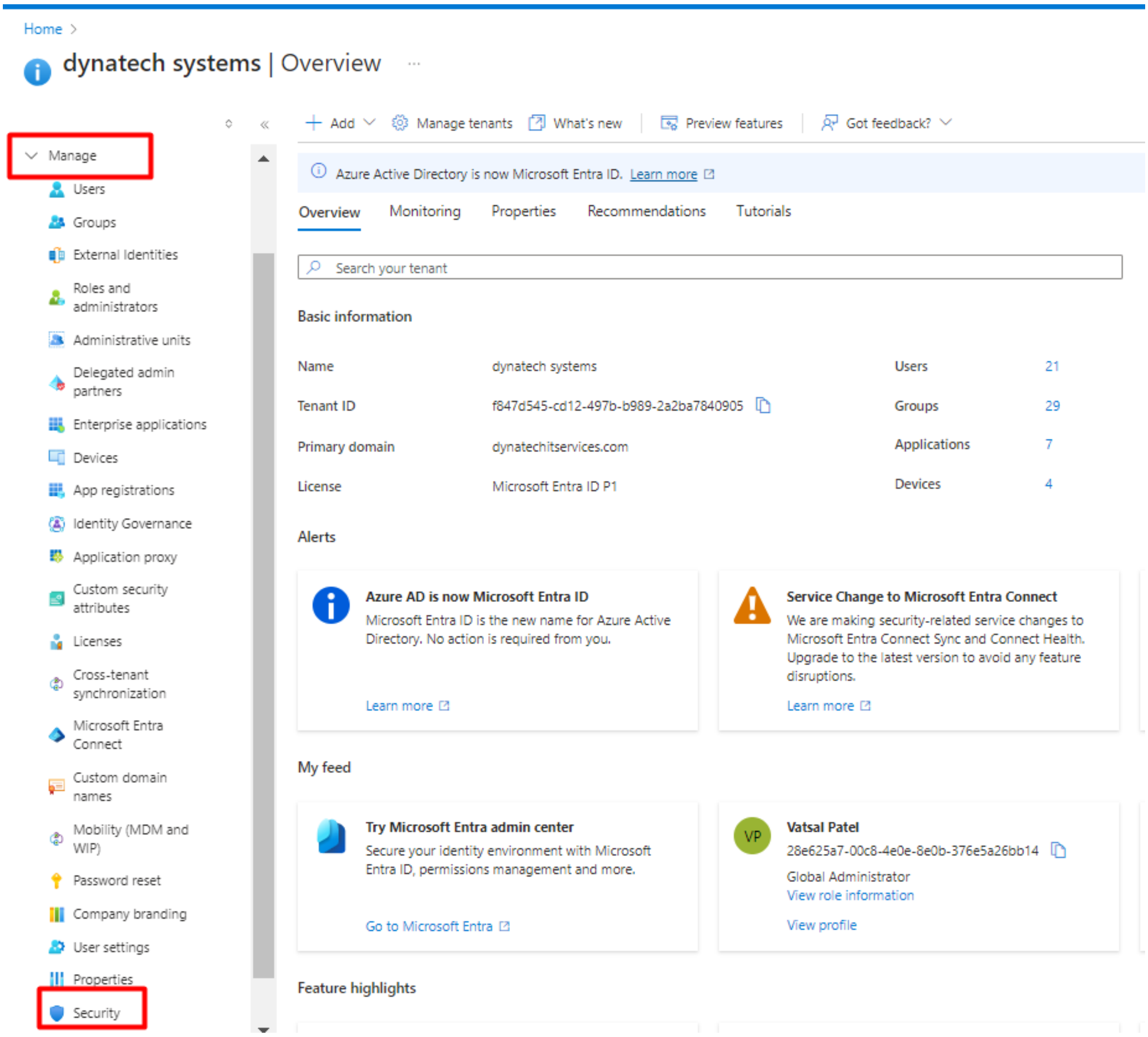
Login in allowed Region with Azure AD Conditional Access

Prepared By:
--Vatsal Patel
--Yash Shah

Reviewed By:
-- Meet Shah

1. **Login into https://portal.azure.com.**

2. **Go to Microsoft Entra ID → Manage → Security.**



dynatech systems | Overview

Azure Active Directory is now Microsoft Entra ID. Learn more

Basic information

Name	dynatech systems	Users	21
Tenant ID	f847d545-cd12-497b-b989-2a2ba7840905	Groups	29
Primary domain	dynatechitservices.com	Applications	7
License	Microsoft Entra ID P1	Devices	4

Alerts

Azure AD is now Microsoft Entra ID
Microsoft Entra ID is the new name for Azure Active Directory. No action is required from you.
Learn more

Service Change to Microsoft Entra Connect
We are making security-related service changes to Microsoft Entra Connect Sync and Connect Health. Upgrade to the latest version to avoid any feature disruptions.
Learn more

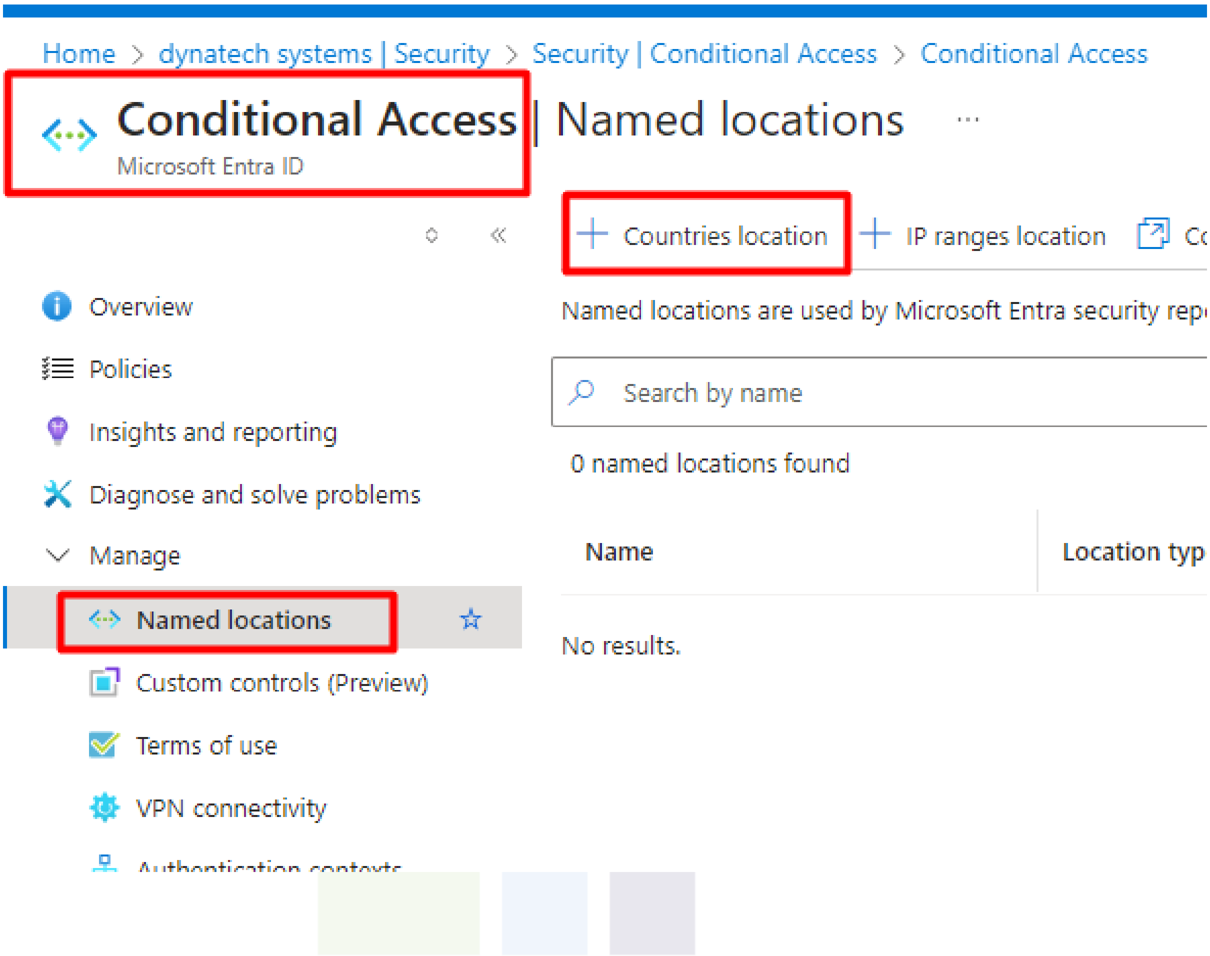
My feed

Try Microsoft Entra admin center
Secure your identity environment with Microsoft Entra ID, permissions management and more.
Go to Microsoft Entra

Vatsal Patel
28e625a7-00c8-4e0e-8e0b-376e5a26bb14
Global Administrator
View role information
View profile

Feature highlights

3. **Conditional access → Named locations → Countries location.**



Home > dynatech systems | Security > Security | Conditional Access > Conditional Access

Conditional Access | Named locations ...
Microsoft Entra ID

Named locations are used by Microsoft Entra security rep

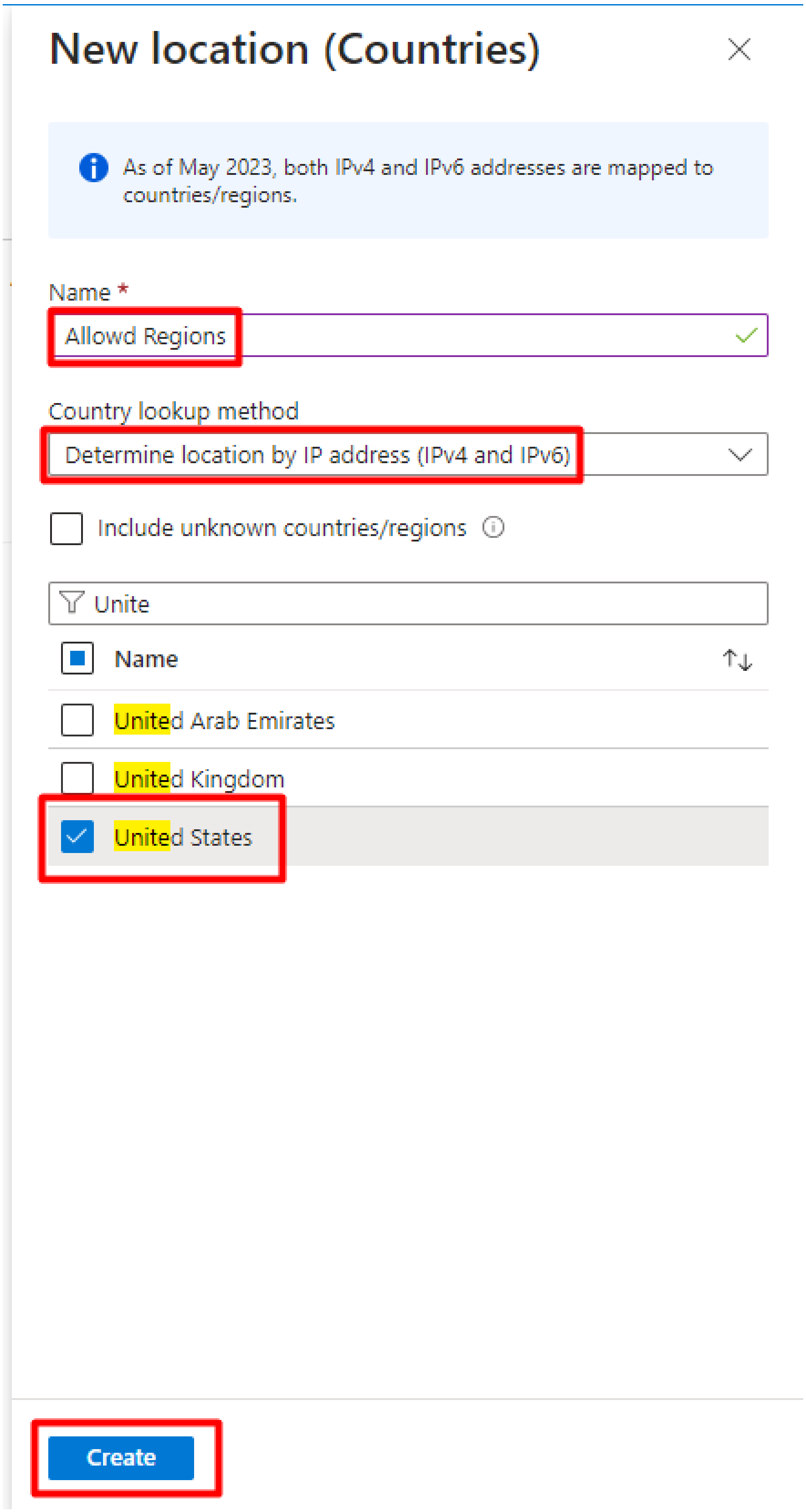
Search by name

0 named locations found

Name	Location typ

No results.

4. **Select country lookup method and countries which you want to allow for login and create.**



New location (Countries)

As of May 2023, both IPv4 and IPv6 addresses are mapped to countries/regions.

Name *

Allowd Regions

Country lookup method

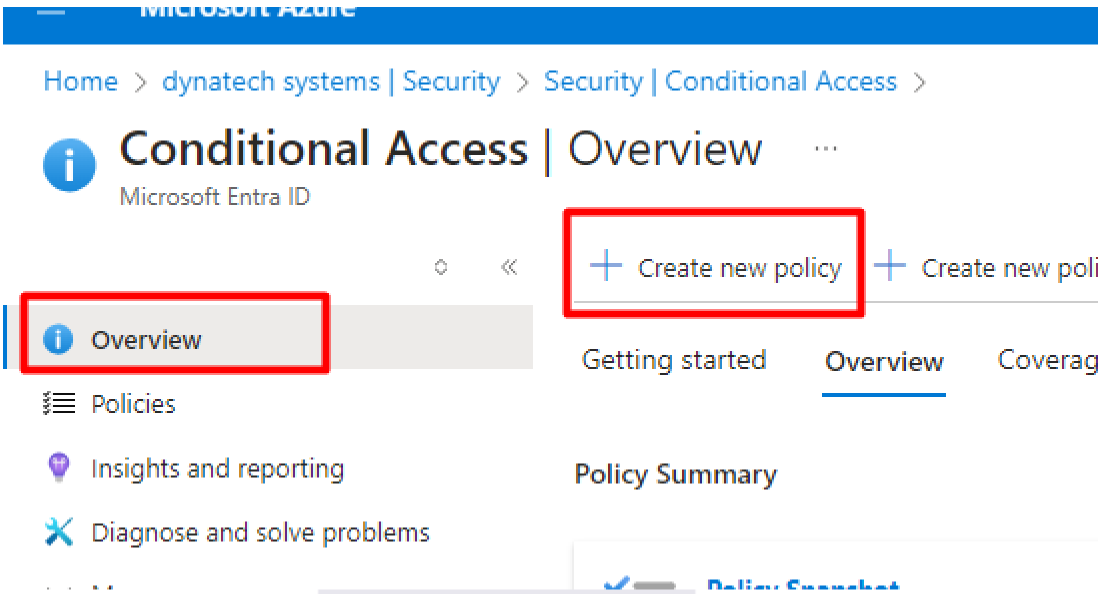
Determine location by IP address (IPv4 and IPv6)

□ Include unknown countries/regions

Unite

	Name
□	United Arab Emirates
□	United Kingdom
☑	United States

5. **Now go to overview → Create new policy.**

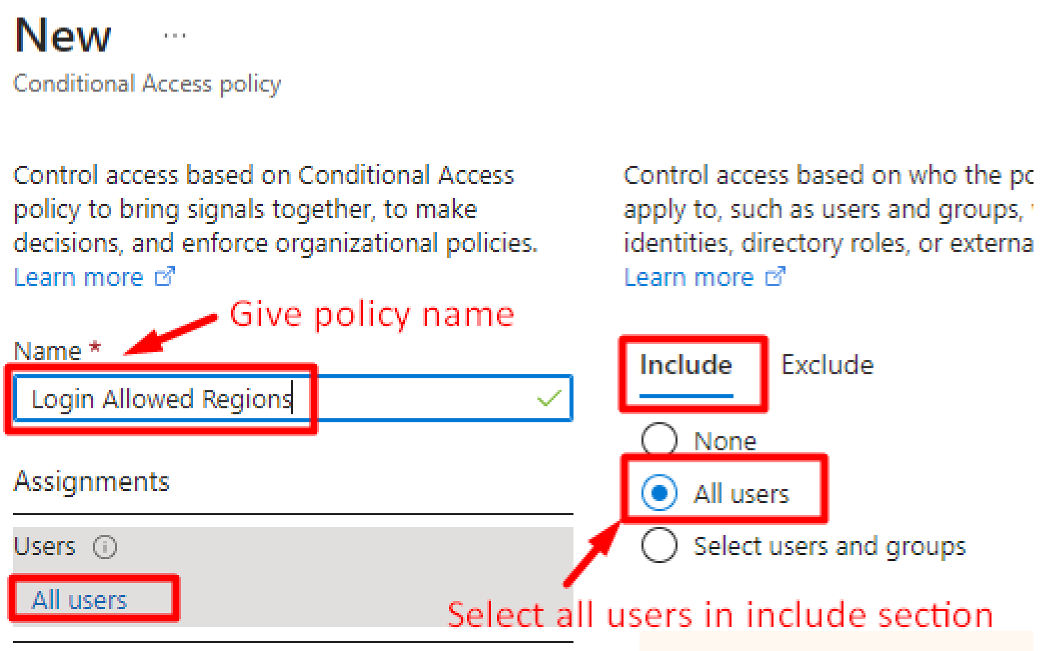


Home > dynatech systems | Security > Security | Conditional Access >

Conditional Access | Overview

Microsoft Entra ID

6. **Assignments → Users → Select Parameters for include and exclude users as per below screenshots.**



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 pc apply to, such as users and groups, identities, directory roles, or externa Learn more

Name * Login Allowed Regions

Assignments

Users: All users

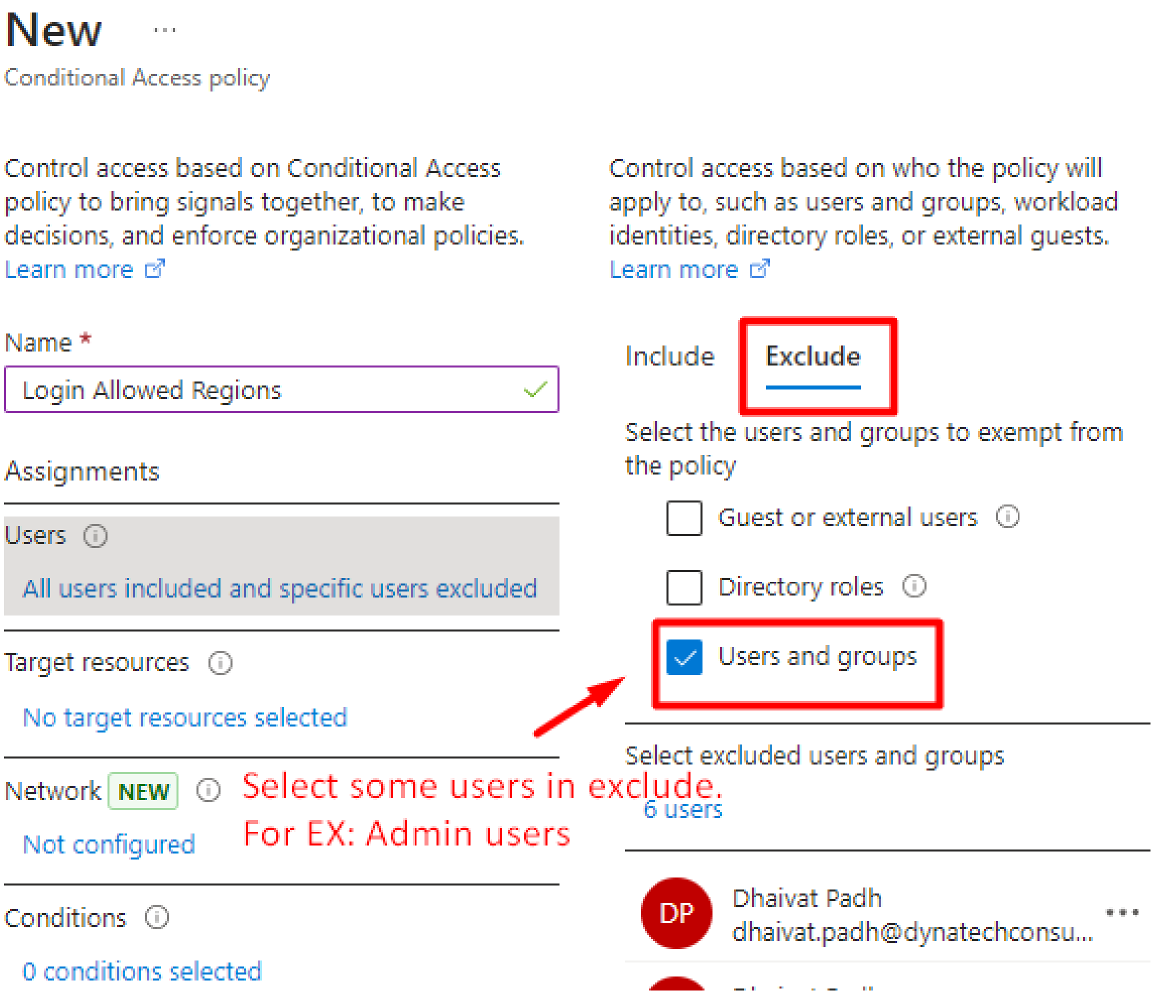
Include ● All users

Give policy name

Select all users in include section

Include Users

Note: Must add some admin users and users from admin team in 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 *

Login Allowed Regions

Assignments

Users

All users included and specific users excluded

Target resources

No target resources selected

Network NEW

Not configured

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

Select the users and groups to exempt from the policy

□ Guest or external users

□ Directory roles

☑ Users and groups

Select excluded users and groups

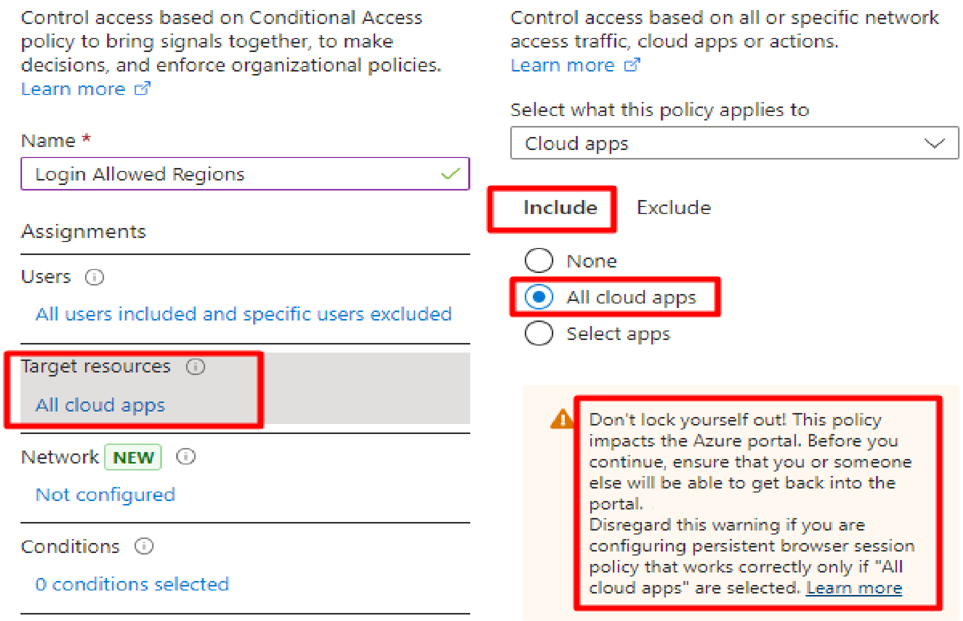
6 users

DP Dhaivat Padh dhaivat.padh@dynatechconsu...

Select some users in exclude.
For EX: Admin users

Exclude users

7. **Target resources → All cloud apps**



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

Name *
Login Allowed Regions

Assignments

Users ⓘ
All users included and specific users excluded

Target resources ⓘ
All cloud apps

Network NEW ⓘ
Not configured

Conditions ⓘ
0 conditions selected

Control access based on all or specific network access traffic, cloud apps or actions.
Learn more

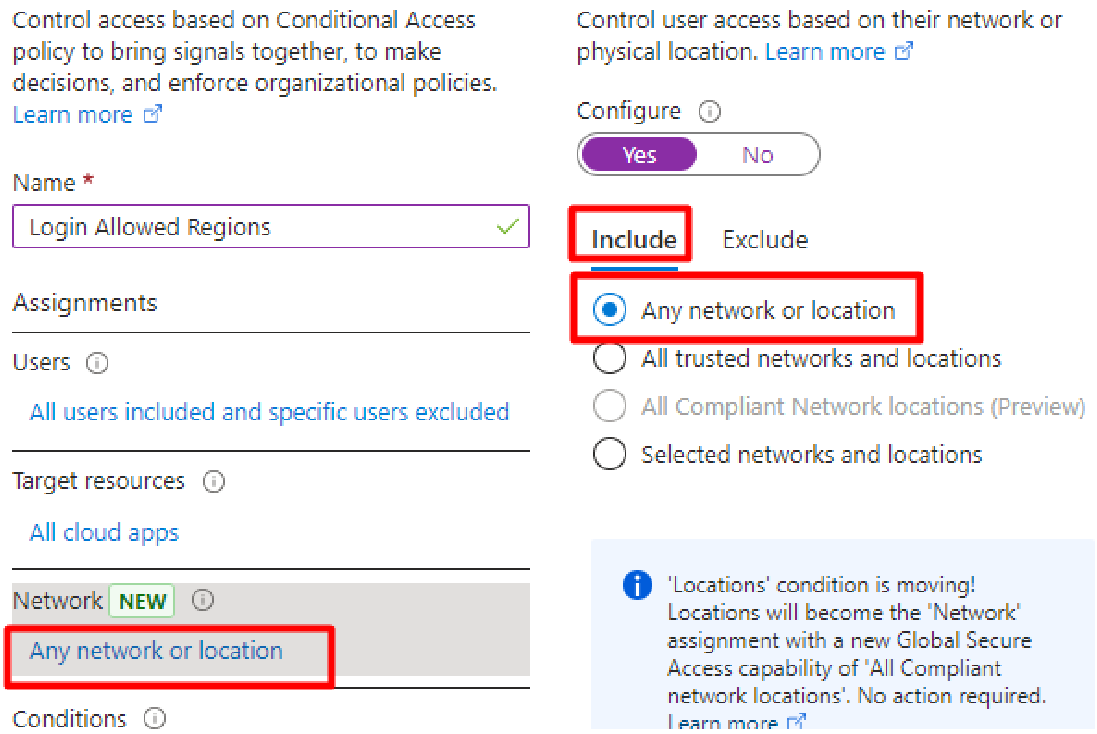
Select what this policy applies to
Cloud apps

Include Exclude

○ None
● All cloud apps
○ Select apps

⚠ Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal.
Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All cloud apps" are selected. Learn more

8. **Network → Any network or location.**



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

Name *
Login Allowed Regions

Assignments

Users ⓘ
All users included and specific users excluded

Target resources ⓘ
All cloud apps

Network NEW ⓘ
Any network or location

Conditions ⓘ

Control user access based on their network or physical location. Learn more

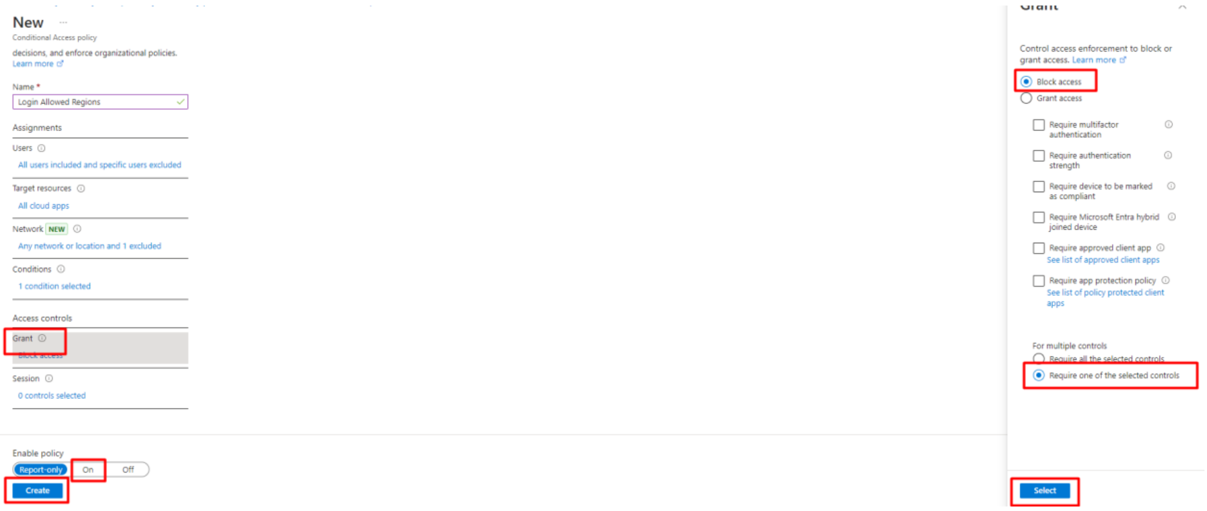
Configure ⓘ
[✓ Yes] No

Include Exclude

● Any network or location
○ All trusted networks and locations
○ All Compliant Network locations (Preview)
○ Selected networks and locations

ⓘ 'Locations' condition is moving! Locations will become the 'Network' assignment with a new Global Secure Access capability of 'All Compliant network locations'. No action required.
Learn more

9. **Grant → Block Access.**



New ···
Conditional Access policy
decisions, and enforce organizational policies.
Learn more

Name *
Login Allowed Regions

Assignments

Users
All users included and specific users excluded

Target resources
All cloud apps

Network NEW
Any network or location and 1 excluded

Conditions
1 condition selected

Access controls

Grant
Block access

Session
0 controls selected

Enable policy
Report-only | On | Off

Create

Grant

Control access enforcement to block or grant access. Learn more

● Block access
○ Grant access

□ Require multifactor authentication
□ Require authentication strength
□ Require device to be marked as compliant
□ Require Microsoft Entra hybrid joined device
□ Require approved client app
See list of approved client apps
□ Require app protection policy
See list of policy protected client apps

For multiple controls
○ Require all the selected controls
● Require one of the selected controls

Select