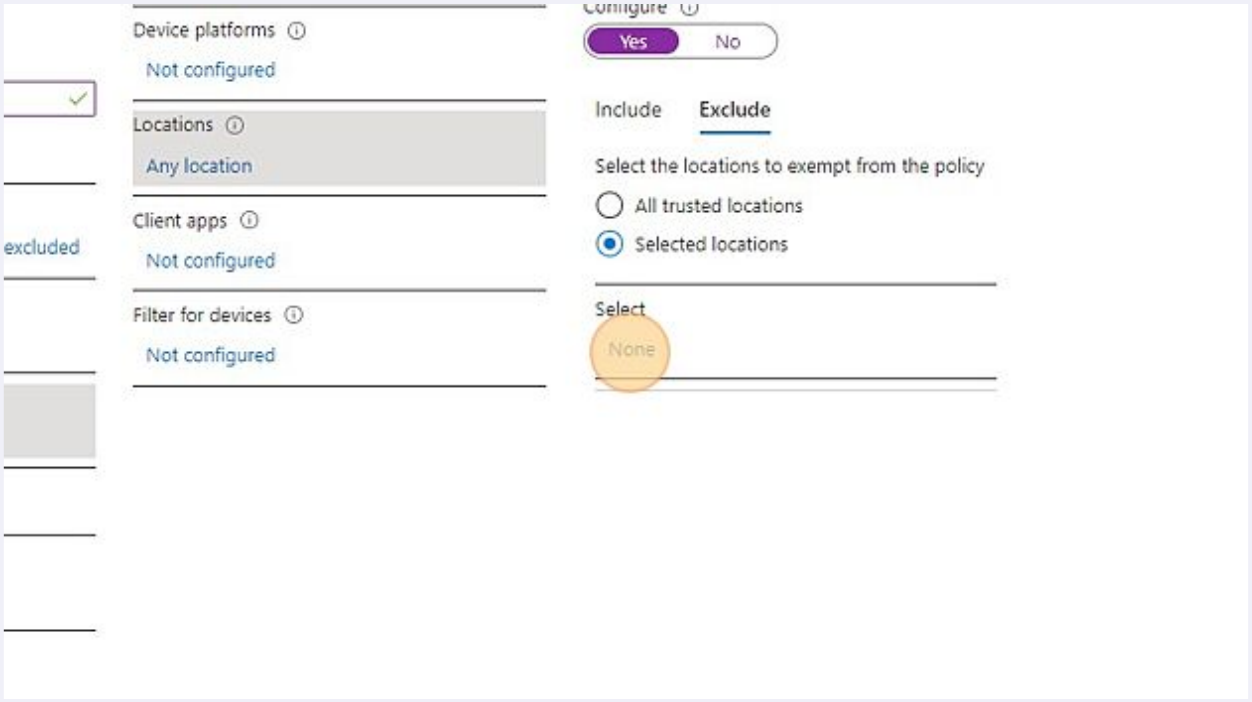
Include "All Locations"



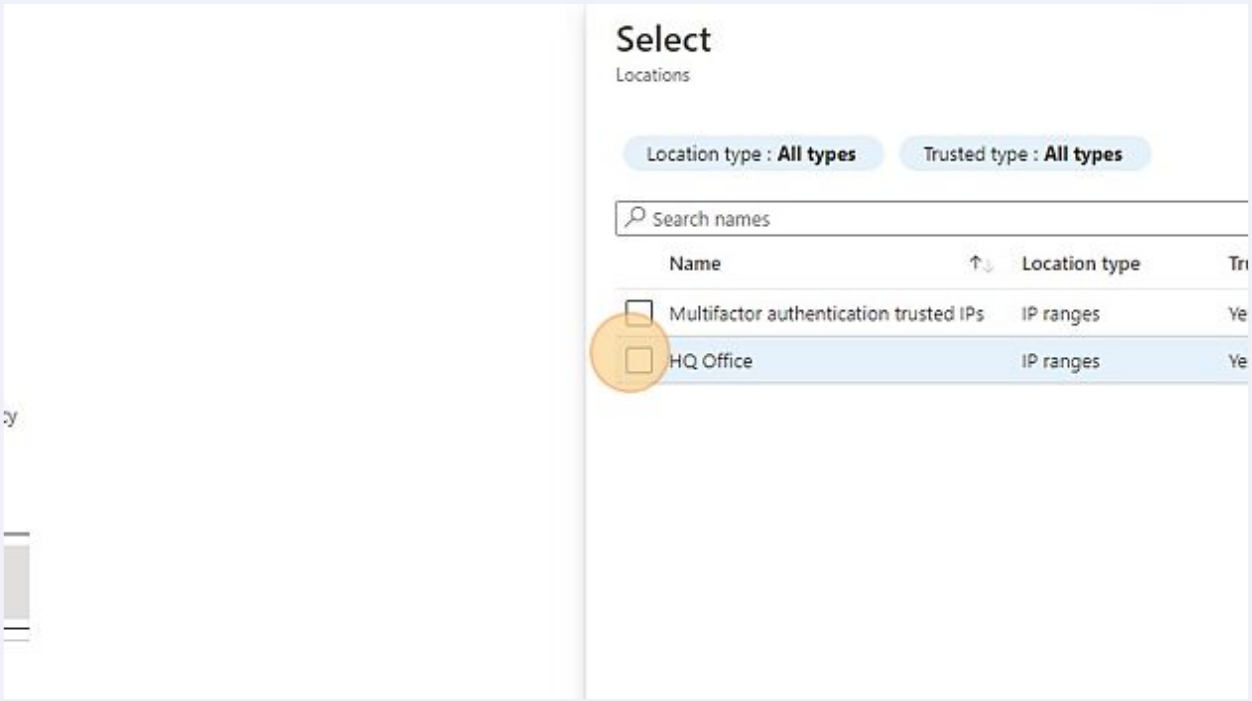
23 Click "Exclude"



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

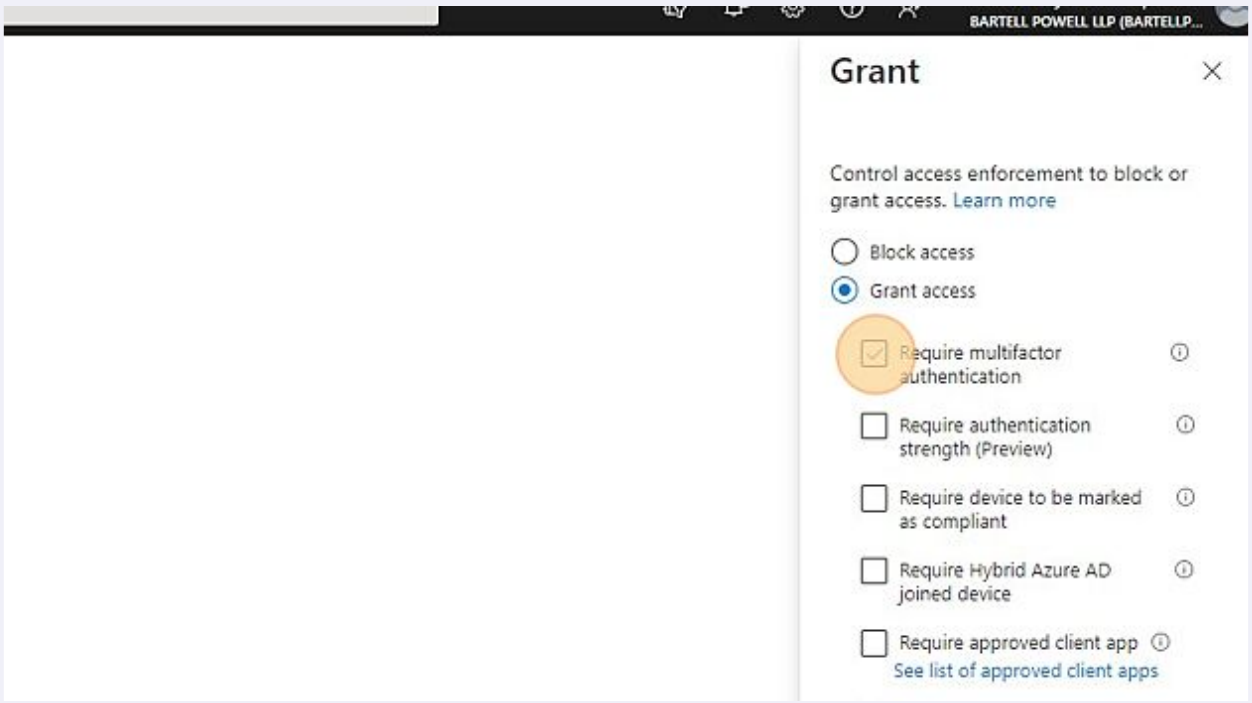


25 Select "HQ Office"

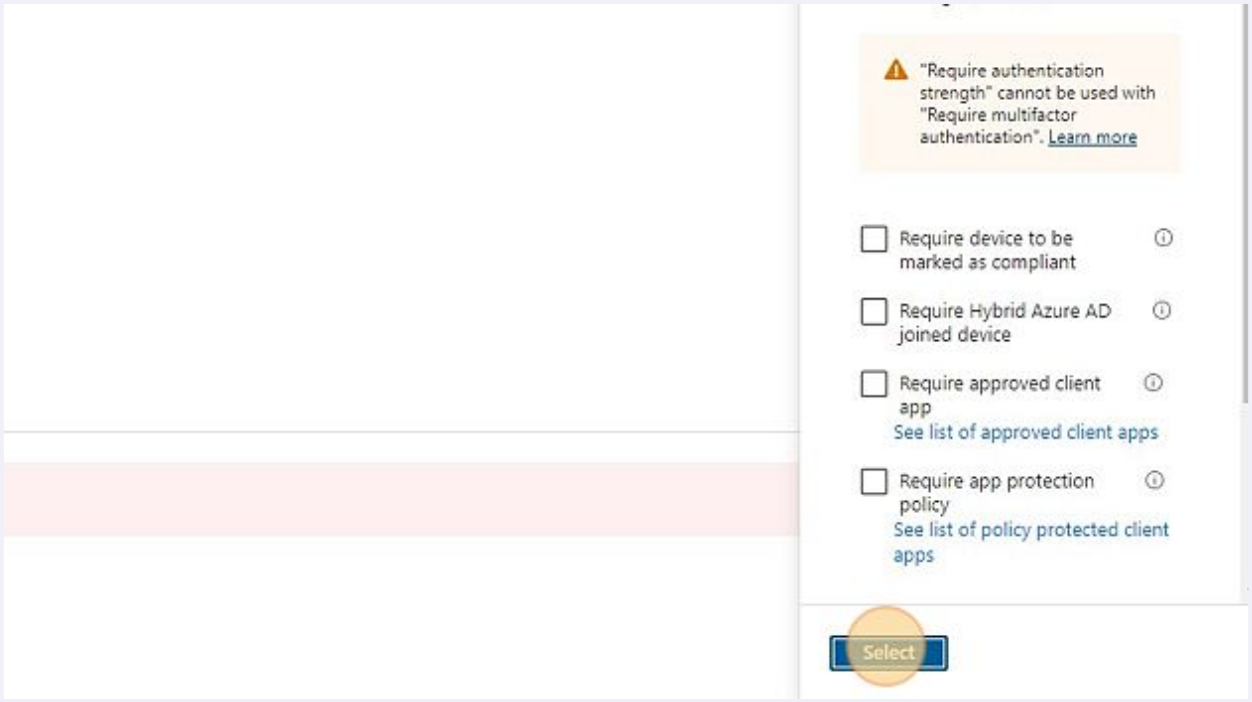


26 Click "Grant"

27 Click "Require MFA"



28 Click "Select"



29 Save the policy and verify it creates successfully.