Fatma Omar Salim
Cloud Security Project 2
CyberSafe Foundation: CyberGirls 2.0
Demonstrating how to set up MFA, Conditional Access, and AAD Identity Protection in Azure.

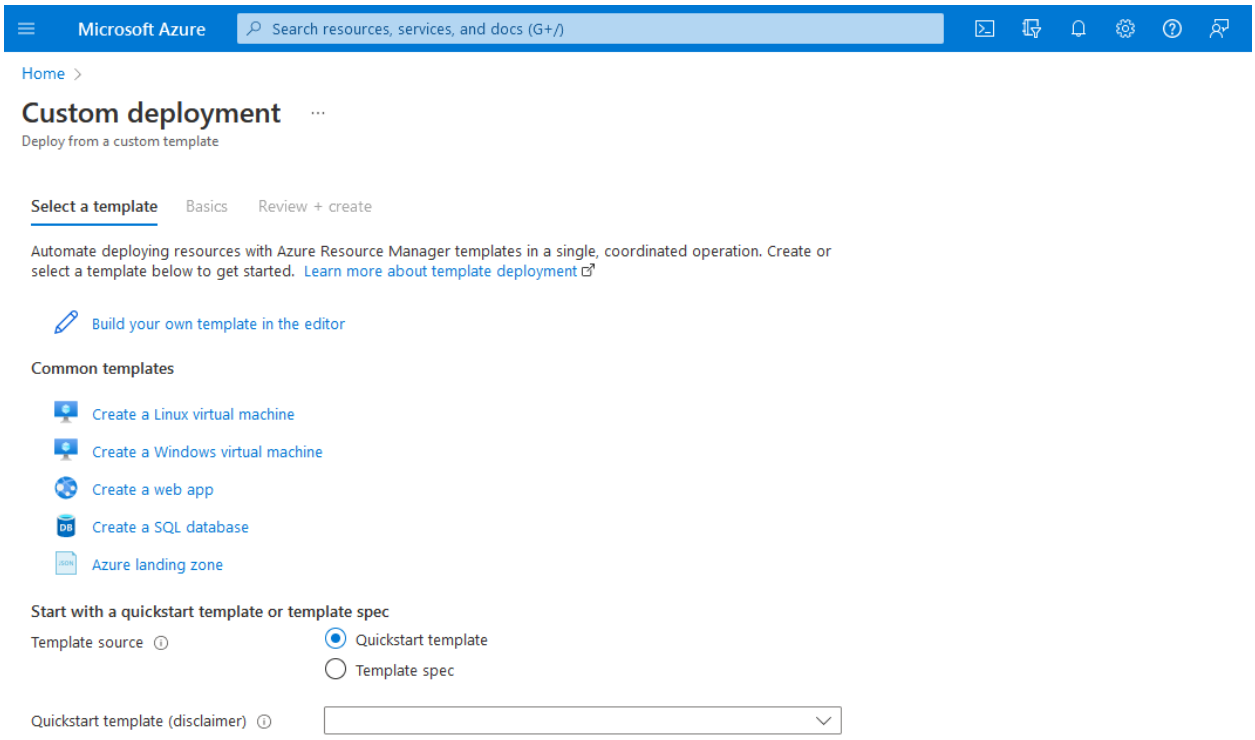
Objectives

1. Deploying an Azure VM by using an Azure Resource Manager template.
2. Implementing Azure MFA.
3. Implementing Azure Ad Conditional Access Policies.
4. Implementing Azure AD Identity Protection.

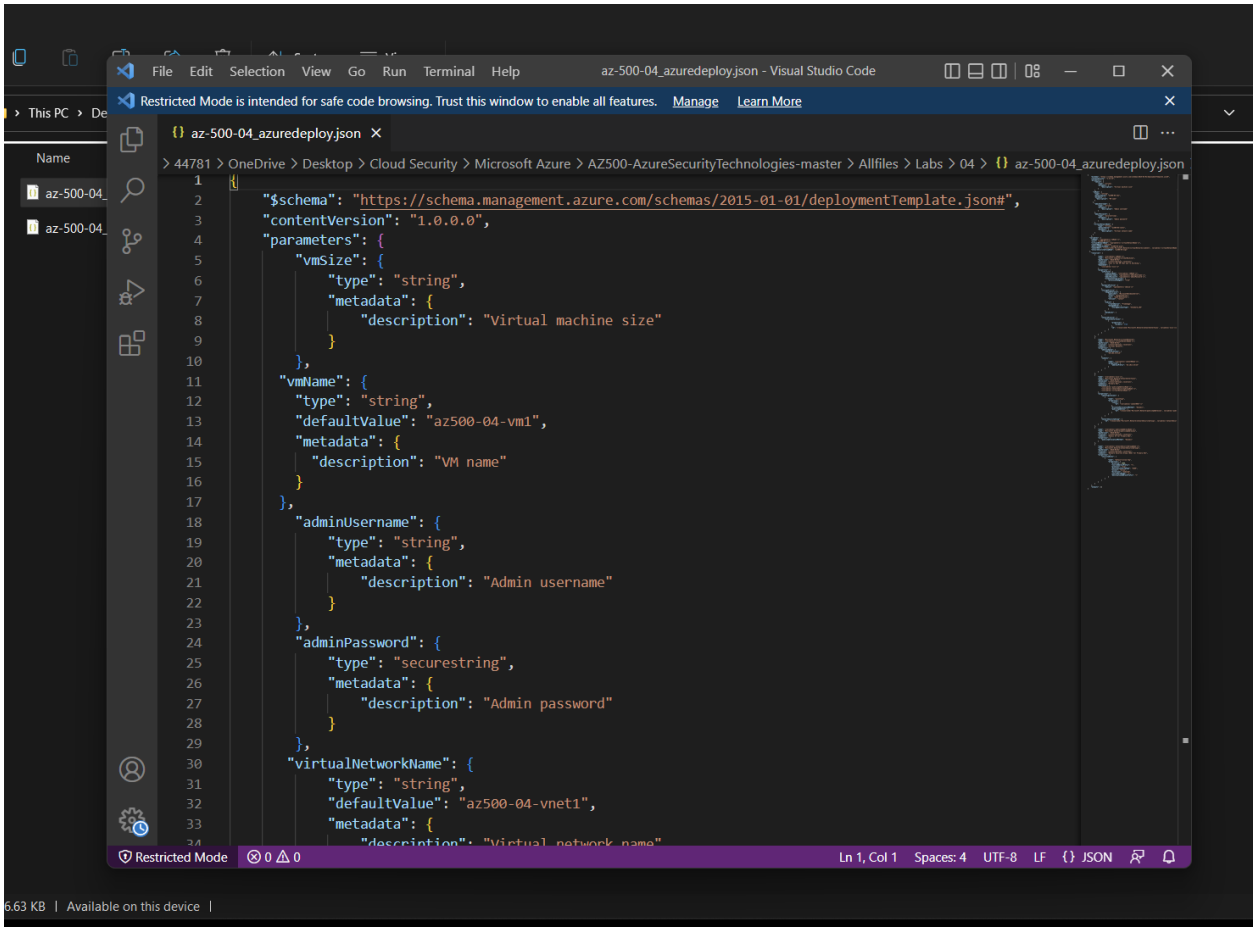
Objective 1: Deploying an Azure VM by using an Azure Resource Manager template.

1. Sign in to the Azure Portal.

2. In the **Search** tab, type **Deploy a custom template** or select **Template Deployment** (**deploy using custom templates**) from the **Marketplace** list.



3. Click on the **Build your own template in the editor** option. Copy paste or upload your deployment codes, click save.



4. Once saved, click on **Edit parameters**, upload code and click **save**.

Custom deployment

Deploy from a custom template

Select a template | **Basics** | Review + create

Template

Customized template
5 resources

Edit template | Edit paramet... | Visualize

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure for Students

Resource group : Loading...
Create new

Instance details

Region : Loading...

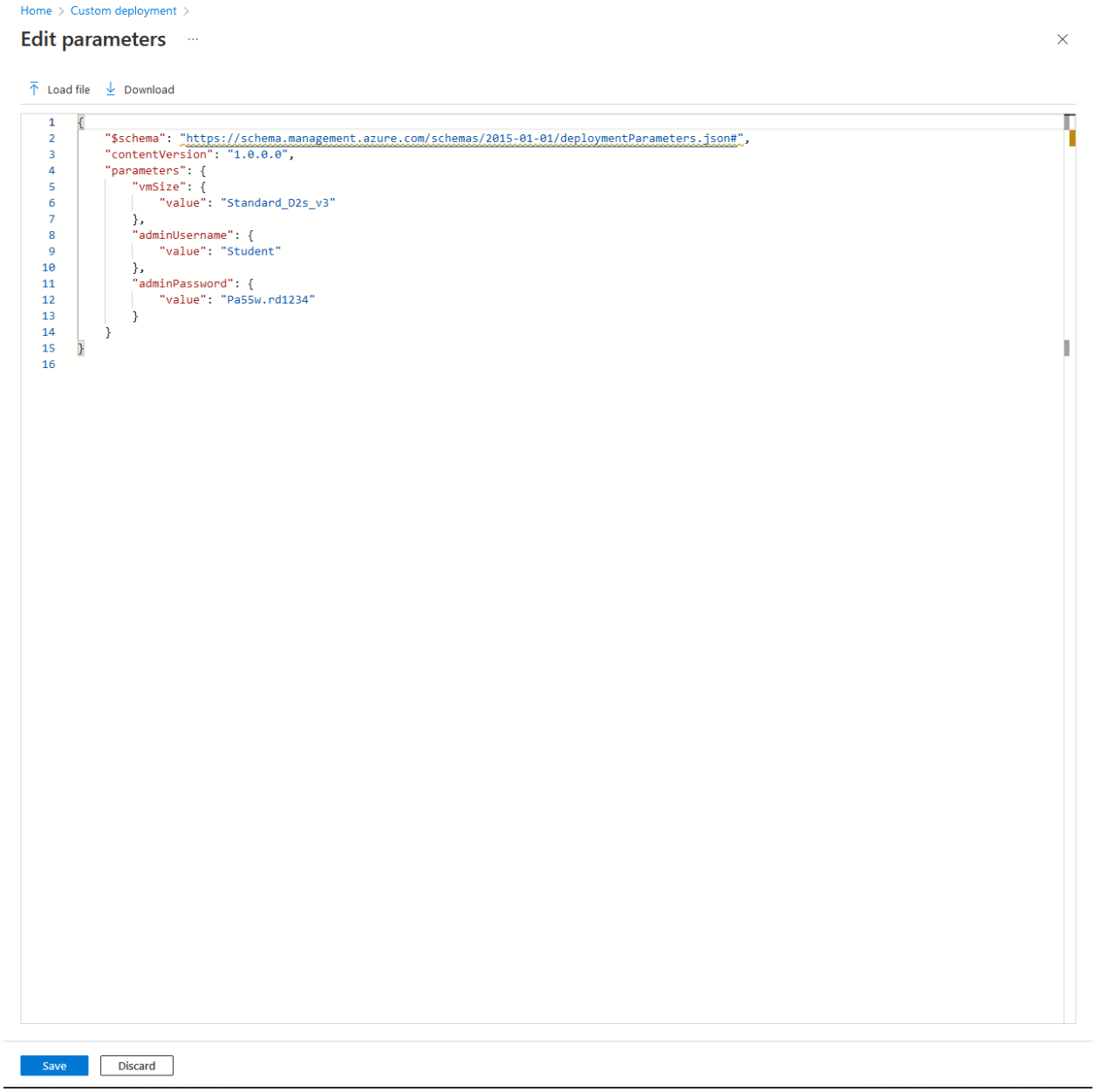
Vm Size * : Change size

Vm Name : az500-04-vm1

Admin Username * :

Admin Password * :

Virtual Network Name : az500-04-vnet1



5. Ensure your details are as follows: Enter your own password and click on **Review + Create**, and then click **Create**.

Home >

Custom deployment

Deploy from a custom template

Select a template | Basics | Review + create

Template

Customized template
5 resources

Edit template | Edit paramet... | Visualize

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure for Students

Resource group * : (New) AZ500LAB04
Create new

Instance details

Region * : East US

Vm Size * : **1x Standard D2s v3**
2 vcpus, 8 GB memory
Change size

Vm Name : az500-04-vm1

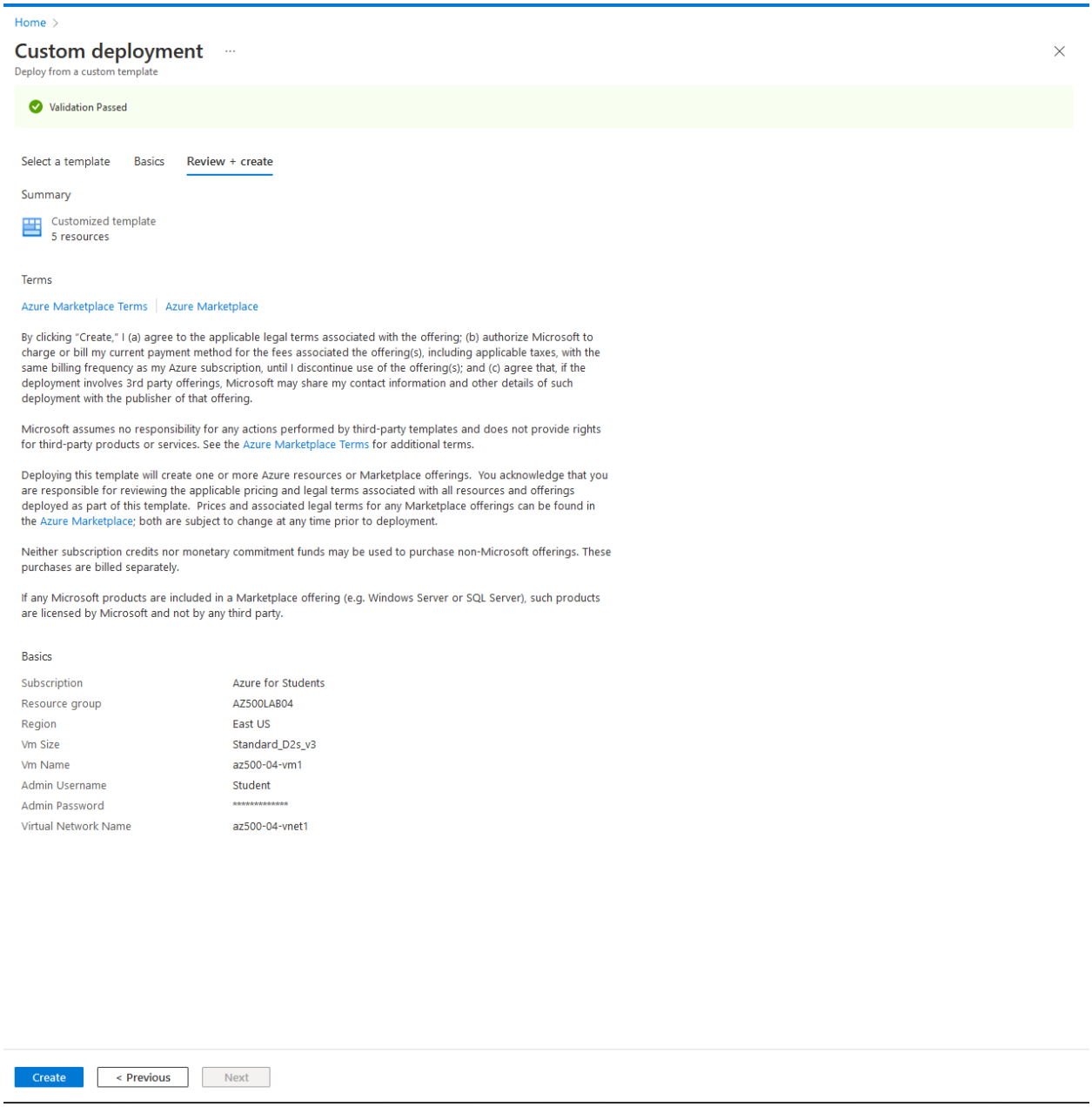
Admin Username * : Student

Admin Password * : ••••••••••••••

Virtual Network Name : az500-04-vnet1

Review + create | < Previous | Next : Review + create >

https://portal.azure.com/#



Objective 2: Implementing Azure MFA

We will divide this objective into 6 tasks. Namely:

- Task 1: Create a new Azure AD tenant.
- Task 2: Activate Azure AD Premium P2 trial.
- Task 3: Create Azure AD users and groups.
- Task 4: Assign Azure AD Premium P2 licenses to Azure AD users.
- Task 5: Configure Azure MFA settings.

- Task 6: Validate MFA configuration

<u>Task 1: Creating a new Azure AD Tenant</u>

1. In the **search** tab, type **Azure Active Directory** and press the **Enter** key.
2. On the blade displaying **Overview** of your current Azure AD tenant, click **Manage tenants**, and then on the next screen, click **+ Create**.
3. On the **Basics** tab of the **Create a tenant** blade, ensure that the option **Azure Active Directory** is selected and click **Next: Configuration >**
4. On the **Configuration** tab of the **Create a tenant** blade, specify the following settings:

Home > Default Directory | Overview > Manage tenants >

Create a tenant

Azure Active Directory

*Basics *Configuration Review + create

Directory details

Configure your new directory

Organization name * AdatumLab500-04

Initial domain name * mutada005

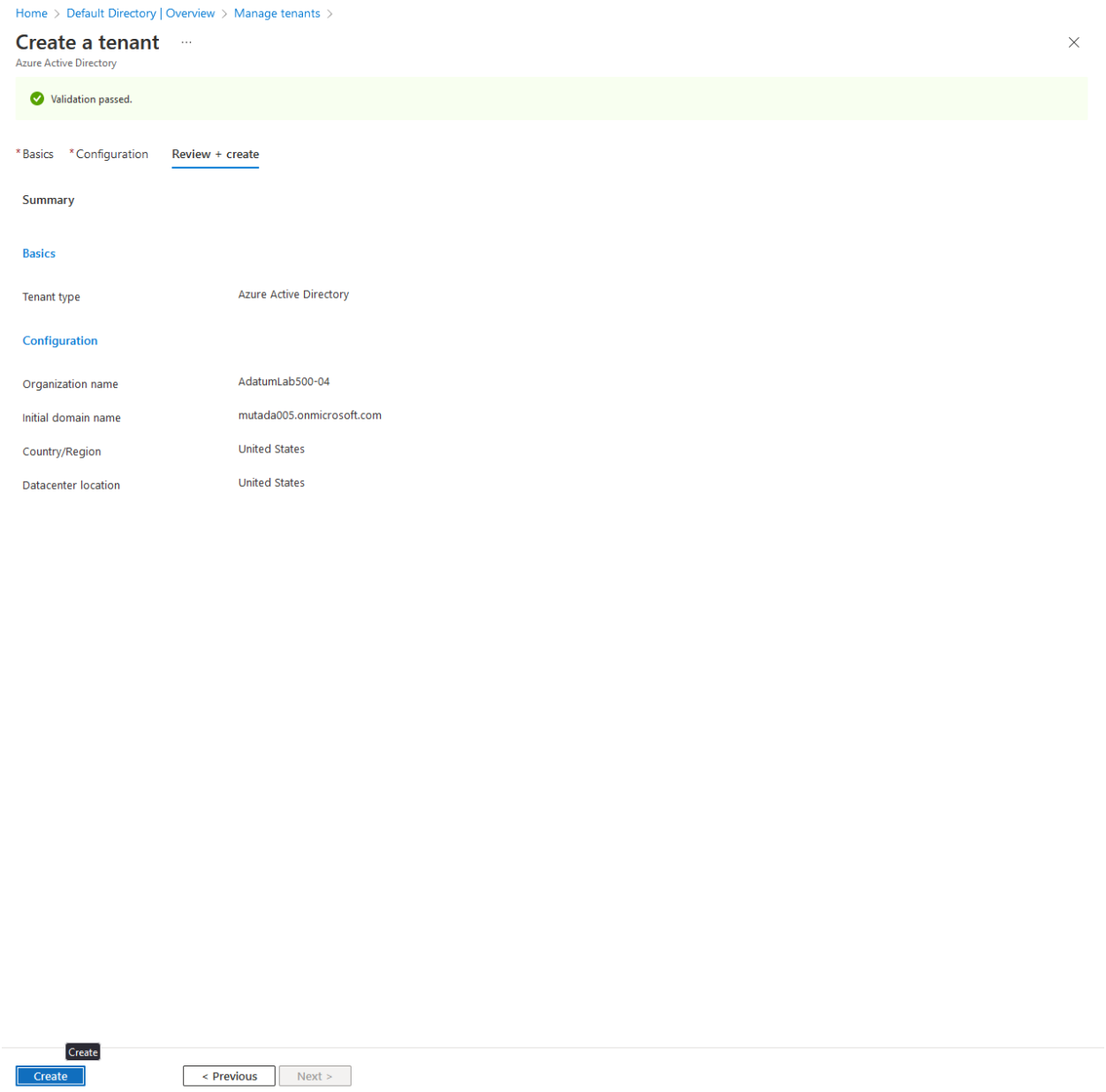
mutada005.onmicrosoft.com

Country/Region United States

Datacenter location - United States

Datacenter location is based on the country/region selected above.

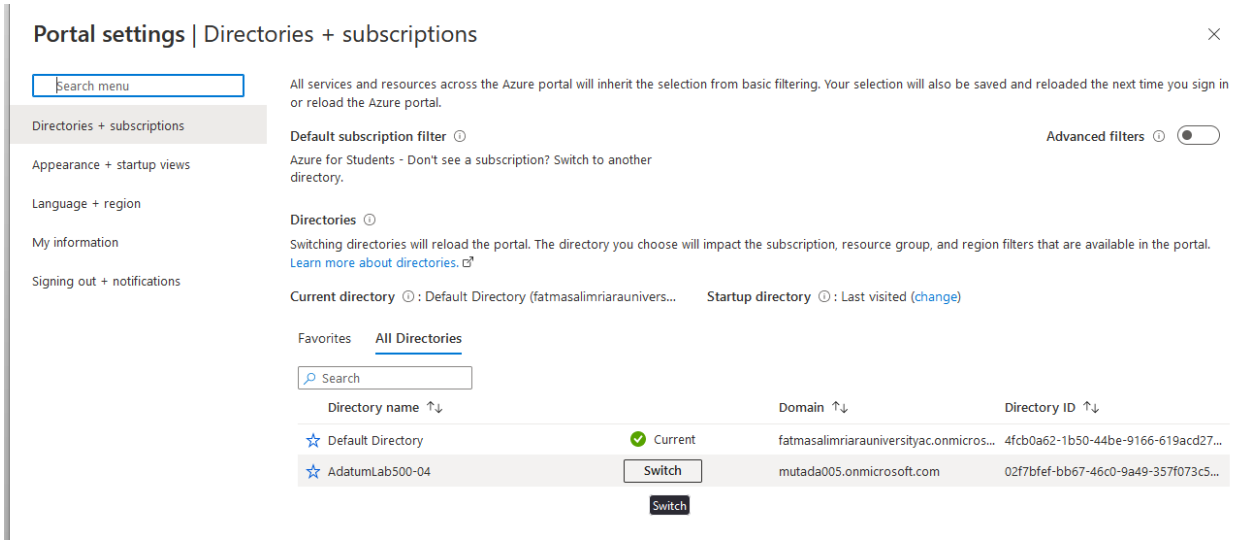
Review + create < Previous Next : Review + create >



Task 2: Activating Azure AD Premium P2 Trial

1. In the Azure portal, in the toolbar, click the **Directory + subscription** icon, located to the right of the Cloud Shell icon.

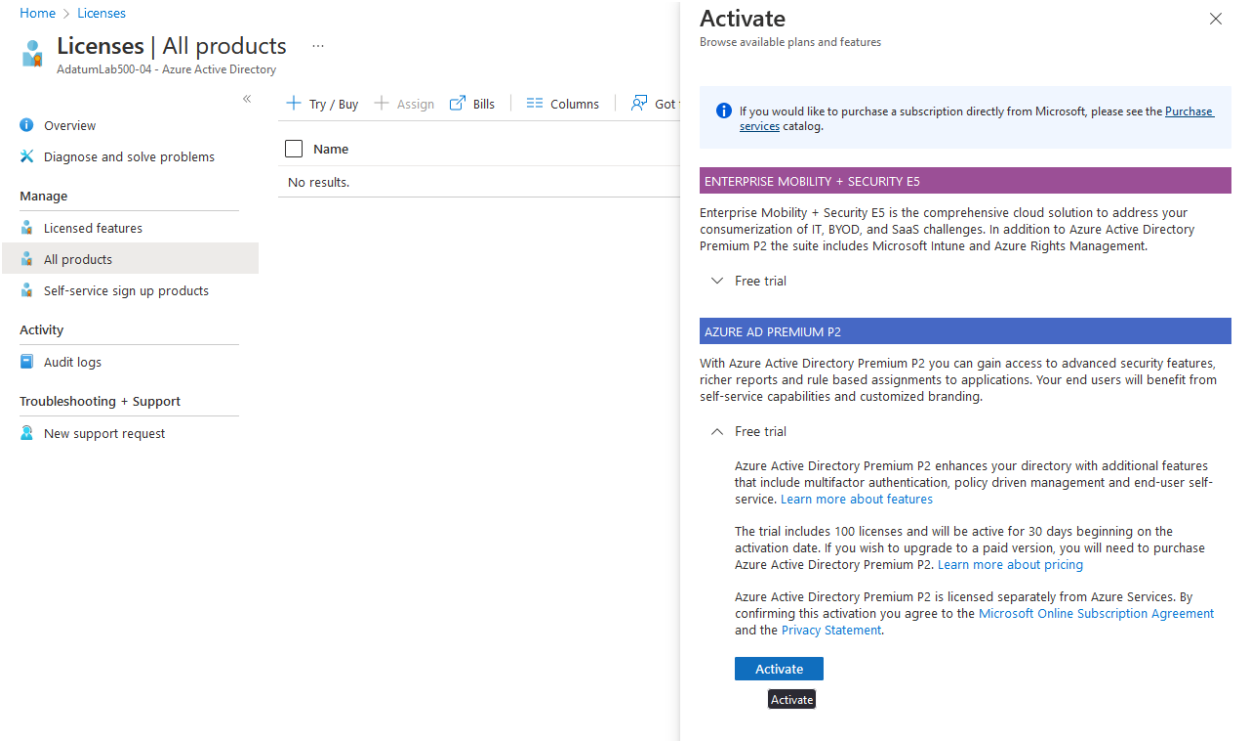
2. In the **Directory + subscription** blade, click the newly created tenant **AdatumLab500-04** and click the **Switch** button to set it as the current directory.



3. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Azure Active Directory** and press the **Enter** key. On the **AdatumLab500-04** blade, in the **Manage** section, click **Licenses**.

4. On the **Licenses | Overview** blade, in the **Manage** section, click **All products** and then click **+ Try / Buy**.

5. On the **Activate** blade, in the Azure AD Premium P2 section, click **Free Trial** and then click **Activate**.



Task 3: Creating Azure AD users and groups.

1. Navigate back to the **AdatumLab500-04** Azure Active Directory blade and, in the **Manage** section, click **Users**.

2. On the **Users | All users** blade, click **+ New User**.

3. On the **New user** blade, ensure that the **Create user** option is selected, and specify the following settings (leave all others with their default values) and click **Create**:

Identity

User name * aaduser1 @ mutada005.onmicrosoft.c...

The domain name I need isn't shown here

Name * aaduser1

First name

Last name

Password

Auto-generate password

Let me create the password

Initial password Pozu7520

Show Password

Groups and roles

Groups 0 groups selected

Roles Global administrator

Settings

Block sign in Yes No

Usage location United States

Job info

Job title

Department

Company name

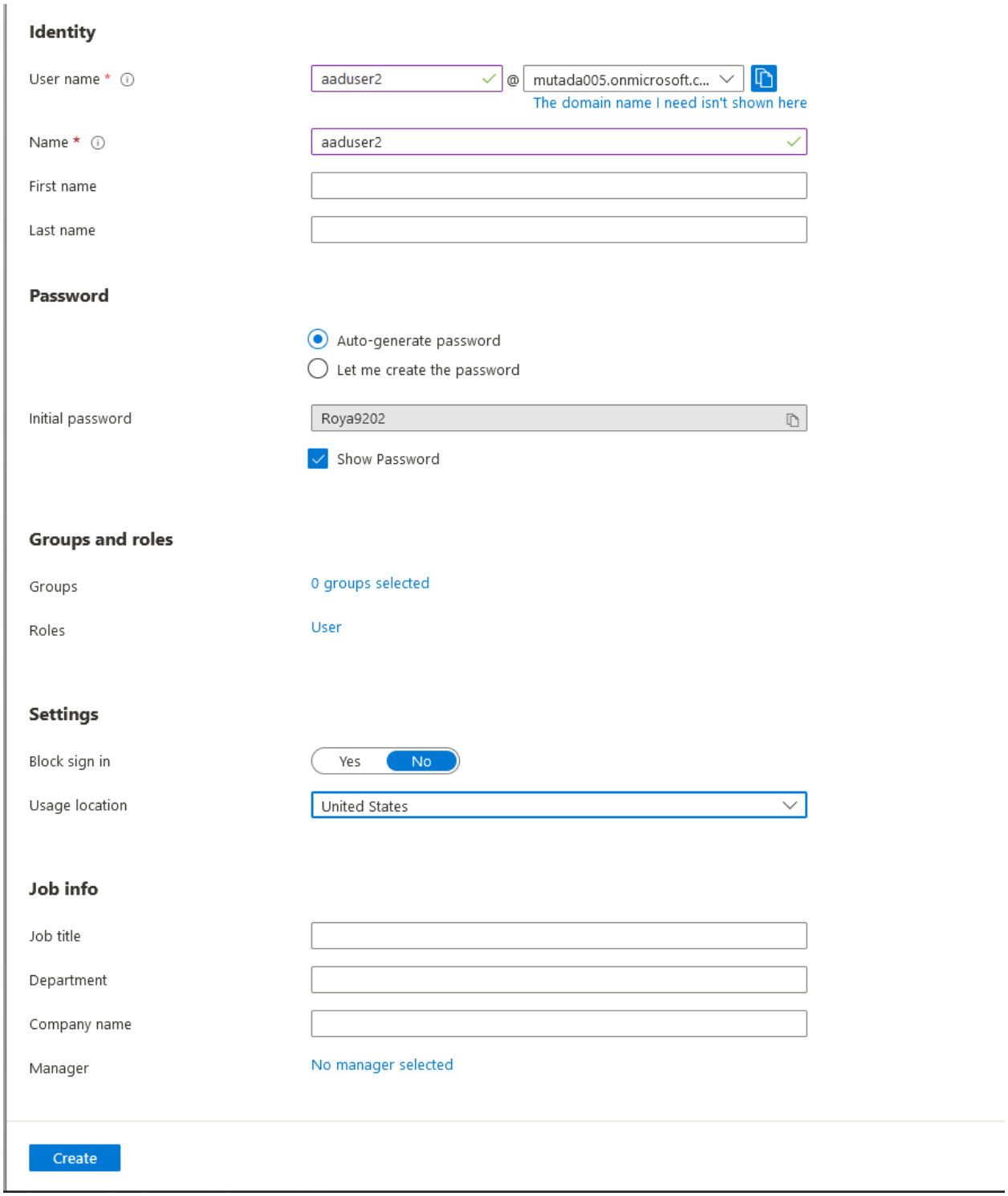
Manager No manager selected

Create

https://portal.azure.com/#

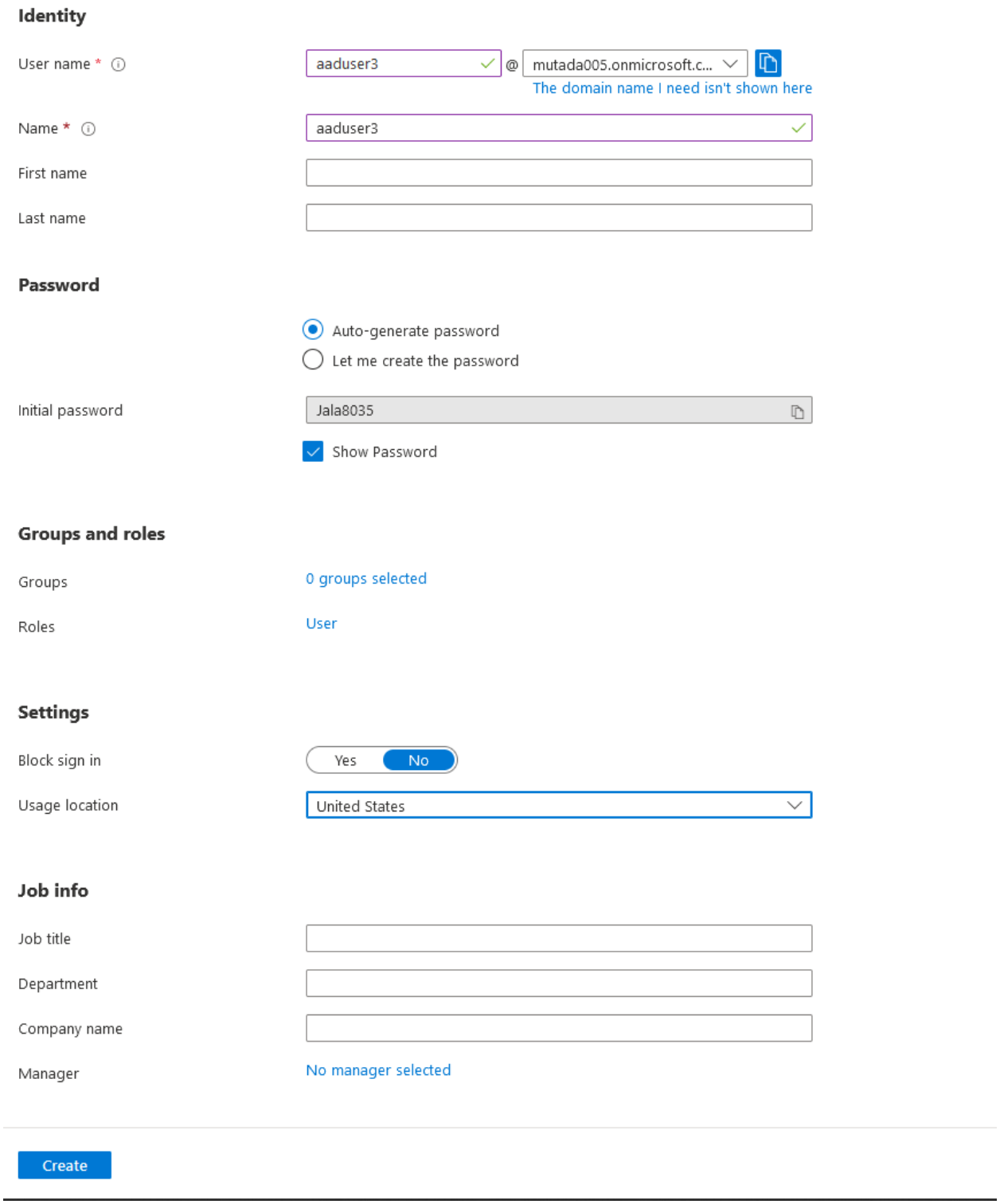
4. Back on the **Users | All users** blade, click **+ New User**.

5. On the **New user** blade, ensure that the **Create user** option is selected,and specify the following settings (leave all others with their default values):



6. Back on the **Users | All users** blade, click **+ New User**.

7. Click **New User**,complete the new user configuration settings, and then click **Create**.



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

1. On the **Users | All users** blade, click the entry representing your user account.

2. On the blade displaying the properties of your user account, click **Edit**. Verify Usage Location is set to **United States** if not set the usage location and click **Save**.

3. Navigate back to the **AdatumLab500-04** Azure Active Directory blade and, in the **Manage** section, click **Licenses**.

4. On the **Licenses | Overview** blade, click **All products**, select the **Azure Active Directory Premium P2** checkbox, and click **+ Assign**.

5. On the **Assign licenses** blade, click **+ Add users and groups**.

6. On the **Users** blade, select **aaduser1**, **aaduser2**, **aaduser3**, and your user account and click **Select**.

7. Back on the **Assign licenses** blade, click **Assignment options**, ensure that all options are enabled, click **Review + asssign**, click **Assign**.

8. Sign out from the Azure portal and sign back in using the same account. This step is necessary in order for the license assignment to take effect

Task 5: Configuring Azure MFA settings

1. In the Azure portal, navigate back to the **AdatumLab500-04** Azure Active Directory tenant blade.

2. On the **AdatumLab500-04** Azure Active Directory tenant blade, in the **Manage** section, click **Security**.

3. On the **Security | Getting started** blade, in the **Manage** section, click **MFA**.

4. On the **Multi-Factor Authentication | Getting started** blade, click the **Additional cloud-based MFA settings** link.

5. On the **multi-factor authentication** page, click the **service settings** tab. Review **verification options**. Note that **Text message to phone**, **Notification through mobile app**, and **Verification code from mobile app or hardware token** are enabled. Click **Save** and then click **close**.

multi-factor authentication

users **service settings**

app passwords (learn more)

- (●) Allow users to create app passwords to sign in to non-browser apps
- ( ) Do not allow users to create app passwords to sign in to non-browser apps

trusted ips (learn more)

- [ ] Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

```
192.168.1.0/27
192.168.1.0/27
192.168.1.0/27
```

verification options (learn more)

Methods available to users:

- [ ] Call to phone
- [x] Text message to phone
- [x] Notification through mobile app
- [x] Verification code from mobile app or hardware token

remember multi-factor authentication on trusted device (learn more)

- [ ] Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)

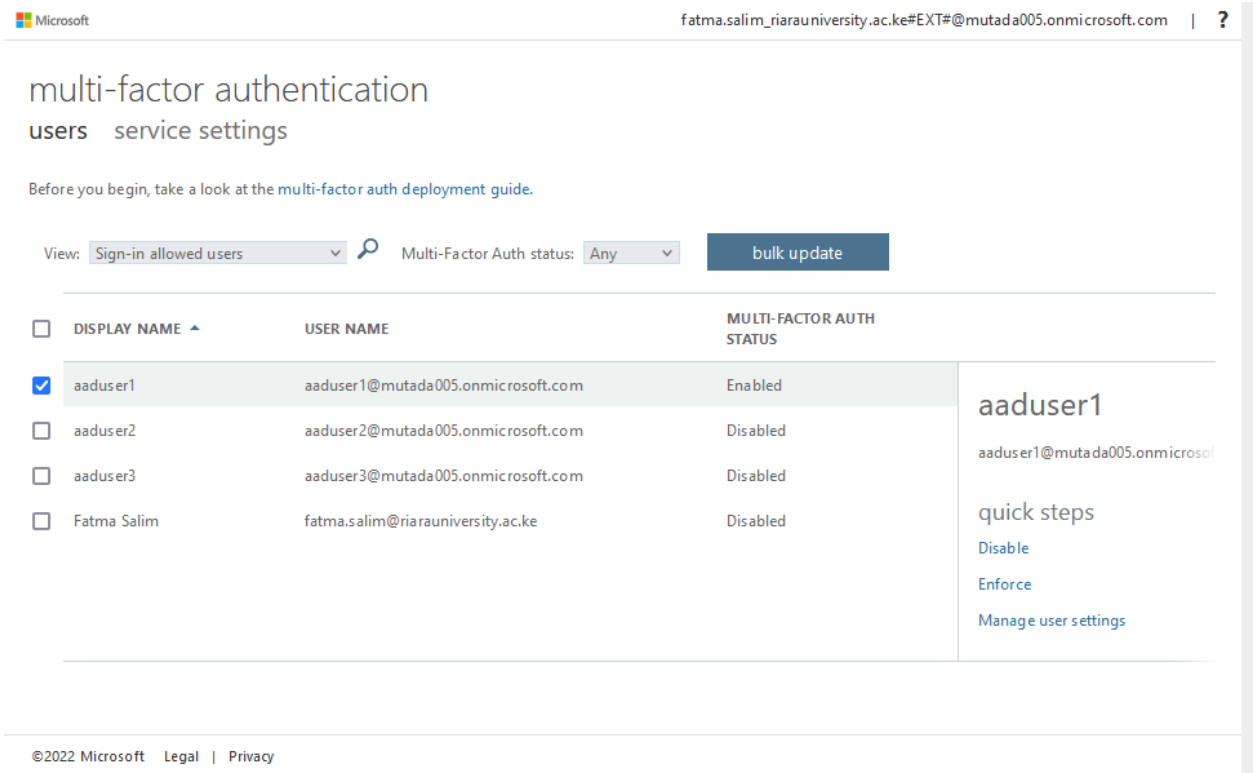
Number of days users can trust devices for 90

NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' be sure to extend the duration to 90 or more days. Learn more about reauthentication prompts.

save

Manage advanced settings and view reports Go to the portal

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



7. Notice the **Multi-Factor Auth status** column for **aaduser1** is now **Enabled**.

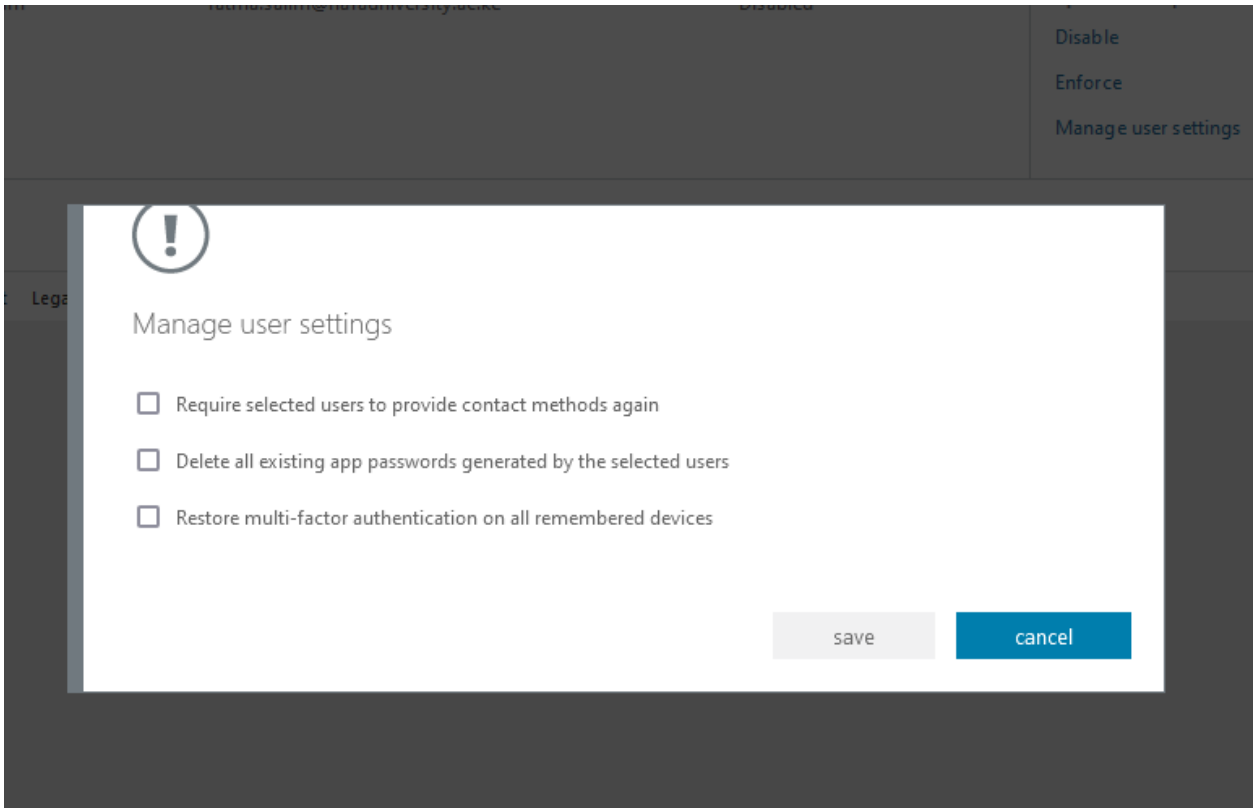
8. Click **aaduser1** and notice that, at this point, you also have the **Enforce** option.

9. With the **aaduser1** entry selected, click **Manage user settings** and review the available options:

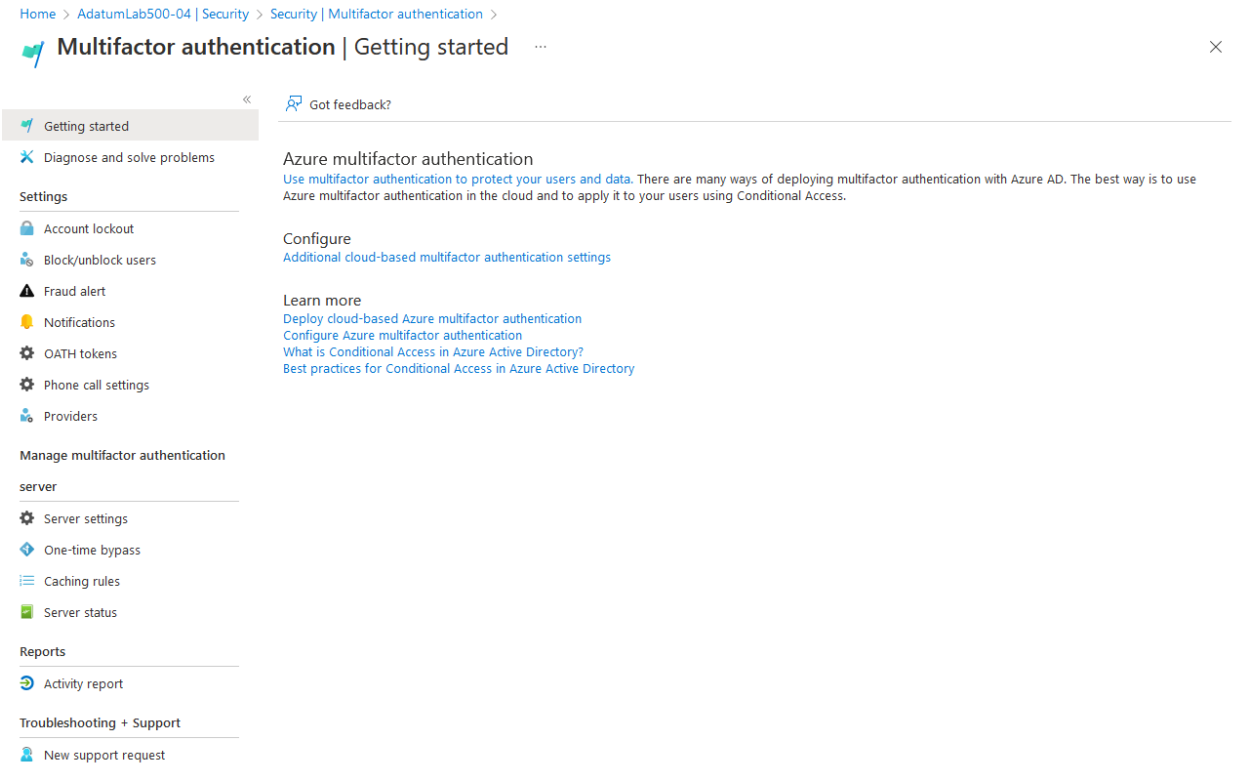
    a. Require selected users to provide contact methods again.

    b. Delete all existing app passwords generated by the selected users.

c. Restore multi-factor authentication on all remembered devices.

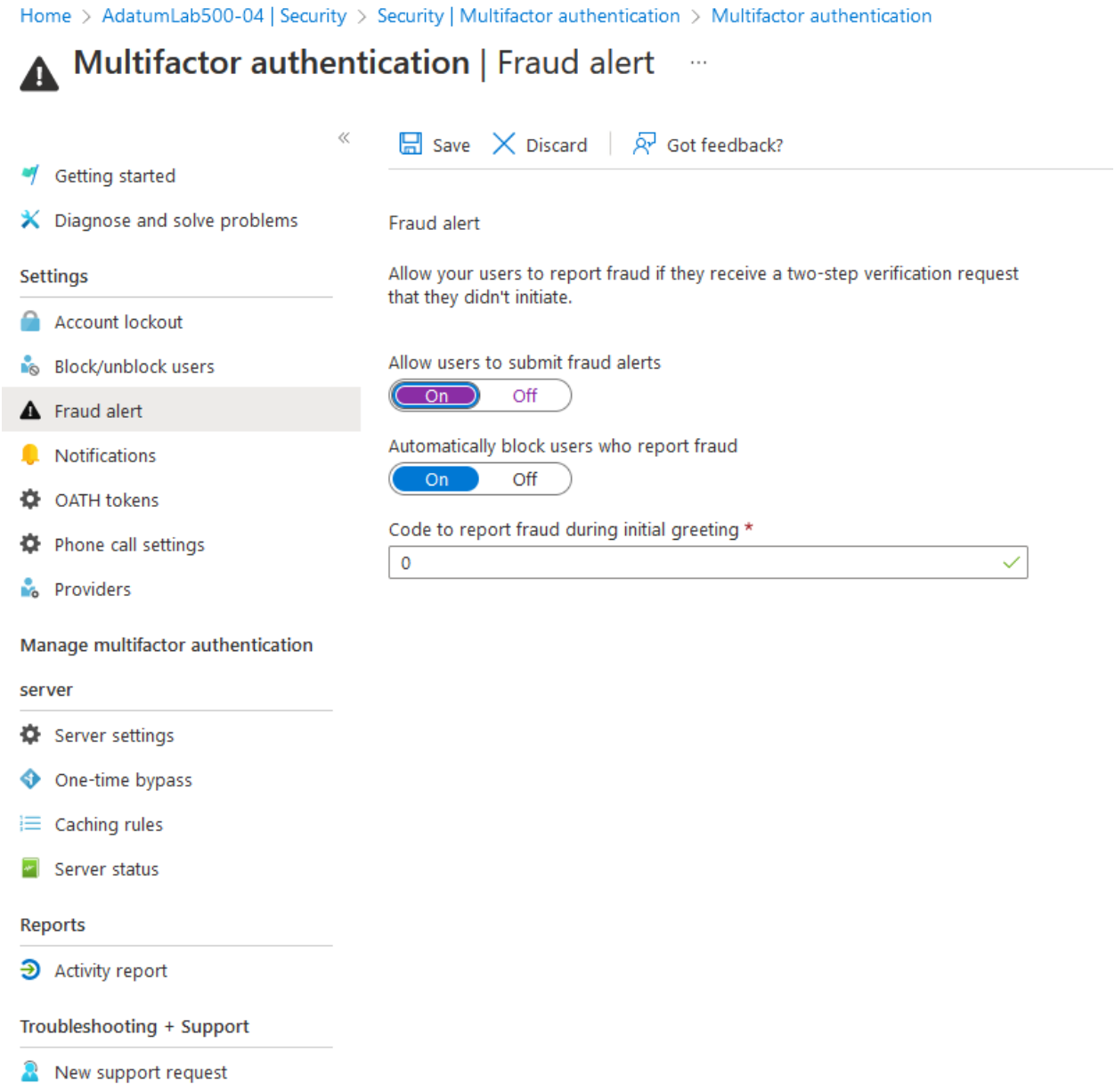


10. Click **Cancel** and switch back to the browser tab displaying the **Multi-Factor Authentication** | **Getting started** blade in the Azure Portal.



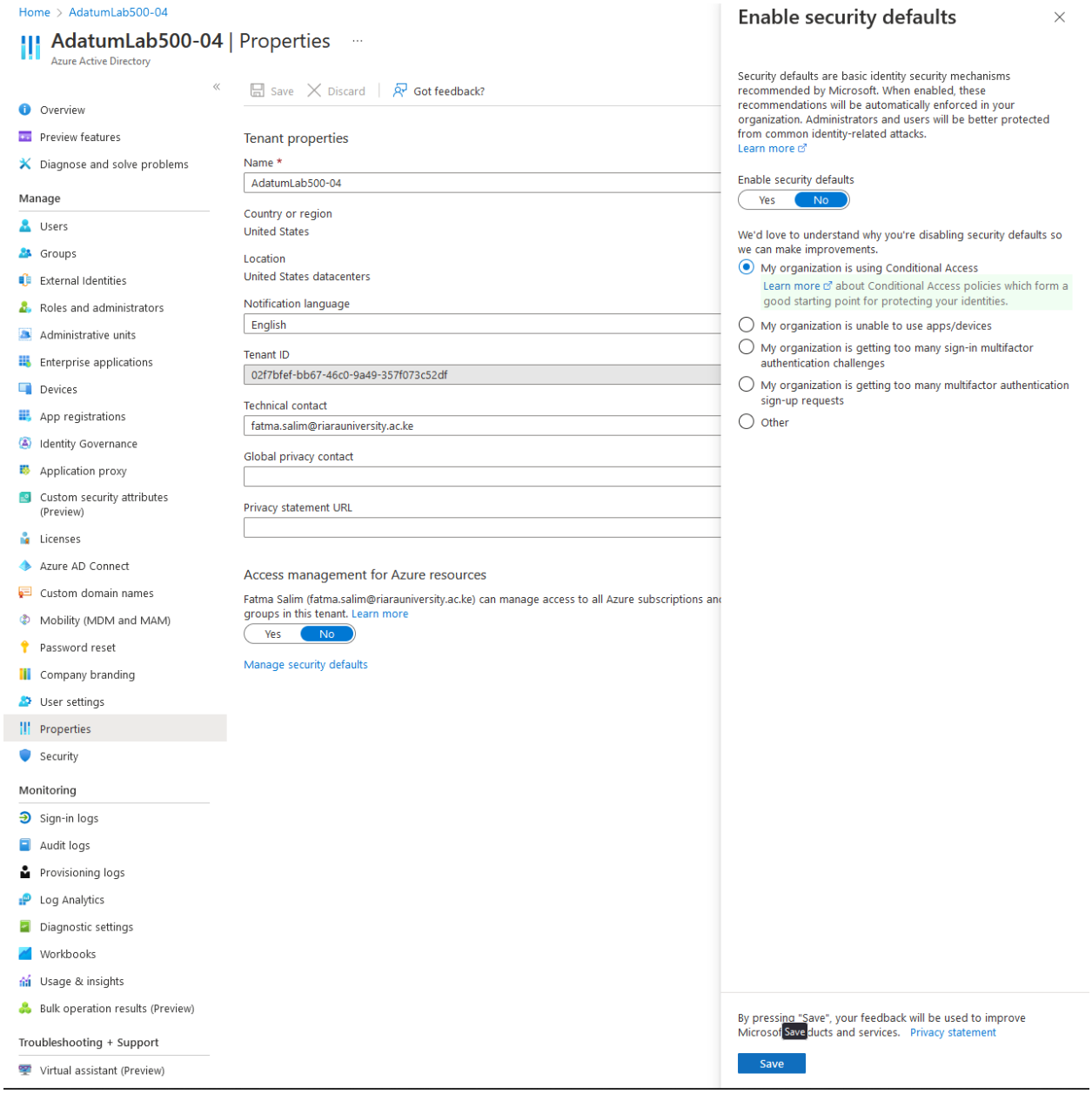
11. In the Settings section, click **Fraud alert**.

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



13. Click **Save**.

14. Navigate back to the **AdatumLab500-04** Azure Active Directory tenant blade, in the **Manage** section, click **Properties**, next click the **Manage Security defaults** link at the bottom of the blade, on the **Enable Security Defaults** blade, click **No**. Select **My Organization is using Conditional Access** as the reason and then click **Save**.



Objective 3:Implementing Azure AD Conditional Access Policies.

Task 1: Configuring a conditional access policy

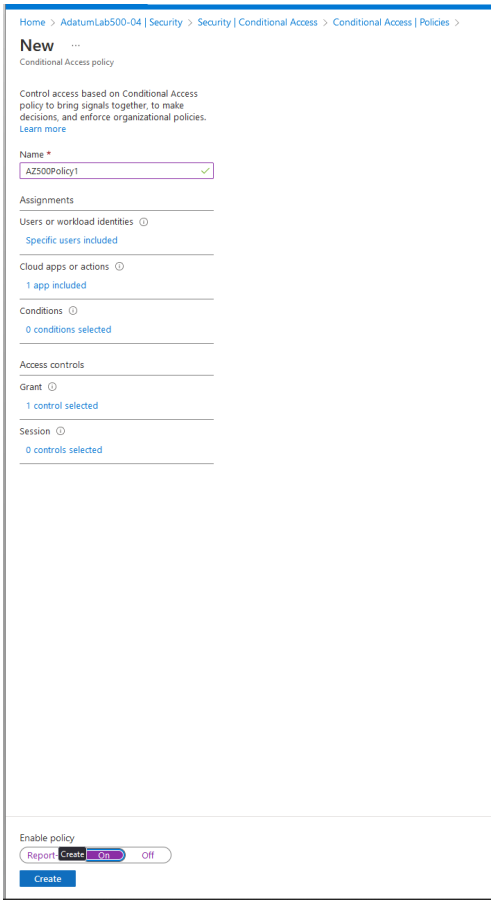
1. In the Azure portal, navigate back to the **AdatumLab500-04** Azure Active Directory tenant blade.

2. On the **AdatumLab500-04** blade, in the **Manage** section, click **Security**.

3. On the **Security | Getting started** blade, in the **Protect** section, click **Conditional Access**.

4. On the **Conditional Access | Policies** blade, click **+ New policy** select the **Create new policy** from the drop-down list.

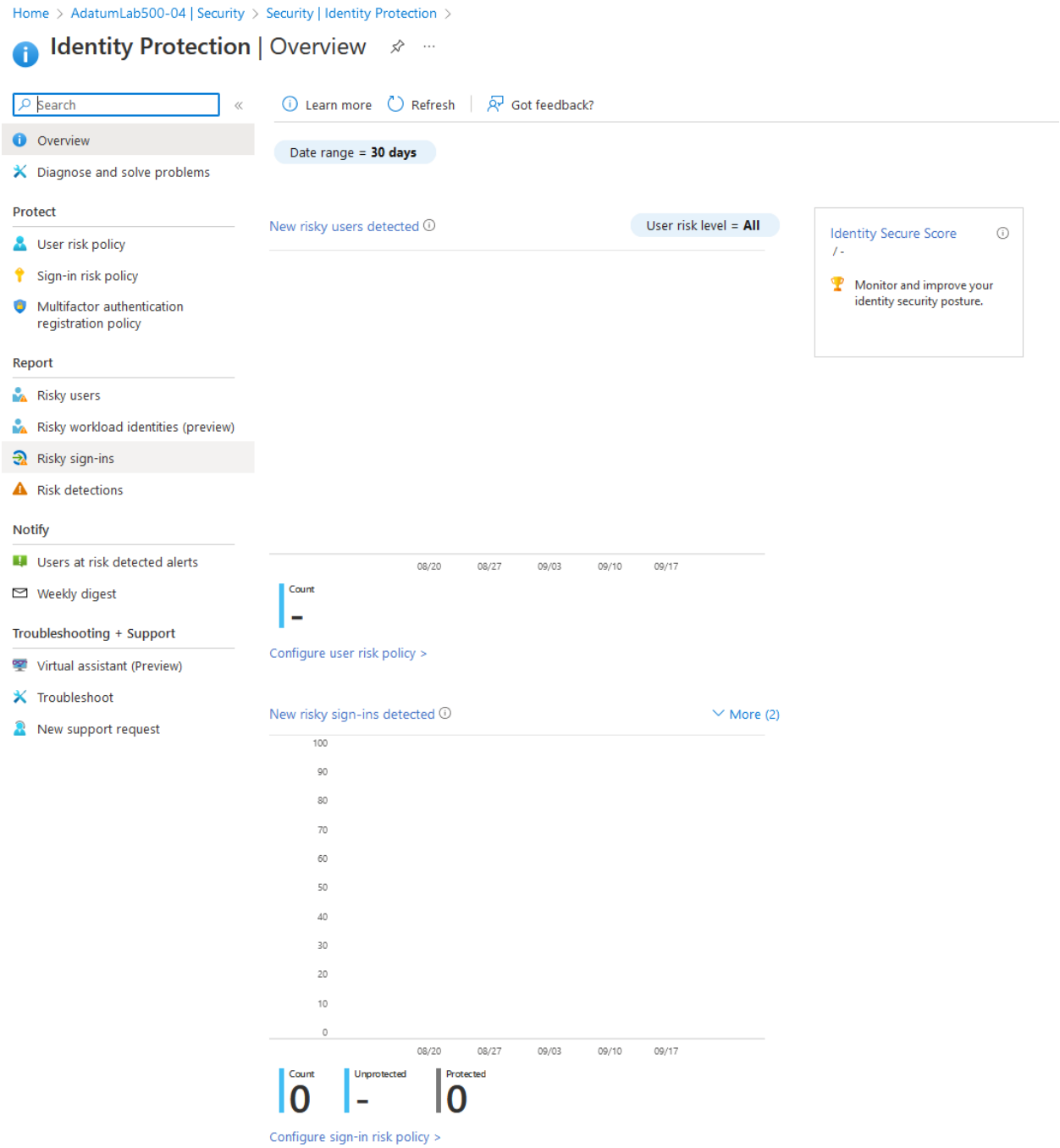
5. On the **New** blade, configure the following settings:
    - In the Name text box, type AZ500Policy1.
    - Click **Users or workload identities selected**. On the right side under the What does this policy apply to » Users and groups » Include » Enable **Select users and groups** » select the **Users and Groups** checkbox, on the **Select** blade, click **aaduser2**, and click **Select**.
    - Click **Cloud apps or actions**, click **Select apps**, on the **Select** blade, click **Microsoft Azure Management**, and click **Select.**
    - Click **Conditions**, click **Sign-in risk**, on the **Sign-in risk** blade, review the risk levels but do not make any changes and close the **Sign-in risk** blade.
    - Click **Device platforms**, review the device platforms that can be included and click **Done**.
    - Click **Locations** and review the location options without making any changes.
    - Click **Grant** in the **Access controls** section, on the **Grant** blade, select the **Require multi-factor authentication** checkbox and click **Select**
    - Set the **Enable policy** to **On**.



Objective 4: Implementing Azure AD Identity Protection

Task 1: Enable Azure AD Identity Protection

1. Sign in into the Azure Portal.
2. On the **AdatumLab500-04** blade, in the **Manage** section, click **Security**.
3. On the **Security | Getting started** blade, in the **Protect** section, click **Identity Protection**.
4. On the **Identity Protection | Overview** blade, review the **New risky users detected** and **New risky sign-ins detected** charts and other information about risky users.



Task 2: Configuring a user risk policy

1. On the **Identity Protection | Overview** blade, in the **Protect** section, click **user risk policy**

2. Configure the **User risk remediation policy** with the following settings:

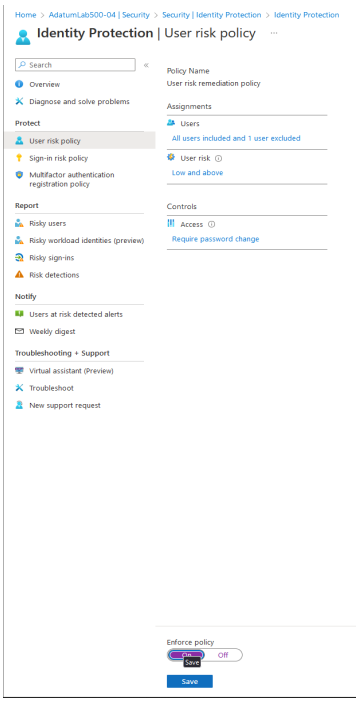
    - Click **Users**; on the **Include** tab of the **Users** blade, ensure that the **All users** option is selected.

    - On the **Users** blade, switch to the **Exclude** tab, click **Select excluded users**, select your user account, and then click **Select**.

    - Click **User risk**; on the **User risk** blade, select **Low and above**, and then click **Done**.

    - Click **Access**; on the **Access** blade, ensure that the **Allow access** option and the **Require password change** checkbox are selected and click **Done**.

    - Set **Enforce policy** to **On** and click **Save**.



Task 3: Configuring sign-in risk policy

1. On the **Identity Protection | User risk policy** blade, in the **Protect** section, click **Sign-in risk policy**

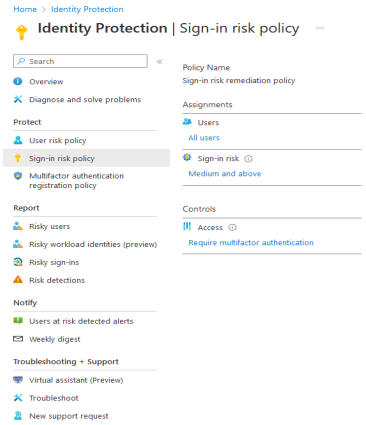
2. Configure the **Sign-in risk remediation policy** with the following settings:

    - Click **Users**; on the **Include** tab of the **Users** blade, ensure that the **All users** option is selected.

    - Click **Sign-in risk**; on the **Sign-in risk** blade, select **Medium and above**, and then click **Done**.

    - Click **Access**; on the **Access** blade, ensure that the **Allow access** option and the **Require multi-factor authentication** checkbox are selected and click **Done**.

    - Set **Enforce Policy** to **On** and click **Save**.



Clean up resources

1. In the Azure portal, navigate back to the **AdatumLab500-04** Azure Active Directory tenant blade.

2. On the **AdatumLab500-04** blade, in the **Manage** section, click **Security**.

3. On the **Security | Getting started** blade, in the **Protect** section, click **Identity Protection**.

4. On the **Identity Protection | Overview** blade, click **User risk policy**.

5. On the **Identity Protection | User risk policy** blade, set **Enforce policy** to **Off** and then click **Save**.

6. On the **Identity Protection | User risk policy** blade, click **Sign-in risk policy**

7. On the **Identity Protection | Sign-in risk policy** blade, set **Enforce policy** to **Off** and then click **Save**.

Use the following steps to stop the Azure VM you provisioned earlier in the lab.

1. In the Azure portal, set the **Directory + subscription** filter to the Azure AD tenant associated with the Azure subscription into which you deployed the **az500-04-vm1** Azure VM.

2. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Virtual machines** and press the **Enter** key.

3. On the **Virtual machines** blade, click the **az500-04-vm1** entry.

4. On the **az500-04-vm1** blade, click **Stop** and, when prompted to confirm, click **OK**