

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.

The screenshot shows the 'Custom deployment' page in the Microsoft Azure portal. The page has a blue header with the Microsoft Azure logo and a search bar. Below the header, there's a breadcrumb 'Home >' and the title 'Custom deployment' with a three-dot menu. Underneath the title is the subtitle 'Deploy from a custom template'. The main content area has a tabbed interface with 'Select a template' selected, followed by 'Basics' and 'Review + create'. Below the tabs, there's a paragraph explaining that Azure Resource Manager templates can be used to deploy resources in a single, coordinated operation. A link 'Learn more about template deployment' is provided. Below this, there's a link 'Build your own template in the editor' with a pencil icon. The 'Common templates' section lists five options: 'Create a Linux virtual machine', 'Create a Windows virtual machine', 'Create a web app', 'Create a SQL database', and 'Azure landing zone'. The 'Start with a quickstart template or template spec' section has two radio buttons: 'Quickstart template' (selected) and 'Template spec'. Below this, there's a dropdown menu for 'Quickstart template (disclaimer)'.

Microsoft Azure Search resources, services, and docs (G+/)

Home >

Custom deployment

Deploy from a custom template

Select a template Basics Review + create

Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Create or select a template below to get started. [Learn more about template deployment](#)

[Build your own template in the editor](#)

Common templates

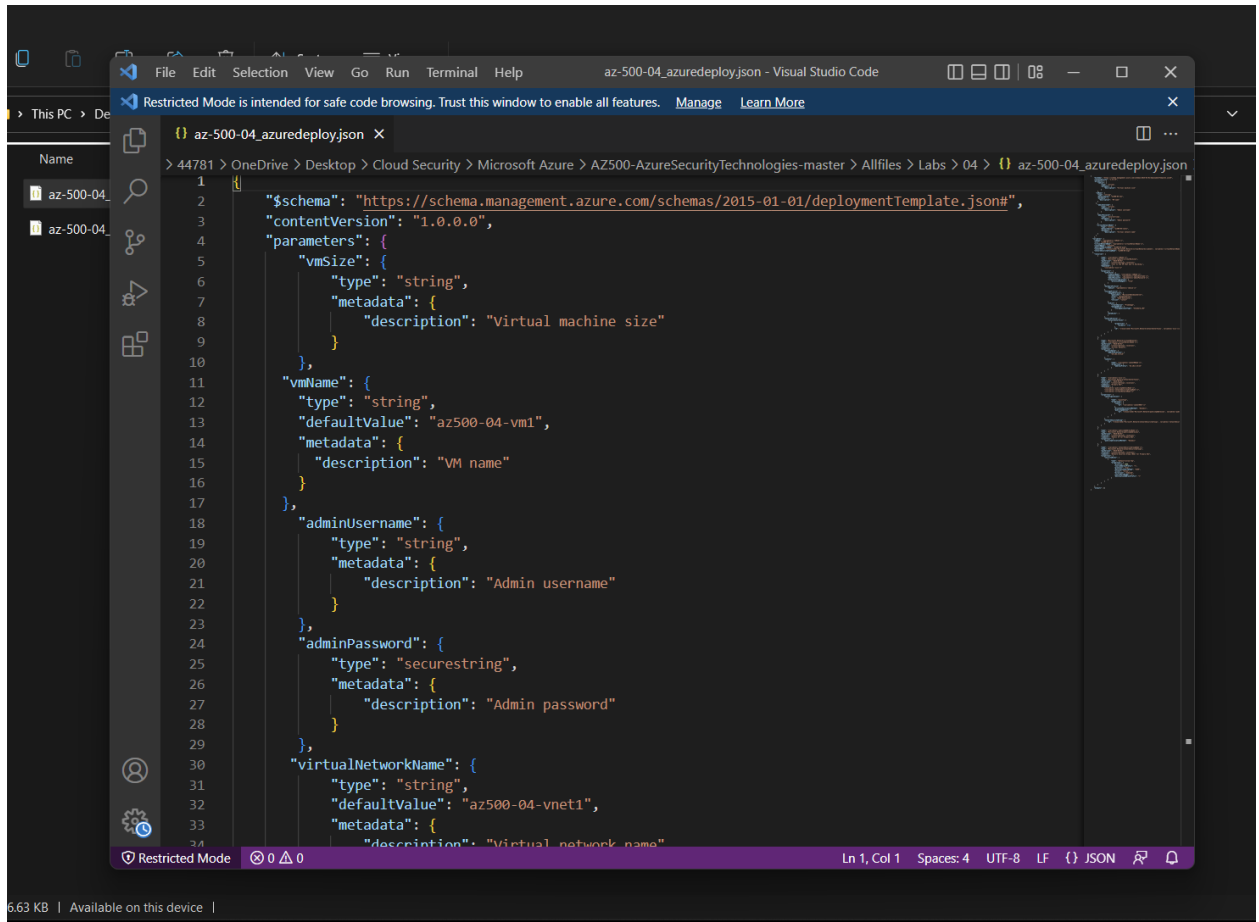
- Create a Linux virtual machine
- Create a Windows virtual machine
- Create a web app
- Create a SQL database
- Azure landing zone

Start with a quickstart template or template spec

Template source ☒ Quickstart template ☐ Template spec

Quickstart template (disclaimer)

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



```
1  {
2    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3    "contentVersion": "1.0.0.0",
4    "parameters": {
5      "vmSize": {
6        "type": "string",
7        "metadata": {
8          "description": "Virtual machine size"
9        }
10     },
11     "vmName": {
12       "type": "string",
13       "defaultValue": "az500-04-vm1",
14       "metadata": {
15         "description": "VM name"
16       }
17     },
18     "adminUsername": {
19       "type": "string",
20       "metadata": {
21         "description": "Admin username"
22       }
23     },
24     "adminPassword": {
25       "type": "securestring",
26       "metadata": {
27         "description": "Admin password"
28       }
29     },
30     "virtualNetworkName": {
31       "type": "string",
32       "defaultValue": "az500-04-vnet1",
33       "metadata": {
34         "description": "Virtual network name"
35       }
36     }
37   }
38 }
```

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

Edit parameters ...



⬆ Load file ⬇ Download

```
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.rd1234"
13     }
14   }
15 }
16
```

Save

Discard

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/#>

Home >


Custom deployment ...

Deploy from a custom template

Validation Passed

Select a template Basics **Review + create**

Summary

 Customized template
5 resources

Terms

[Azure Marketplace Terms](#) | [Azure Marketplace](#)

By clicking "Create," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

Deploying this template will create one or more Azure resources or Marketplace offerings. You acknowledge that you are responsible for reviewing the applicable pricing and legal terms associated with all resources and offerings deployed as part of this template. Prices and associated legal terms for any Marketplace offerings can be found in the [Azure Marketplace](#); both are subject to change at any time prior to deployment.

Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately.

If any Microsoft products are included in a Marketplace offering (e.g. Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Basics

Subscription	Azure for Students
Resource group	AZ500LAB04
Region	East US
Vm Size	Standard_D2s_v3
Vm Name	az500-04-vm1
Admin Username	Student
Admin Password	*****
Virtual Network Name	az500-04-vnet1

Create

< Previous

Next

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

Task 1: Creating a new Azure AD Tenant

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:

Create a tenant

Azure Active Directory



[* Basics](#) [* Configuration](#) [Review + create](#)

Directory details

Configure your new directory

Organization name *	<input type="text" value="AdatumLab500-04"/>	✓
Initial domain name *	<input type="text" value="mutada005"/>	✓
	mutada005.onmicrosoft.com	
Country/Region	<input type="text" value="United States"/>	▼
	✓ Datacenter location - United States	
	Datacenter location is based on the country/region selected above.	

Create a tenant

Azure Active Directory

✓ Validation passed.

* Basics * Configuration Review + create

Summary

Basics

Tenant type Azure Active Directory

Configuration

Organization name AdatumLab500-04

Initial domain name mutada005.onmicrosoft.com

Country/Region United States

Datacenter location United States

Create

Create

< Previous

Next >

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.

Portal settings | Directories + subscriptions

Search menu

Directories + subscriptions

Appearance + startup views

Language + region

My information

Signing out + notifications

All services and resources across the Azure portal will inherit the selection from basic filtering. Your selection will also be saved and reloaded the next time you sign in or reload the Azure portal.

Default subscription filter ⓘ Advanced filters ⓘ ☐

Azure for Students - Don't see a subscription? Switch to another directory.

Directories ⓘ

Switching directories will reload the portal. The directory you choose will impact the subscription, resource group, and region filters that are available in the portal. [Learn more about directories.](#) ⓘ

Current directory ⓘ : Default Directory (fatmasalimriaraunivers... **Startup directory** ⓘ : Last visited ([change](#))

Favorites All Directories

Search

Directory name ↑↓		Domain ↑↓	Directory ID ↑↓
★ Default Directory	✓ Current	fatmasalimriarauniversityac.onmicros...	4fcb0a62-1b50-44be-9166-619acd27...
★ AdatumLab500-04	Switch	mutada005.onmicrosoft.com	02f7bfef-bb67-46c0-9a49-357f073c5...

Switch

- 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**.
- 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**.

Home > Licenses

Licenses | All products ...
AdatumLab500-04 - Azure Active Directory

« + Try / Buy + Assign Bills Columns Got it

Overview
Diagnose and solve problems

Manage

- Licensed features
- All products
- Self-service sign up products

Activity

- Audit logs

Troubleshooting + Support

- New support request

Activate

Browse available plans and features

If you would like to purchase a subscription directly from Microsoft, please see the [Purchase services catalog](#).

ENTERPRISE MOBILITY + SECURITY E5

Enterprise Mobility + Security E5 is the comprehensive cloud solution to address your consumerization of IT, BYOD, and SaaS challenges. In addition to Azure Active Directory Premium P2 the suite includes Microsoft Intune and Azure Rights Management.

Free trial

AZURE AD PREMIUM P2

With Azure Active Directory Premium P2 you can gain access to advanced security features, richer reports and rule based assignments to applications. Your end users will benefit from self-service capabilities and customized branding.

Free trial

Azure Active Directory Premium P2 enhances your directory with additional features that include multifactor authentication, policy driven management and end-user self-service. [Learn more about features](#)

The trial includes 100 licenses and will be active for 30 days beginning on the activation date. If you wish to upgrade to a paid version, you will need to purchase Azure Active Directory Premium P2. [Learn more about pricing](#)

Azure Active Directory Premium P2 is licensed separately from Azure Services. By confirming this activation you agree to the [Microsoft Online Subscription Agreement](#) and the [Privacy Statement](#).

Activate

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):

Identity

User name *

aaduser2



@

mutada005.onmicrosoft.c...



The domain name I need isn't shown here

Name

aaduser2



First name

Last name

Password☒ Auto-generate password

☐ Let me create the password

Initial password

Roya9202

☒ Show Password

Groups and roles

Groups

0 groups selected

Roles

User

Settings

Block sign in

Yes

No

Usage location

United States



Job info

Job title

Department

Company name

Manager


No manager selected

Create

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**.

Identity

User name * ⓘ ✓ @ ✓ 
[The domain name I need isn't shown here](#)


Name * ⓘ ✓

First name

Last name

Password

☒ Auto-generate password
☐ Let me create the password

Initial password 

☒ Show Password

Groups and roles

Groups [0 groups selected](#)

Roles [User](#)

Settings

Block sign in ☐ Yes ☒ No

Usage location ✓

Job info

Job title

Department

Company name

Manager [No manager selected](#)

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 + assign**, 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
- ☒ Text message to phone
- ☒ Notification through mobile app
- ☒ 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

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](#)

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

Microsoft fatma.salim_riarauniversity.ac.ke#EXT#@mutada005.onmicrosoft.com | ?

multi-factor authentication

users service settings

Before you begin, take a look at the [multi-factor auth deployment guide](#).

View: Sign-in allowed users Multi-Factor Auth status: Any bulk update

<input type="checkbox"/>	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
<input checked="" type="checkbox"/>	aaduser1	aaduser1@mutada005.onmicrosoft.com	Enabled
<input type="checkbox"/>	aaduser2	aaduser2@mutada005.onmicrosoft.com	Disabled
<input type="checkbox"/>	aaduser3	aaduser3@mutada005.onmicrosoft.com	Disabled
<input type="checkbox"/>	Fatma Salim	fatma.salim@riarauniversity.ac.ke	Disabled

aaduser1

aaduser1@mutada005.onmicrosoft.com

quick steps

[Disable](#)

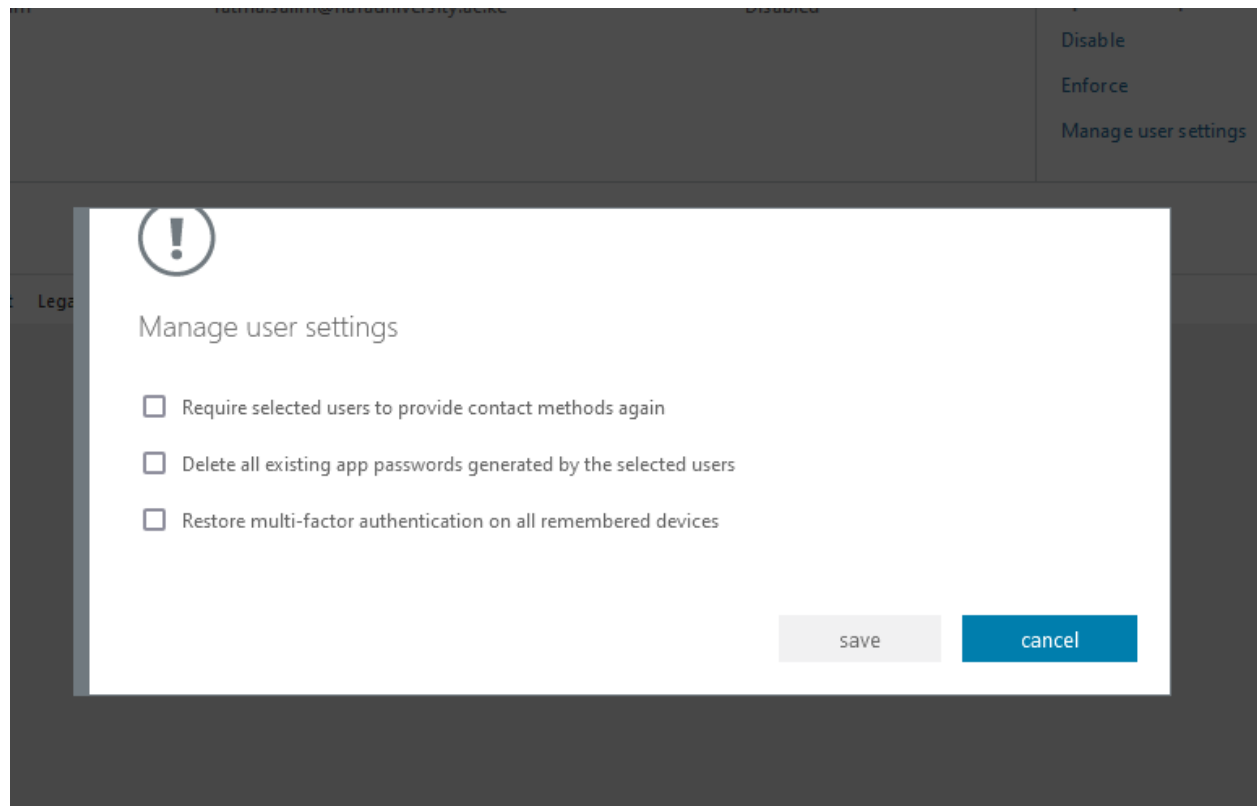
[Enforce](#)

[Manage user settings](#)

©2022 Microsoft [Legal](#) | [Privacy](#)

- Notice the **Multi-Factor Auth status** column for **aaduser1** is now **Enabled**.
- Click **aaduser1** and notice that, at this point, you also have the **Enforce** option.
- With the **aaduser1** entry selected, click **Manage user settings** and review the available options:
 - Require selected users to provide contact methods again.
 - 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.

Multifactor authentication | Getting started ...



«

Got feedback?

Getting started

Diagnose and solve problems

Settings

Account logout

Block/unblock users

Fraud alert

Notifications

OATH tokens

Phone call settings

Providers

Manage multifactor authentication

server

Server settings

One-time bypass

Caching rules

Server status

Reports

Activity report

Troubleshooting + Support

New support request

Azure multifactor authentication

Use [multifactor authentication to protect your users and data](#). There are many ways of deploying multifactor authentication with Azure AD. The best way is to use Azure multifactor authentication in the cloud and to apply it to your users using Conditional Access.

Configure

[Additional cloud-based multifactor authentication settings](#)

Learn more

[Deploy cloud-based Azure multifactor authentication](#)

[Configure Azure multifactor authentication](#)

[What is Conditional Access in Azure Active Directory?](#)


[Best practices for Conditional Access in Azure Active Directory](#)


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

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


Multifactor authentication | Fraud alert ...

«

 Save

 Discard

|

 Got feedback?

Getting started

Diagnose and solve problems

Settings

Account lockout

Block/unblock users

Fraud alert

Notifications

OATH tokens

Phone call settings

Providers

Manage multifactor authentication

server

Server settings

One-time bypass

Caching rules

Server status

Reports

Activity report

Troubleshooting + Support

New support request

Fraud alert

Allow your users to report fraud if they receive a two-step verification request that they didn't initiate.

Allow users to submit fraud alerts

On

Off

Automatically block users who report fraud

On

Off

Code to report fraud during initial greeting *

0

✓

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**.

Home > AdatumLab500-04

AdatumLab500-04 | Properties

Azure Active Directory

« Save Discard Got feedback?

Overview

Preview features

Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Custom security attributes (Preview)
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties**
- Security

Monitoring

- Sign-in logs
- Audit logs
- Provisioning logs
- Log Analytics
- Diagnostic settings
- Workbooks
- Usage & insights
- Bulk operation results (Preview)

Troubleshooting + Support

- Virtual assistant (Preview)

Tenant properties

Name *

AdatumLab500-04

Country or region

United States

Location

United States datacenters

Notification language

English

Tenant ID

02f7bfef-bb67-46c0-9a49-357f073c52df

Technical contact

fatma.salim@riarauniversity.ac.ke

Global privacy contact

Privacy statement URL

Access management for Azure resources

Fatma Salim (fatma.salim@riarauniversity.ac.ke) can manage access to all Azure subscriptions and groups in this tenant. [Learn more](#)

Yes No

[Manage security defaults](#)

Enable security defaults

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity-related attacks. [Learn more](#)

Enable security defaults

Yes No

We'd love to understand why you're disabling security defaults so we can make improvements.

☒ My organization is using Conditional Access
[Learn more](#) about Conditional Access policies which form a good starting point for protecting your identities.

☐ My organization is unable to use apps/devices

☐ My organization is getting too many sign-in multifactor authentication challenges

☐ My organization is getting too many multifactor authentication sign-up requests

☐ Other

By pressing "Save", your feedback will be used to improve Microsoft products and services. [Privacy statement](#)

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**.

Home > AdatumLab500-04 | Security > Security | Conditional Access > Conditional Access | Policies >

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 *

AZ500Policy1 ✓

Assignments

Users or workload identities ⓘ

[Specific users included](#)

Cloud apps or actions ⓘ

[1 app included](#)

Conditions ⓘ

[0 conditions selected](#)

Access controls

Grant ⓘ

[1 control selected](#)

Session ⓘ

[0 controls selected](#)

Enable policy

[Report](#) [Create](#) [On](#) [Off](#)

[Create](#)

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.

Identity Protection | Overview

Search

Learn more Refresh Got feedback?

Overview

Diagnose and solve problems

Date range = 30 days

Protect

User risk policy

Sign-in risk policy

Multifactor authentication registration policy

New risky users detected

User risk level = All

Identity Secure Score
/-

Monitor and improve your identity security posture.

Report

Risky users

Risky workload identities (preview)

Risky sign-ins

Risk detections

Notify

Users at risk detected alerts

Weekly digest

Troubleshooting + Support

Virtual assistant (Preview)

Troubleshoot

New support request

Count



Configure user risk policy >

New risky sign-ins detected

More (2)



Count Unprotected Protected

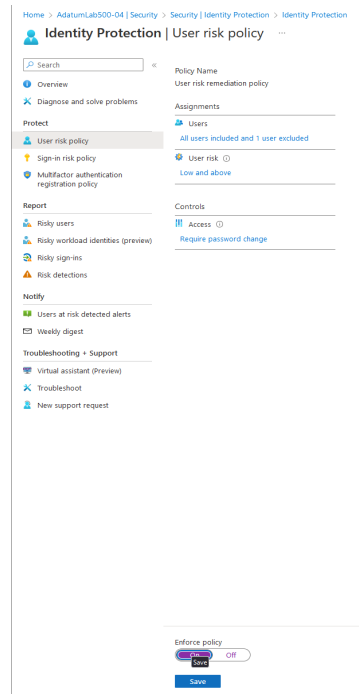
Configure sign-in risk policy >

Task 2: Configuring a user risk policy

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

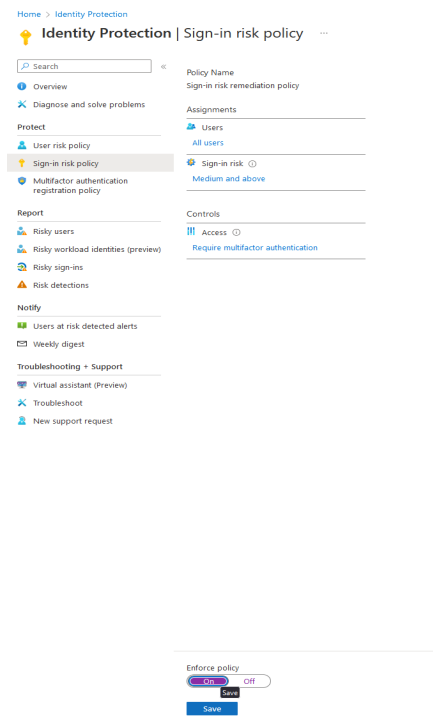
2. Configure the **User risk remediation policy** with the following settings:

- 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**.

