

# Unlocking Security: Microsoft Entra ID Policy Deployment

---

**Prepared By**

**Md. Rishad Istiak Sachcha**

**Md. Oliullah**

## Contents

Introduction to Entra ID .....	3
Benefits: .....	3
Features: .....	3
Task-01: Location Based Access Policy .....	4
Scenario-01: .....	4
Policy-01:.....	4
Task-02: Device Based Access Policy .....	6
Scenario-02: .....	6
Policy-02:.....	6
Task-03: Client App Based Access Policy .....	7
Scenario-03: .....	7
Policy-03:.....	7
Task-04: Terms Based Access Policy .....	9
Scenario-04: .....	9
Policy-04:.....	9
Task-05: Multifactor Authentication Registration Policy .....	11
Scenario-05: .....	11
Policy-05:.....	12

## Introduction to Entra ID

Microsoft Entra ID is a cloud-based identity and access management (IAM) solution that helps organizations secure and manage identities for hybrid and multi-cloud environments. It provides a unified identity management experience for users, applications, and devices, and it helps organizations to protect their data and resources from unauthorized access.

### Benefits:

There are many benefits to using Microsoft Entra ID, including:

- **Improved security:** Microsoft Entra ID helps to protect organizations from unauthorized access by providing strong authentication and authorization capabilities.
- **Increased efficiency:** Microsoft Entra ID helps to streamline identity management tasks, such as user provisioning and deprovisioning.
- **Reduced costs:** Microsoft Entra ID can help to reduce costs by eliminating the need for on-premises IAM infrastructure.

### Features:

Microsoft Entra ID offers a wide range of features, including:

- **User management:** Create, manage, and delete user accounts.
- **Application management:** Integrate applications with Microsoft Entra ID to control user access.
- **Device management:** Manage devices that access Microsoft Entra ID-protected resources.
- **Access control:** Control who can access what resources.
- **Reporting and auditing:** Monitor and audit user activity.

## Task-01: Location Based Access Policy

### Scenario-01:

Recently Smart Digital Bank is facing different identity related attacks like spamming, bruteforce attack etc. The security team has informed that the attacks are coming from Bangladesh region. So We have to Block access from Bangladesh region. In this case we have blocked access from Bangladesh for our most critical user Nipa.

### Policy-01:

First of all we will have to select the location. We can select location in two ways – 1. Geolocation 2. Ip address. Here we have selected Bangladesh region according to geolocation.

The screenshot shows the Microsoft Entra admin center interface for Conditional Access. The left sidebar lists various management options, with 'Named locations' selected under the 'Manage' section. The main content area displays a table of named locations. The 'BD' location is highlighted with a red box. Below is a table representing the data shown in the screenshot:

Name	Location type	Trusted	Conditional Access policies
BD	Countries (...)		Policy-01
india	IP ranges	Yes	Not configured in any policy yet
norway	Countries (...)		Not configured in any policy yet
smart ip	IP ranges	Yes	Policy-01

Then from conditional access we have created a new policy policy-01 for the user Nipa. We have selected the target app Office365 & under condition, we have blocked access from Bangladesh region that we created earlier.

# Policy-01 ...

Conditional Access policy

Delete View policy information

Policy-01

## Assignments

Users ⓘ

[Specific users included](#)

Target resources ⓘ

[1 app included](#)

Conditions ⓘ

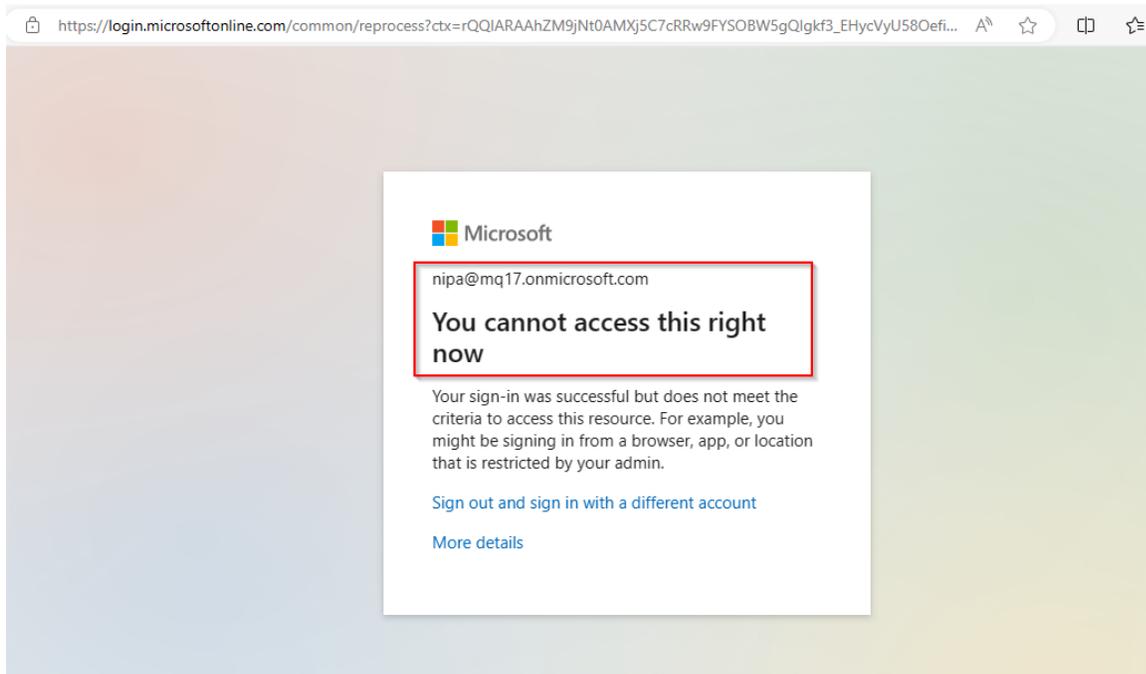
[1 condition selected](#)

## Access controls

Grant ⓘ

[Block access](#)

After creating the policy, we have tried to login to O365 as the user Nipa & our access is blocked which means our policy is working successfully.



## Task-02: Device Based Access Policy

**Scenario-02:** Humayra- an employee of Smart Digital Bank. She is a user of Microsoft 365. Recently Smart Digital Bank has created a policy that M365 will only be accessible from Linux & Mac device. So they have to update their policy at Entra Conditional Access.

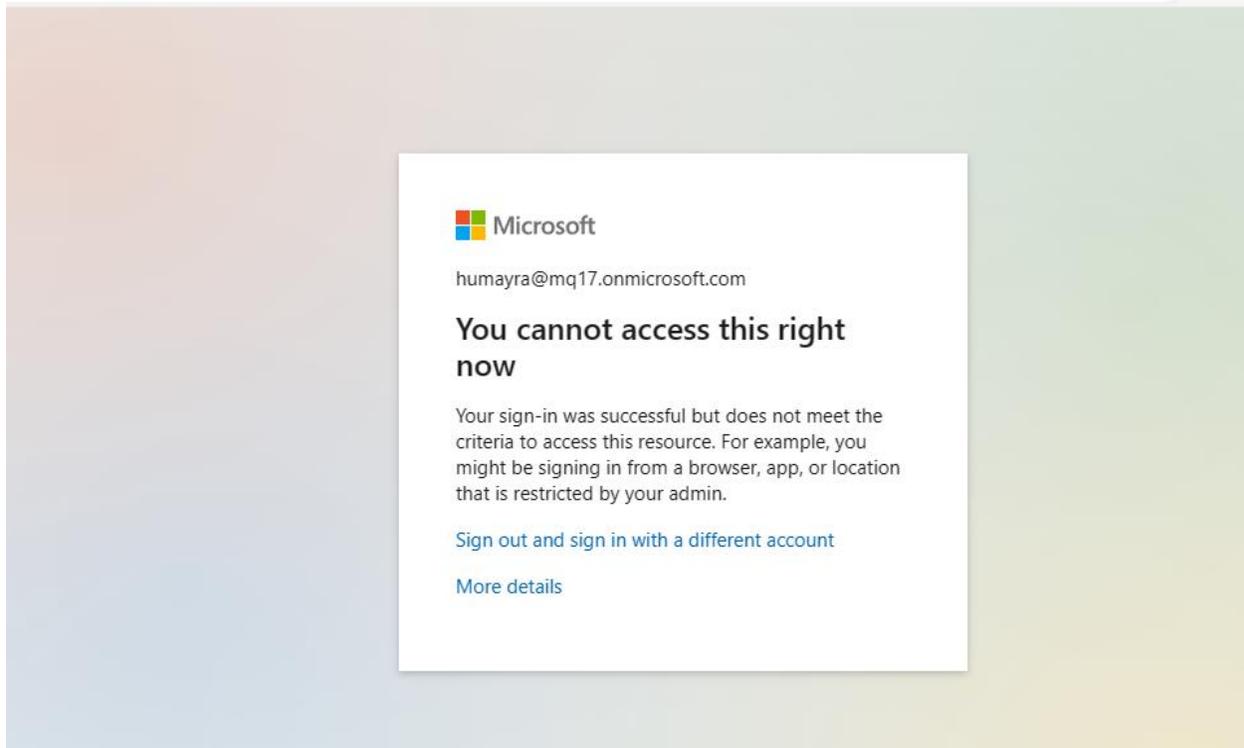
### Policy-02:

We have selected the user Humayra first. For Microsoft admin portal, we have blocked access from other devices excluding Linux & Mac.

The screenshot shows the configuration page for a Conditional Access policy named "Policy-02". The page includes the following sections:

- Policy-02** (Conditional Access policy)
- Actions: Delete, View policy information
- Learn more (link)
- Name \***: Policy-02
- Assignments**
- Users** (1 icon): Specific users included
- Target resources** (1 icon): 1 app included
- Conditions** (1 icon): 1 condition selected
- Access controls**
- Enable policy**: Report-only, **On**, Off

We tried to access to the account of humayra from windows-10 device & it didn't allow us to enter.



## Task-03: Client App Based Access Policy

### Scenario-03:

Smart Digital Bank wanted that some of their users shouldn't browse O365 from browser rather they should use app. They already applied the policy. But the new employee Apon wasn't under the policy. He must have to use app to use O365 service & smart need to create that policy immediately.

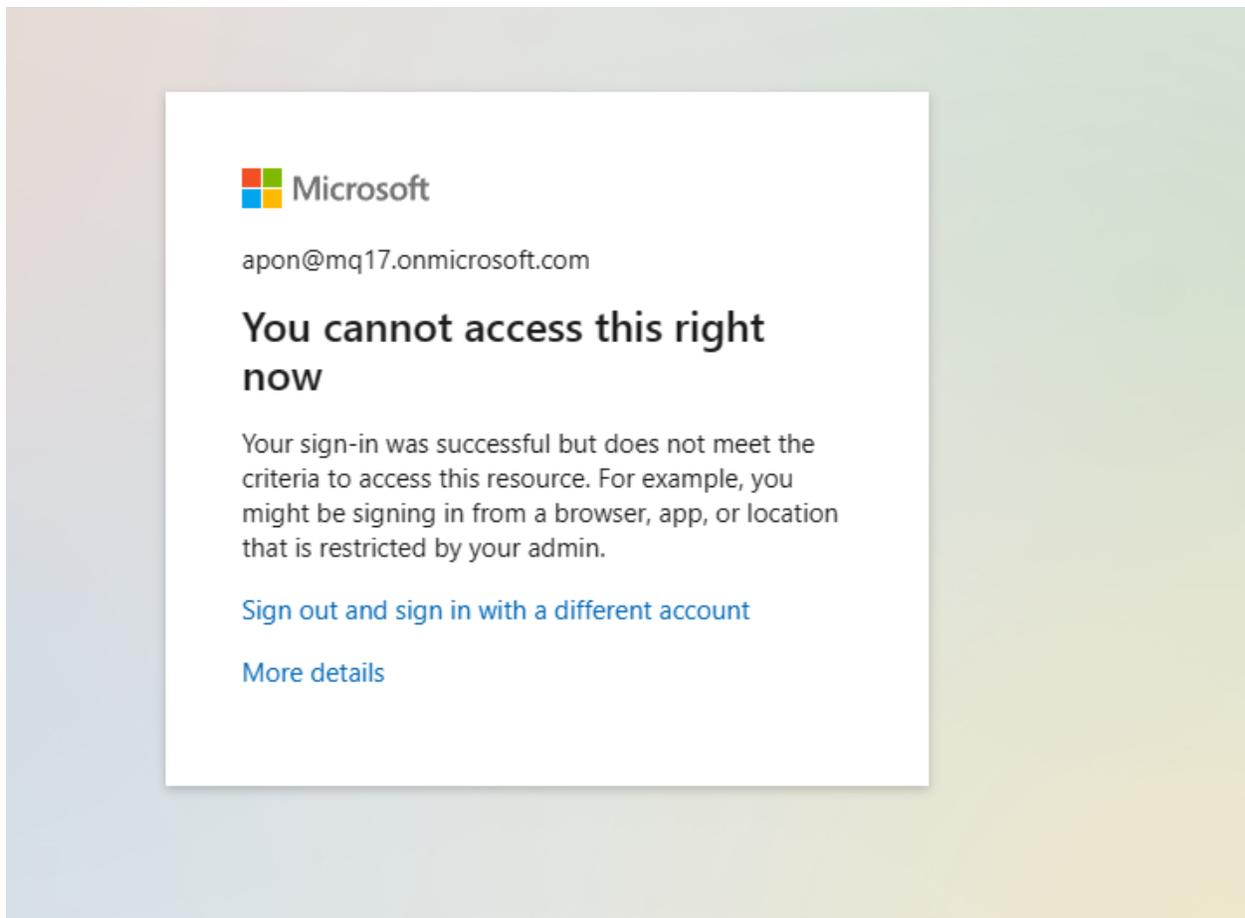
### Policy-03:

For the user Apon, we have created a conditional access policy where we have blocked O365 app access from the client app – "Browser"

The screenshot shows the Microsoft Entra Conditional Access Policy configuration page for a policy named "Policy-03". The browser address bar shows the URL: `entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade/policyId/1a2bc067-23fd-48e1-bb...`. The page has a search bar at the top with the text "Search resources, services, and docs (G+/)". The breadcrumb navigation is "Home > Conditional Access | Policies >". The policy name is "Policy-03" and it is identified as a "Conditional Access policy". There are two action buttons: "Delete" and "View policy information". A brief description states: "policy to bring signals together, to make decisions, and enforce organizational policies. Learn more". The configuration details are as follows:

- Name \***: Policy-03
- Assignments**:
  - Users**: Specific users included
  - Target resources**: 1 app included
  - Conditions**: 1 condition selected
- Enable policy**: Report-only, **On**, Off
- Save** button

Here we tried to access the account of apon from browser & our policy has successfully restricted access from browser.

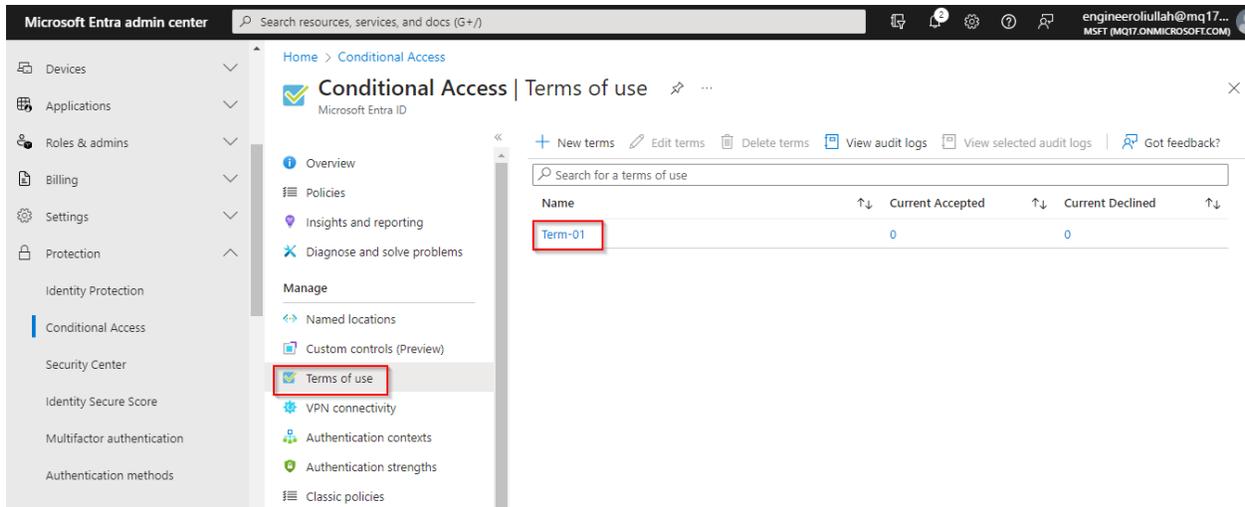


## Task-04: Terms Based Access Policy

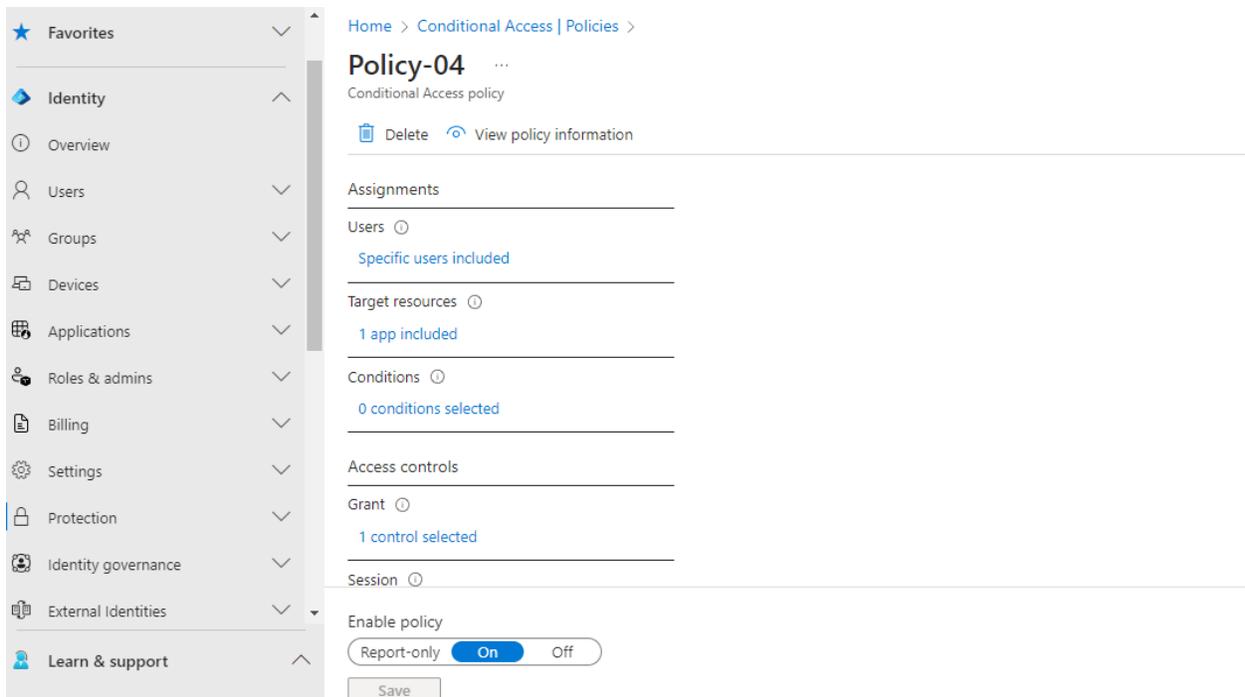
**Scenario-04:** Mr. Tanjil is an employee of Smart Digital Bank. Recently a Microsoft Entra ID user account has been created for him. But when he will login first time, he will have to accept the terms & conditions. Otherwise his access will be limited or denied.

### Policy-04:

At first we have created a pdf file of Terms & Conditions. We have gone to the following path Conditional access → Manage → Terms of Use & have uploaded our file & created Term-01.



Then we have gone to the conditional access policy, added the user Tanjil & selected the Term-01 under allow access

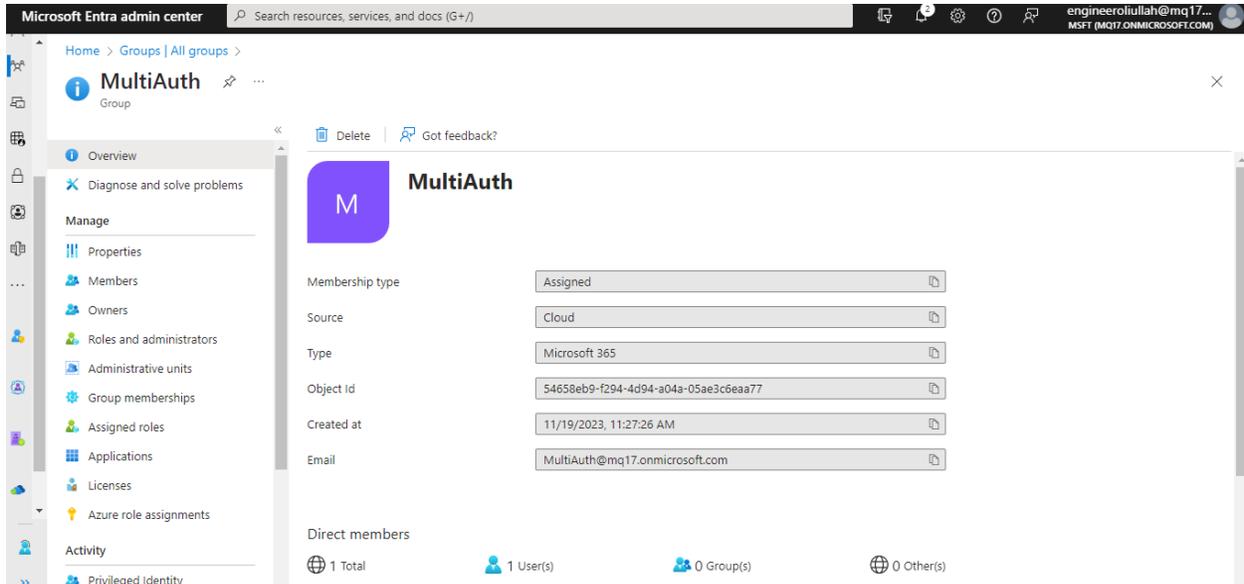


Now we can see when the user logged in his account, a new page with terms & conditions have come out. The user must have to accept it to access the resources.

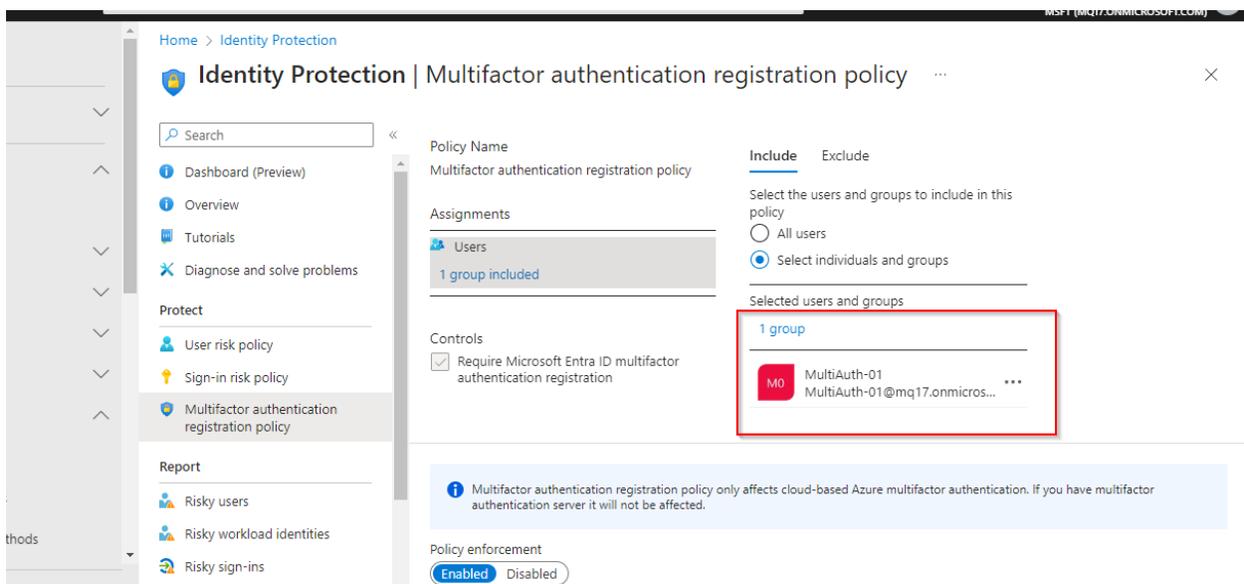


### Policy-05:

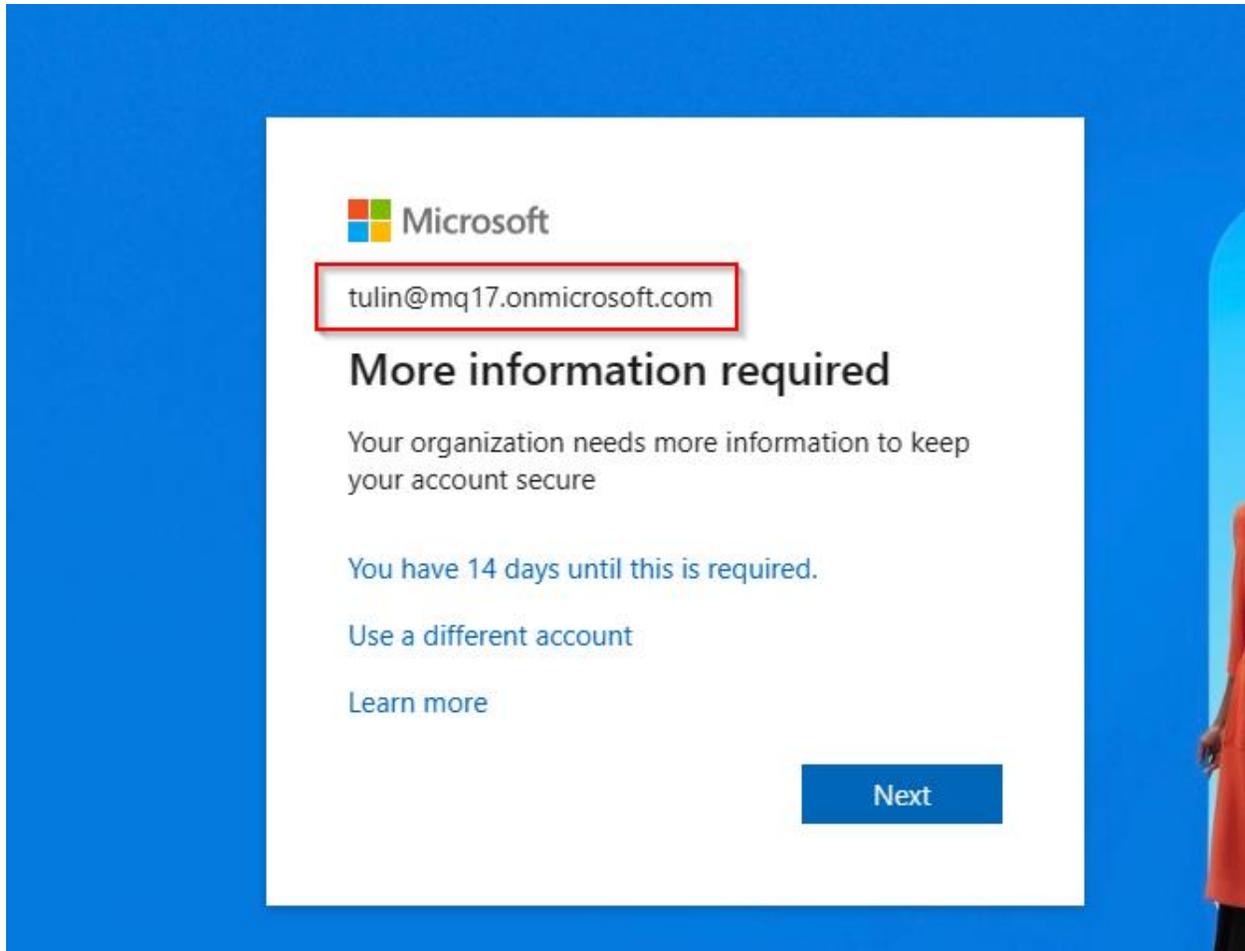
Before applying the multifactor authentication policy, we have created a group called “MultiAuth” & have assigned user Tulin in the group. We can put all the users who requires multifactor authentication in this group.



Then we have selected the Multifactor authentication registration policy from Identity Protection. We have added the group – “MultiAuth-01” in this policy & enabled this policy.



Here we can see that even after submitting the username & password, it's not letting us to enter. Rather it's asking for more information.



When will clicked next to go forward it's asking to authenticate using Microsoft Authenticator App. We can connect with the app by scanning the QR code & verify with a two digit code. Only after completing these two steps, a user can access the service.

**Keep your account secure**

Your organization requires you to set up the following methods of proving who you are.

### Microsoft Authenticator



**Start by getting the app**

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

[Next](#)

[I want to set up a different method](#)

**Thank You**