Unlocking Security: Microsoft Entra ID Policy Deployment

Prepared By

Md. Rishad Istiak Sachcha

Md. Oliullah

Contents

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.

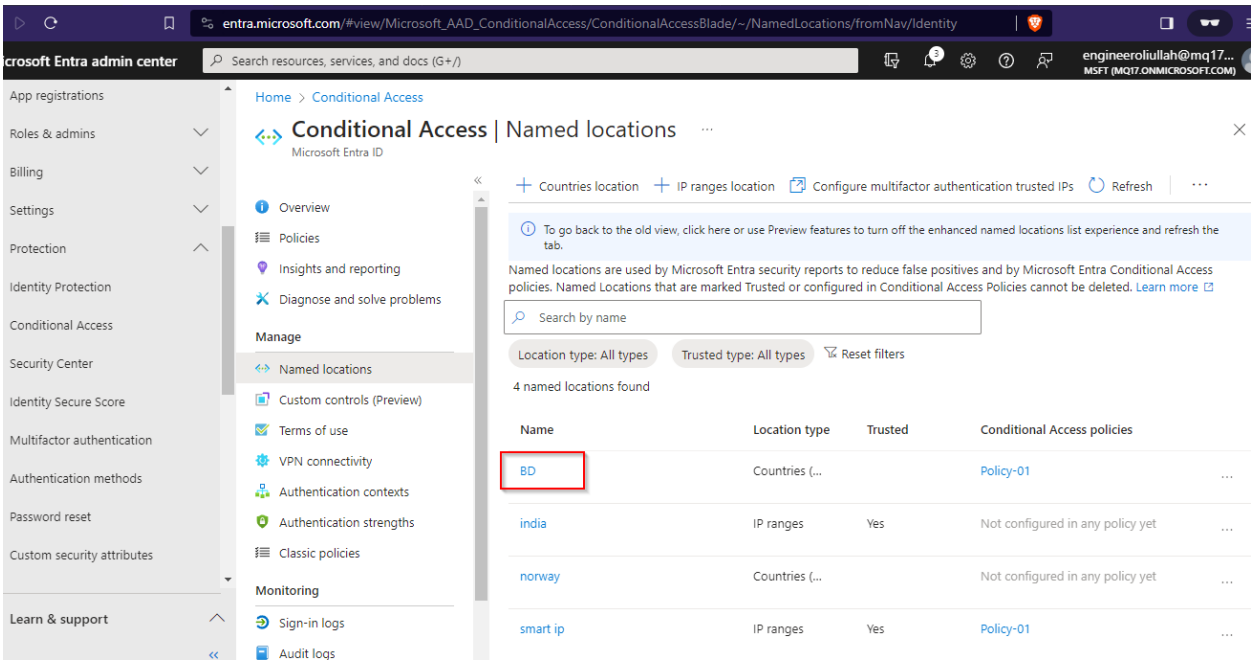
Task-01: Location Based Access Policy

Scenario-01:

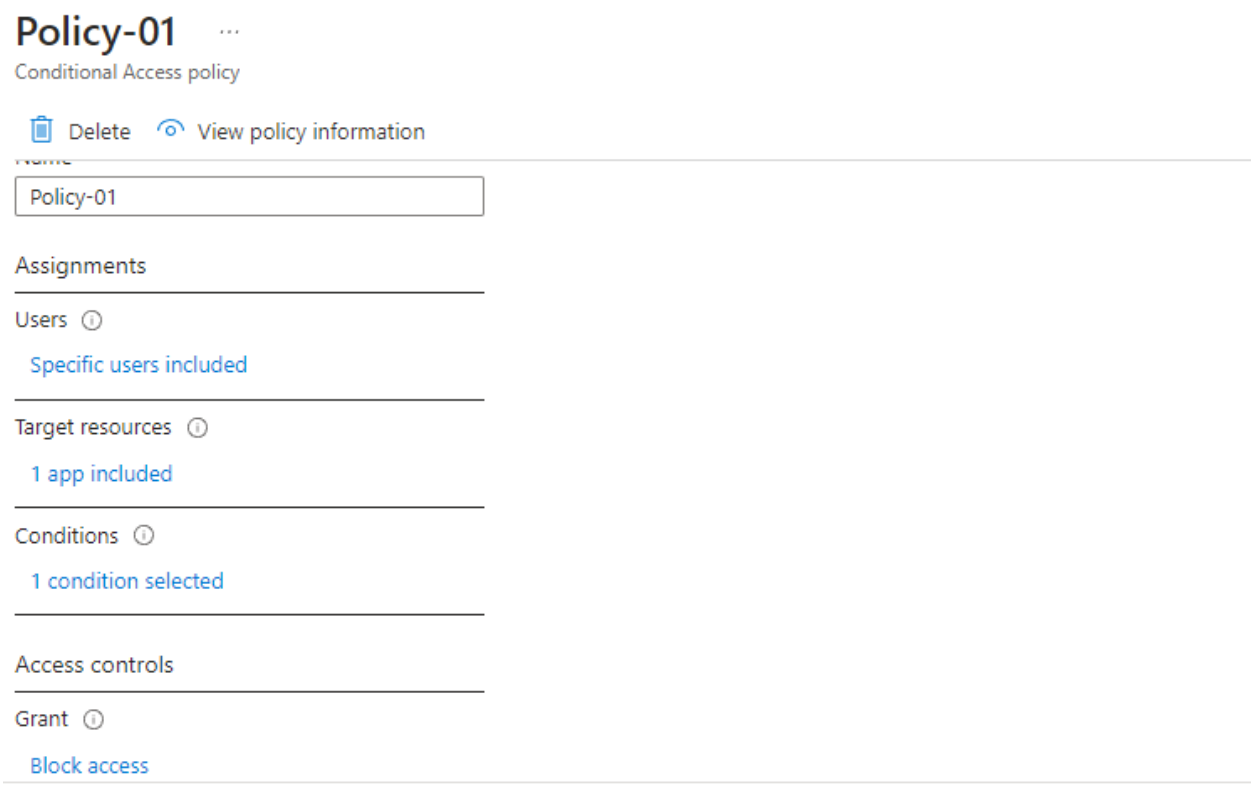
Recently Smart Digital Bank is facing different identity related attacks like spamming, bruteforce attack etc. The security team has informed that the attacks are coming from Bangladesh region. So We have to Block access from Bangladesh region. In this case we have blocked access from Bangladesh for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

Policy-01:

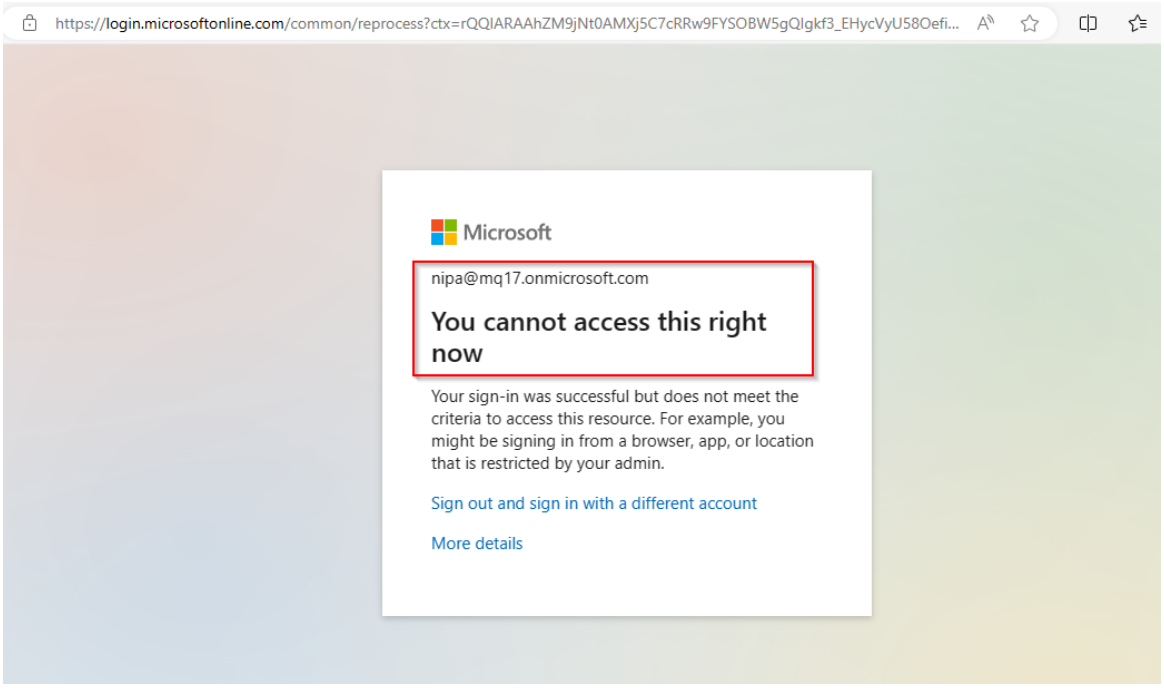
First of all we will have to select the location. We can select location in two ways – 1. Geolocation 2. Ip address. Here we have selected Bangladesh region according to geolocation.



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.



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.

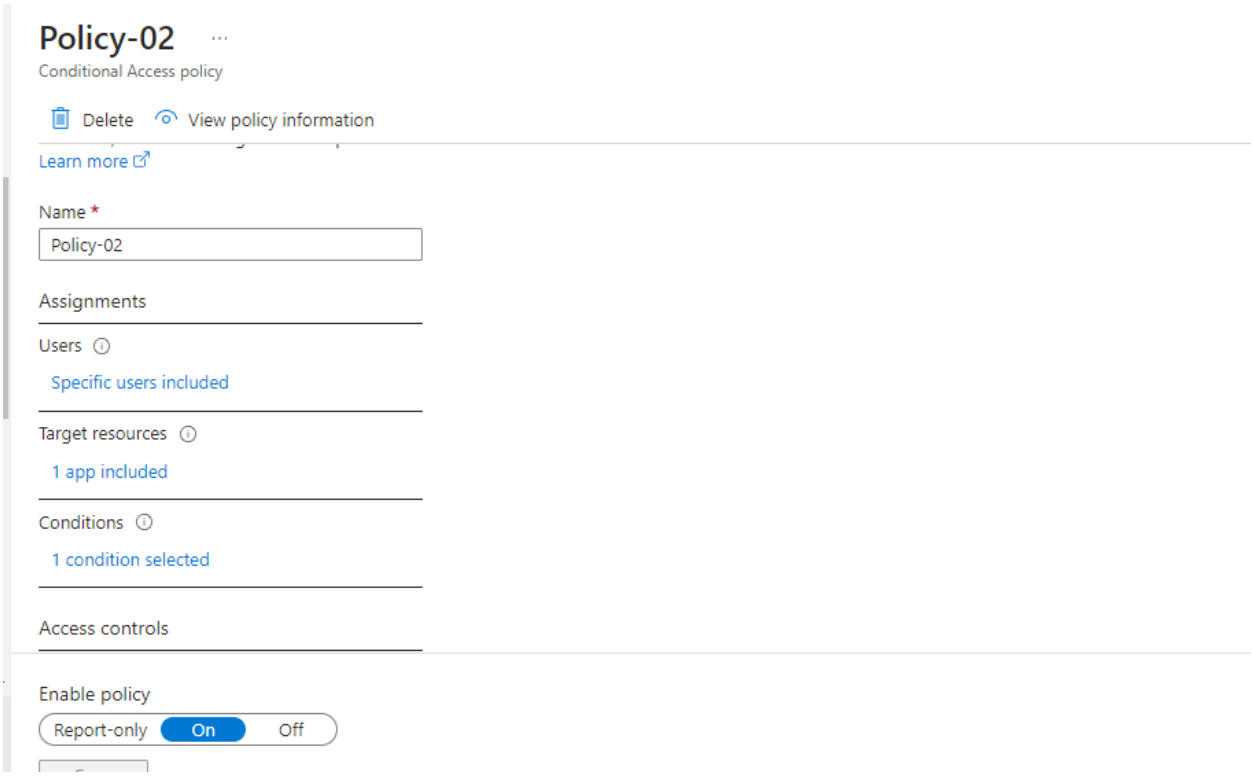


Task-02: Device Based Access Policy

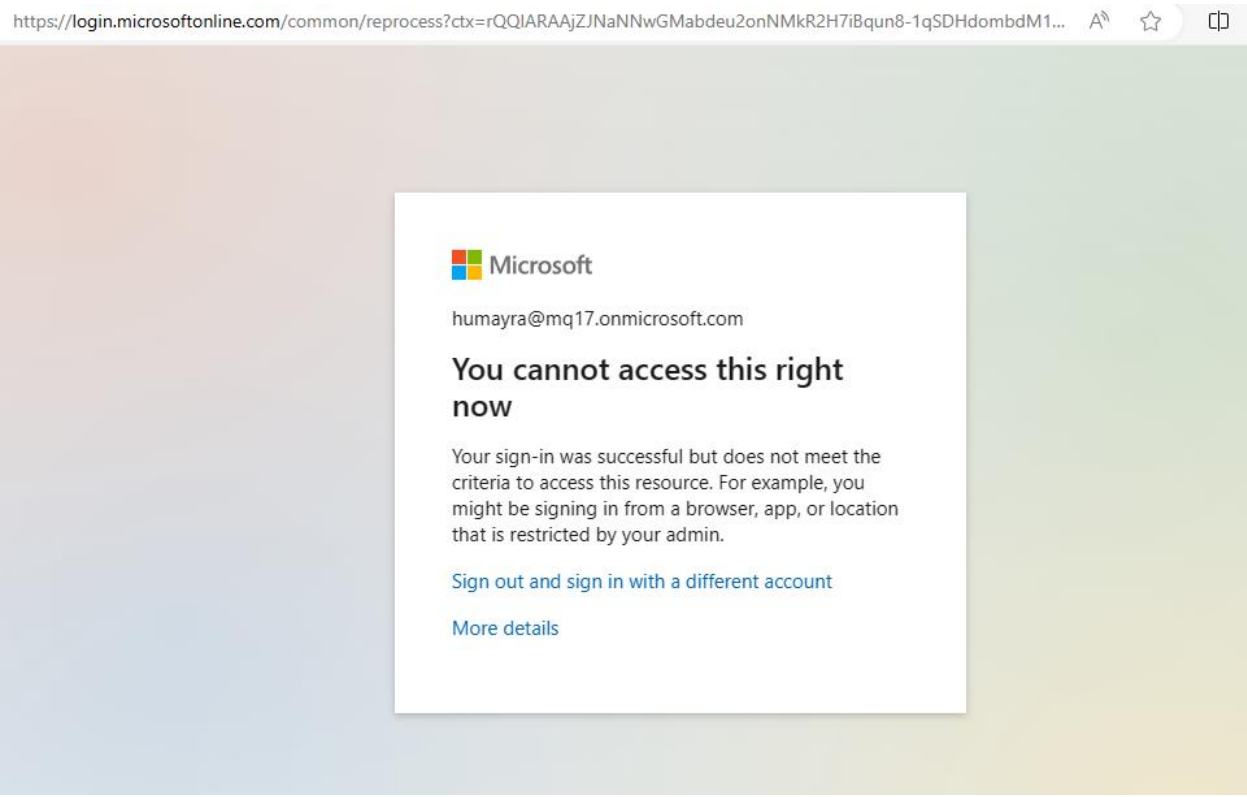
Scenario-02: Humayra- an employee of Smart Digital Bank. She is a user of Microsoft 365. Recently Smart Digital Bank has created a policy that M365 will only be accessible from Linux & Mac device. So they have to update their policy at Entra Conditional Access.

Policy-02:

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



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



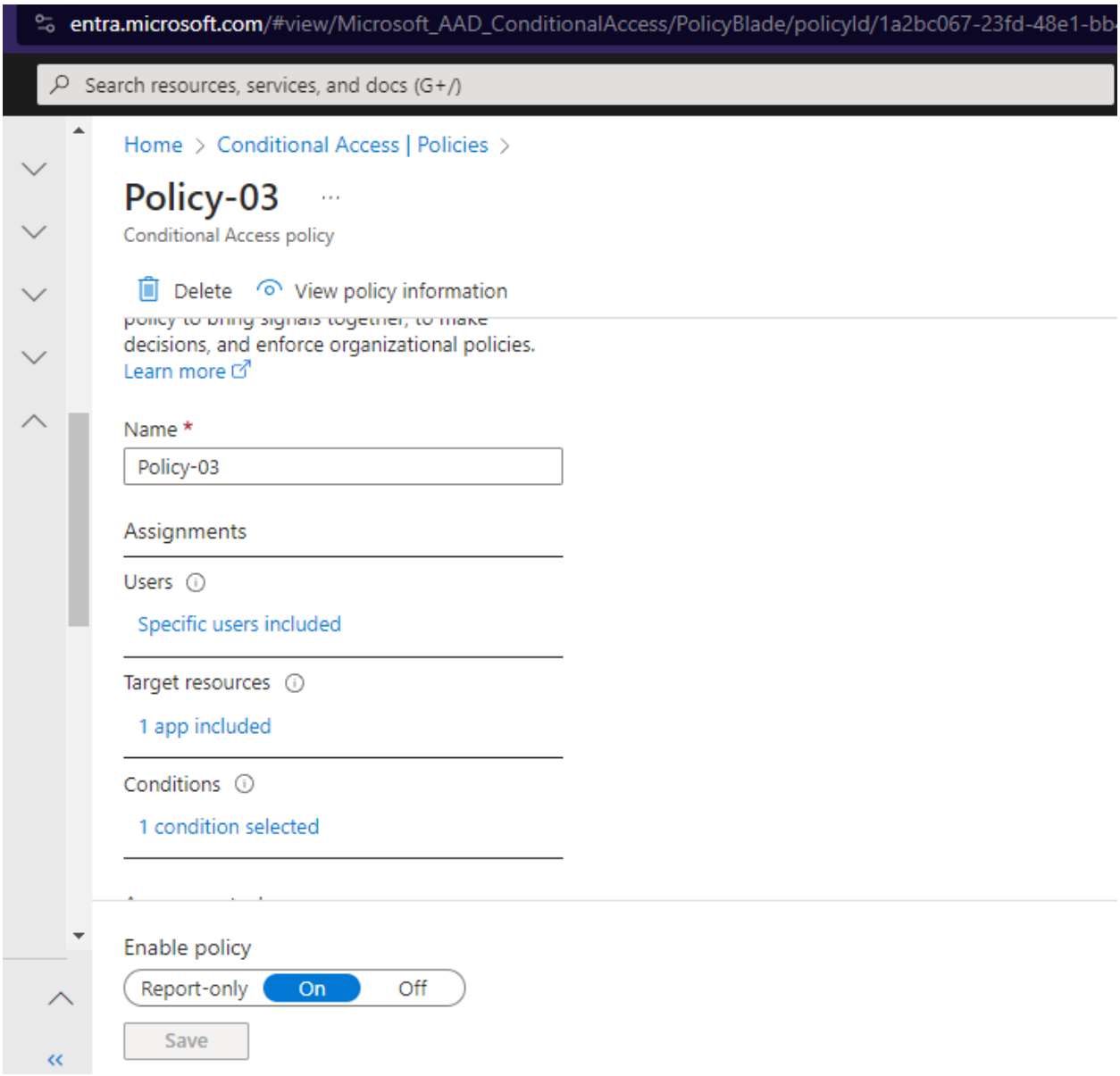
Task-03: Client App Based Access Policy

Scenario-03:

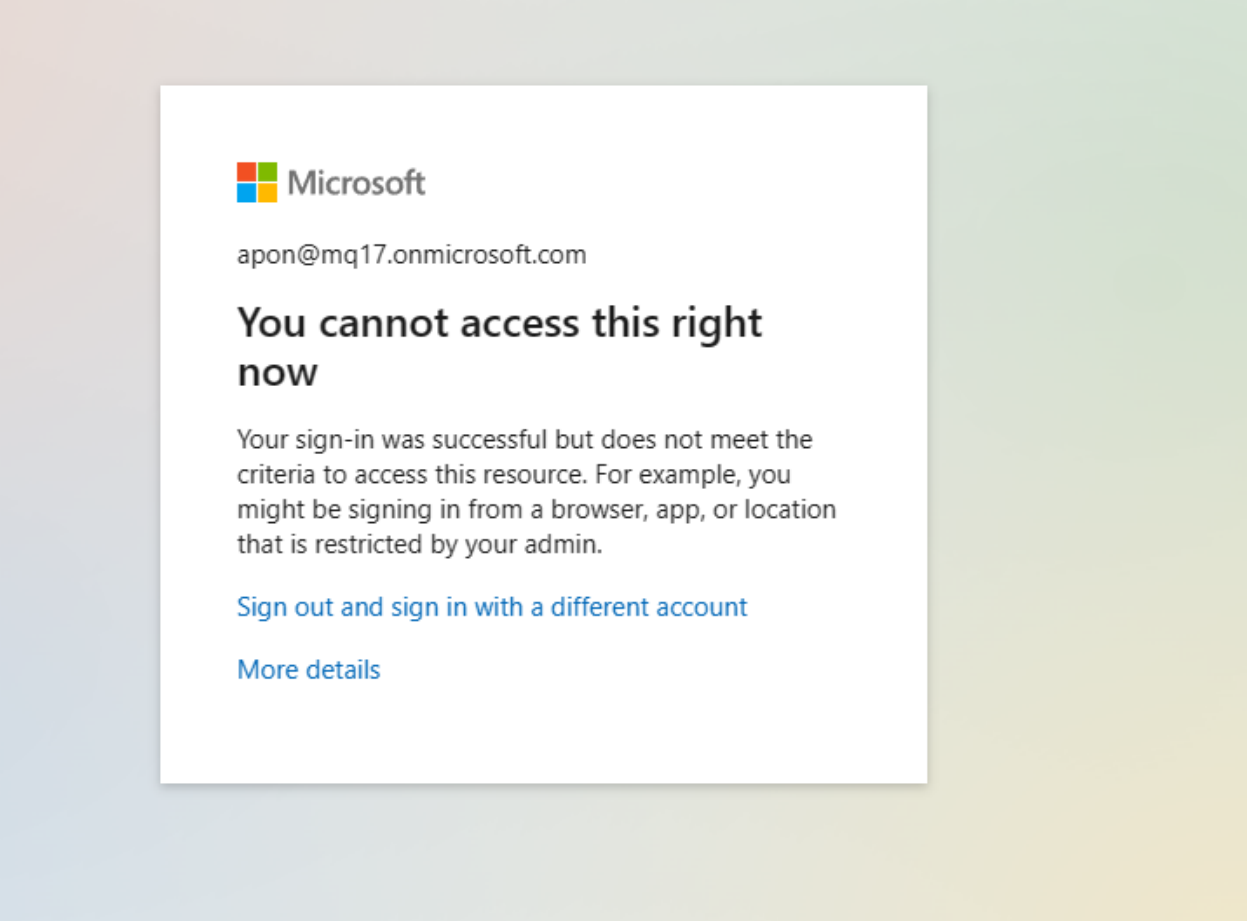
Smart Digital Bank wanted that some of their users shouldn't browse O365 from browser rather they should use app. They already applied the policy. But the new employee Apon wasn't under the policy. He must have to use app to use O365 service & smart need to create that policy immediately.

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"



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

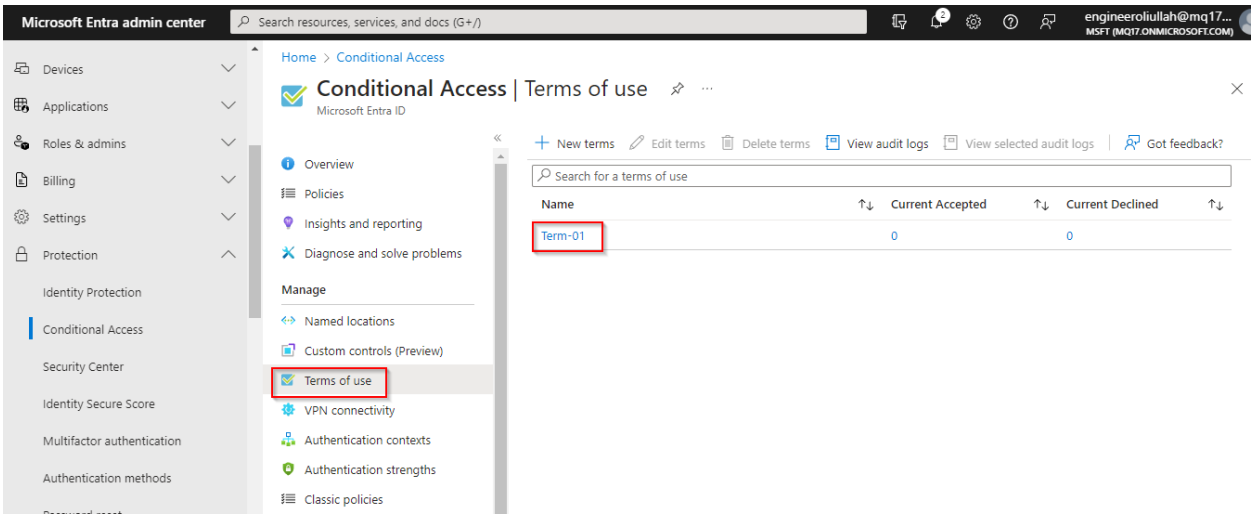


Task-04: Terms Based Access Policy

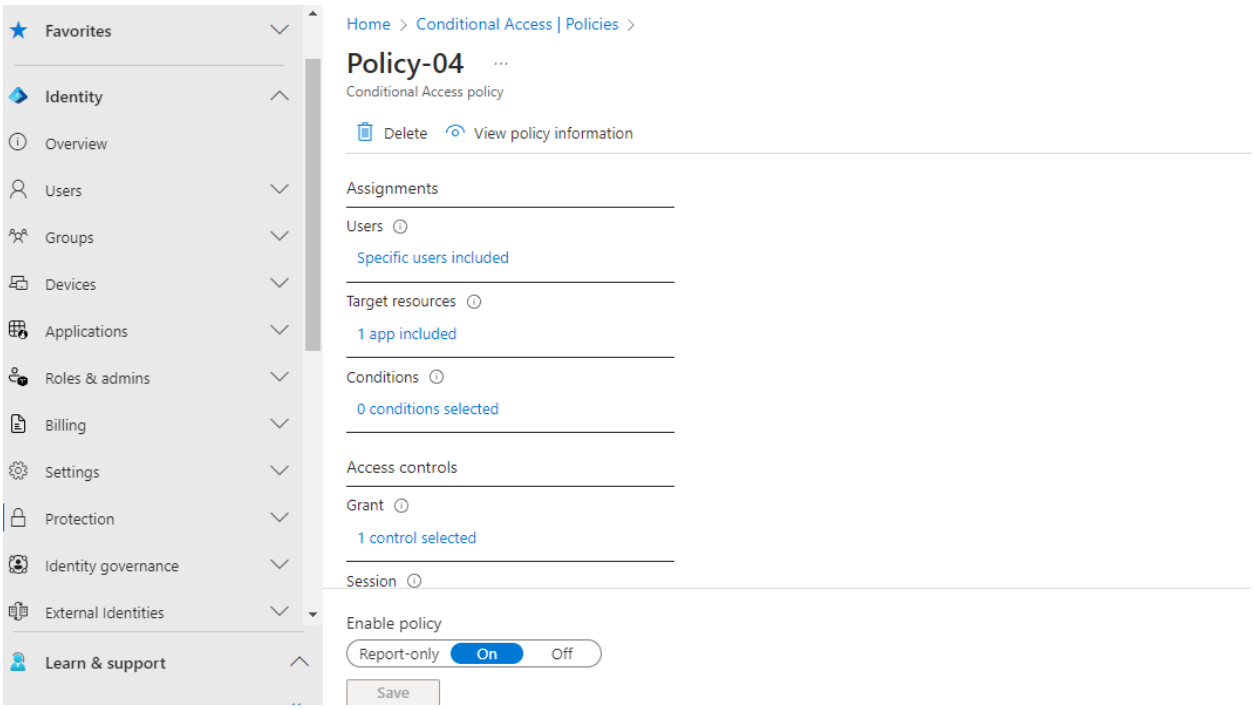
Scenario-04: Mr. Tanjil is an employee of Smart Digital Bank. Recently a Microsoft Entra ID user account has been created for him. But when he will login first time, he will have to accept the terms & conditions. Otherwise his access will be limited or denied.

Policy-04:

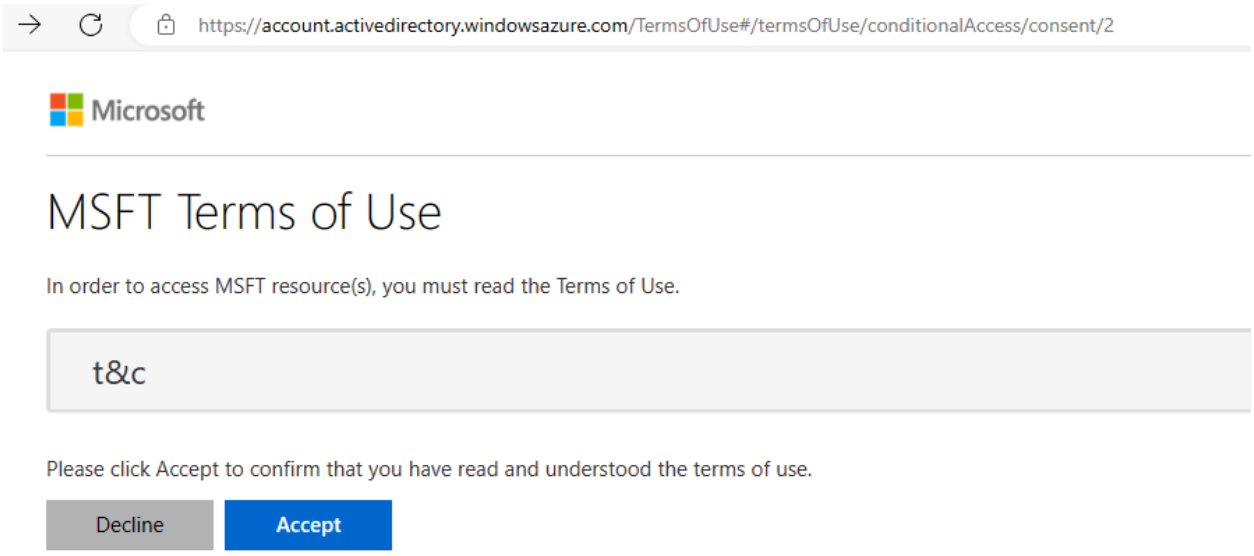
At first we have created a pdf file of Terms & Conditions. We have gone to the following path Conditional access → Manage → Terms of Use & have uploaded our file & created Term-01.



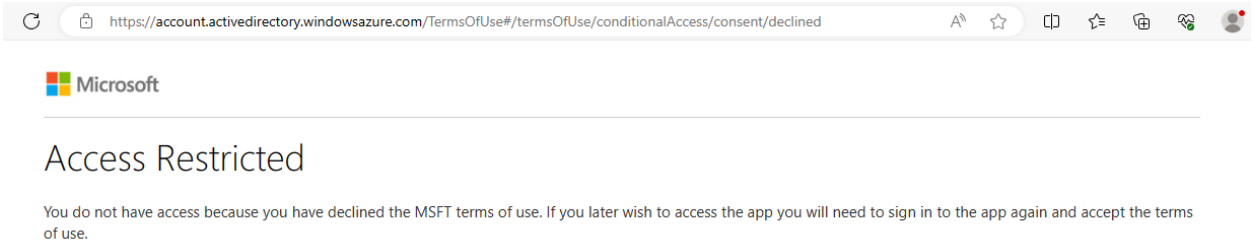
Then we have gone to the conditional access policy, added the user Tanjil & selected the Term-01 under allow access



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.



Here we can see that the user declined and failed to access the resources.

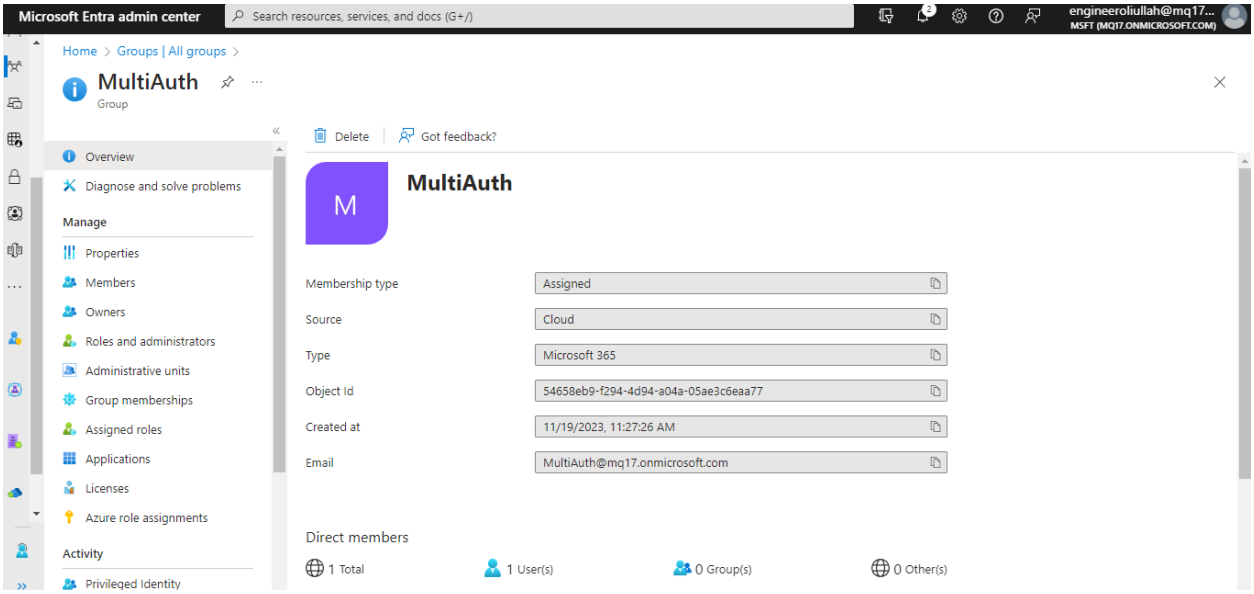


Task-05: Multifactor Authentication Registration Policy

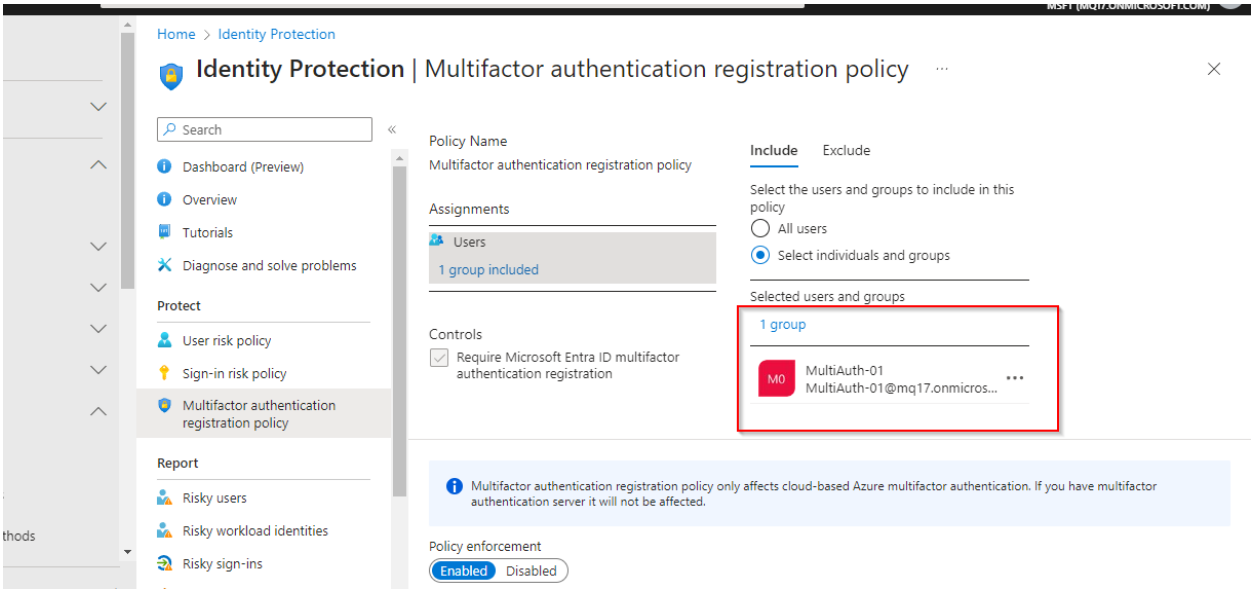
Scenario-05: Recently authentication related attacks like bruteforce, password spraying etc has increased. Some of the employees has already become victim of this attack. Smart Digital Bank is concerned about this issue. So Smart Digital Bank have decided to deploy multifactor authentication policy to a certain group of users. Tulin is one of them.

Policy-05:

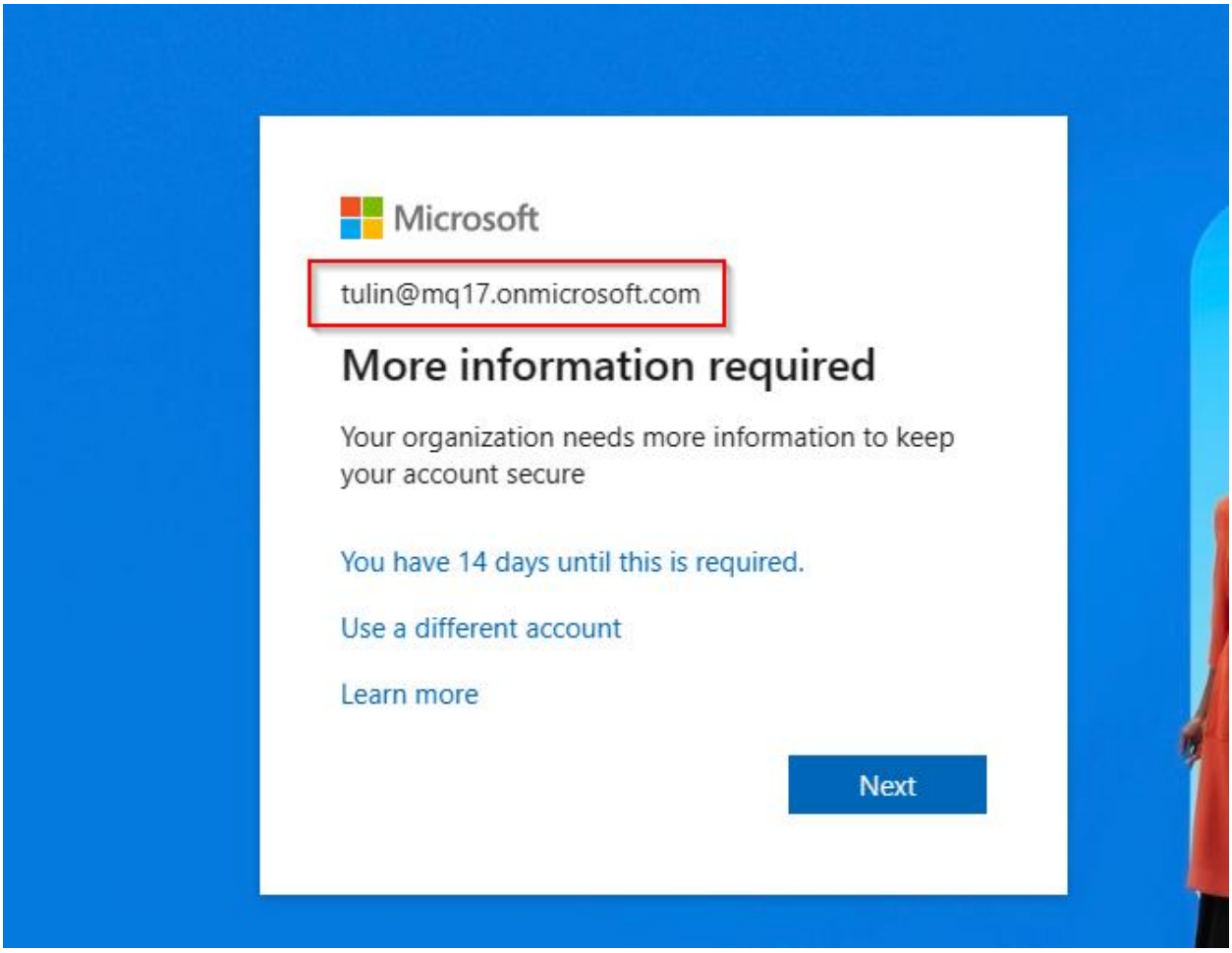
Before applying the multifactor authentication policy, we have created a group called “MultiAuth” & have assigned user Tulin in the group. We can put all the users who requires multifactor authentication in this group.



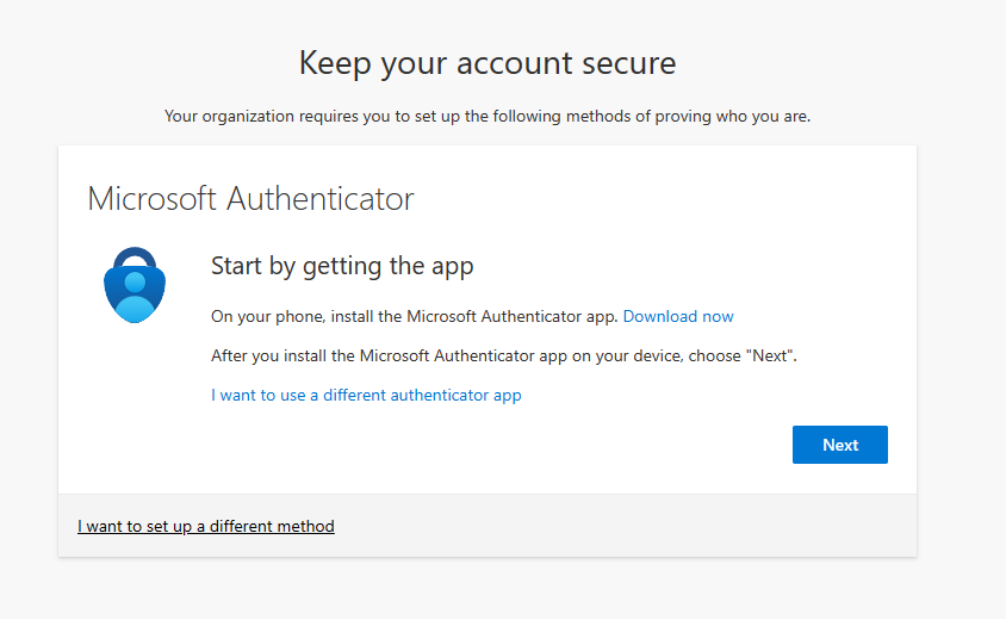
Then we have selected the Multifactor authentication registration policy from Identity Protection. We have added the group – “MultiAuth-01” in this policy & enabled this policy.



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.



Thank You