

# Azure lab conditional Access

## Objective.

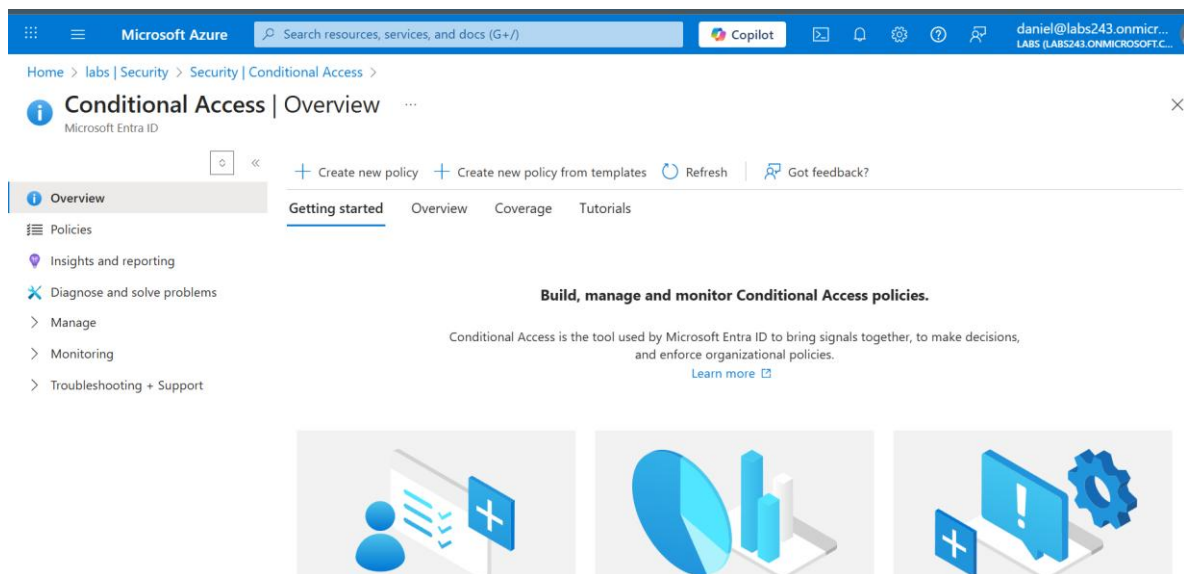
Set up test conditional access policies in azure AD to control user access on conditions such as MFA, location and device compliance.

## Part I.

First instance log in as global admin in our tenant.

Go to Azure portal → Entra ID → security → protect → conditional access

Here select new policy



Here we select adequate name for the policy “require MFA for Sales”

Include groups or users at the policy

Microsoft Azure

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

Copilot

Home > Conditional Access | Overview >

## New

Conditional Access policy

Users ⓘ

Specific users included

Target resources ⓘ

No target resources selected

Network **NEW** ⓘ

Not configured

Conditions ⓘ

0 conditions selected

Select users and groups

☐ Guest or external users ⓘ

☐ Directory roles ⓘ

☒ Users and groups

Select

1 group

SA Sales ...

Enable policy

Report-only On Off

Configure the access control to grant this case require MFA

Microsoft Azure

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

Copilot

daniel@labs243.onmicr... LABS (LABS243.ONMICROSOFTC...

Home > Conditional Access | Overview >

## New

Conditional Access policy

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Enable policy

Report-only On Off

It looks like you're about to manage your organization's security configurations. That's great! You must first [disable security defaults](#) before enabling a Conditional Access policy.

Create

### Grant

Control access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☒ Require multifactor authentication ⓘ

**i** Consider testing the new "Require authentication strength". [Learn more](#)

☐ Require authentication strength ⓘ

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

Select

\*Make sure that all resources or the specific for you case are selected

Next step is test if our new policy is enabled, lets log in as sales member

# Microsoft Azure



bob@labs243.onmicrosoft.com

## Let's keep your account secure

We'll help you set up another way to verify it's you.  
Follow the prompts to download and set up the  
Microsoft Authenticator app.

[Use a different account](#)

[Learn more about the Microsoft Authenticator app](#)

[Next](#)

Let's check with other user to make sure that CA policy are working well

# Microsoft Azure



george@labs243.onmicrosoft.com

## Let's keep your account secure

We'll help you set up another way to verify it's you.

[Use a different account](#)

[Learn more about verifying your identity](#)

[Next](#)

## Part II. (Block Legacy Authentication)

Let's create a new CA policy called Block Legacy Authentication with the following parameters

### Assignments:

- Users/Groups → Select **All users** (except Global Admins for safety).

- Cloud apps → All.

## Conditions:

- Client apps → Select **Other clients, Legacy Authentication clients**.

**Access controls** → Block access.

Enable → Create.

Home > labs | Security > Security | Conditional Access > Conditional Access | Overview > Policies >

## New

Conditional Access policy

Network **NEW** ⓘ  
Not configured

Conditions ⓘ  
1 condition selected

Access controls

Grant ⓘ  
0 controls selected

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 ⓘ

**Select**

Home > labs | Security > Security | Conditional Access > Conditional Access | Overview > Policies >

## New

Conditional Access policy

Not configured

Conditions ⓘ  
0 conditions selected

Access controls

Grant ⓘ  
0 controls selected

Session ⓘ  
0 controls selected

Device platforms ⓘ  
Not configured

Locations ⓘ  
Not configured

Client apps ⓘ  
Not configured

Filter for devices ⓘ  
Not configured

Authentication flows ⓘ

Enable policy  
Report-only On Off  
**Create**

## Client apps

Control user access to target specific client applications not using modern authentication. [Learn more](#) ⓘ

Configure ⓘ  
**Yes** No

Select the client apps this policy will apply to

Modern authentication clients

☐ Browser  
☐ Mobile apps and desktop clients

Legacy authentication clients

☐ Exchange ActiveSync clients  
☒ Other clients ⓘ

**Done**


Then test if the policy is working, we'll use what if tool

Set the parameters to simulated try to sing by unsupported client app and see the results

What if

Reset

Evaluation result

 Classic policies are not evaluated by this tool.

Policies that will apply

Policies that will not apply

1 policy found

Display name	Grant controls	Session Controls	State	Has filter? ⓘ
<a href="#">Block Legacy Authentication</a>	Block access		On	No

Here we can see the CA policy is blocking the attempt to log in when don't use modern client or unsupported versions

### Part III (Location Based Access Control)

Create a new CA policy “Location Based Access Control”

Before to start we need to prerequisite create a “named location” for use in our CA policy

## New location (Countries) ×

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

Name \*

costa rica location

Country lookup method

Determine location by IP address (IPv4 and IPv6) ▼

☐ Include unknown countries/regions i

🔍 costa ×

☒ Name ↑

☒ Costa Rica

Create

Cancel

### Assignments :

- Users/Groups → Select **HelpDesk**.
- Cloud apps → All .

**Conditions** → Locations → Include any network any location that means the location will be blocked, and exclude we select our named location previously create.

This pattern blocks any region except the country configured in named location

**Access controls** → Block access.

Enable → Create.

Then we test our CA policy with the what if tool,

IP address

111.113.88.3

Country

China

Filter for devices

Property	Value	Delete
Select a property...	<Pick a property and operator first>	

What if

Reset

Evaluation result

Classic policies are not evaluated by this tool.

Policies that will apply

Policies that will not apply

1 policy found

Display name	Grant controls	Session Controls	State	Has filter?
Block Location Access	Block access		On	No