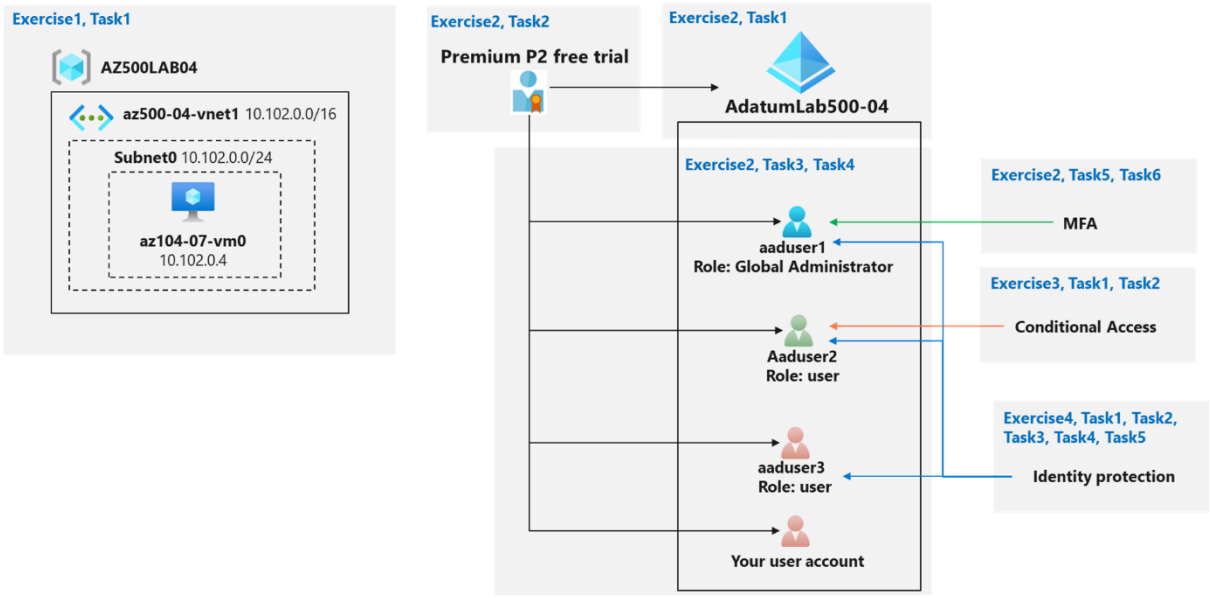
Lab 04: MFA, Conditional Access and AAD Identity Protection

MFA - Conditional Access - Identity Protection diagram

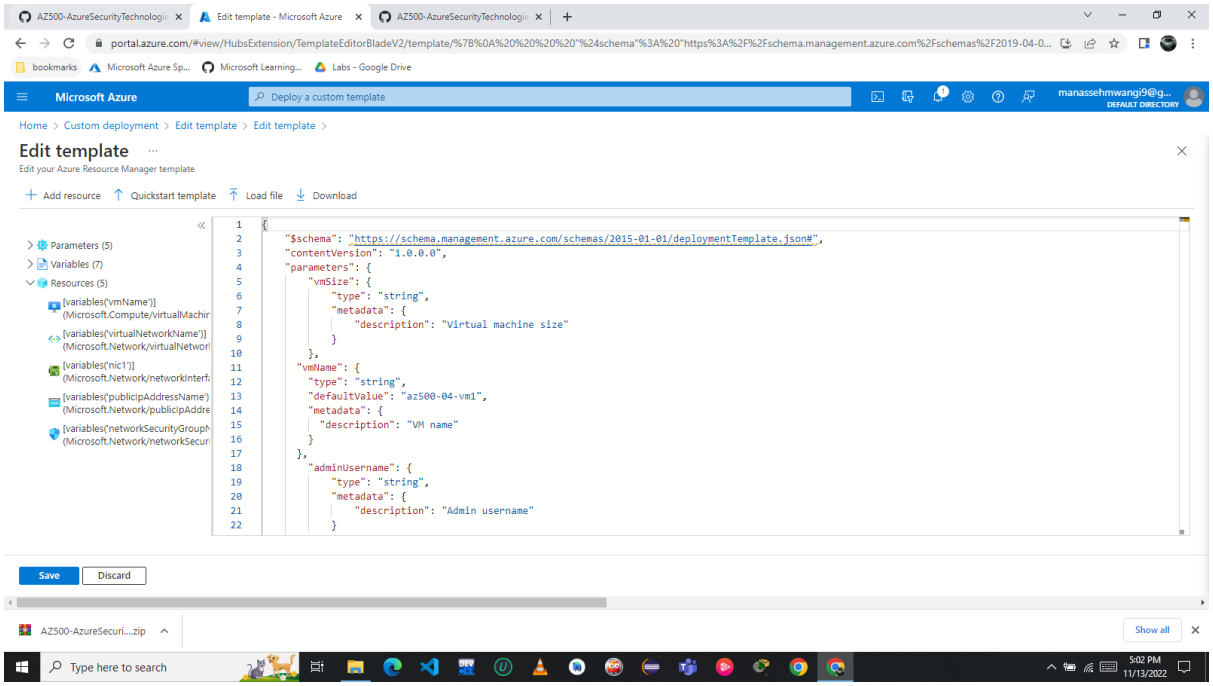


Exercise 1: Deploy an Azure VM by using an Azure Resource Manager template

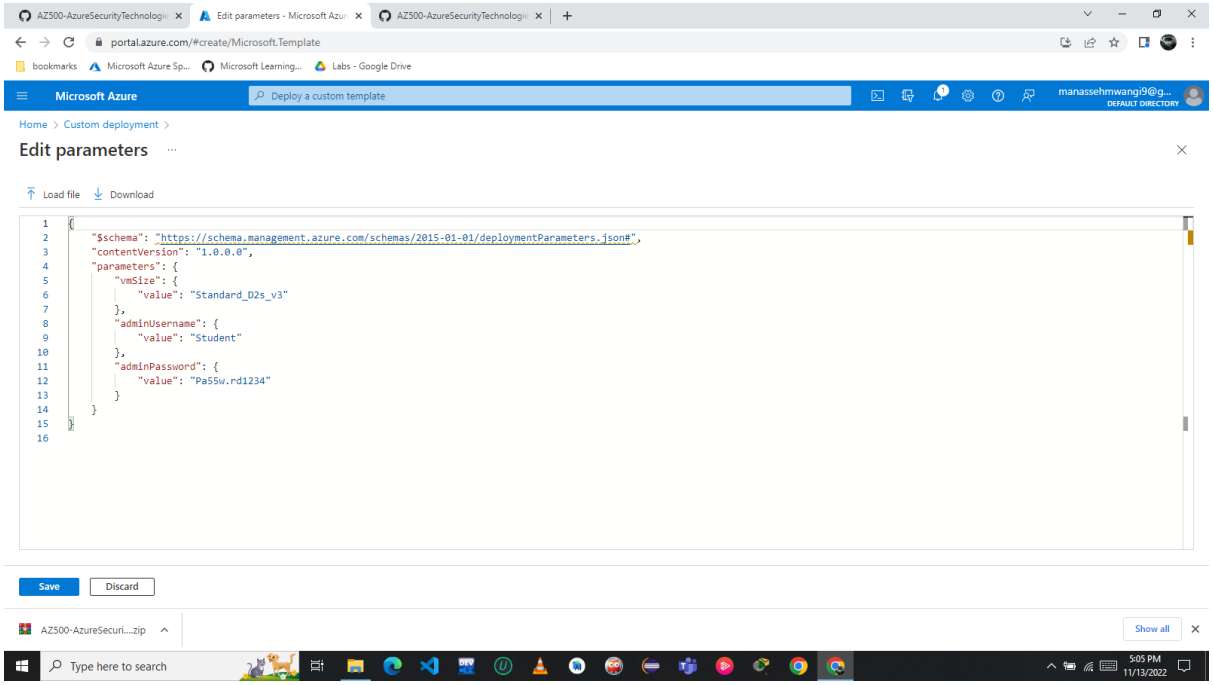
Task 1: Deploy an Azure VM by using an Azure Resource Manager template

In this task, you will create a virtual machine by using an ARM template. This virtual machine will be used in the last exercise for this lab.

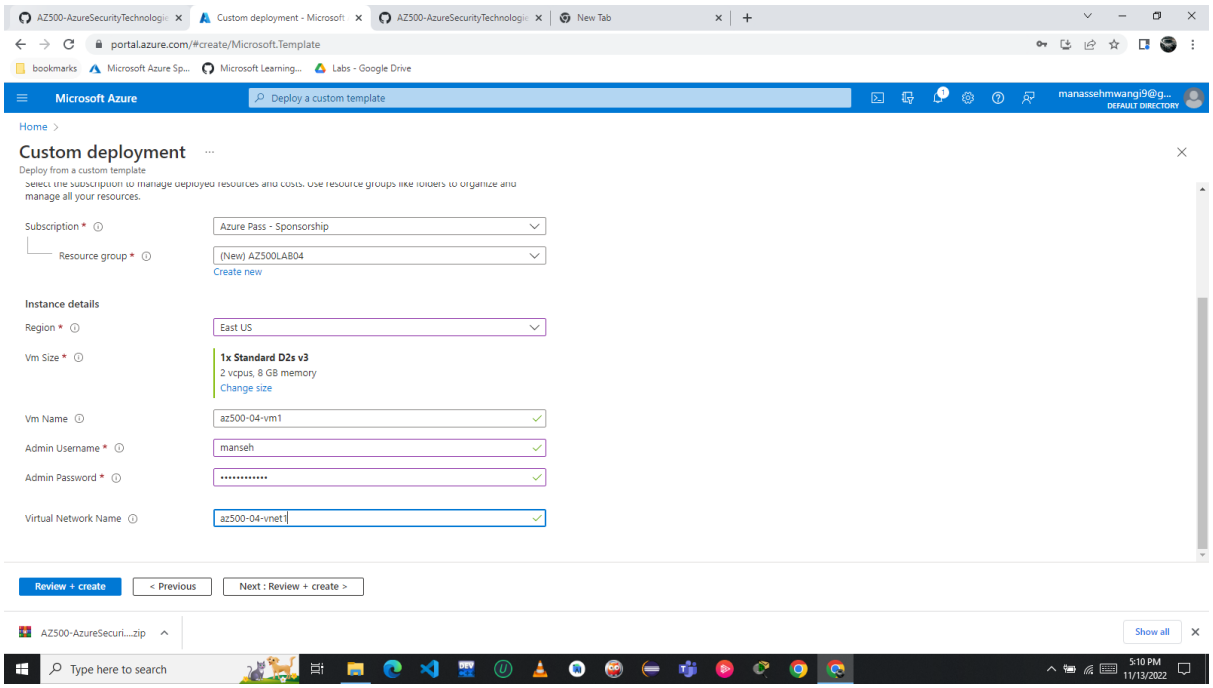
The template deploys an Azure VM hosting Windows Server 2019 Datacenter.



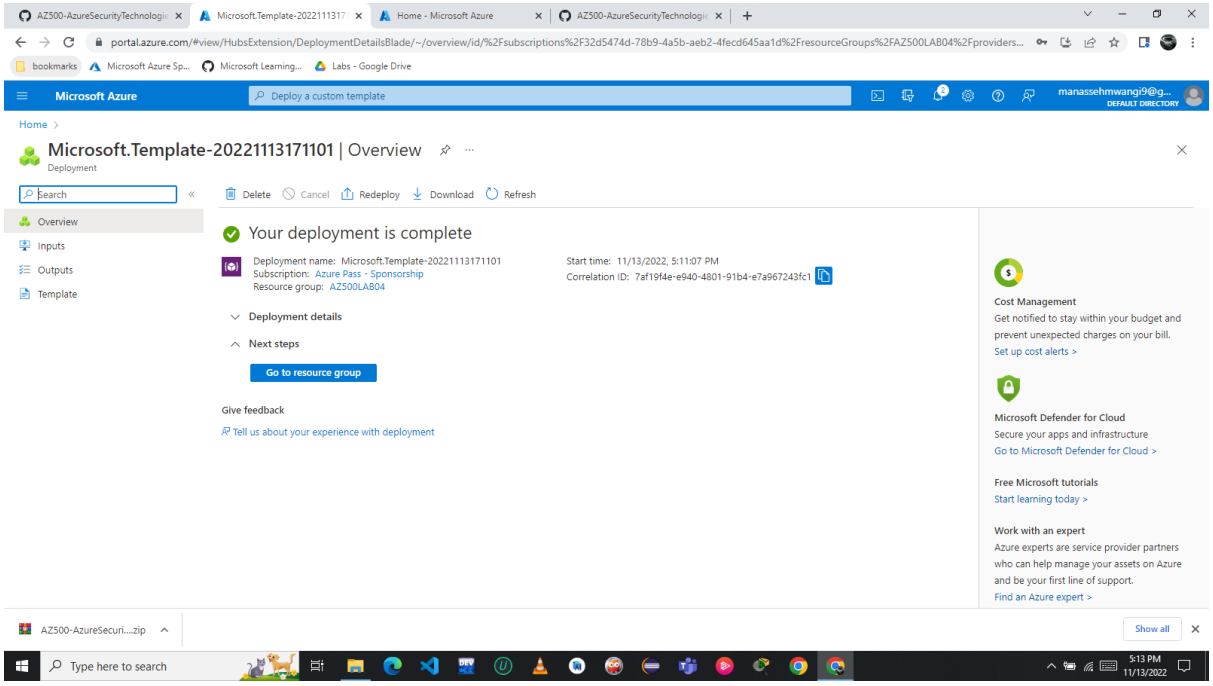
Review the content of the parameters file noting the adminUsername and adminPassword values.



Ensure that the following settings are configured (leave any others with their default values):

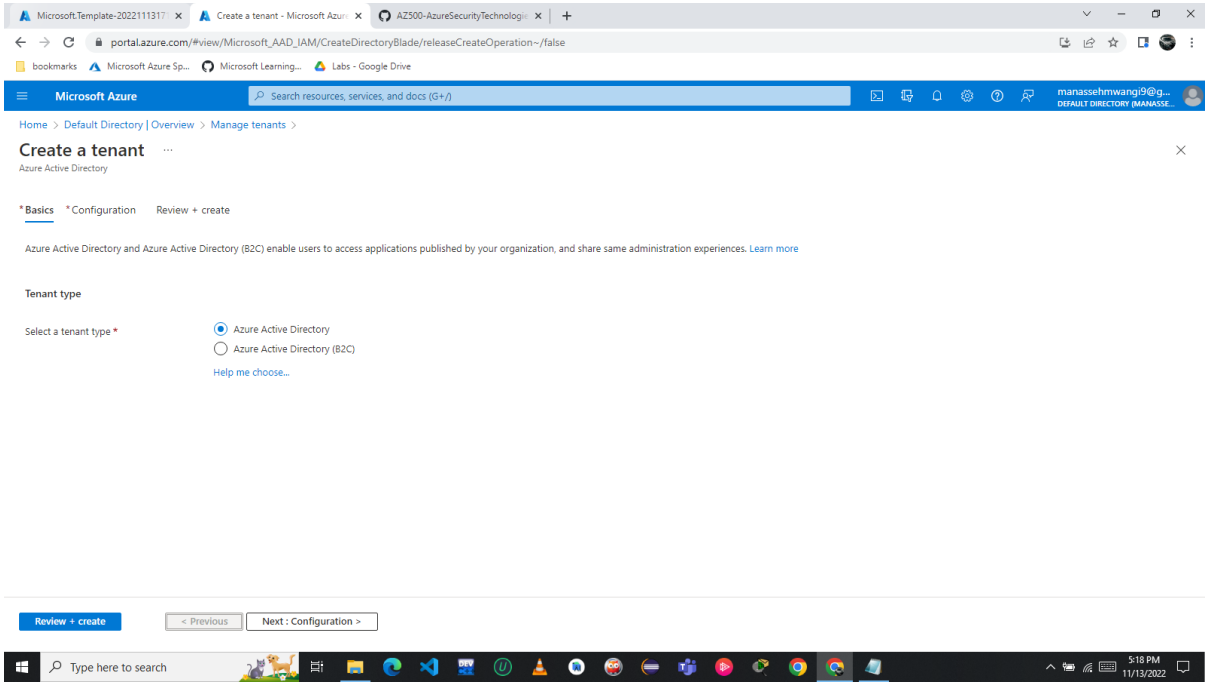


You have initiated a template deployment of an Azure VM **az500-04-vm1**



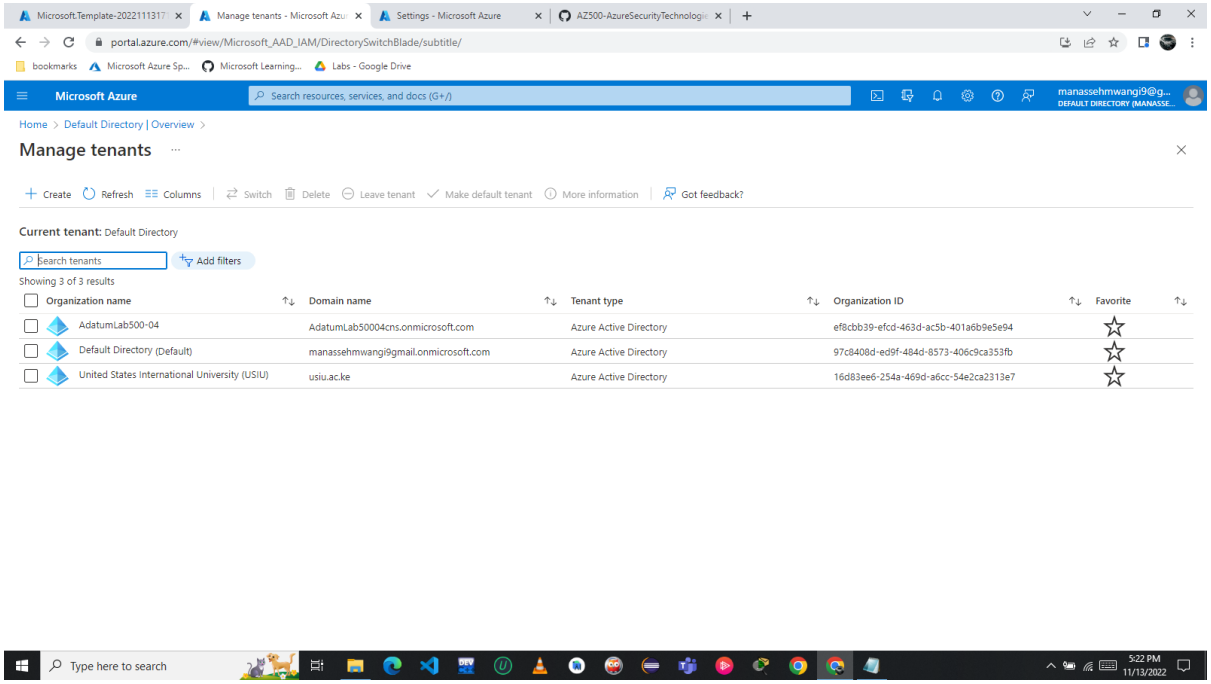
Exercise 2: Implement Azure MFA (Multi factor authentication)

Task 1: Create a new Azure AD tenant

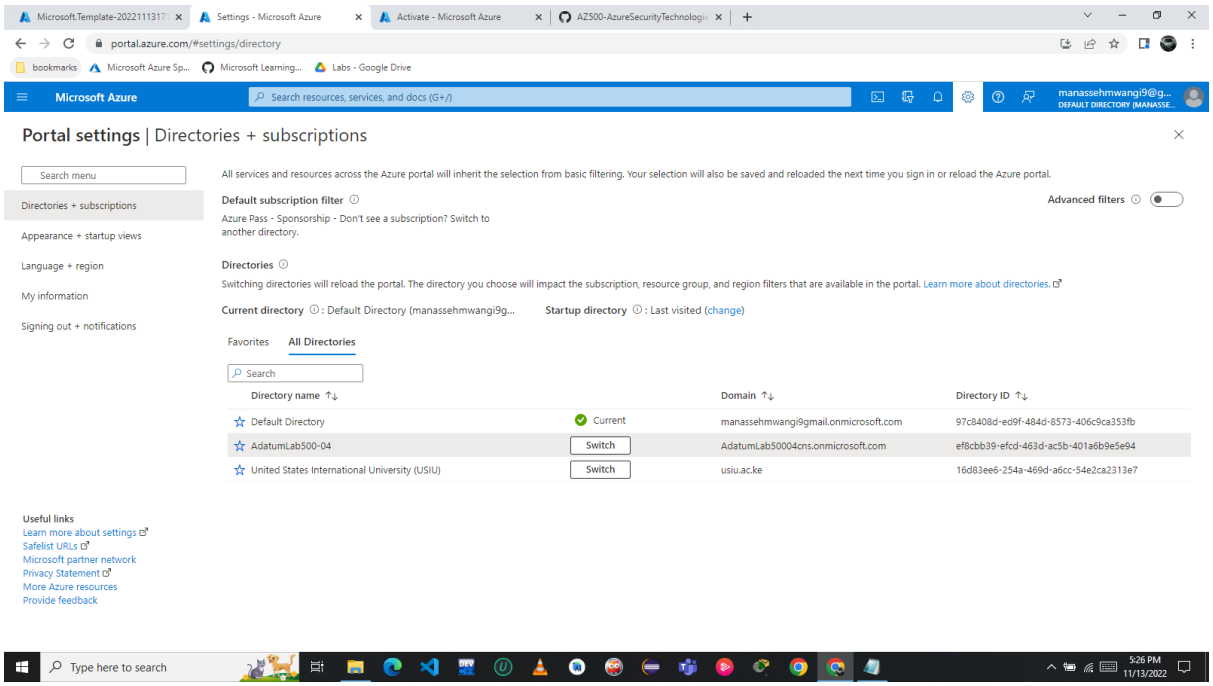


In the **Configuration** tab of the **Create a tenant** blade, specify the following settings:
AdatumLab500-04 & United States

The tenant AdatumLab500-04 is created

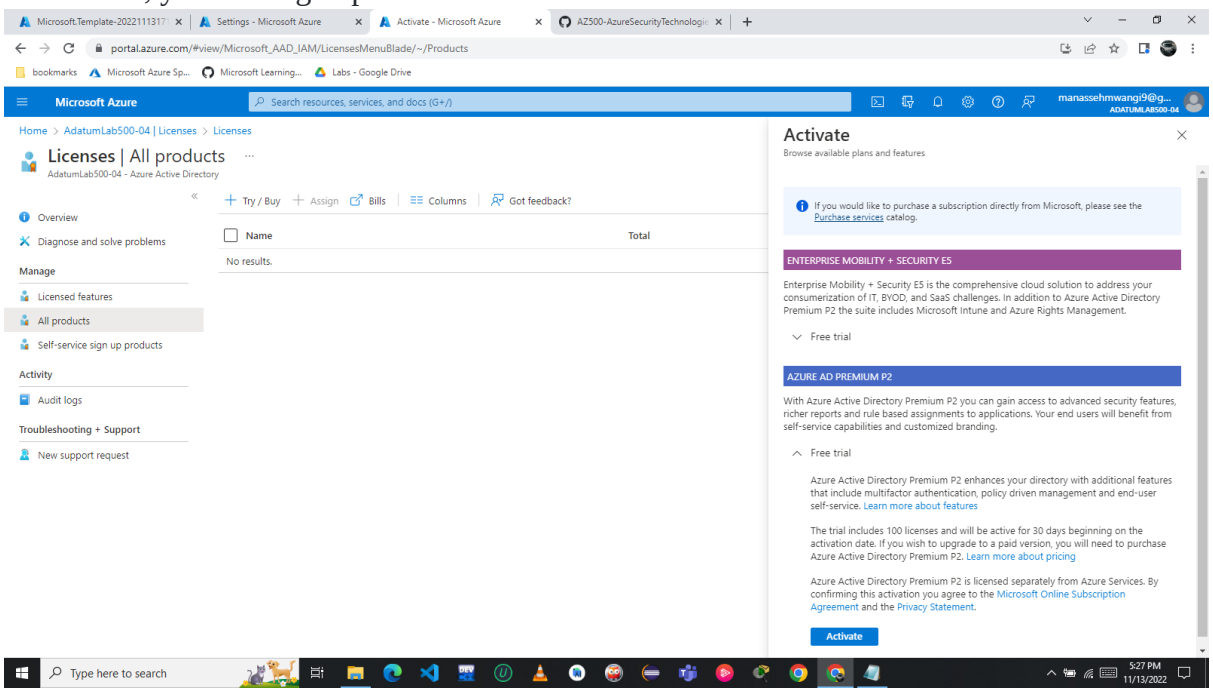


Switch to the AdatumLab500-04 directory



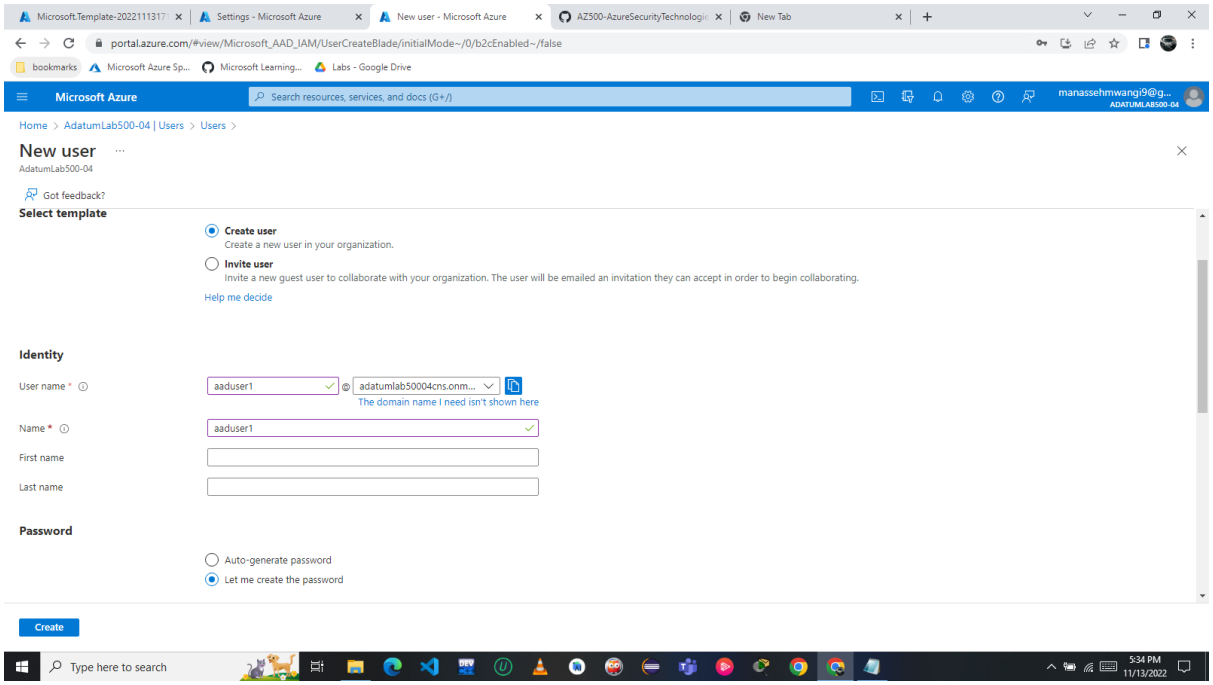
Task 2: Activate Azure AD Premium P2 t

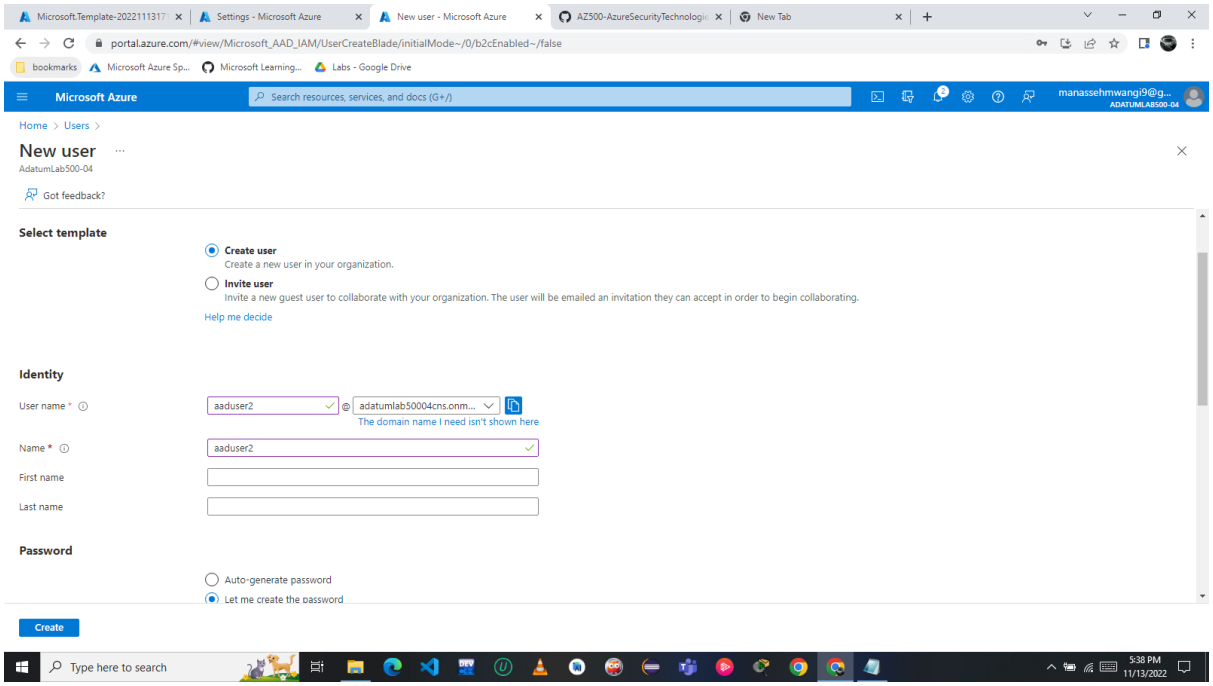
In this task, you will sign up for the Azure AD Premium P2 free trial.



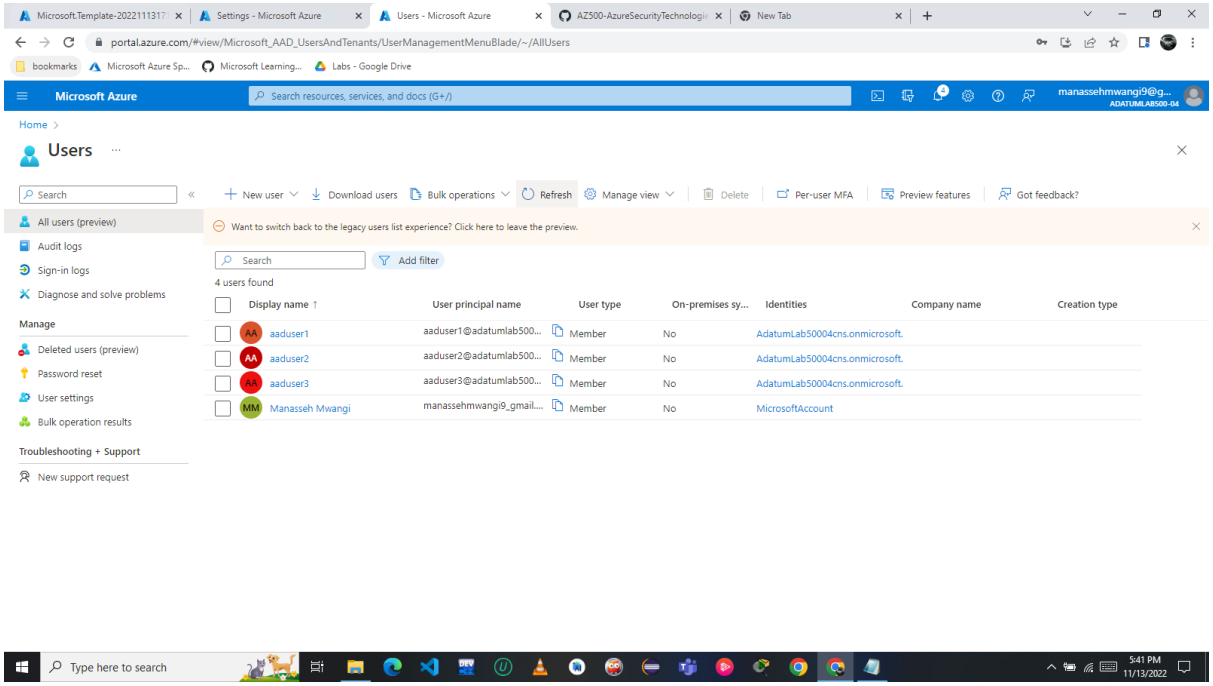
Task 3: Create Azure AD users and groups.

In this task, you will create three users: aaduser1 (Global Admin), aaduser2 (user), and aaduser3 (user). You will need each user's principal name and password for later tasks.



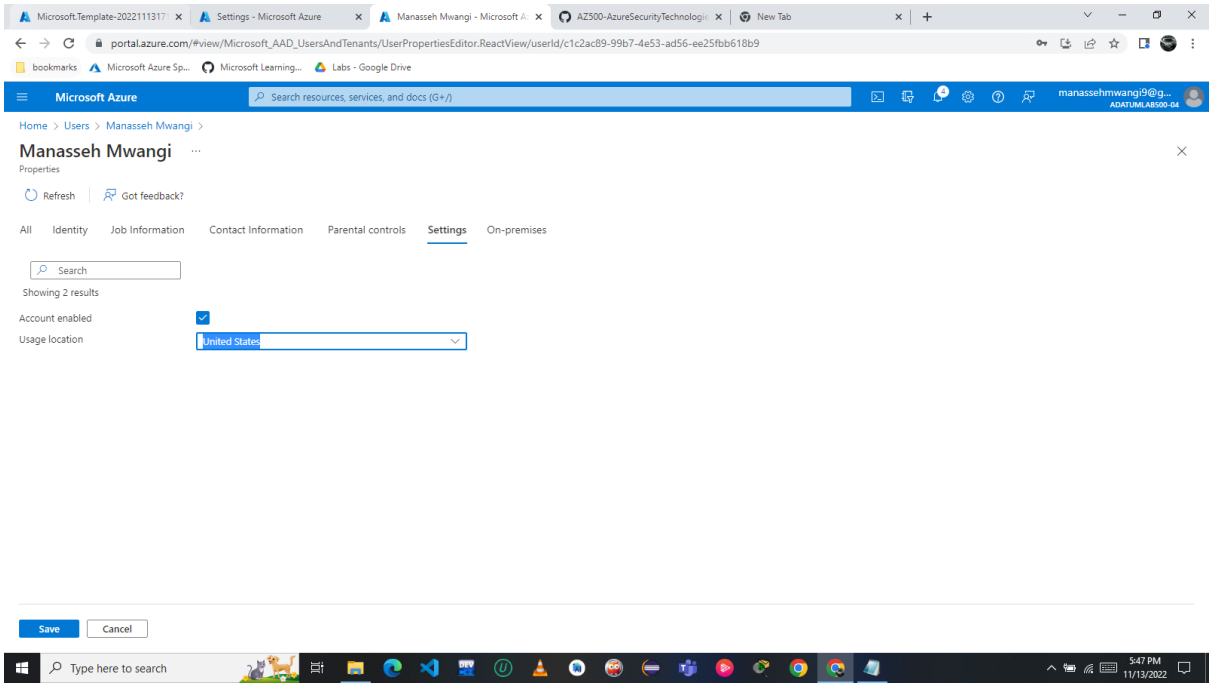


At this point, you should have three new users listed on the **Users** page

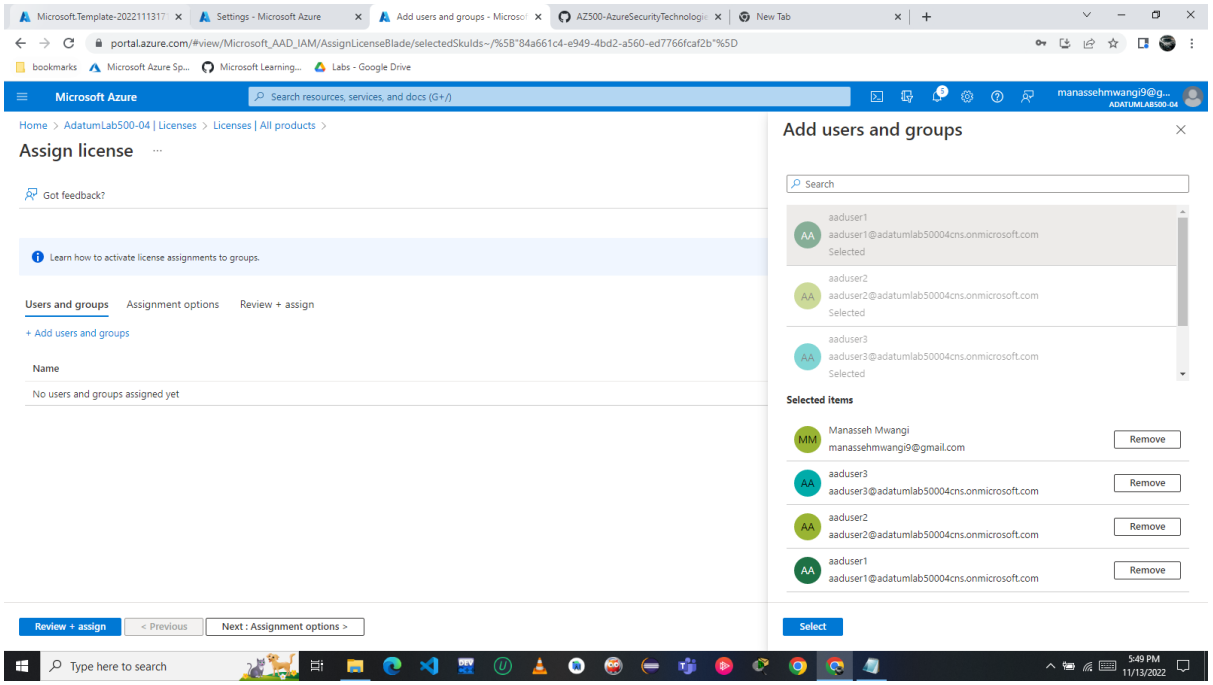


Task 4: Assign Azure AD Premium P2 licenses to Azure AD users

Verify Usage Location is set to **United States** if not set the usage location and click **Save**.



In this task, you will assign each user to the Azure Active Directory Premium P2 license.

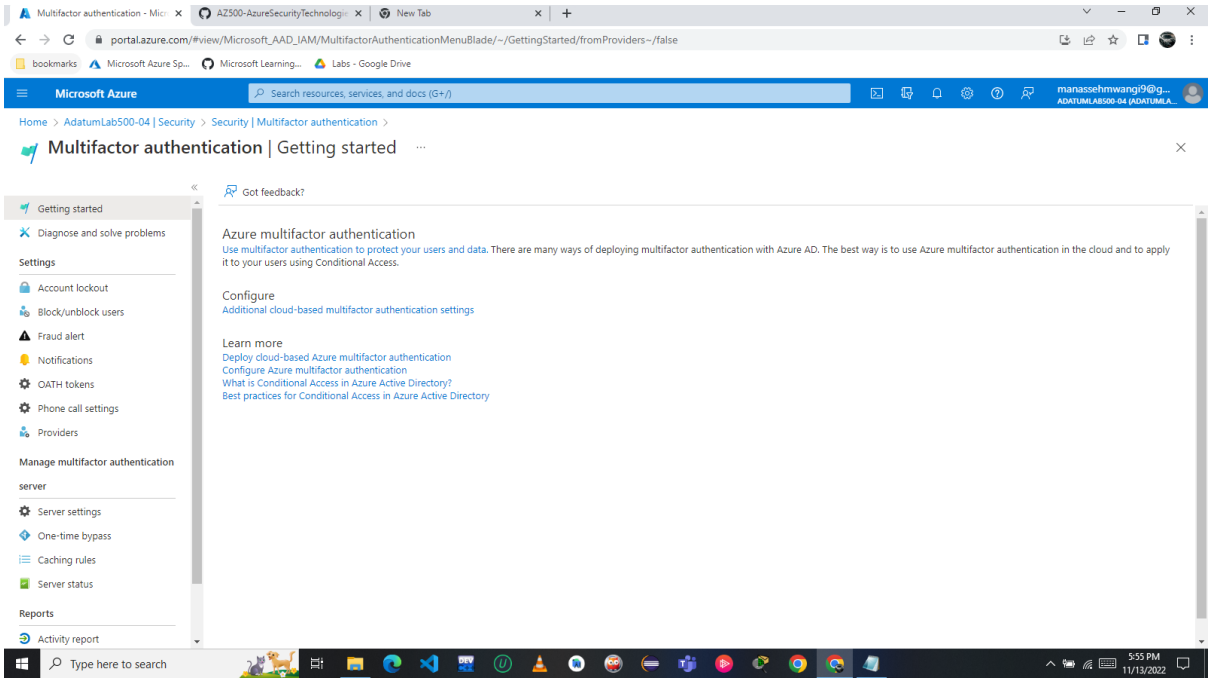


At this point, you assigned Azure Active Directory Premium P2 licenses to all user accounts you will be using in this lab. Be sure to sign out and then sign back in.

Task 5: Configure Azure MFA settings.

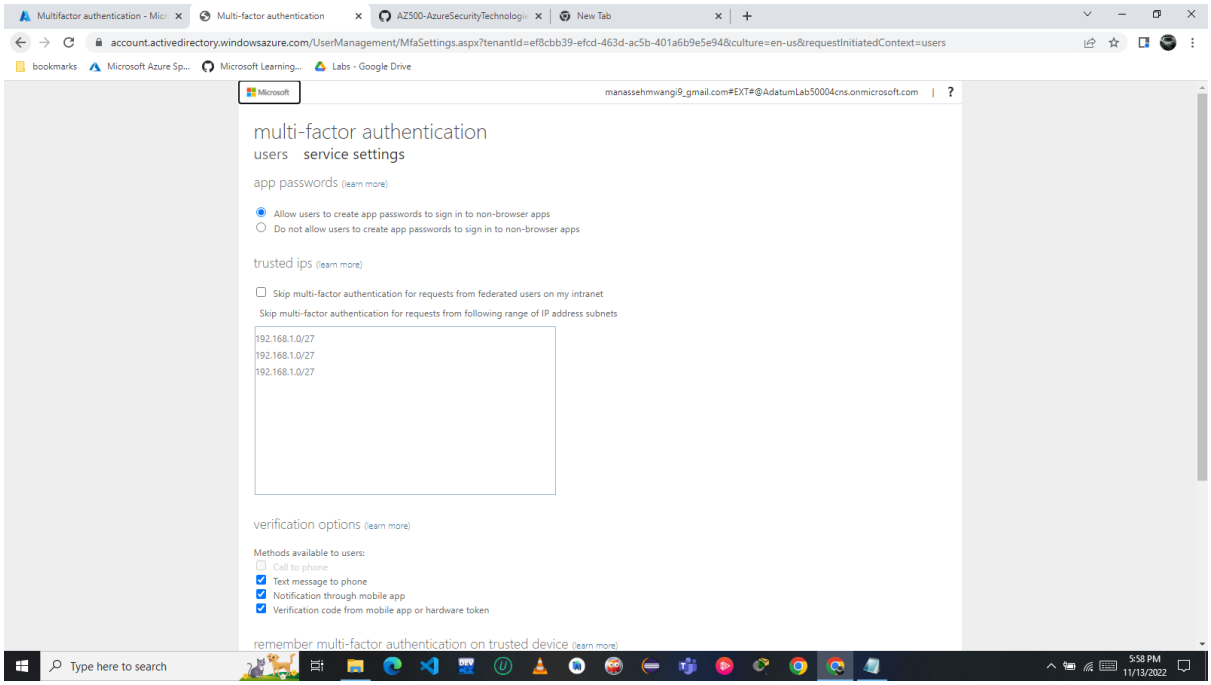
In this task, you will configure MFA and enable MFA for aaduser1.

Make sure you are using the AdatumLab500-04 Azure AD tenant.

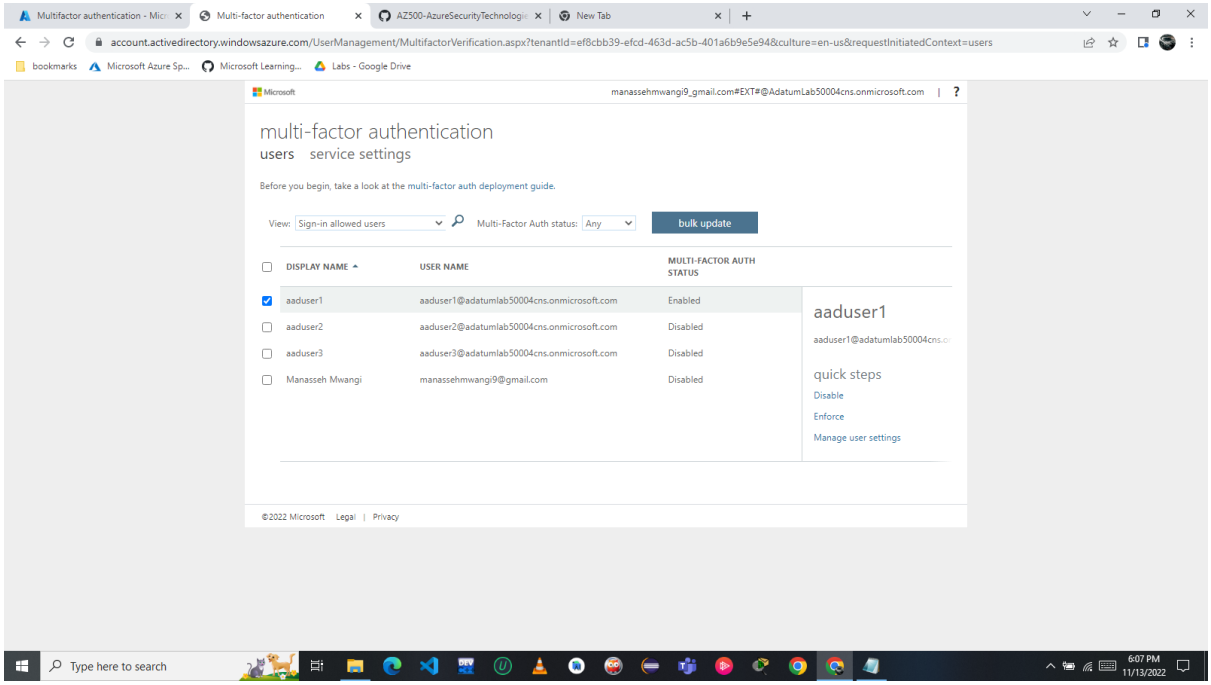


This will open a new browser tab, displaying **multi-factor authentication** page

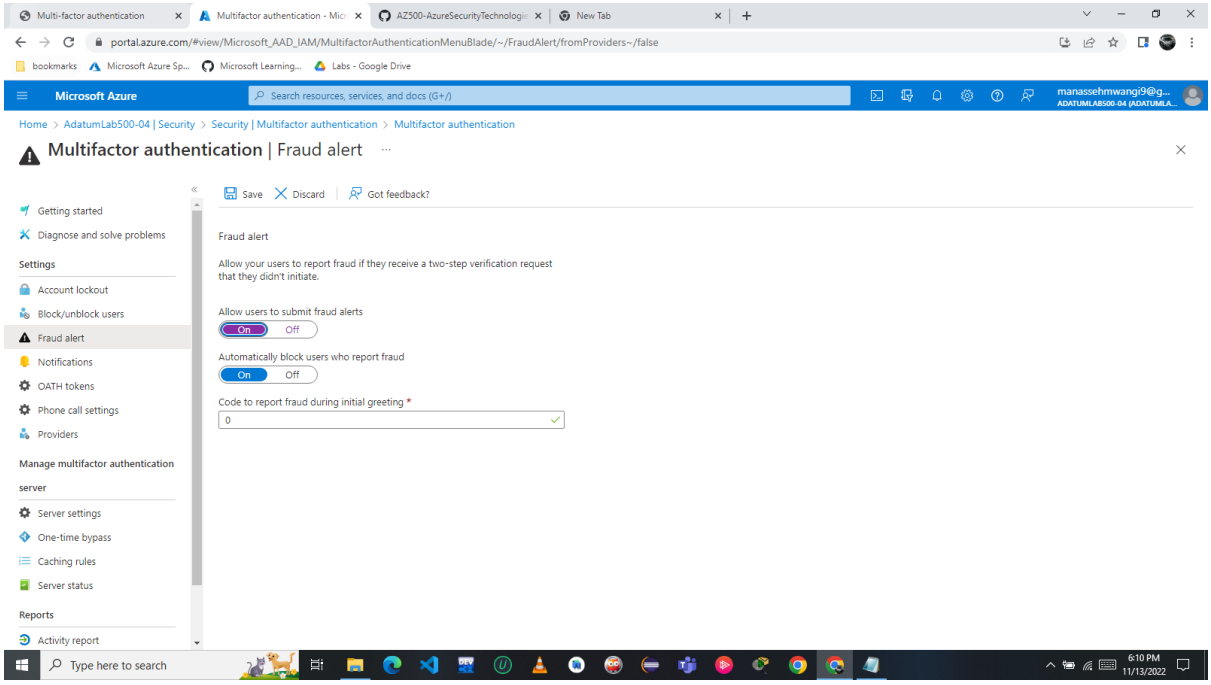
Note that **Text message to phone**, **Notification through mobile app**, and **Verification code from mobile app or hardware token** are enabled



Switch to the **users** tab, click **aaduser1** entry, click the **Enable** link, and, when prompted, click **enable multi-factor auth**.

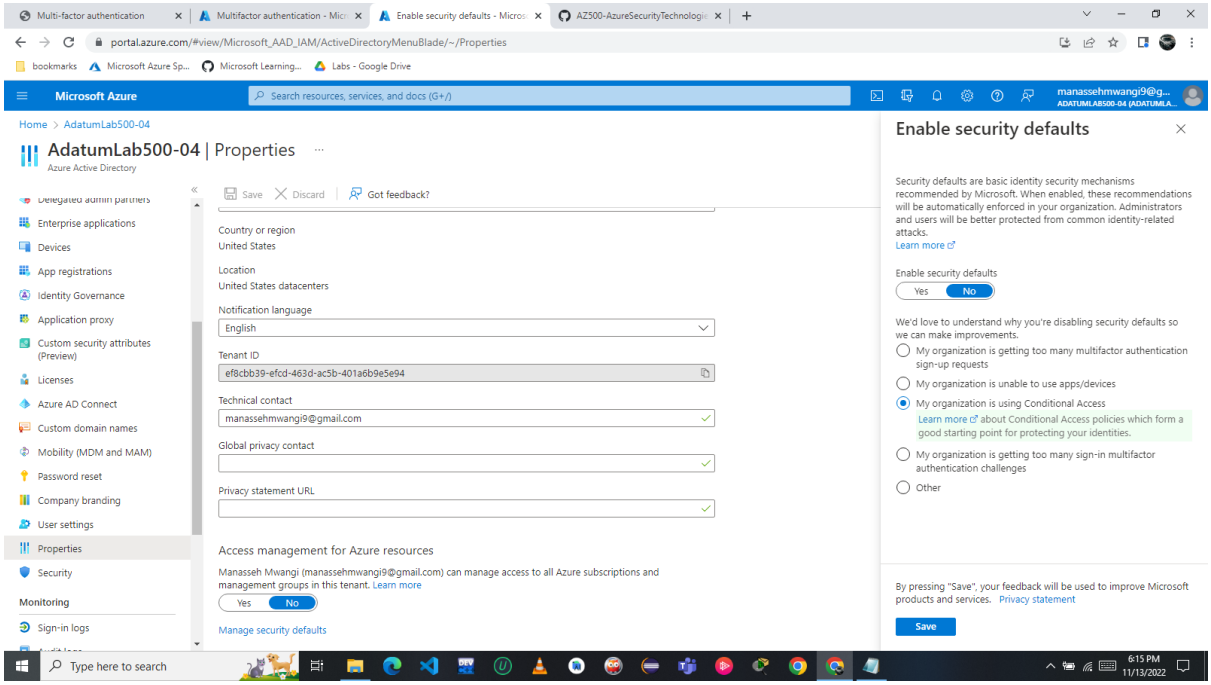


On the **Multi-Factor Authentication | Fraud alert** blade, configure the following settings:



At this point, you have enabled MFA for aaduser1 and setup fraud alert settings.

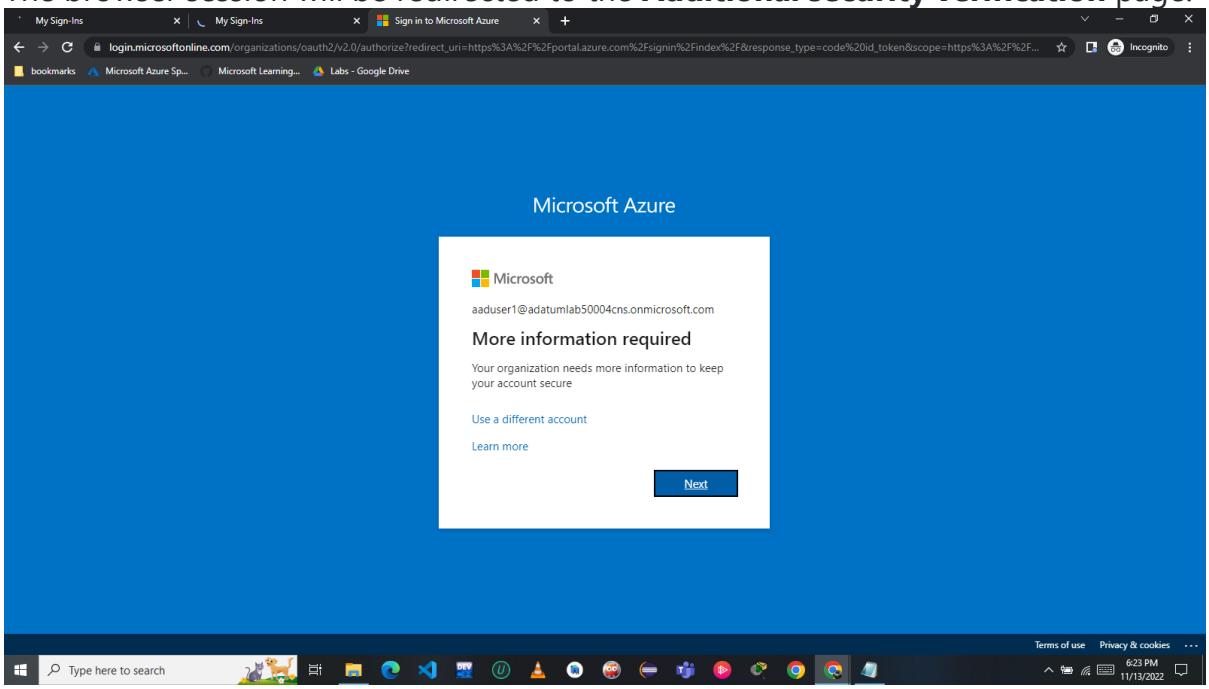
On the **Enable Security Defaults** blade, click **No**. Select **My Organization is using Conditonal Access** as the reason and and then click **Save**.



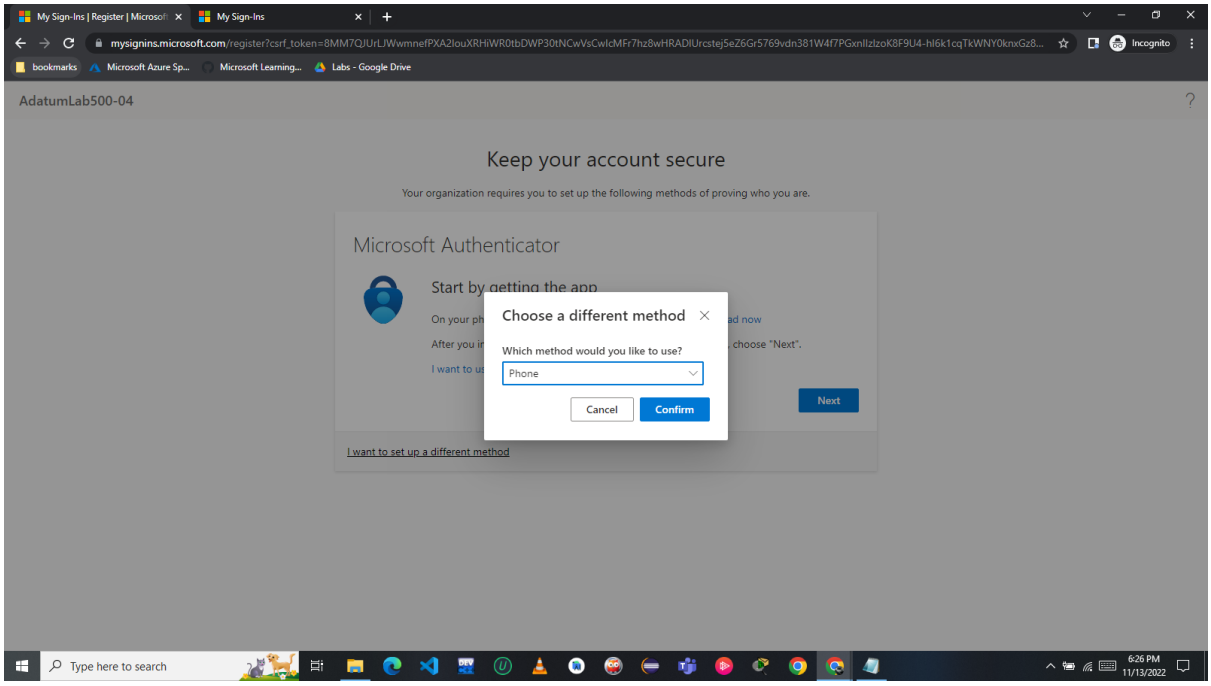
Task 6: Validate MFA configuration

In this task, you will validate the MFA configuration by testing sign in of the aaduser1 user account.

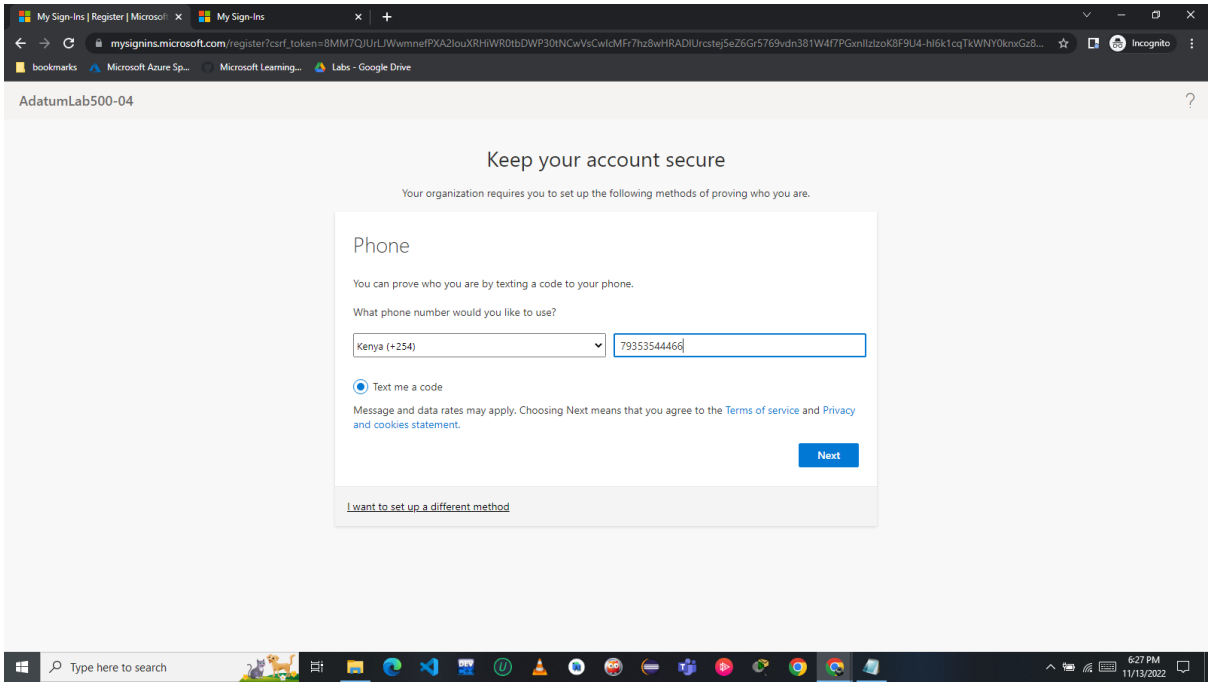
The browser session will be redirected to the **Additional security verification** page.



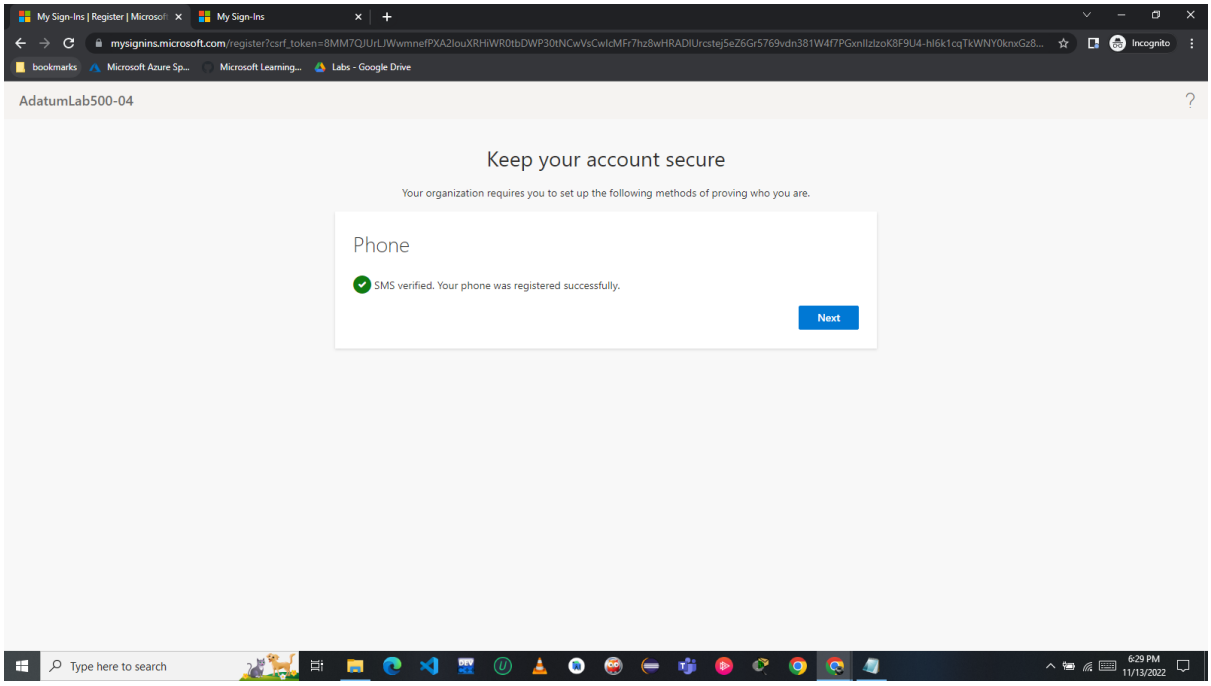
select **Phone**, and select **Confirm**



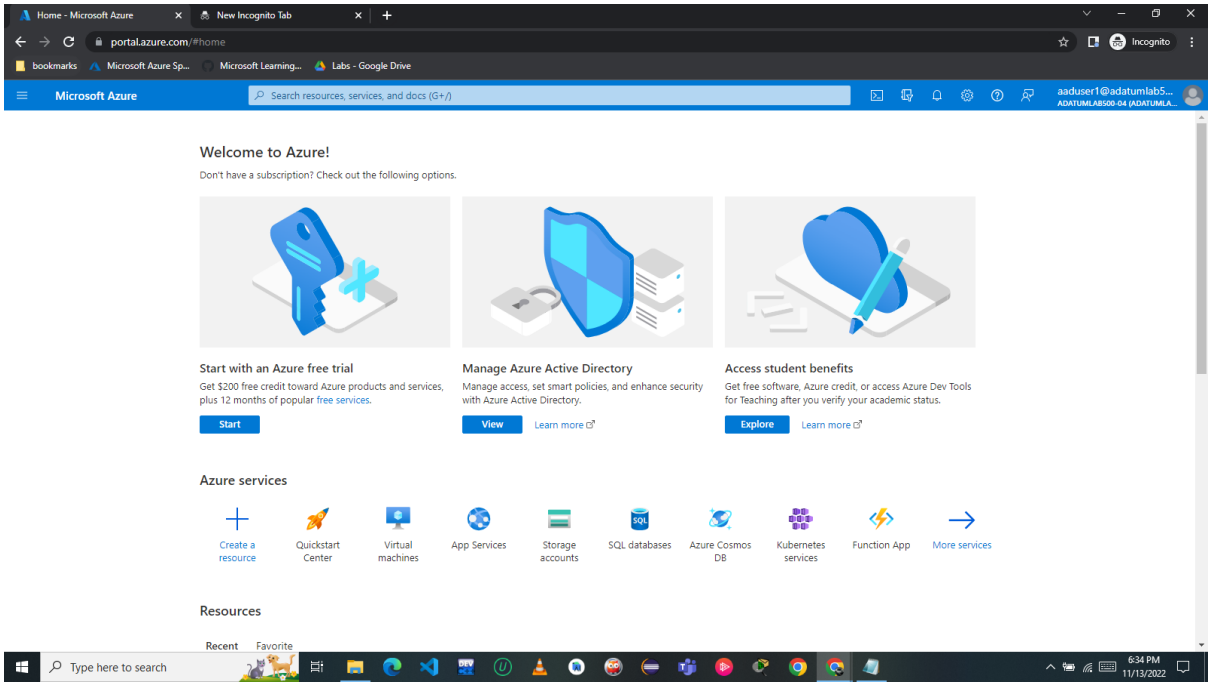
Select your country or region, type your mobile phone number in the **Enter phone number** area, ensure that the **Text me a code** option is selected, and click **Next**.



Verify that you successfully signed in to the Azure portal



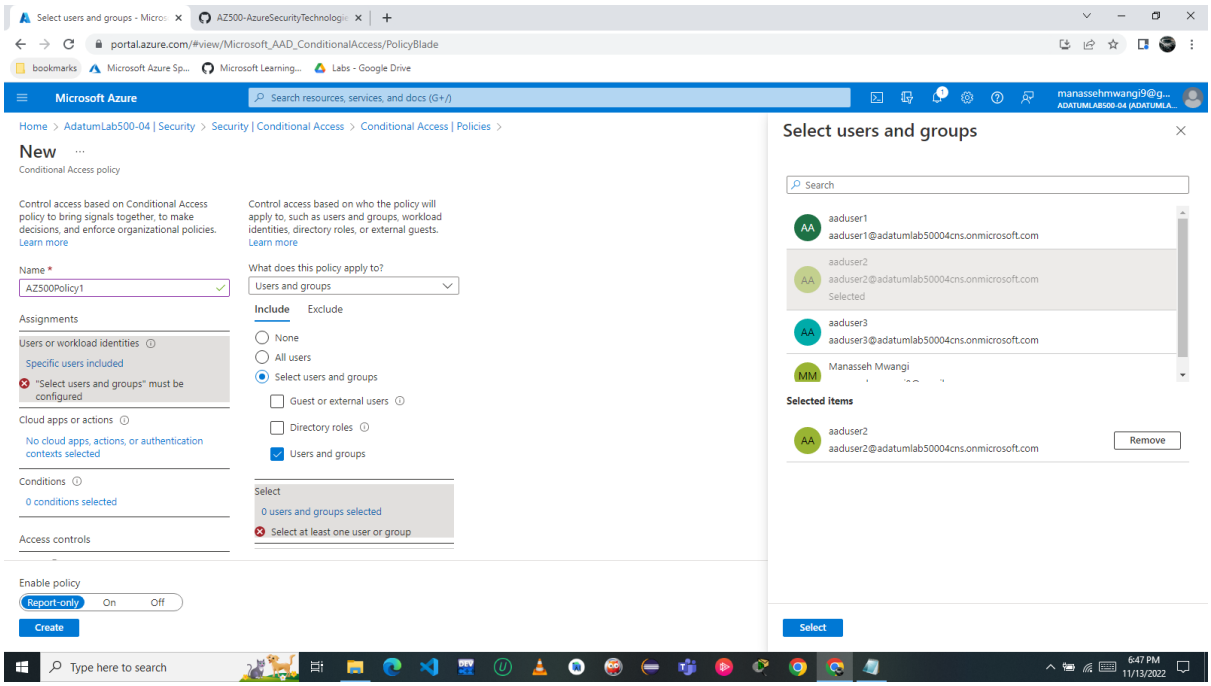
You have created a new AD tenant, configured AD users, configured MFA, and tested the MFA experience for a user.



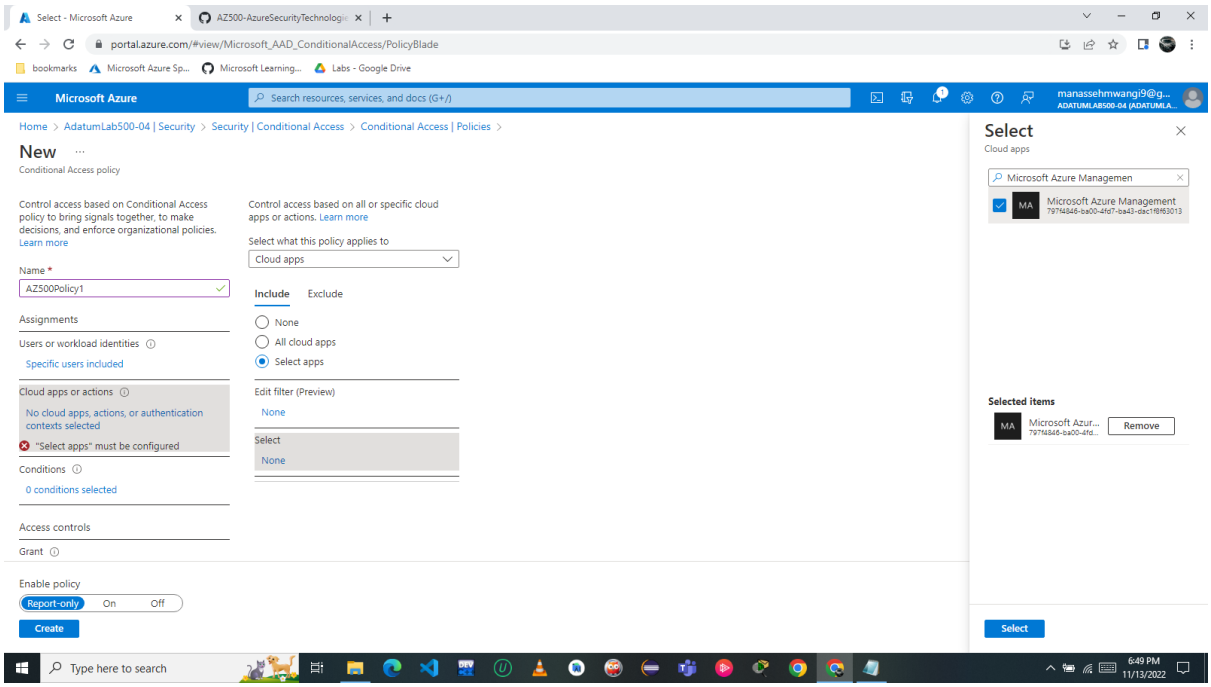
Exercise 3: Implement Azure AD Conditional Access Policies

Task 1 - Configure a conditional access policy.

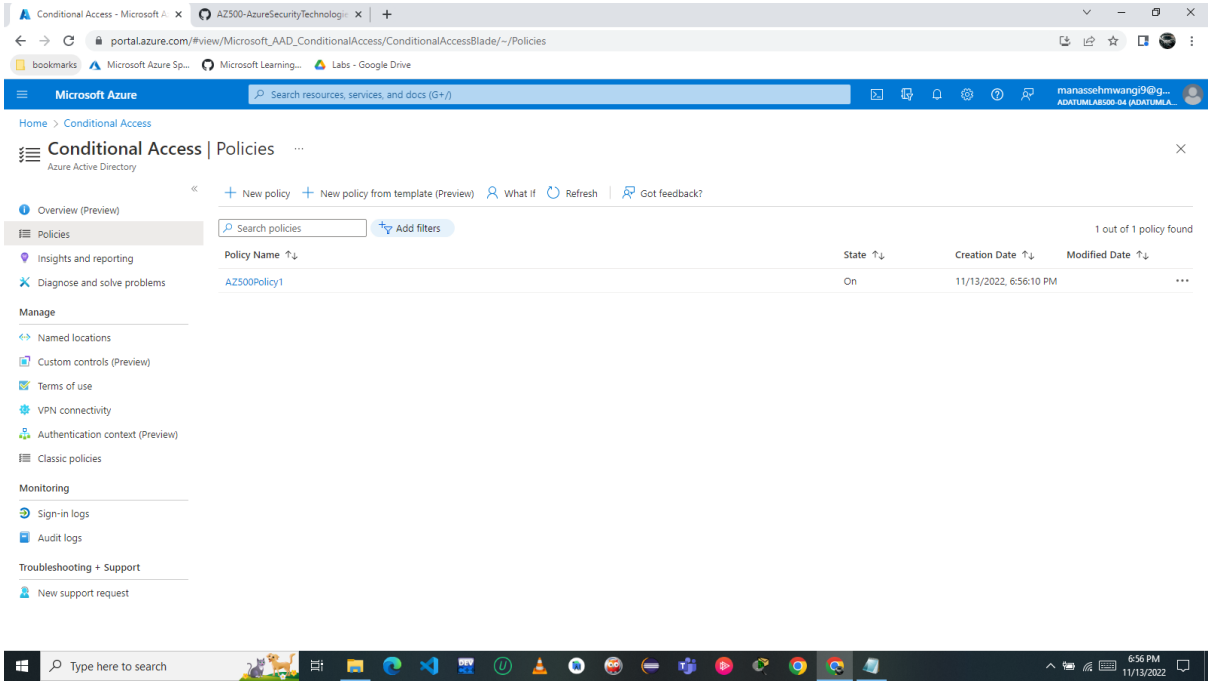
In this task, you will review conditional access policy settings and create a policy that requires MFA when signing in to the Azure portal.



At this point, you have a conditional access policy that requires MFA to sign in to the Azure portal.



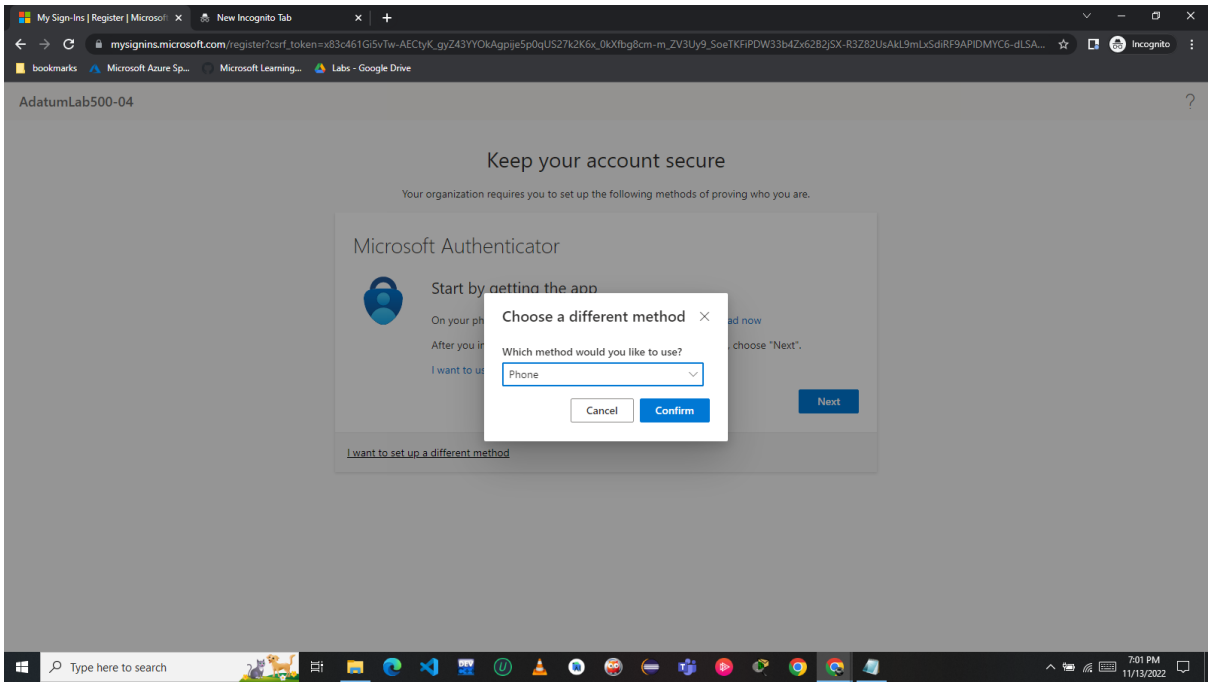
The azure policy AZ500Policy1 has been created



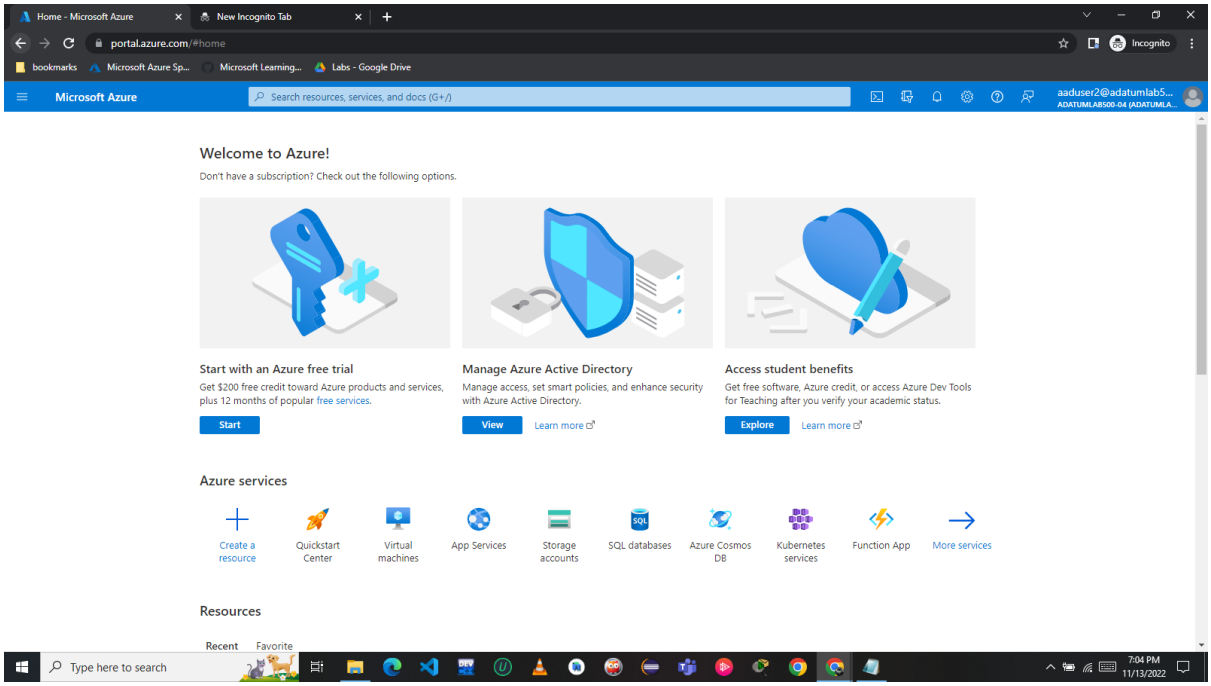
Task 2 - Test the conditional access policy.

In this task, you will sign in to the Azure portal as **aaduser2** and verify MFA is required. You will also delete the policy before continuing on to the next exercise.

Select **Phone**, and select **Confirm**



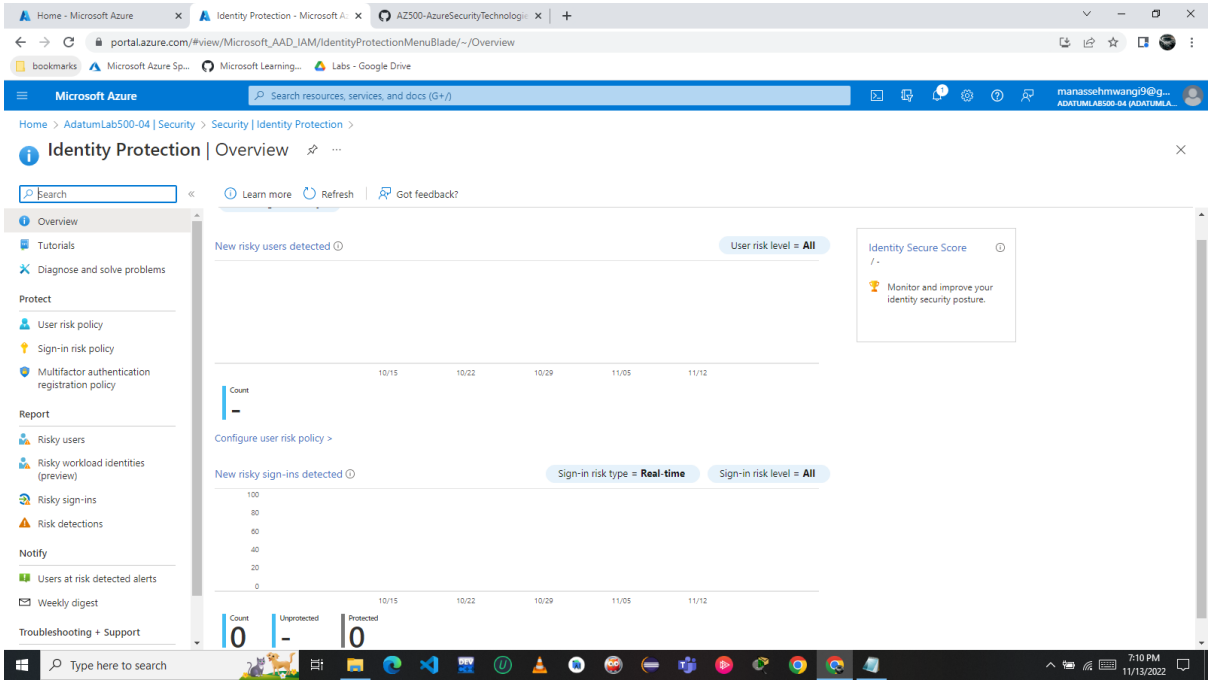
Verify that you successfully signed in to the Azure portal. In this exercise you implement a conditional access policy to require MFA when a user signs into the Azure portal.



Exercise 4: Implement Azure AD Identity Protection

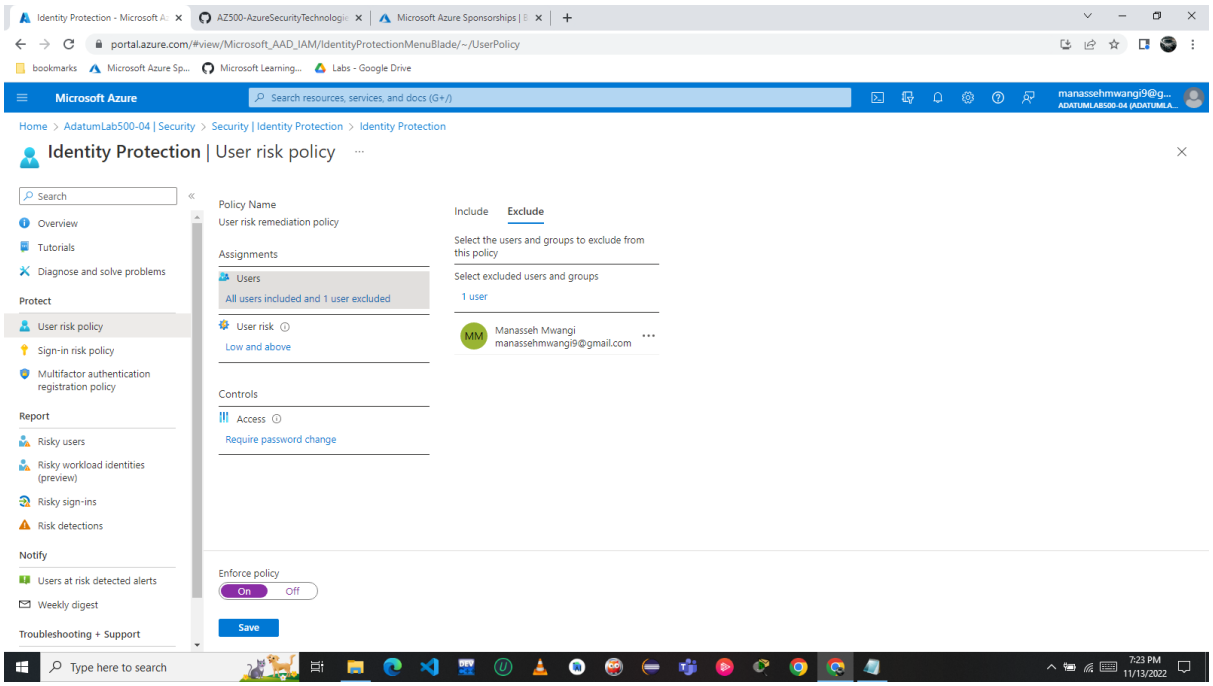
Task 1: Enable Azure AD Identity Protection

Review the **New risky users detected** and **New risky sign-ins detected** charts and other information about risky users.



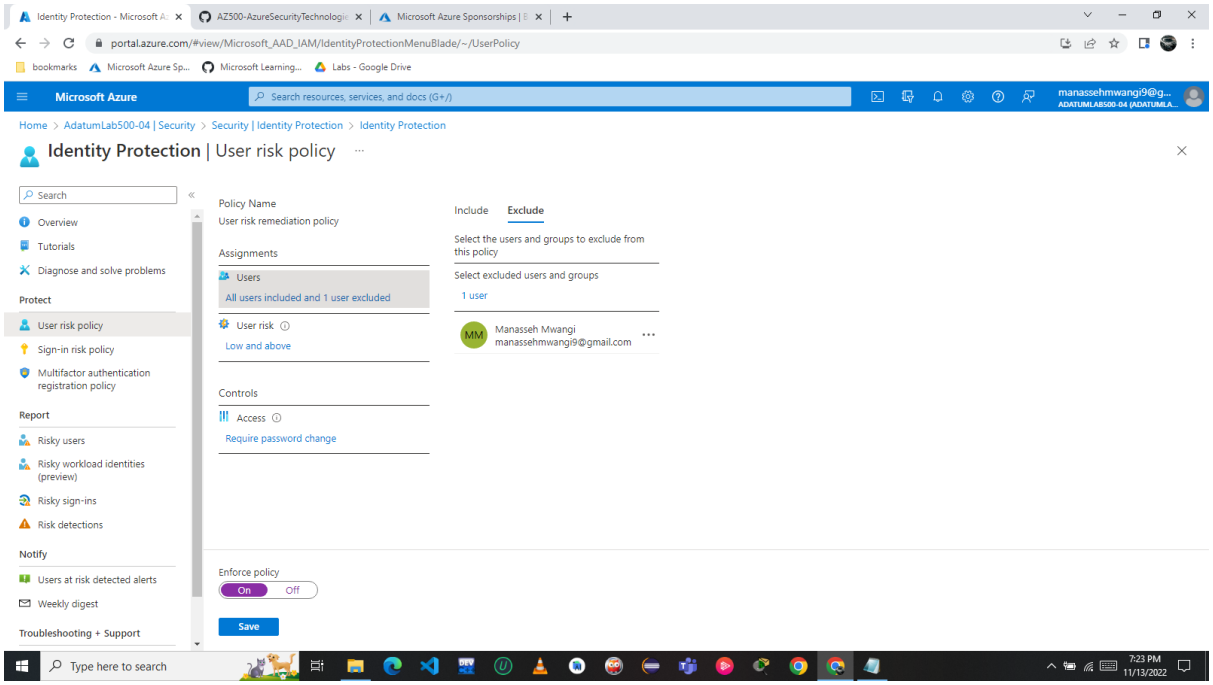
Task 2: Configure a user risk policy

In this task, you will create a user risk policy.



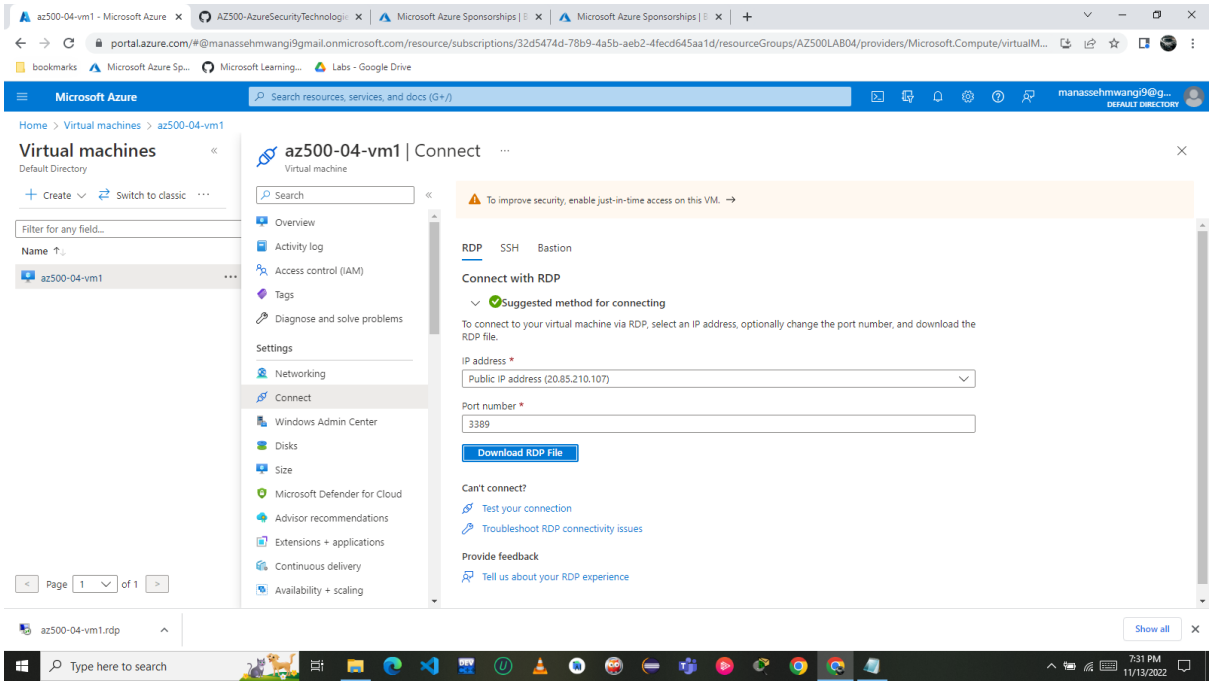
Task 3: Configure sign-in risk policy

In this task, you will configure a sign-in risk policy.

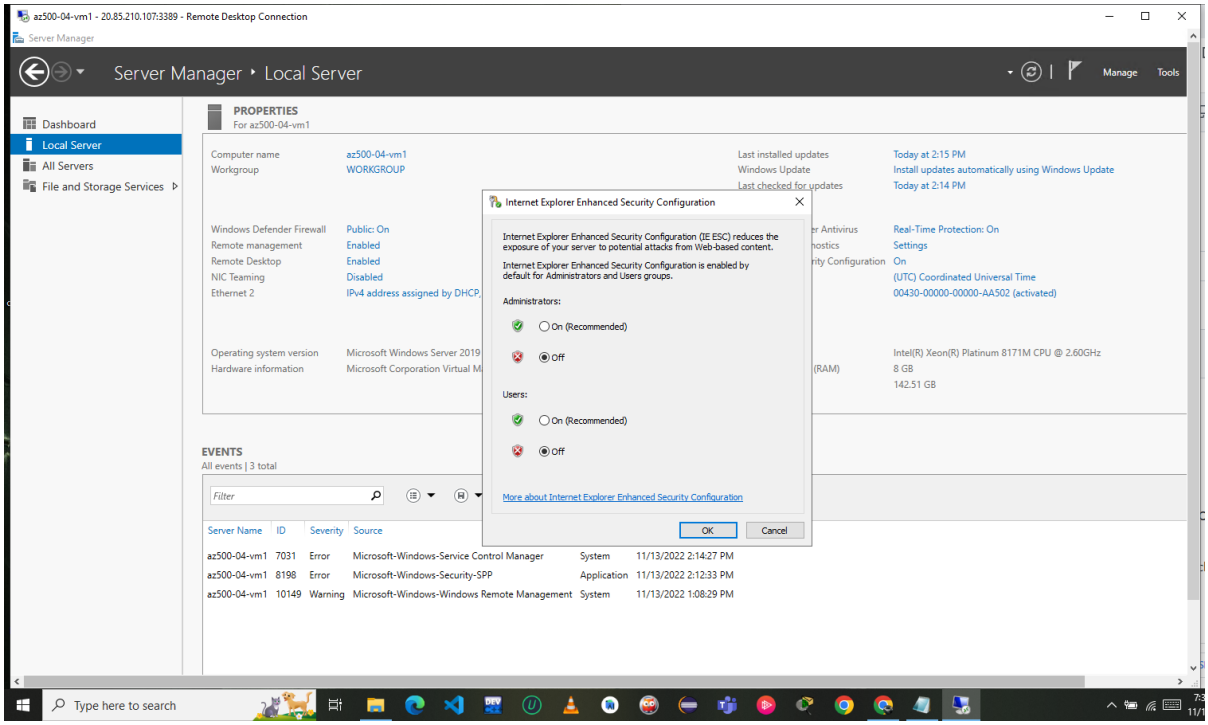


Task 4: Simulate risk events against the Azure AD Identity Protection policies

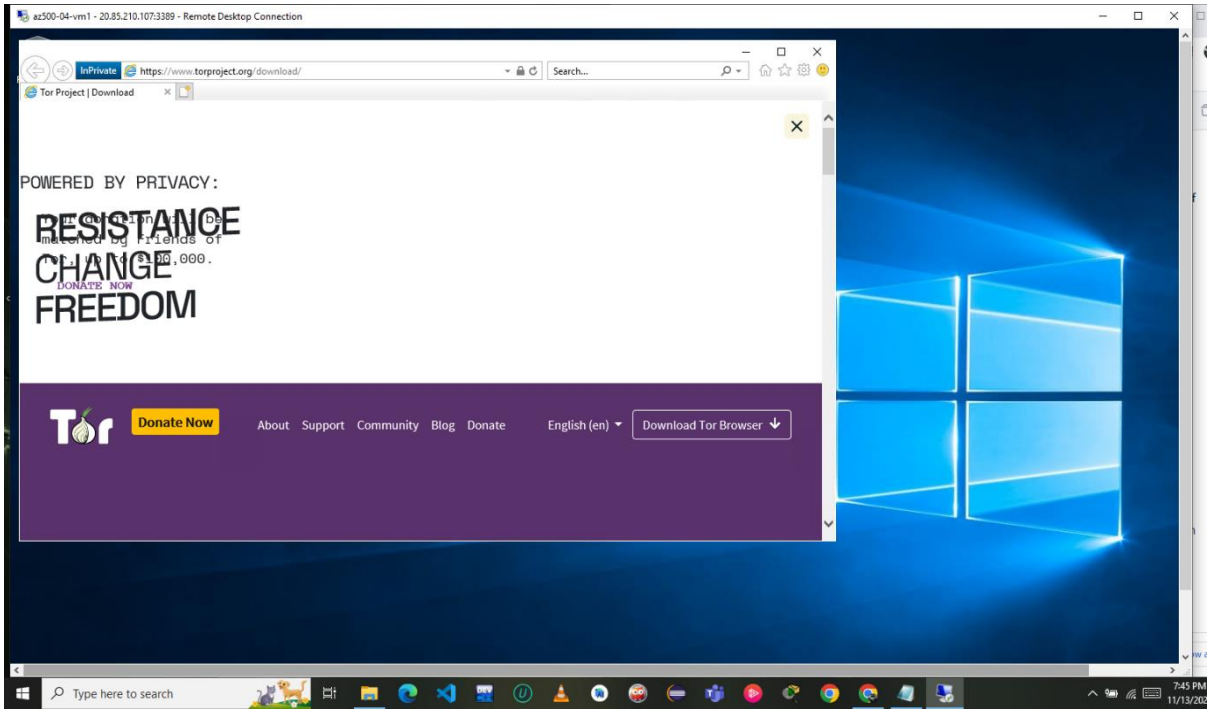
Click Download RDP File and use it to connect to the az500-04-vm1 via Remote Desktop.



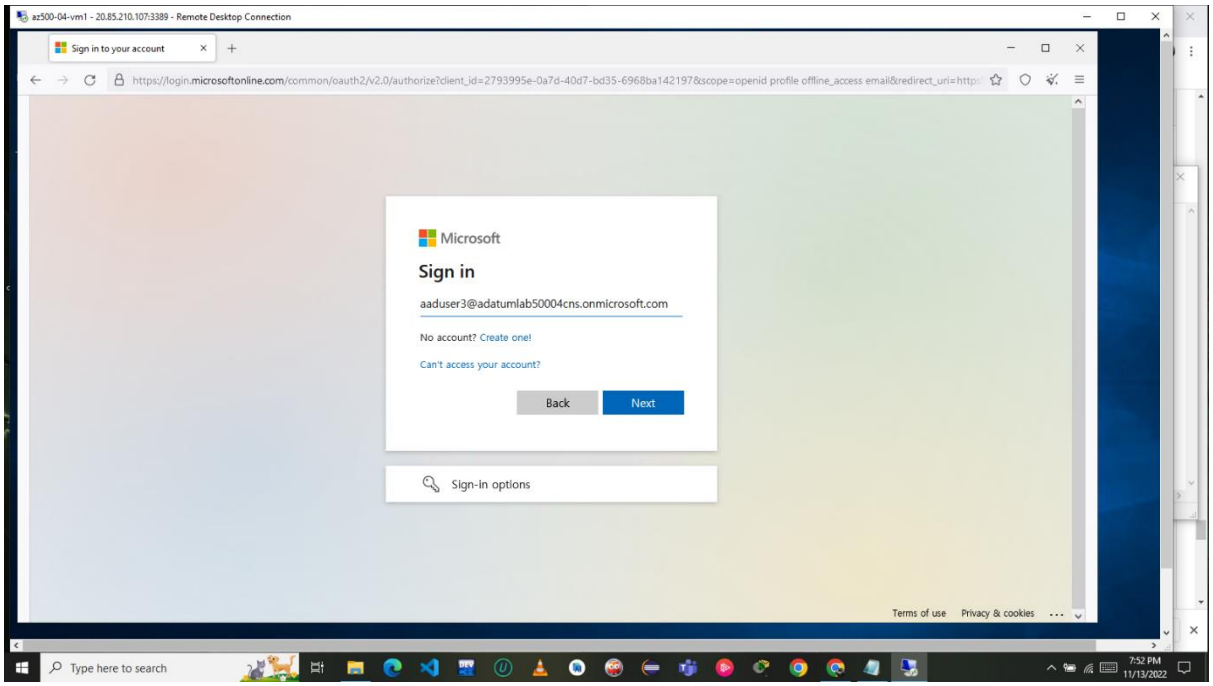
In **Server Manager**, click **Local Server** and then click **IE Enhanced Security Configuration**. set both options to Off and click OK.



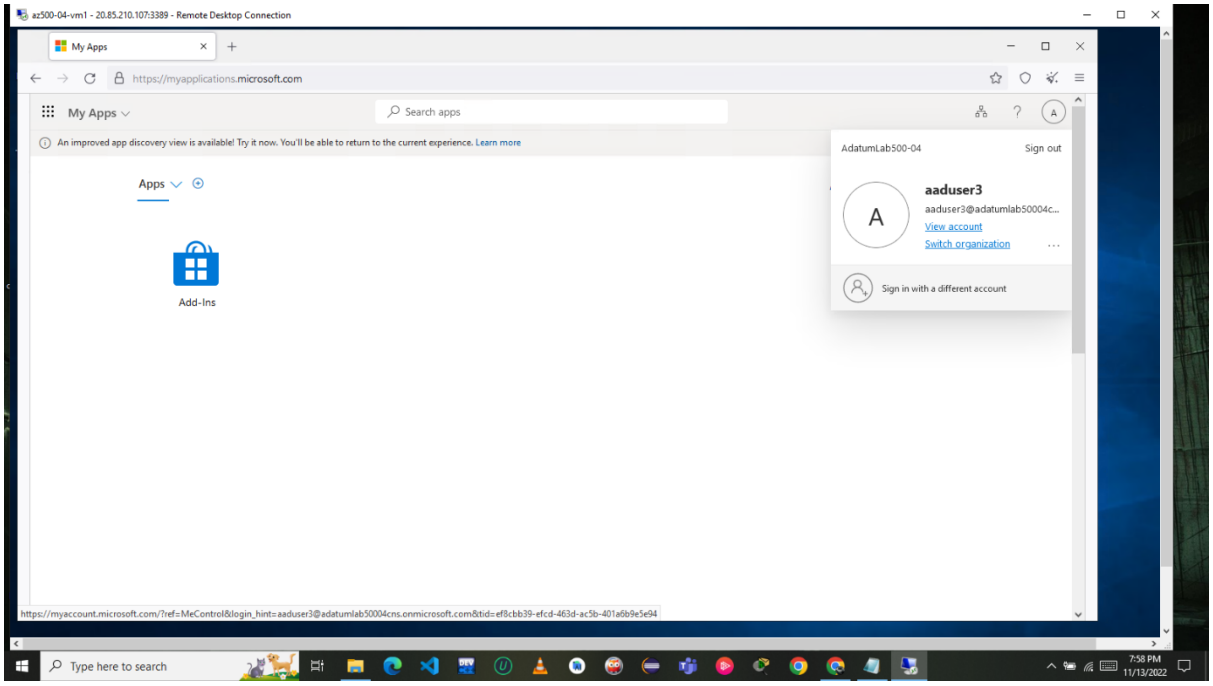
In the InPrivate Internet Explorer window, navigate to the ToR Browser Project



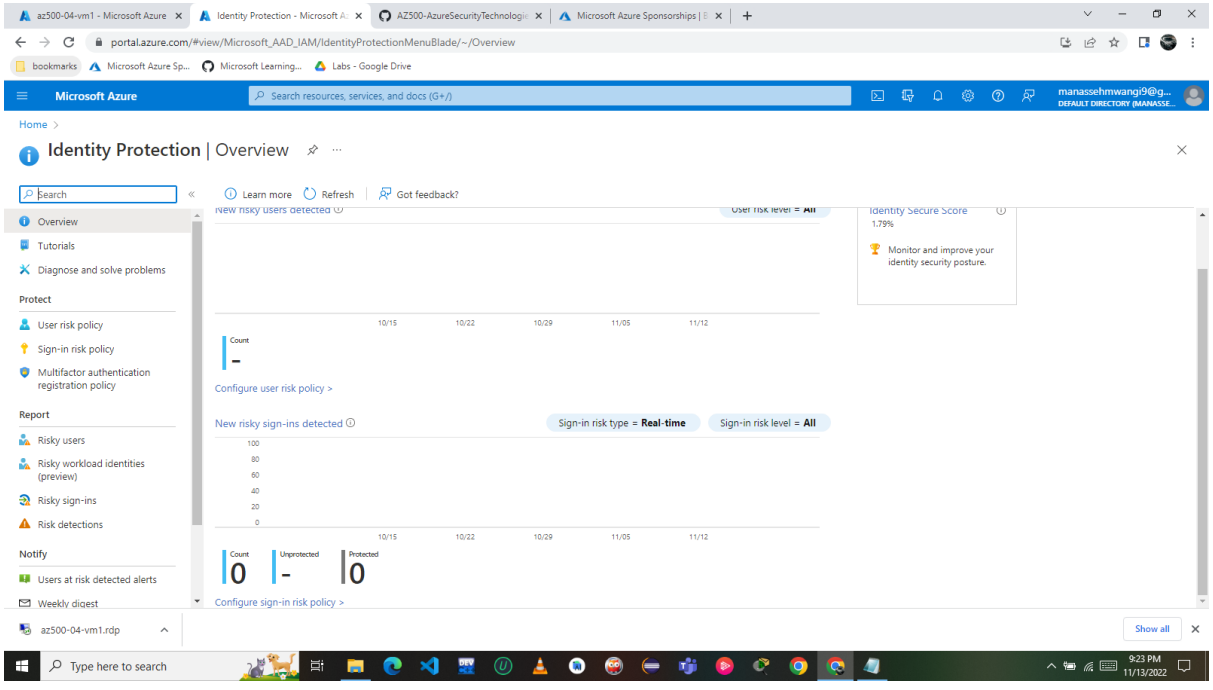
attempt to sign in with the **aaduser3** account.



browse to the Application Access Panel at **https://myapps.microsoft.com**.



You have enabled Azure AD Identity Protection, configured user risk policy and sign-in risk policy, as well as validated Azure AD Identity Protection configuration by simulating risk events.



The risks did not show up in reports