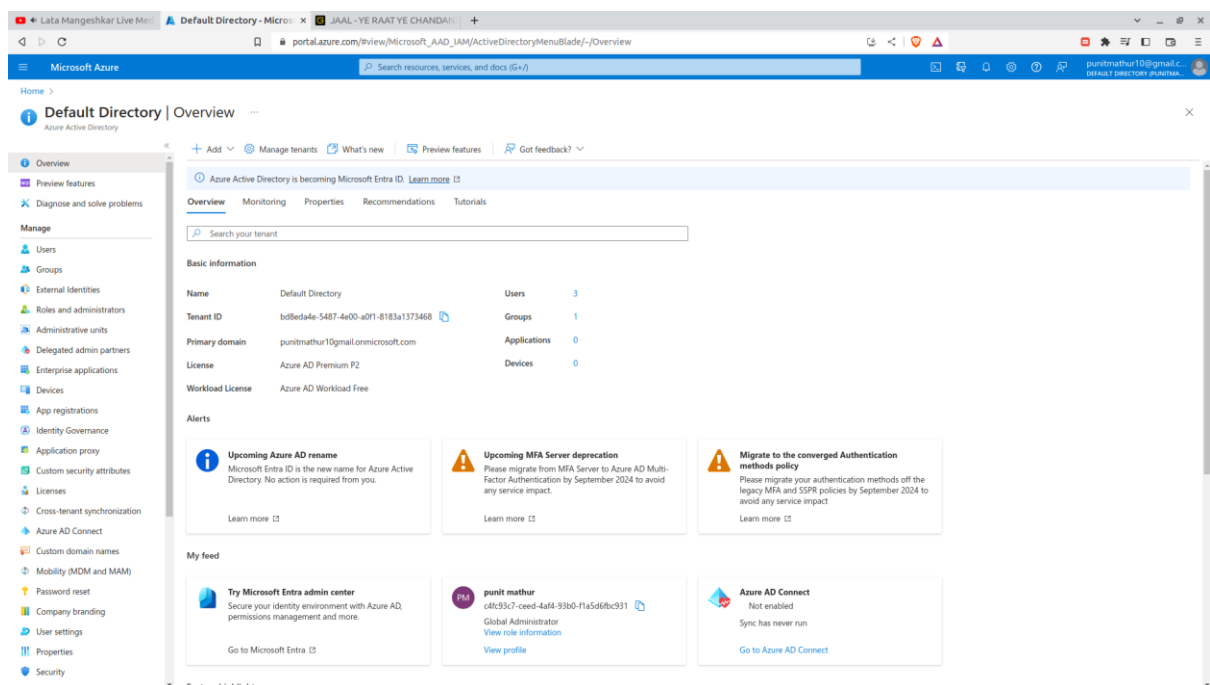


Users, Groups and MFA

Task - in this particular task we will make users and groups using azure active directory and then after that we will implement Multi-Factor Authentication.

Follow the following instructions to create test users and test groups from azure AD

Now search for azure AD directory in the search bar.



Now, go to the Users on the left side and then in the users panel, click on new user and then select Create New User.

New user will be named TestUser1.

Now after deploying TestUser1 go to the assigned roles section of it and add an assignment as “User Administrator”.

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation pane is visible with the 'Assigned roles' section selected. The main content area is titled 'TestUser1 | Assigned roles'. The 'Administrative roles' section is active, showing a list of roles. The 'Directory roles' panel is open, displaying a list of roles. The 'User Administrator' role is selected, and its description is visible: 'Can manage all aspects of users and groups, including resetting passwords for limited admins.'

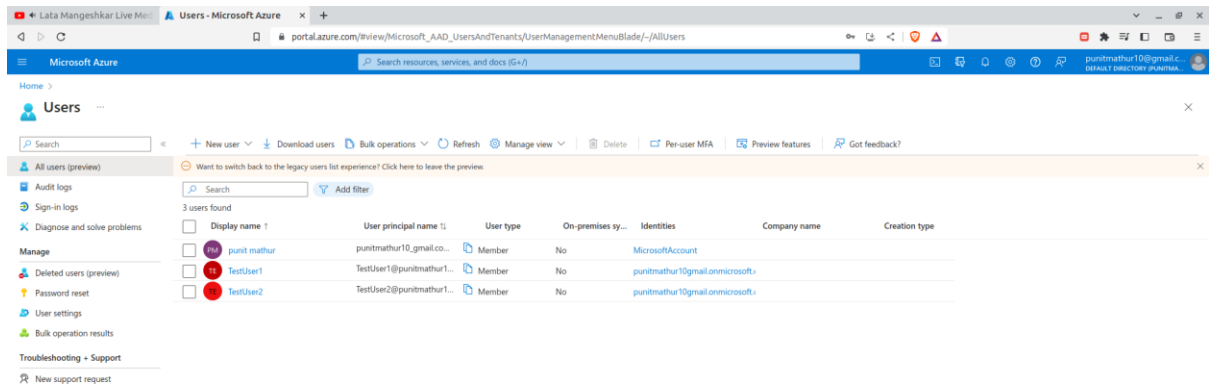
Role	Description
<input type="checkbox"/> Application Developer	Can create application registrations independent of the 'Users can register applications' setting.
<input type="checkbox"/> Authentication Administrator	Can access to view, set and reset authentication method information for any non-admin user.
<input type="checkbox"/> Authentication Extensibility Administrator	Customize sign in and sign up experiences for users by creating and managing custom authentication extensions.
<input type="checkbox"/> Azure AD Joined Device Local Administrator	Users assigned to this role are added to the local administrators group on Azure AD-joined devices.
<input type="checkbox"/> Directory Writers	Can read and write basic directory information. For granting access to applications, not intended for users.
<input type="checkbox"/> Extended Directory User Administrator	Manage all aspects of external user profiles in the extended directory for Teams.
<input type="checkbox"/> External ID User Flow Administrator	Can create and manage all aspects of user flows.
<input type="checkbox"/> External ID User Flow Attribute Administrator	Can create and manage the attribute schema available to all user flows.
<input type="checkbox"/> Guest Inviter	Can invite guest users independent of the 'members can invite guests' setting.
<input type="checkbox"/> License Administrator	Can manage product licenses on users and groups.
<input type="checkbox"/> Office Apps Administrator	Can manage Office apps cloud services, including policy and settings management, and manage the ability to select, unselect and publish 'what's new' feature content to end-user's devices.
<input type="checkbox"/> Organizational Messages Writer	Write, publish, manage, and review the organizational messages for end-users through Microsoft product surfaces.
<input type="checkbox"/> Privileged Authentication Administrator	Can access to view, set and reset authentication method information for any user (admin or non-admin).
<input checked="" type="checkbox"/> User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.
<input type="checkbox"/> User Experience Success Manager	View product feedback, survey results, and reports to find training and communication opportunities.

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation pane is visible with the 'Assigned roles' section selected. The main content area is titled 'TestUser1 | Assigned roles'. The 'Administrative roles' section is active, showing a list of roles. The 'User Administrator' role is assigned to the user, and its details are visible in the table below.

Role	Description	Resource Name	Resource Type	Assignment Path	Type
<input checked="" type="checkbox"/> User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	Directory	Organization	Direct	Built-in

Now repeat the following steps to make another user named TestUser2.

Note - remember their username and password so that we can sign into them later on.



Both the test users are created. Now we will log into them later on but first we will create some test groups.

Now in your default directory, go to groups and click on it. Now, in the New Group window, write the Group Name and then click on Yes for Azure AD roles can be assigned to this group. Now in lower sections select TestUser1 as Group owner and TestUser2 as Group member and then click on Create.

Microsoft Azure

Home > Groups | All groups >

New Group

Got feedback?

Group type *

Group name *

Group description

Azure AD roles can be assigned to the group ☒ Yes ☐ No

Membership type

Owners
1 owner selected

Members
1 member selected

Roles
No roles selected

Create

TestGroup is Created

Microsoft Azure

Home > Groups | All groups

Default Directory - Azure Active Directory

New group Download groups Refresh Manage view Delete Got feedback?

Dynamic group memberships have not been updated due to system delays. We're working to resolve the issue.

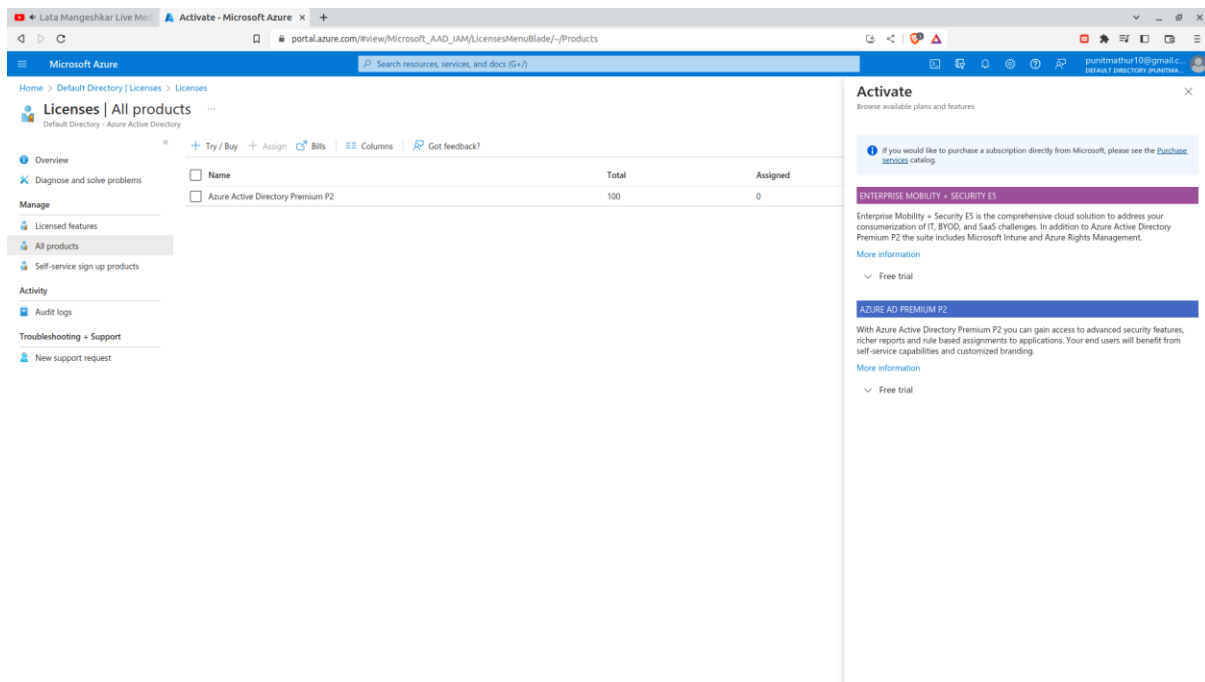
Search Add filter

Search mode ☒ Contains

1 group found

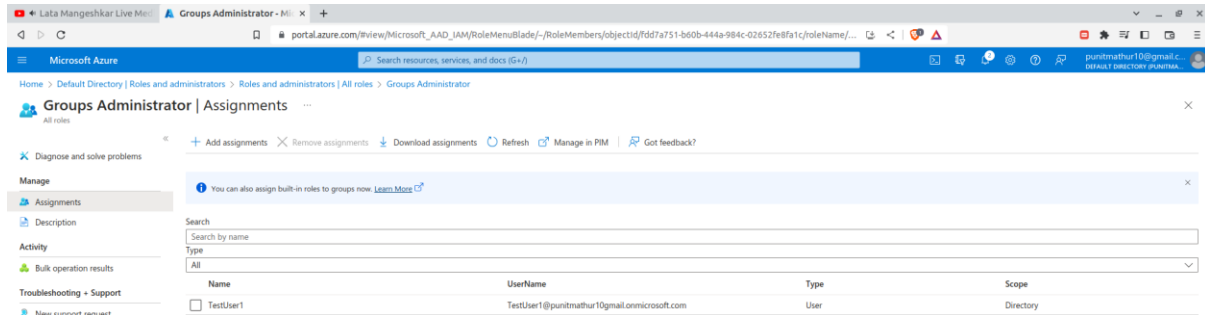
<input type="checkbox"/>	Name	Object Id	Group type	Membership type	Email	Source
<input checked="" type="checkbox"/>	TestGroup	f84ce4e6-3137-4ea6-a17a-b46ac1232c3f	Security	Assigned		Cloud

Now we will take a free trial of Azure AD Premium P2 licence. Go to the Default directory and then licences and then all products and then click on the free trial. Then open roles and administrator and there we can see assignments, there we can see TestUser1



Microsoft Azure portal screenshot showing the 'Licenses | All products' page. The page displays a table with columns for Name, Total, and Assigned. The table shows 'Azure Active Directory Premium P2' with a total of 100 and 0 assigned. On the right, the 'Activate' panel shows the 'Free trial' option for 'AZURE AD PREMIUM P2'.

Name	Total	Assigned
Azure Active Directory Premium P2	100	0

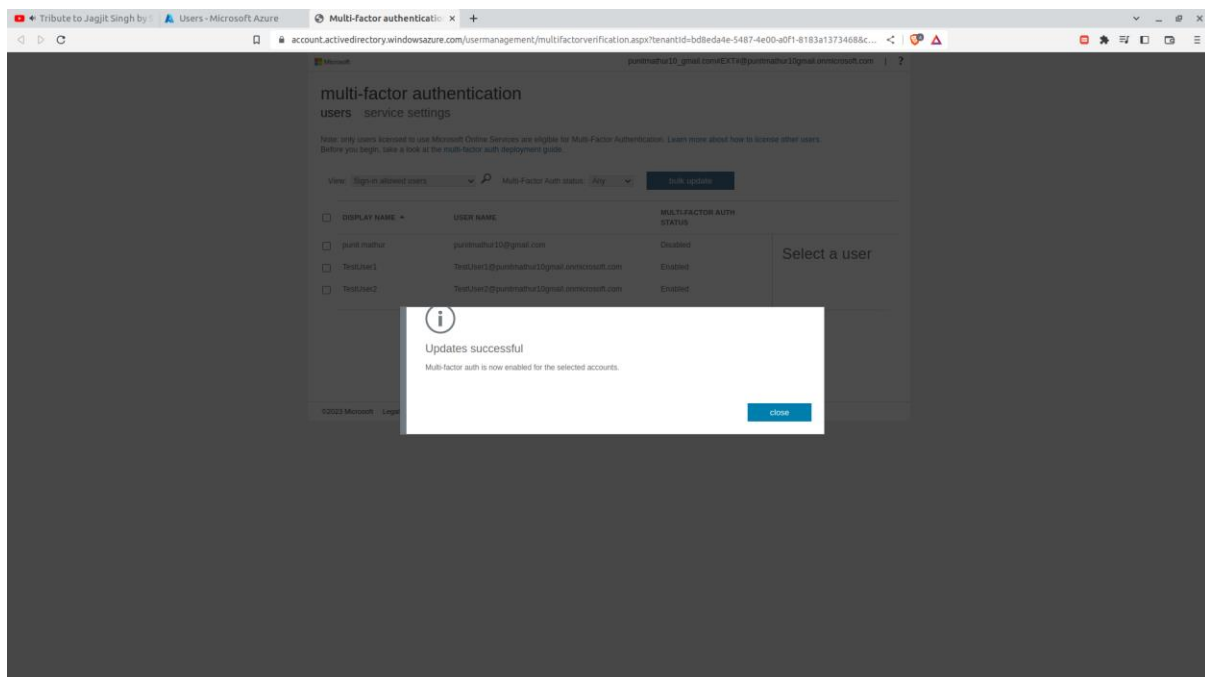
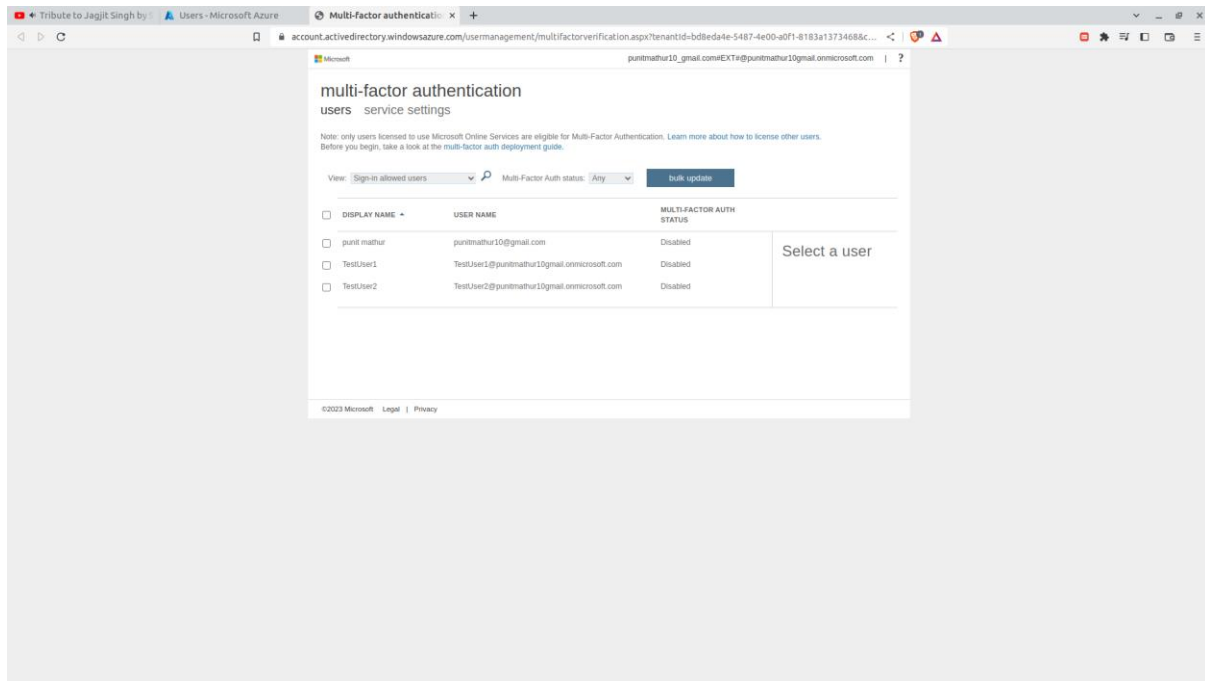


Microsoft Azure portal screenshot showing the 'Groups Administrator | Assignments' page. The page displays a table with columns for Name, Username, Type, and Scope. The table shows 'TestUser1' with a username of 'TestUser1@punitmathur10gmail.onmicrosoft.com', type of 'User', and scope of 'Directory'.

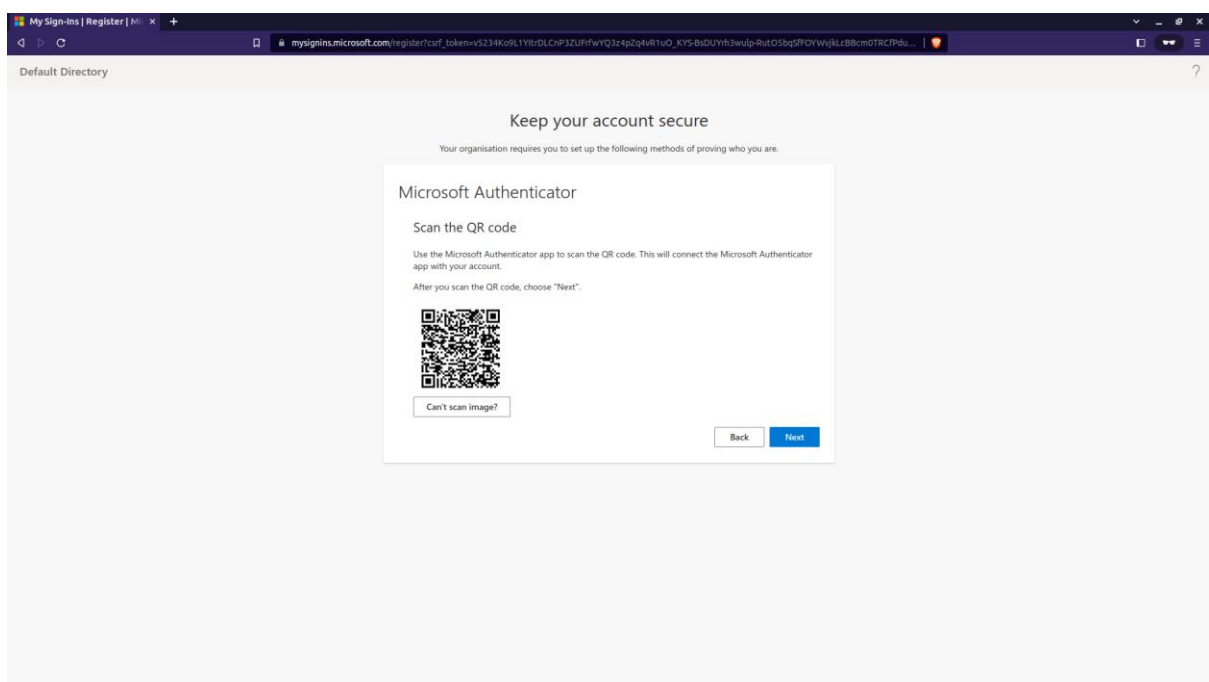
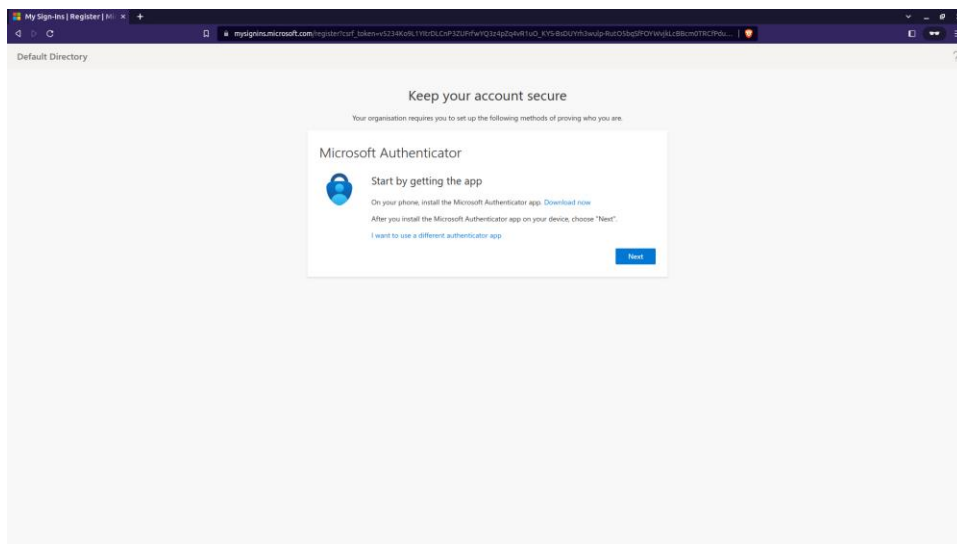
Name	Username	Type	Scope
TestUser1	TestUser1@punitmathur10gmail.onmicrosoft.com	User	Directory

Now after creating Groups and users, We will Implement Multi-Factor Authentication.

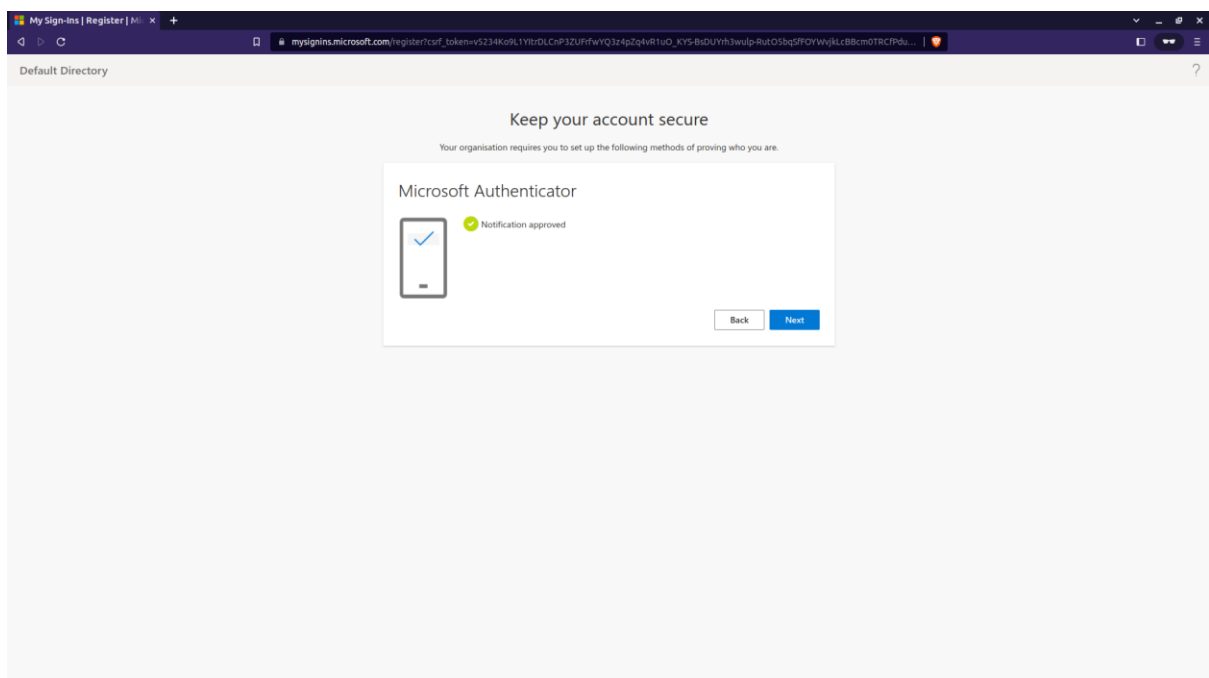
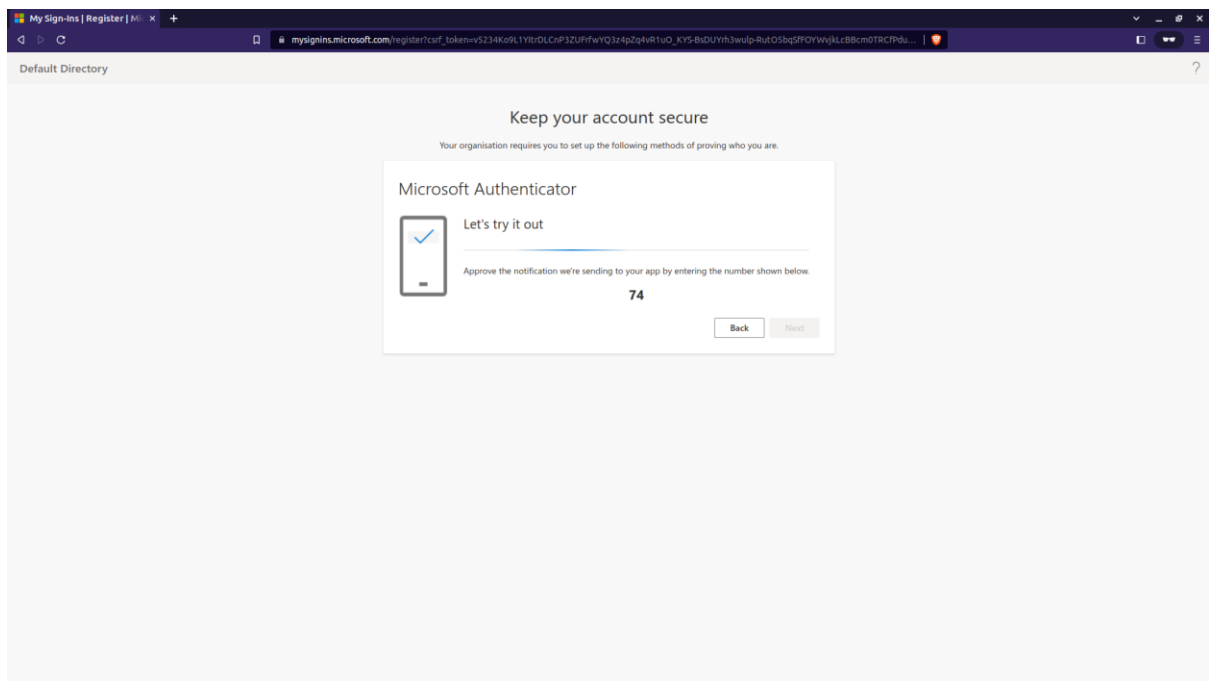
Now, to enable Multi Factor Authentication (MFA) for testuser1, go to the Users from the left side in Azure Active Directory and then in the navigation bar, click on Per-user MFA. This will open the new tab of MFA. Now, in the MFA tab, select the user (in this case testuser1) whose MFA we have to enable and then on the right side click on enable. This will pop up a new window, in that window click on enable multi-factor auth.

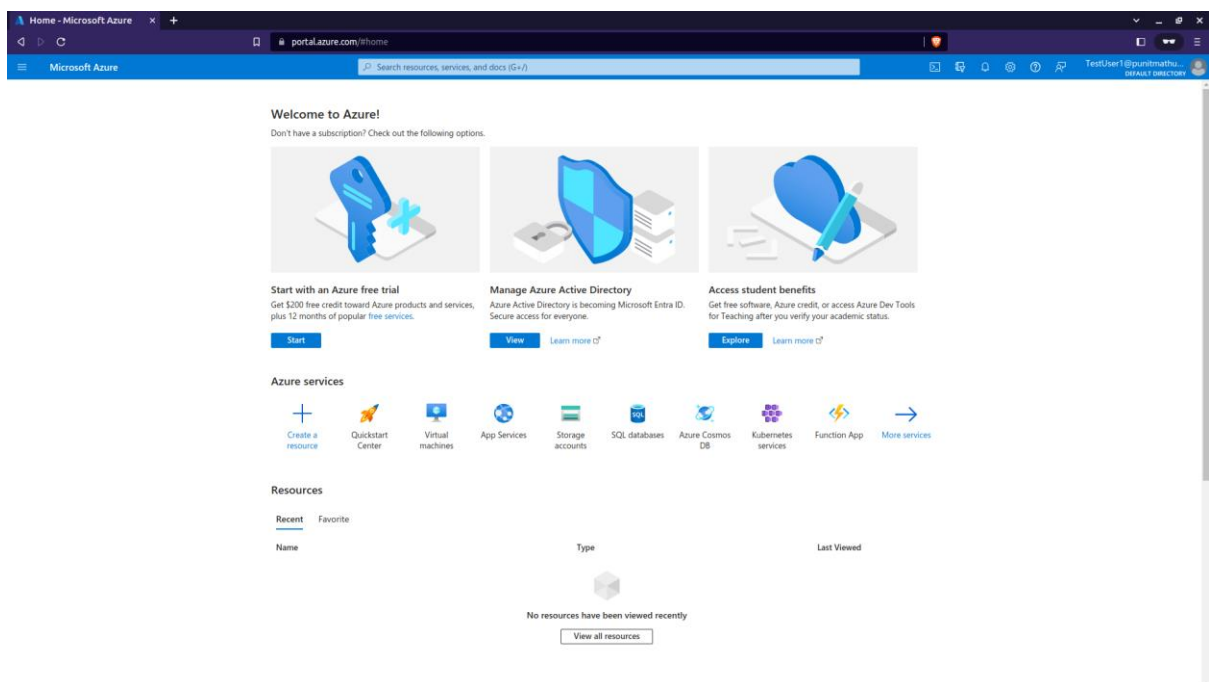
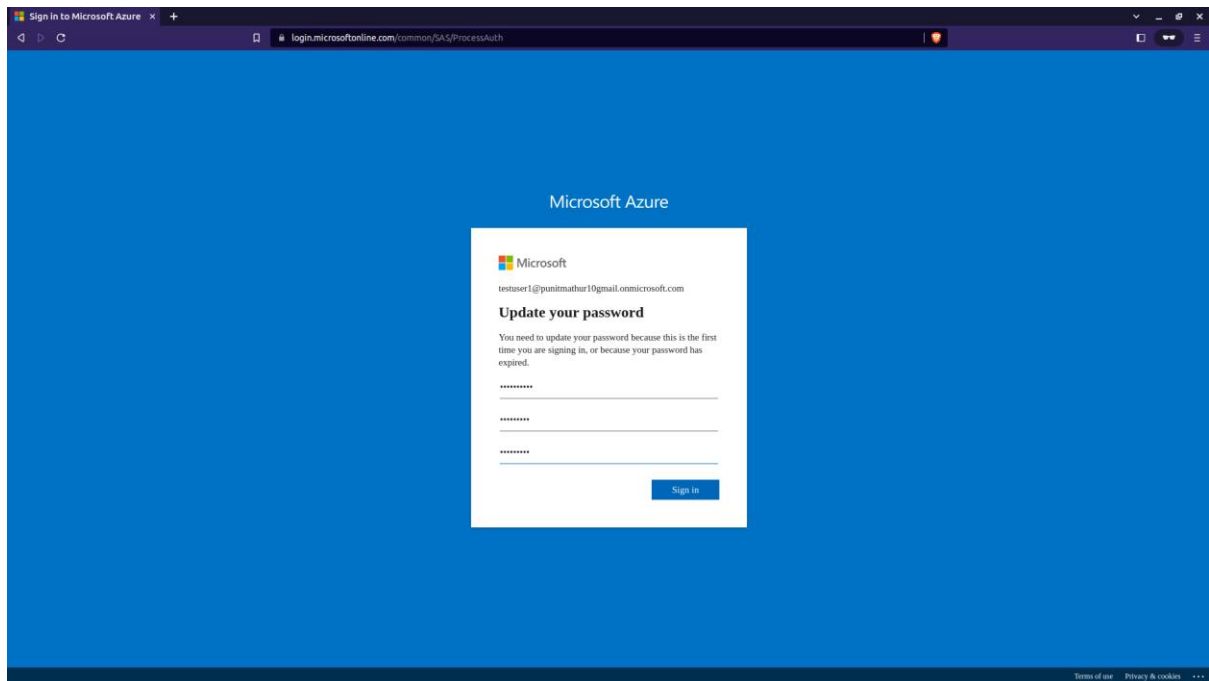


Now, to start the MFA for the user (testuser1) sign in with the testuser1 user principal name and then write the password and after clicking on sign in you will be redirected to a new window. And in that window click on Next. Again, click on Next. Now, scan the below QR Code from the Microsoft Authenticator app which is installed on your mobile after successfully scanning the code and add this user in your authenticator app click on Next.



Now, to verify that you have added a user successfully, write down the below number which is asked by the authenticator app. If you enter the correct number then you will show the below message and then click on Next. Now, click on Done. This indicates that we have successfully created MFA for the testuser1. Similarly, we can enable MFA for all the other users.





Task is Completed.

