😊 Conditional Access Policies

Conditional Access policies in Azure Active Directory (AAD) are rules and restrictions applied to control access to cloud applications and resources. These policies evaluate certain conditions, such as user identity, location, device compliance, and session risk, before granting access to resources. They serve as a key component of identity and access management (IAM) strategy, allowing organizations to enforce security measures based on contextual factors.

The main goal of Conditional Access policies is to ensure secure access to resources by allowing or blocking access based on predefined conditions, thereby reducing the risk of unauthorized access and data breaches. They enable organizations to implement granular access controls tailored to their specific security requirements, ultimately safeguarding sensitive data and protecting against potential threats.

😄 Use cases of Conditional Access Policies:

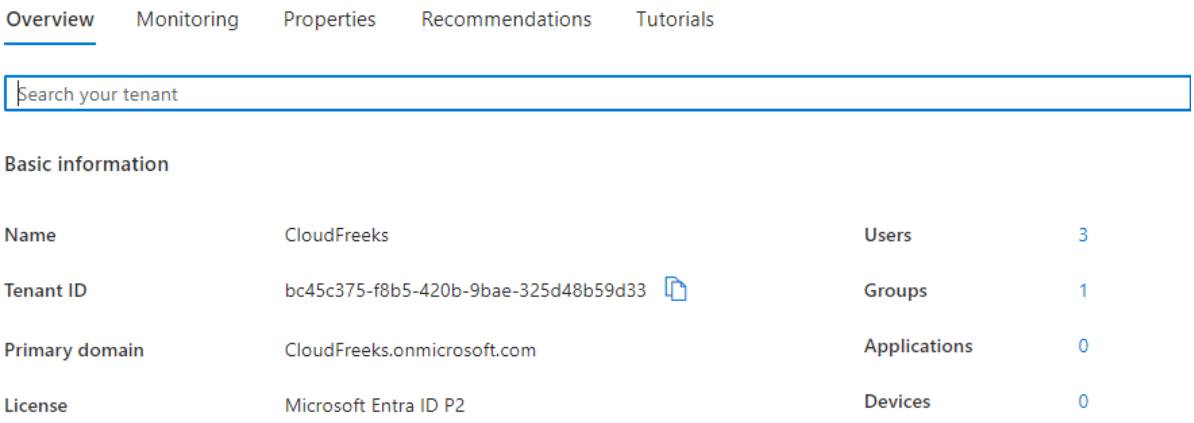
Conditional Access policies in Azure Active Directory are versatile and can be tailored to various use cases. Here are some common scenarios where Conditional Access policies are valuable:

1. **Device Compliance:** Ensure that only devices that meet certain compliance standards, such as being enrolled in Intune and having up-to-date security configurations, can access corporate resources.
2. **Location-Based Access:** Restrict access to sensitive applications or data to specific geographic locations. For example, only allow access to financial data from within the company's offices or from trusted locations.
3. **Multi-Factor Authentication (MFA) Enforcement:** Require users to authenticate using multiple factors, such as a password and a one-time passcode sent to their mobile device, when accessing critical applications or resources.
4. **Risk-Based Access:** Evaluate the risk associated with a user's sign-in attempt based on factors like unusual sign-in behavior, unfamiliar locations, or suspicious activities. If the risk level is high, prompt for additional authentication or block access altogether.
5. **Application Controls:** Control access to specific applications based on user roles or group memberships. For example, only grant access to the HR system to users in the HR department.
6. **Session Controls:** Monitor and control active user sessions in real-time. For instance, automatically sign out users if their session is inactive for a specified period or if their risk level increases during the session.
7. **Granular Access Policies:** Implement policies that grant access based on user attributes such as group membership, user location, device platform, or user license status. This allows for fine-grained access control tailored to specific user populations.
8. **Guest User Access:** Define policies that govern access for guest users or external collaborators accessing your organization's resources. For example, require guest users to complete MFA or comply with certain device requirements before accessing shared files.

In this lab, we're configuring Conditional Access Policies in Azure Active Directory to enforce Multi-Factor Authentication (MFA) for accessing cloud applications. The end goal is to enhance security by requiring additional authentication factors, thus reducing the risk of unauthorized access and data breaches.

😁 To begin with this Lab:

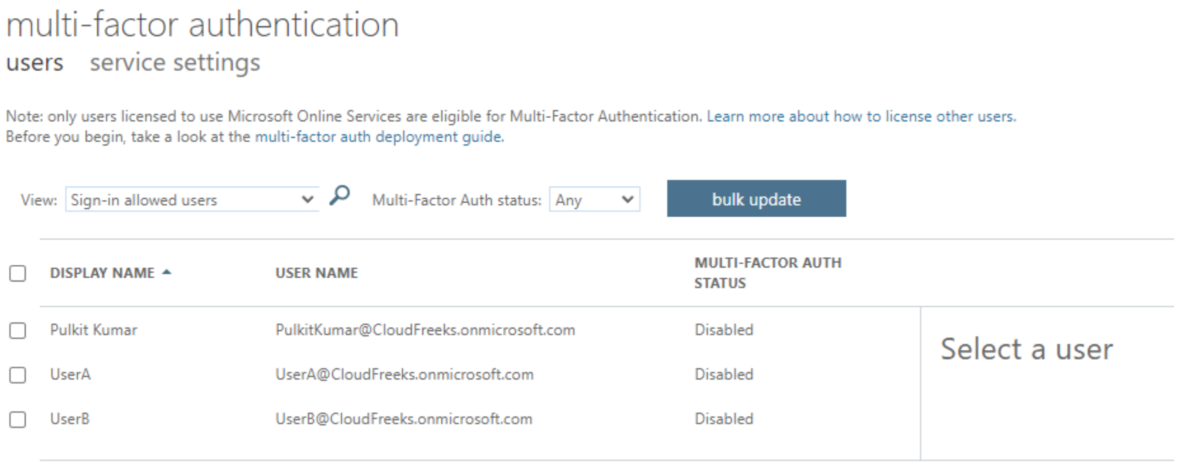
1. The prerequisite for this lab is that you should have a Microsoft Entra ID P2 license.



Basic information

Name	CloudFreeks	Users	3
Tenant ID	bc45c375-f8b5-420b-9bae-325d48b59d33	Groups	1
Primary domain	CloudFreeks.onmicrosoft.com	Applications	0
License	Microsoft Entra ID P2	Devices	0

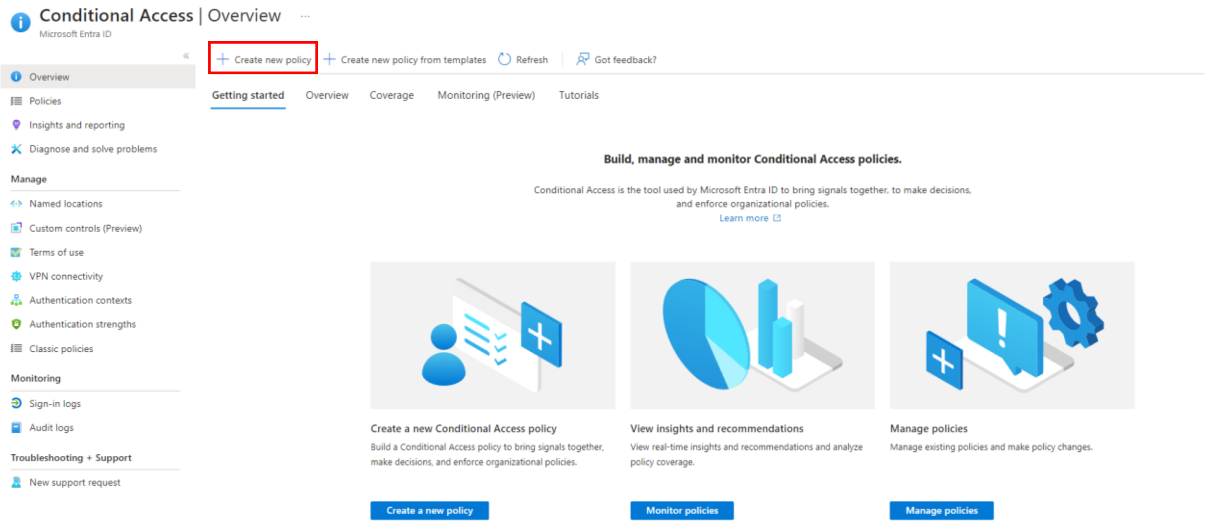
2. After that you need to go to users then go to per-user MFA and turn it off in case it is enabled.



Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users.
Before you begin, take a look at the multi-factor auth deployment guide.

☐	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
☐	Pulkit Kumar	PulkitKumar@CloudFreeks.onmicrosoft.com	Disabled
☐	UserA	UserA@CloudFreeks.onmicrosoft.com	Disabled
☐	UserB	UserB@CloudFreeks.onmicrosoft.com	Disabled

3. Now in Microsoft Entra ID, from the left pane scroll down and navigate to Security.
4. Then inside security you need to go to Conditional Access. Here you can define some policies. Now you need to click on Create new policy.



Build, manage and monitor Conditional Access policies.

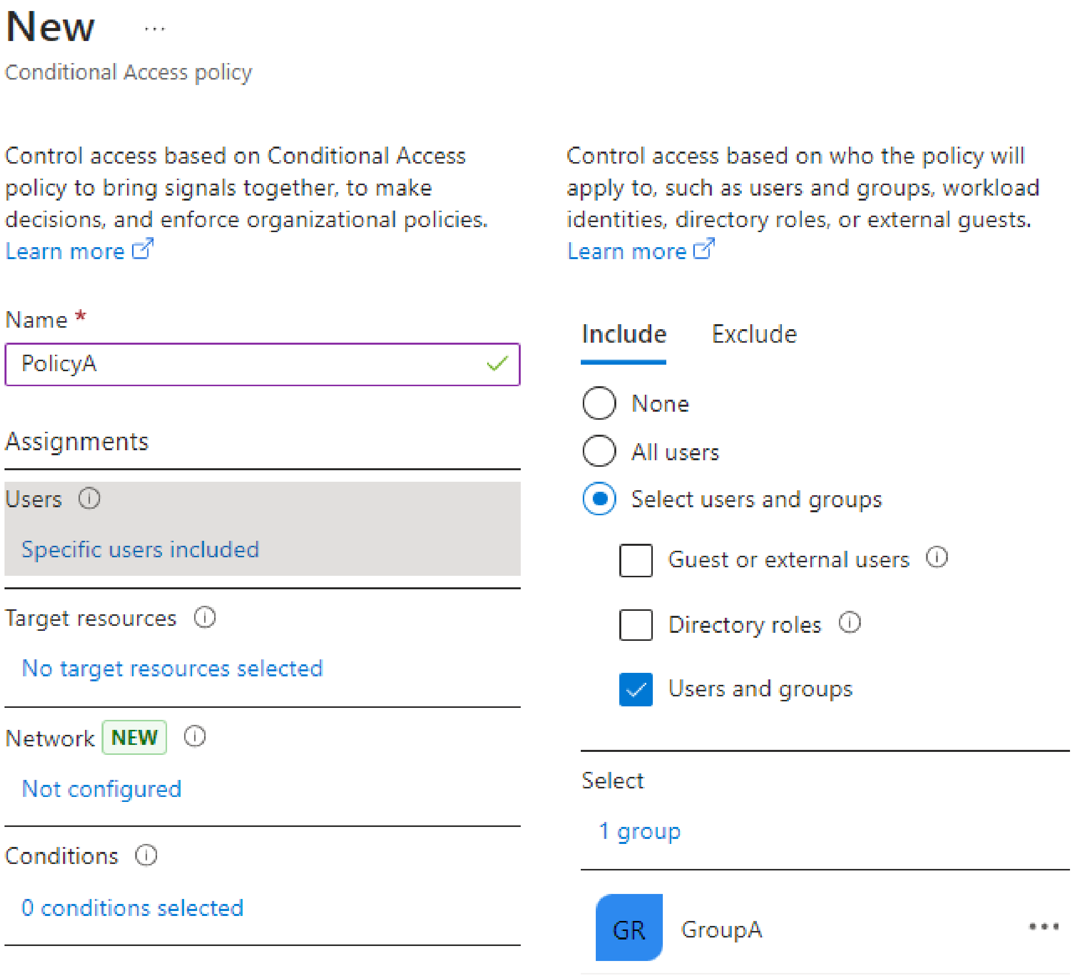
Conditional Access is the tool used by Microsoft Entra ID to bring signals together, to make decisions, and enforce organizational policies.
Learn more

Create a new Conditional Access policy
Build a Conditional Access policy to bring signals together, make decisions, and enforce organizational policies.

View insights and recommendations
View real-time insights and recommendations and analyze policy coverage.

Manage policies
Manage existing policies and make policy changes.

5. First you have to give it a name then choose the users tab and from there you need to choose Select users and groups.
6. After that you will have the option to choose either your users or a group.
7. Below you can see that we choose a group which has two users in it.



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

Name *
PolicyA

Assignments

Users
Specific users included

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

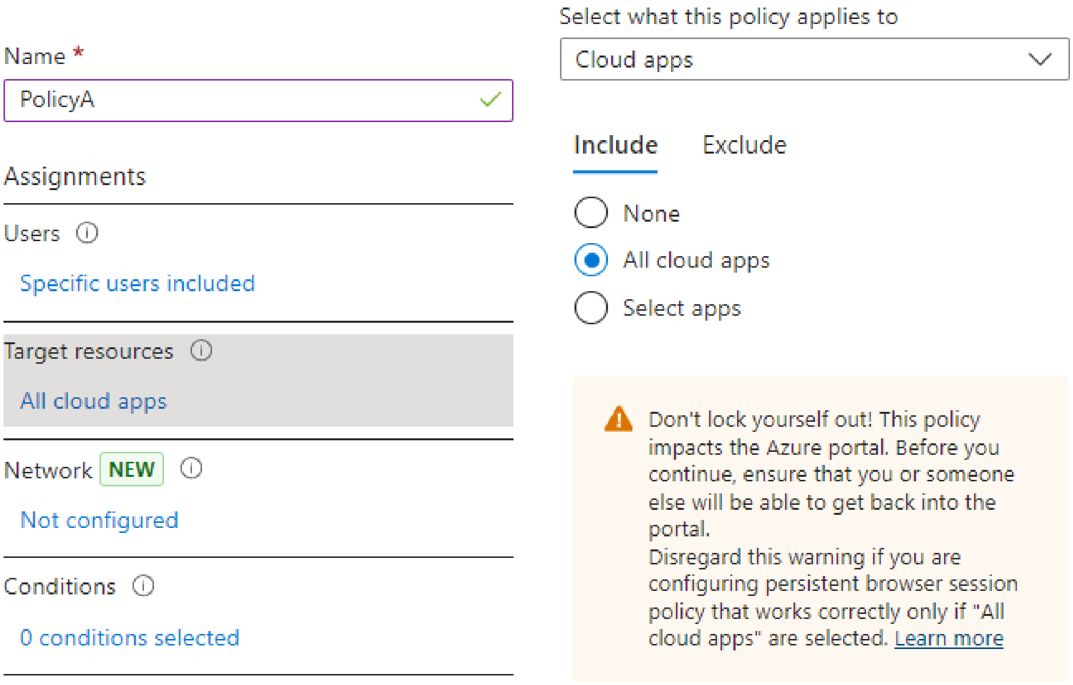
○ None
○ All users
● Select users and groups

□ Guest or external users
□ Directory roles
☑ Users and groups

Select
1 group

GR GroupA

8. Then in the target resources choose all cloud apps.



Name *

PolicyA

Assignments

Users ⓘ

Specific users included

Target resources ⓘ

All cloud apps

Network NEW ⓘ

Not configured

Conditions ⓘ

0 conditions selected

Select what this policy applies to

Cloud apps

Include Exclude

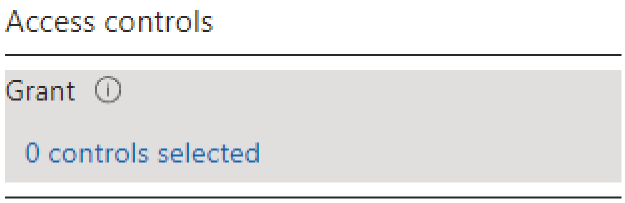
○ None

● 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

9. Now in the Access control section you need to click on grant.

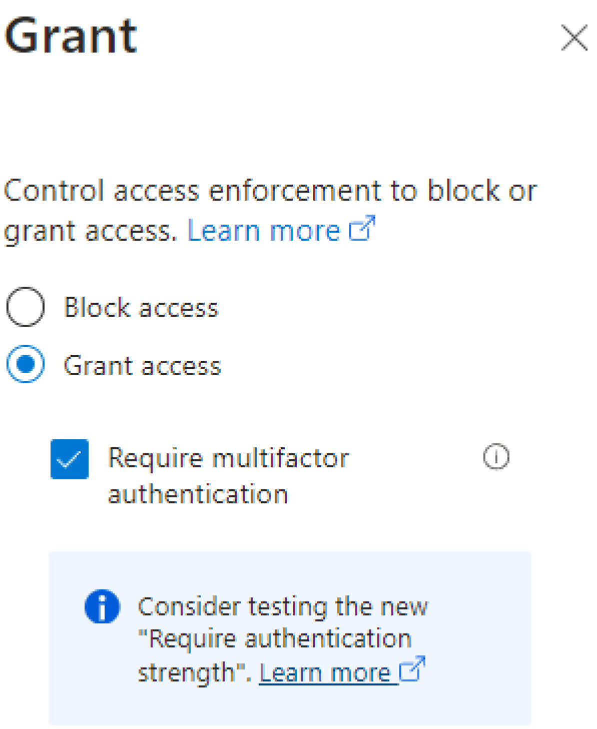


Access controls

Grant ⓘ

0 controls selected

10. Then you need to enable grant access and choose require multifactor authentication only.



Grant

Control access enforcement to block or grant access. Learn more

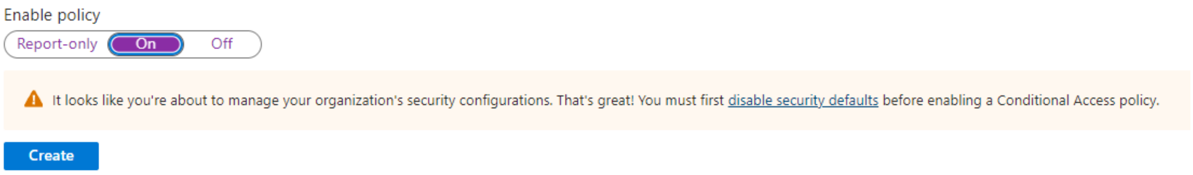
○ Block access

● Grant access

☑ Require multifactor authentication

Consider testing the new "Require authentication strength". Learn more

11. Then just enable the policy and click on create.

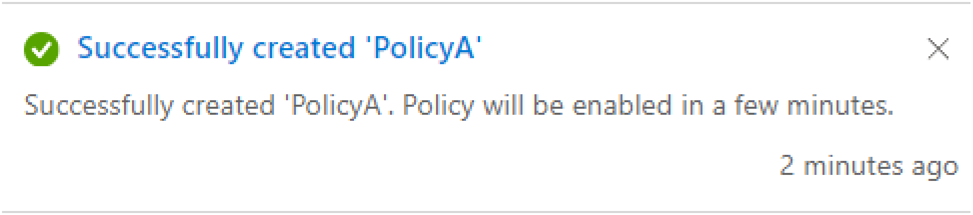


Enable policy

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.

12. After some time, you will see that your policy has been created successfully.

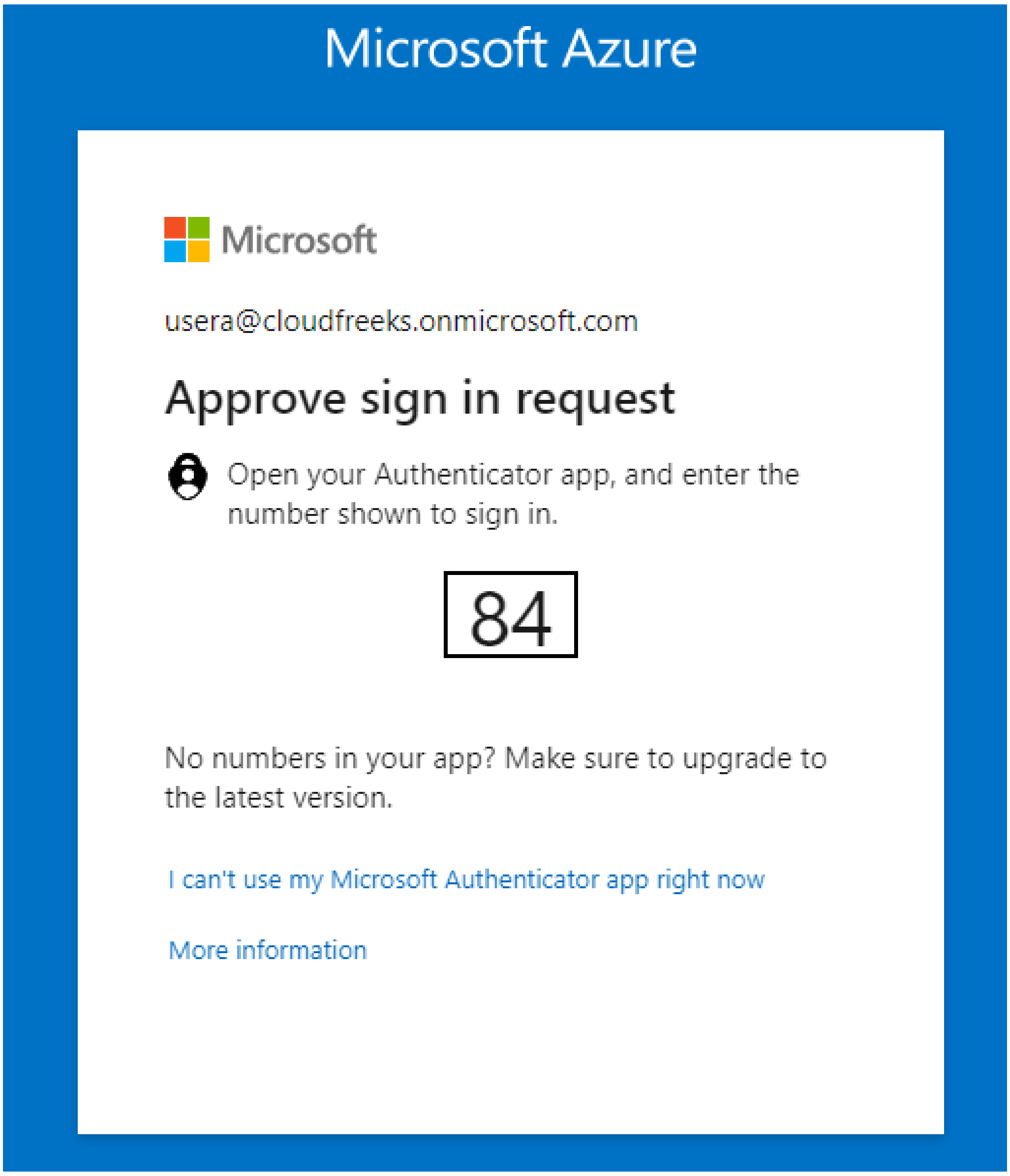


Successfully created 'PolicyA'

Successfully created 'PolicyA'. Policy will be enabled in a few minutes.

2 minutes ago

13. Now you need to log in with one of the user accounts. After you have entered the password it is still asking you to approve your sign in through authenticator app because in the conditional access we allowed MFA in the security section.



Microsoft Azure

usera@cloudfreeks.onmicrosoft.com

Approve sign in request

Open your Authenticator app, and enter the number shown to sign in.

84

No numbers in your app? Make sure to upgrade to the latest version.

I can't use my Microsoft Authenticator app right now

More information