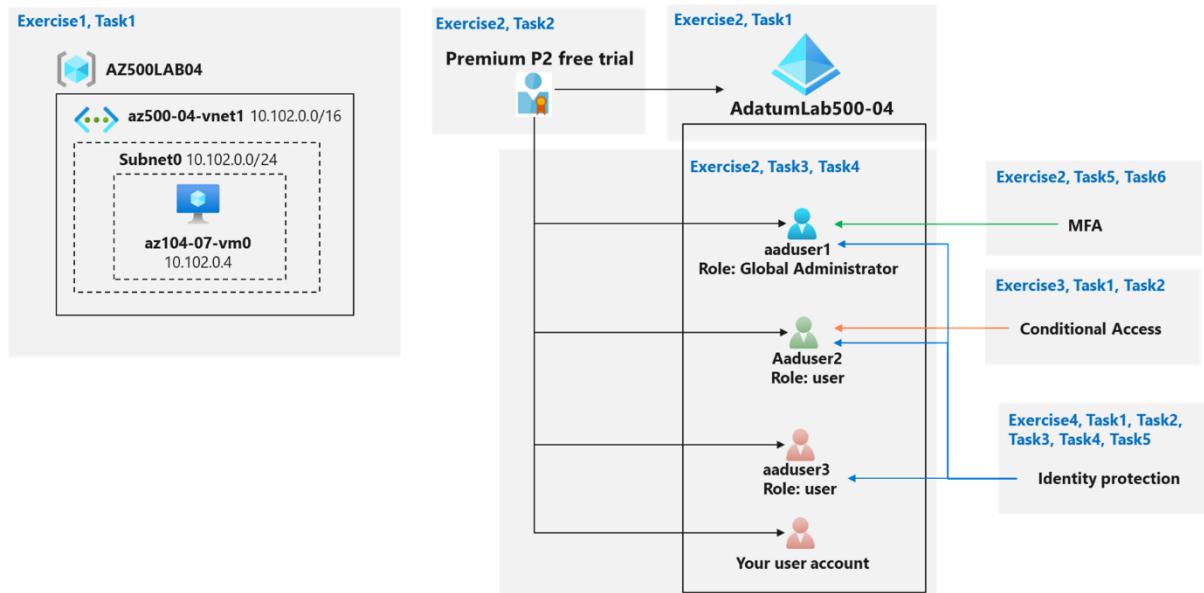


Lab 04: MFA, Conditional Access and AAD Identity Protection

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.

The screenshot shows the Microsoft Azure portal interface for editing an ARM template. The template code is displayed in a large text area, and the left sidebar shows the resource structure with parameters, variables, and resources defined.

```
$schema: "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
contentVersion: "1.0.0.0",
parameters": {
  "vmSize": {
    "type": "string",
    "metadata": {
      "description": "Virtual machine size"
    }
  },
  "vmName": {
    "type": "string",
    "defaultValue": "az500-04-vm1",
    "metadata": {
      "description": "VM name"
    }
  },
  "adminUsername": {
    "type": "string",
    "metadata": {
      "description": "Admin username"
    }
  }
},
variables: [
  "publicIpAddressName": "az500-04-vm1-public-ip",
  "networkSecurityGroupName": "az500-04-vm1-nsg"
],
resources: [
  {
    "name": "az500-04-vm1",
    "type": "Microsoft.Compute/virtualMachines",
    "properties": {
      "hardwareProfile": {
        "vmSize": "[parameters('vmSize')]"
      },
      "osProfile": {
        "computerName": "[parameters('vmName')]",
        "adminUsername": "[parameters('adminUsername')]",
        "adminPassword": "[secureString]"
      },
      "networkProfile": {
        "networkInterfaces": [
          {
            "id": "[resourceId('Microsoft.Network/networkInterfaces', parameters('nic1'))]"
          }
        ]
      }
    }
  },
  {
    "name": "az500-04-vm1-public-ip",
    "type": "Microsoft.Network/publicIPAddresses",
    "properties": {
      "ipAddress": "[ipAddress]"
    }
  },
  {
    "name": "az500-04-vm1-nsg",
    "type": "Microsoft.Network/networkSecurityGroups"
  }
]
```

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

```
1 {
2     "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
3     "contentVersion": "1.0.0.0",
4     "parameters": {
5         "vmSize": {
6             "value": "Standard_D2s_v3"
7         },
8         "adminUsername": {
9             "value": "Student"
10        },
11        "adminPassword": {
12            "value": "Pa55w.rdi1234"
13        }
14    }
15 }
16
```

Save Discard

AZ500-AzureSecurityTechnologies.zip Show all

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

Custom deployment

Subscription: Azure Pass - Sponsorship

Resource group: (New) AZ500LAB04

Region: East US

Vm Size: 1x Standard D2s v3

Vm Name: az500-04-vm1

Admin Username: mansleh

Admin Password: *****

Virtual Network Name: az500-04-vnet

Review + create < Previous Next : Review + create >

AZ500-AzureSecurityTechnologies.zip Show all

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

The screenshot shows the Microsoft Azure portal interface. The main title bar says "Microsoft.Template-20221113171101 | Overview". Below it, there's a search bar and several action buttons: Delete, Cancel, Redeploy, Download, and Refresh. A sidebar on the left has sections for Overview, Inputs, Outputs, and Template. The main content area displays a green checkmark indicating "Your deployment is complete". It shows deployment details: Deployment name: Microsoft.Template-20221113171101, Subscription: Azure Pass - Sponsorship, Resource group: AZ500LAB04. It also shows the start time: 11/13/2022, 5:11:07 PM and Correlation ID: 7af19f4e-e940-4801-91b4-e7a967243fc1. To the right, there are promotional cards for Cost Management, Microsoft Defender for Cloud, Free Microsoft tutorials, and Work with an expert. At the bottom, there's a "Show all" link and a taskbar with various icons.

Exercise 2: Implement Azure MFA (Multi factor authentication)

Task 1: Create a new Azure AD tenant

The screenshot shows the Microsoft Azure portal with the title bar "Create a tenant - Microsoft Azure". The main content area is titled "Create a tenant" and has a sub-section "Azure Active Directory". It includes tabs for "Basics", "Configuration", and "Review + create". Under "Basics", there's a note about Azure Active Directory and Azure Active Directory (B2C) enabling users to access applications published by your organization. The "Tenant type" section asks "Select a tenant type *", with "Azure Active Directory" selected (indicated by a blue circle). There are other options like "Azure Active Directory (B2C)" and "Help me choose...". At the bottom, there are "Review + create" and "Next : Configuration >" buttons. The taskbar at the bottom has various icons.

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

The tenant AdatumLab500-04 is created

Microsoft Azure - Manage tenants

Current tenant: Default Directory

Organization name	Domain name	Tenant type	Organization ID	Favorite
AdatumLab500-04	AdatumLab50004cns.onmicrosoft.com	Azure Active Directory	ef8ccb39-efcd-463d-ac5b-401a6b9e5e94	★
Default Directory (Default)	manassehwang@gmail.onmicrosoft.com	Azure Active Directory	97c8408d-ed9f-484d-8573-406c9ca353fb	★
United States International University (USIU)	usu.ac.ke	Azure Active Directory	16d83ee6-254a-469d-a6cc-54e2ca2313e7	★

Type here to search

Switch to the AdatumLab500-04 directory

Microsoft Azure - Portal settings | Directories + subscriptions

Directories + subscriptions

Default subscription filter: Azure Pass - Sponsorship - Don't see a subscription? Switch to another directory.

Directories

Current directory: Default Directory (manassehwang@gmail.onmicrosoft.com)

Directory name	Domain	Directory ID
Default Directory	manassehwang@gmail.onmicrosoft.com	97c8408d-ed9f-484d-8573-406c9ca353fb
AdatumLab500-04	AdatumLab50004cns.onmicrosoft.com	ef8ccb39-efcd-463d-ac5b-401a6b9e5e94
United States International University (USIU)	usu.ac.ke	16d83ee6-254a-469d-a6cc-54e2ca2313e7

Useful links:

- Learn more about settings
- Safelist URLs
- Microsoft partner network
- Privacy Statement
- More Azure resources
- Provide feedback

Type here to search

Task 2: Activate Azure AD Premium P2

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

The screenshot shows the Microsoft Azure portal interface. On the left, there is a sidebar with navigation links like Overview, Diagnose and solve problems, Manage (with Licensed features, All products selected, and Self-service sign up products), Activity (Audit logs), Troubleshooting + Support, and New support request. The main content area has a search bar at the top. Below it, there's a section titled "Activate" with a sub-section for "Enterprise Mobility + Security E5". This section includes a "Free trial" button and a detailed description of the service. To the right of this, another section titled "AZURE AD PREMIUM P2" is shown, also with a "Free trial" button and a detailed description. At the bottom of the main content area, there is an "Activate" button. The status bar at the bottom of the screen shows the date and time as 5:27 PM 11/13/2022.

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.

The screenshot shows the Microsoft Azure portal interface. The left sidebar has a "New user" link under the "Users" category. The main content area is titled "New user" and shows a "Select template" section with two options: "Create user" (selected) and "Invite user". Below this is a "Identity" section where "User name" is set to "aaduser1" and "Name" is also "aaduser1". There are fields for "First name" and "Last name" which are currently empty. Under the "Password" section, the "Let me create the password" option is selected. At the bottom of the form is a "Create" button. The status bar at the bottom of the screen shows the date and time as 5:34 PM 11/13/2022.

New user

Select template

Create user
Create a new user in your organization.

Invite user
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.

[Help me decide](#)

Identity

User name * adatumlab50004cn.onmicrosoft.com

Name *

First name

Last name

Password

Auto-generate password

Let me create the password.

Create

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

Users

All users (preview)

Want to switch back to the legacy users list experience? Click here to leave the preview.

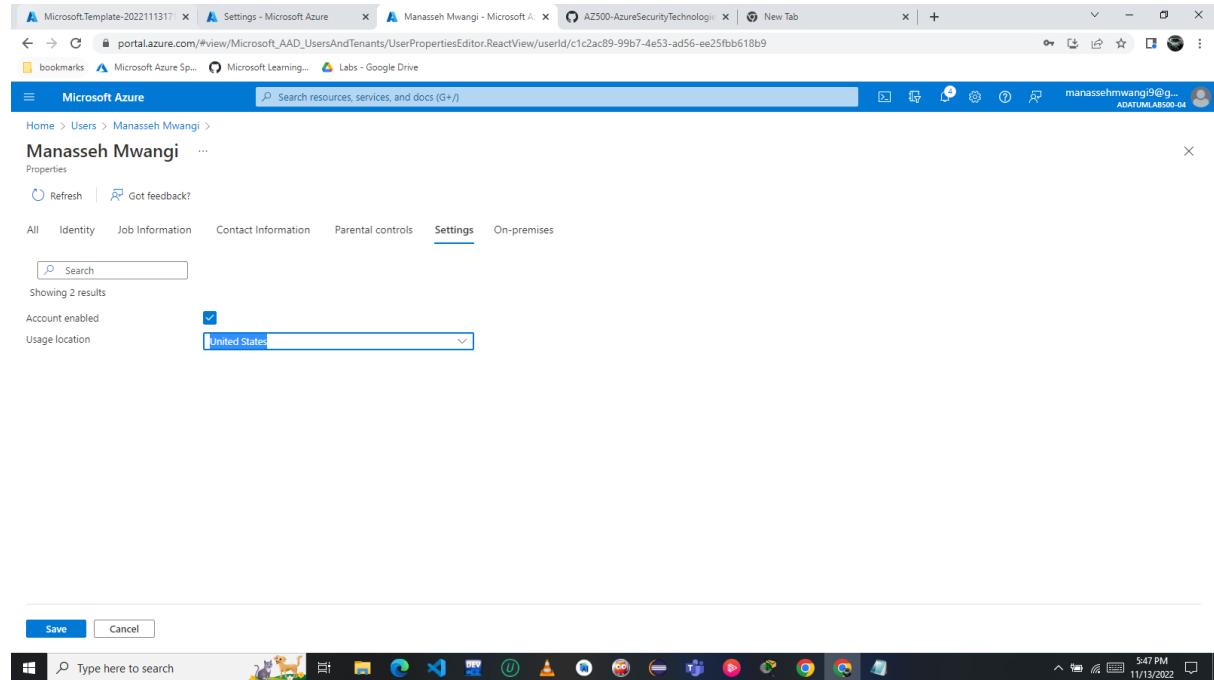
4 users found

Display name	User principal name	User type	On-premises sync	Identities	Company name	Creation type
aaduser1	aaduser1@adatumlab500...	Member	No	AdatumLab50004cn.onmicrosoft.com		
aaduser2	aaduser2@adatumlab500...	Member	No	AdatumLab50004cn.onmicrosoft.com		
aaduser3	aaduser3@adatumlab500...	Member	No	AdatumLab50004cn.onmicrosoft.com		
Manasseh Mwangi	manassehmwangi9@gmail...	Member	No	MicrosoftAccount		



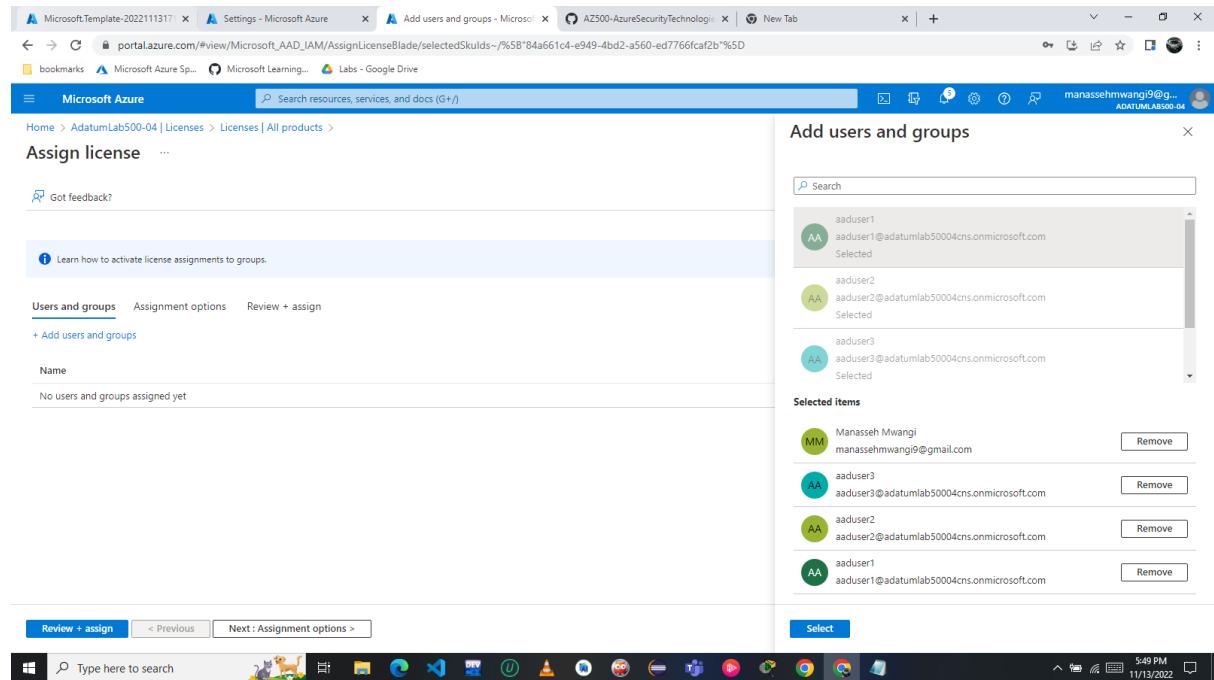
Task 4: Assign Azure AD Premium P2 licenses to Azure AD users

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



The screenshot shows the Microsoft Azure portal interface. The user is viewing the properties of 'Manasseh Mwangi'. In the 'Settings' tab, under 'Usage location', 'United States' is selected. At the bottom of the page, there is a 'Save' button.

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



The screenshot shows the 'Add users and groups' blade in the Microsoft Azure portal. Under 'Users and groups', several users are listed: 'aaduser1', 'aaduser2', 'aaduser3'. These users are selected, as indicated by a green circle icon next to their names. On the right side, a 'Selected items' section shows the same three users with their email addresses and a 'Remove' button next to each. At the bottom, there are 'Review + assign' and 'Next : Assignment options >' buttons.

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.

The screenshot shows the Microsoft Azure portal interface. The left sidebar has a 'Getting started' section with various options like 'Account lockout', 'Fraud alert', and 'Manage multifactor authentication server'. The main content area is titled 'Azure multifactor authentication' with a sub-section 'Additional cloud-based multifactor authentication settings'. A 'Configure' button is visible. The top navigation bar shows the URL 'portal.azure.com/#view/Microsoft_AAD_IAM/MultifactorAuthenticationMenuBlade/~/GettingStarted/fromProviders-/false' and the user 'manaszehmwang9@gmail.com#EXT#@AdatumLab50004crs.onmicrosoft.com'. The bottom taskbar shows the Windows Start button, a search bar, and several pinned icons.

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

The screenshot shows the 'Multi-factor authentication' configuration page in the Azure portal. It includes sections for 'app passwords', 'trusted ips' (with IP ranges 192.168.1.0/27 listed), and 'verification options'. Under 'Methods available to users', 'Text message to phone' and 'Notification through mobile app' are checked. The bottom of the page has a 'remember multi-factor authentication on trusted device' checkbox. The browser taskbar at the bottom shows the URL 'account.activedirectory.windowsazure.com/UserManagement/MfaSettings.aspx?tenantId=ef8ccb39-efcd-463d-ac5b-401a6b9e5e94&culture=en-us&requestInitiatedContext=users' and the date/time '5:58 PM 11/13/2022'.

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

The screenshot shows the 'multi-factor authentication users service settings' page in the Azure portal. A user named 'aaduser1' is selected, and the 'Multi-factor auth status' is set to 'Enabled'. A context menu is open for 'aaduser1' with options: 'aaduser1', 'quick steps', 'Disable', 'Enforce', and 'Manage user settings'.

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

The screenshot shows the 'Multifactor authentication | Fraud alert' blade in the Microsoft Azure portal. The 'Fraud alert' section is configured with 'Allow users to submit fraud alerts' set to 'On' and 'Automatically block users who report fraud' set to 'On'. The 'Code to report fraud during initial greeting' field contains '0'.

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 Conditional Access** as the reason and and then click **Save**.

The screenshot shows the Azure Active Directory Properties blade for the 'AdatumLab500-04' tenant. On the left, the 'Properties' section is selected. In the center, there's a 'Save' button and a 'Discard' button. Below them, there are fields for 'Country or region' (United States), 'Location' (United States datacenters), 'Notification language' (English), 'Tenant ID' (ef8cb39-efcd-ac5b-401a6b9e5e94), 'Technical contact' (manassehwangi@gmail.com), 'Global privacy contact' (empty), and 'Privacy statement URL' (empty). At the bottom of this section, there's a note about access management for Azure resources and a 'Yes' or 'No' button. To the right, a 'Enable security defaults' blade is open. It contains a description of security defaults, a 'Yes' or 'No' button for enabling them, and a list of reasons why security defaults might be disabled. One reason, 'My organization is using Conditional Access', is selected. At the bottom of the blade, there's a note about saving feedback and a 'Save' button.

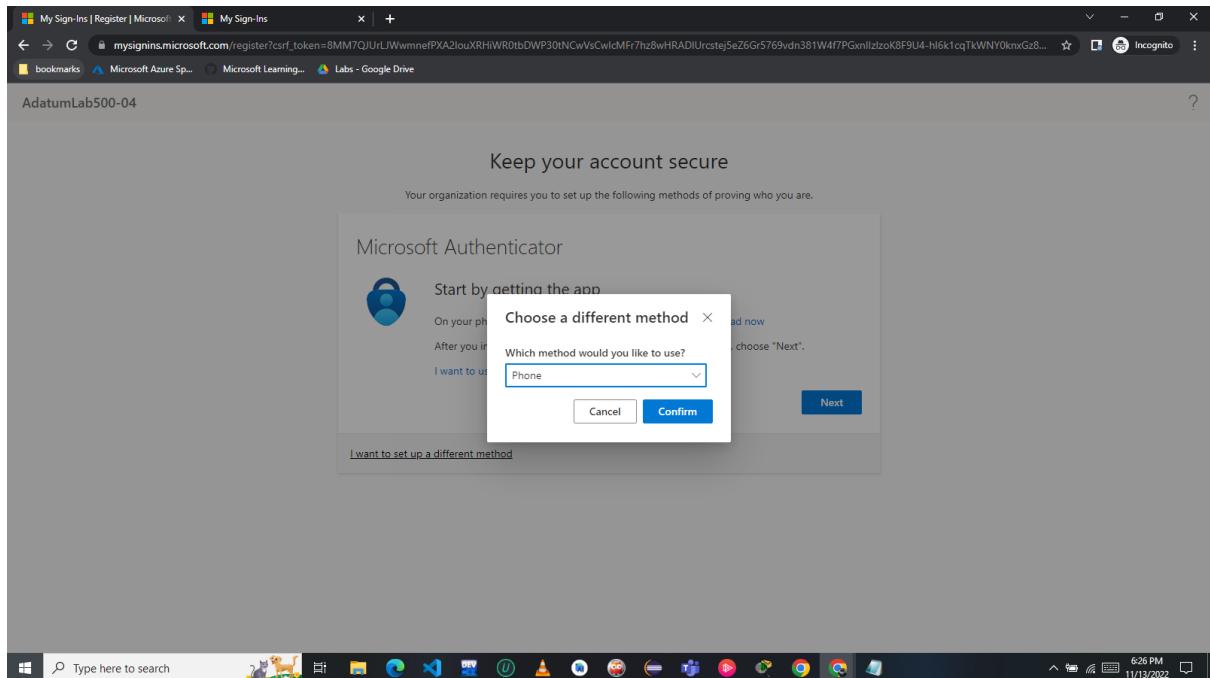
Task 6: Validate MFA configuration

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

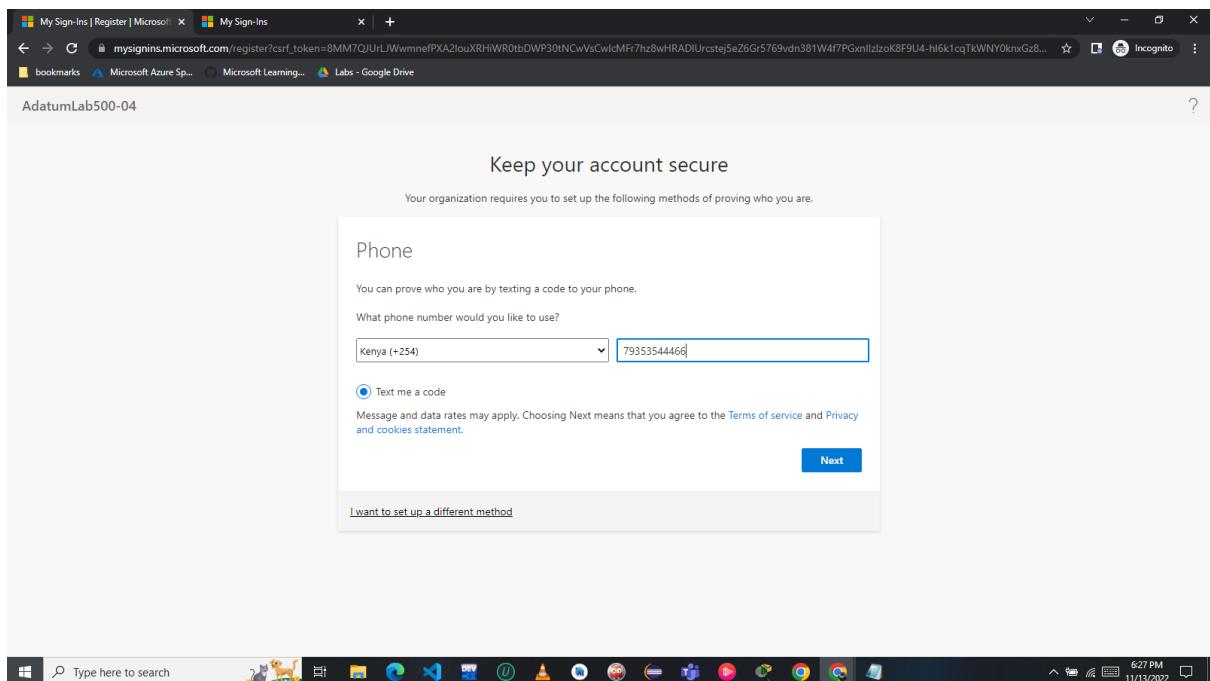
The browser session will be redirected to the **Additional security verification** page.

The screenshot shows a Microsoft Azure browser window. The title bar says 'My Sign-Ins'. The main content area has a blue background with a white 'Microsoft' logo and the text 'aaduser1@adatumlab50004cns.onmicrosoft.com'. Below that, it says 'More information required' and 'Your organization needs more information to keep your account secure'. There are 'Use a different account' and 'Learn more' links, and a large 'Next' button at the bottom. The browser taskbar at the bottom shows various pinned icons and the date/time (6:23 PM 11/13/2022).

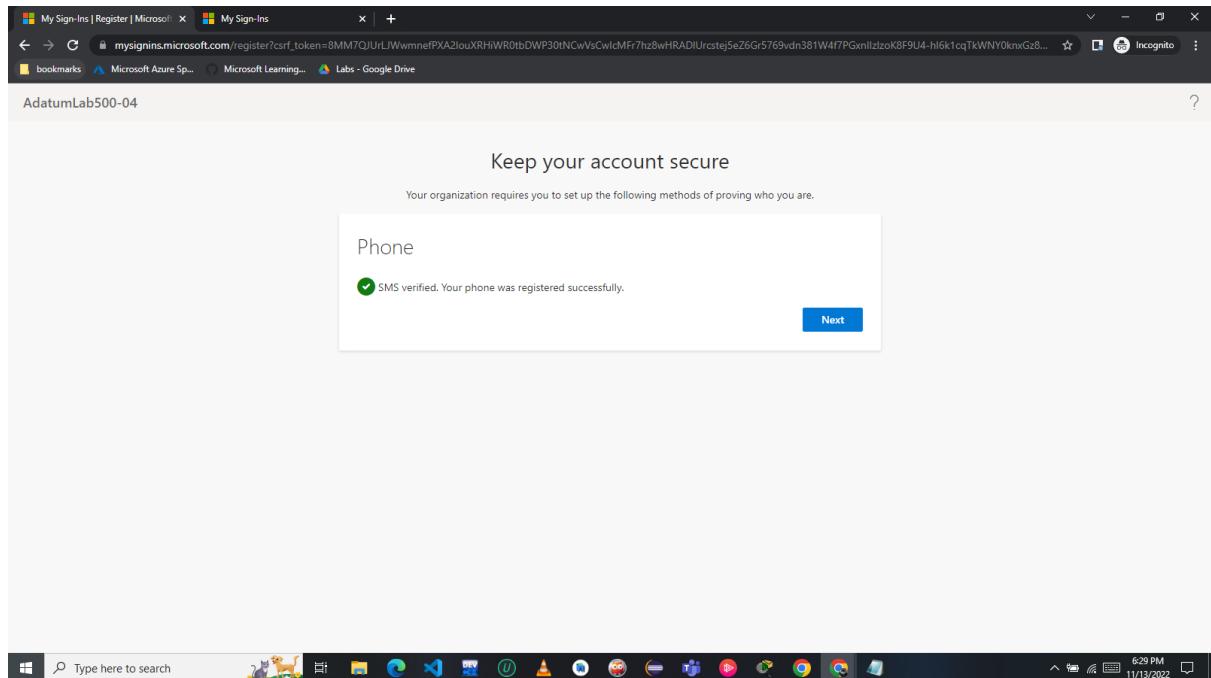
select **Phone**, and select **Confirm**



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.

New ...
Conditional Access policy

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

Name *

Assignments

Users or workload identities [\(i\)](#)
Specific users included "Select users and groups" must be configured

Cloud apps or actions [\(i\)](#)
No cloud apps, actions, or authentication contexts selected

Conditions [\(i\)](#)
0 conditions selected

Access controls

Enable policy [Report-only](#) On Off [Create](#)

Select users and groups

Search

aaduser1
aaduser1@adatumlab5004cns.onmicrosoft.com

aaduser2
aaduser2@adatumlab5004cns.onmicrosoft.com Selected

aaduser3
aaduser3@adatumlab5004cns.onmicrosoft.com

Manasseh Mwangi

Selected items aaduser2
aaduser2@adatumlab5004cns.onmicrosoft.com [Remove](#)

Select

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

New ...
Conditional Access policy

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

Name *

Assignments

Users or workload identities [\(i\)](#)
Specific users included "Select apps" must be configured

Cloud apps or actions [\(i\)](#)
No cloud apps, actions, or authentication contexts selected "Select apps" must be configured

Conditions [\(i\)](#)
0 conditions selected

Access controls

Enable policy [Report-only](#) On Off [Create](#)

Select

Cloud apps

Microsoft Azure Management MA 79748d6-ea00-4f57-aa43-9c1fb483013

Selected items MA Microsoft Azur... 79748d6-ea00-4f57-aa43-9c1fb483013 [Remove](#)

Select

The azure policy AZ500Policy1 has been created

The screenshot shows the Microsoft Azure Conditional Access Policies page. The URL is portal.azure.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Policies. The page title is "Conditional Access | Policies". On the left, there's a sidebar with sections like "Overview (Preview)", "Policies" (which is selected), "Insights and reporting", "Diagnose and solve problems", "Manage" (with options like "Named locations", "Custom controls (Preview)", "Terms of use", "VPN connectivity", "Authentication context (Preview)", and "Classic policies"), "Monitoring" (with "Sign-in logs" and "Audit logs"), and "Troubleshooting + Support" (with "New support request"). The main area shows a table with one policy listed:

Policy Name	State	Creation Date	Modified Date
AZ500Policy1	On	11/13/2022, 6:56:10 PM	

At the bottom right of the table, it says "1 out of 1 policy found". Below the table, there are three filter buttons: "Search policies", "Add filters", and "Get feedback?". The status bar at the bottom shows "6:56 PM 11/13/2022".

Task 2 - Test the conditional access policy.

In this task, you will sign in to the Azure portal as **aduser2** and verify MFA is required. You will also delete the policy before continuing on to the next exercise.

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

The screenshot shows a Microsoft Authenticator setup page. The URL is my.signins.microsoft.com/register?csrf_token=x83c461G5vTw-AECtyK_gy243YYOkAgnije5p0qUSz7k2K6x_0kXfbg8cm-m_ZV3Uy9_SoeTKFjPDW33b4Zx62B2SX-R3Z82UsAkL9mLySdIRF9APIDMYC6-dLSA.... The page title is "Keep your account secure". It says "Your organization requires you to set up the following methods of proving who you are." A modal window titled "Microsoft Authenticator" is open, asking "Start by [getting the app](#)". It says "Choose a different method" and "I want to use". A dropdown menu shows "Phone" selected. There are "Cancel" and "Next" buttons. At the bottom of the modal, it says "I want to set up a different method". The status bar at the bottom shows "7:01 PM 11/13/2022".

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.

The screenshot shows the Microsoft Azure portal homepage. At the top, there's a navigation bar with tabs for Home - Microsoft Azure, portal.azure.com/#home, and a New Incognito Tab. Below the navigation bar, the main content area starts with a "Welcome to Azure!" message and a note about not having a subscription. It features three promotional cards: "Start with an Azure free trial" (Get \$200 free credit toward Azure products and services, plus 12 months of popular free services), "Manage Azure Active Directory" (Manage access, set smart policies, and enhance security with Azure Active Directory), and "Access student benefits" (Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status). Below these cards is a section titled "Azure services" with icons for Create a resource, Quickstart Center, Virtual machines, App Services, Storage accounts, SQL databases, Azure Cosmos DB, Kubernetes services, Function App, and More services. Further down is a "Resources" section with a search bar and a taskbar at the bottom showing various application icons.

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.

The screenshot shows the "Identity Protection | Overview" page in the Microsoft Azure portal. The left sidebar contains navigation links for Overview, Tutorials, Diagnose and solve problems, Protect (User risk policy, Sign-in risk policy, Multifactor authentication registration policy), Report (Risky users, Risky workload identities (preview), Risky sign-ins, Risk detections), Notify (Users at risk detected alerts, Weekly digest), and Troubleshooting + Support. The main content area displays two charts: "New risky users detected" (a line chart showing the count of new risky users from 10/15 to 11/12) and "New risky sign-ins detected" (a line chart showing the count of new risky sign-ins from 10/15 to 11/12, with categories Unprotected and Protected). To the right of the charts is a box titled "Identity Secure Score" with a score of 7/10 and a callout "Monitor and improve your identity security posture". The bottom of the screen shows a Windows taskbar with various application icons.

Task 2: Configure a user risk policy

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

The screenshot shows the Microsoft Azure portal interface. The left sidebar is titled 'Identity Protection' and includes sections for Overview, Tutorials, Diagnose and solve problems, Protect (User risk policy selected), Report, Notify, Troubleshooting + Support, and a search bar. The main content area is titled 'Identity Protection | User risk policy'. It shows a policy named 'User risk remediation policy' with the 'Exclude' tab selected. Under 'Assignments', it lists 'Users' with 'All users included and 1 user excluded'. Under 'User risk', it shows 'Low and above' and a specific user 'Manasseh Mwangi' (manassehmwang9@gmail.com). Under 'Controls', it has 'Access' (radio button set to 'On') and 'Require password change'. At the bottom, there is an 'Enforce policy' switch set to 'On' and a 'Save' button. The top right corner shows the user's name 'manassehmwang9@gmail.com' and the environment 'ADATUMLAB500-04 (ADATUMA...)'.

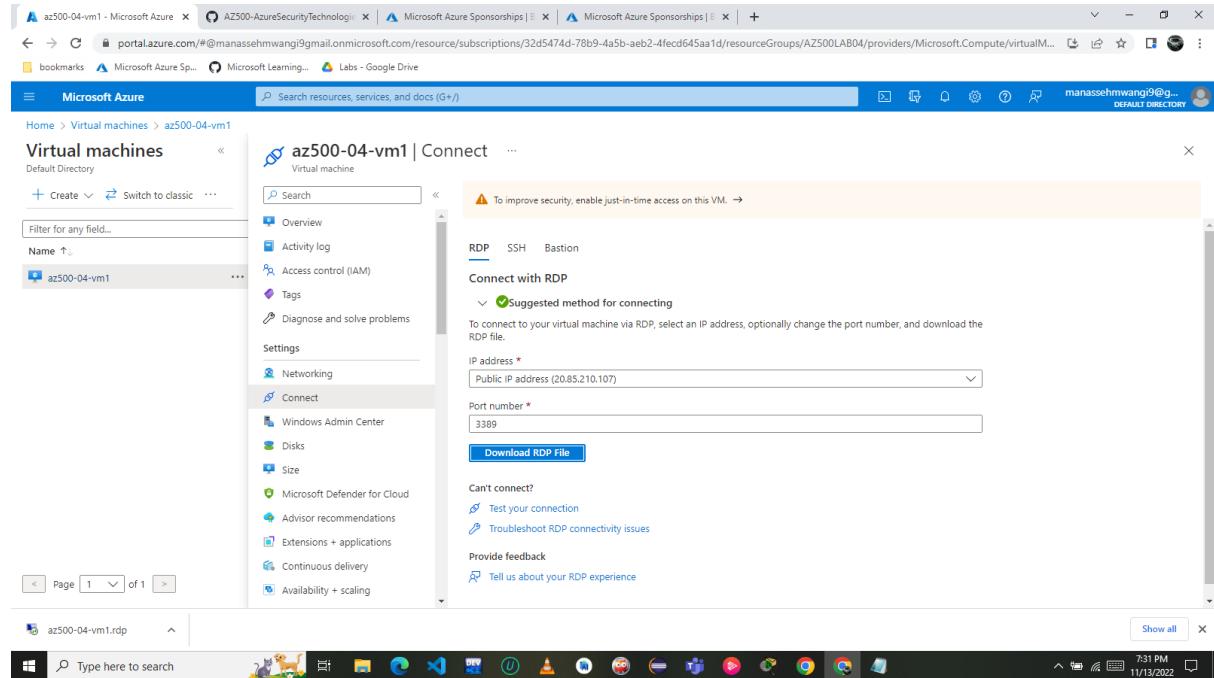
Task 3: Configure sign-in risk policy

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

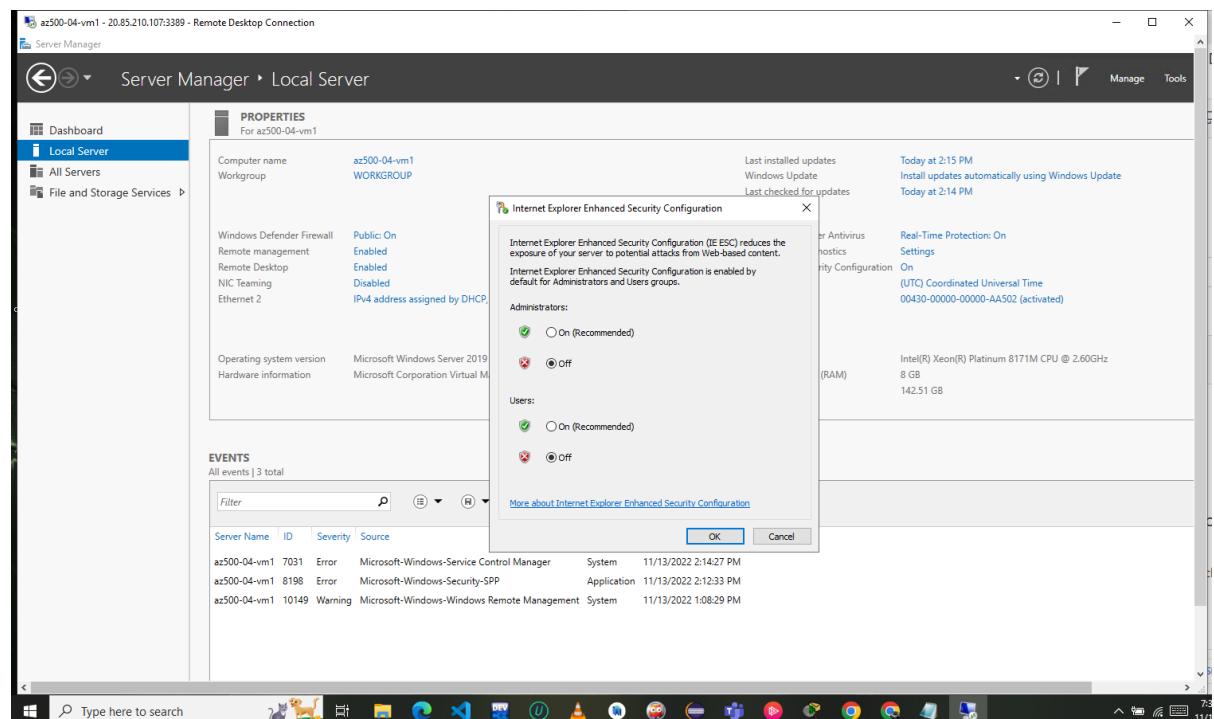
This screenshot is identical to the one in Task 2, showing the 'User risk policy' configuration page. The left sidebar and main content area are the same, including the policy name 'User risk remediation policy', the 'Exclude' tab selected, the 'Users' assignment, the 'User risk' setting for 'Low and above', and the 'Access' control set to 'On'. The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray indicating the date and time as 11/13/2022 at 7:23 PM.

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

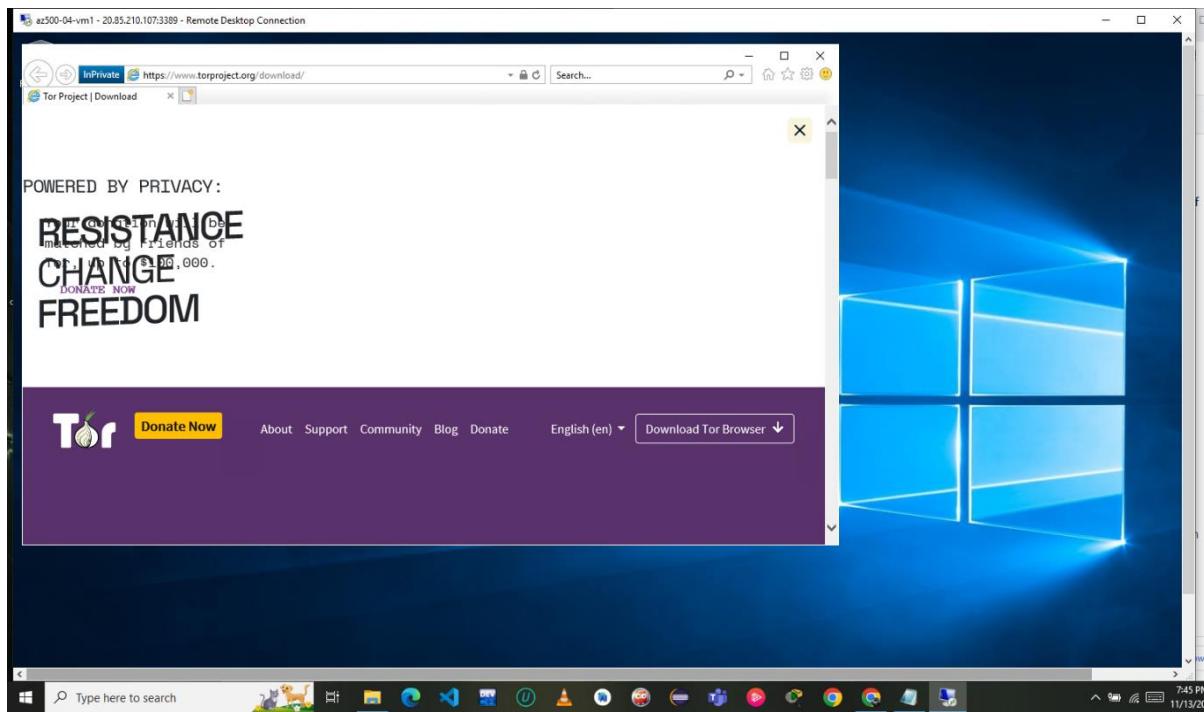
Click Download RDP File and use it to connect to the az500-04-vm1 via Remote Desktop.



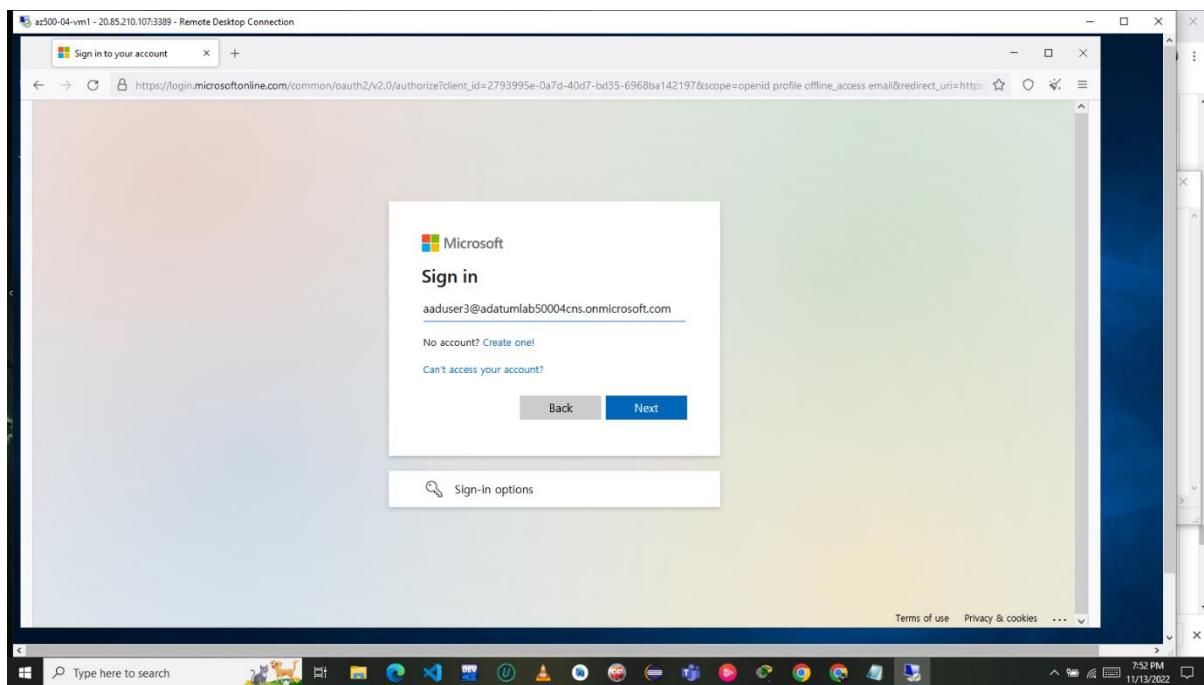
In Server Manager, click Local Server and then click IE Enhanced Security Configuration. set both options to Off and click OK.



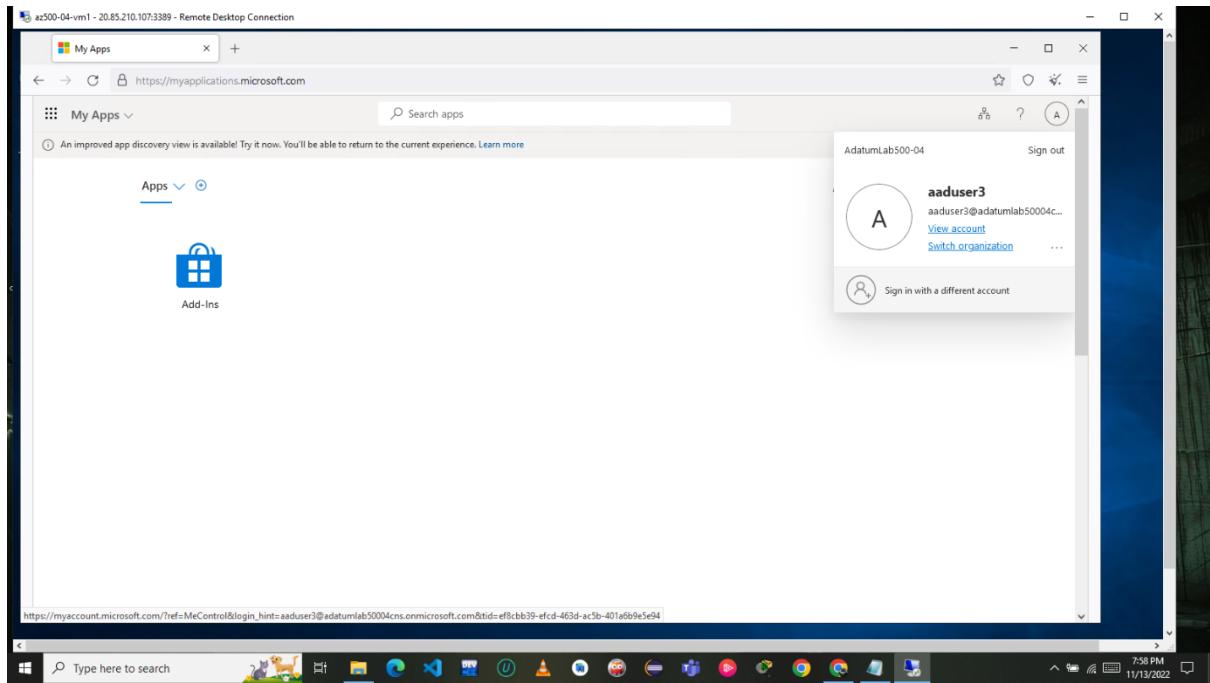
In the InPrivate Internet Explorer window, navigate to the ToR Browser Project



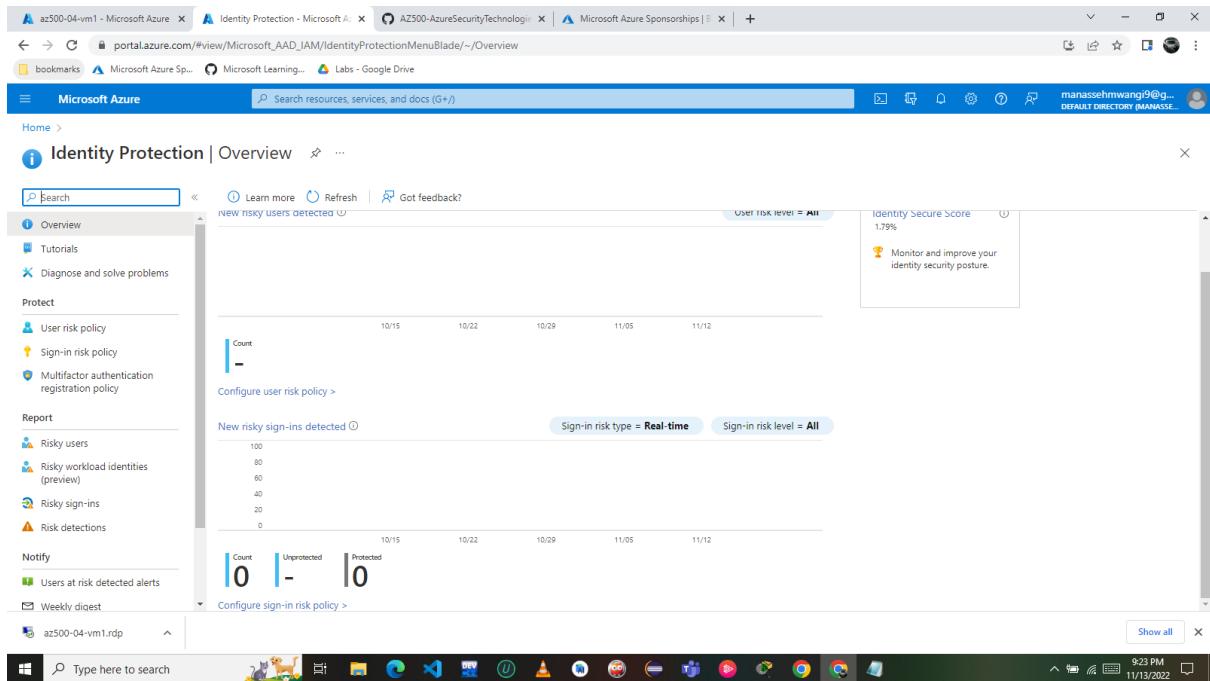
attempt to sign in with the **aaduser3** account.



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