MFA, Conditional Access and AAD Identity Protection

Lab scenario

You have been asked to create a proof of concept of features that enhance Azure Active Directory (Azure AD) authentication. Specifically, you want to evaluate:

* Azure AD multi-factor authentication
* Azure AD conditional access
* Azure AD Identity Protection

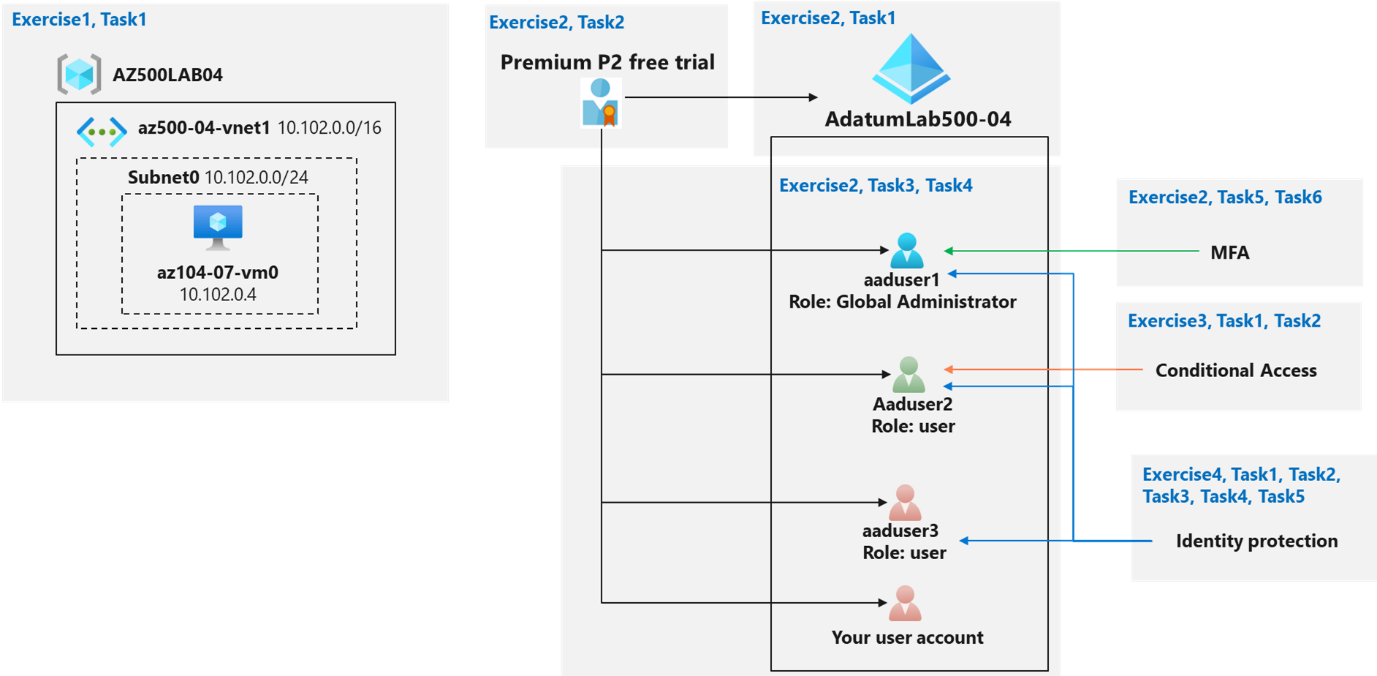
For all the resources in this lab, we are using the **East US** region. Verify with your instructor this is the region to use for class.

Lab Objectives

In this lab, you will complete the following exercises:

* Exercise 1: Deploy an Azure VM by using an Azure Resource Manager template
* Exercise 2: Implement Azure MFA
* Exercise 3: Implement Azure AD Conditional Access Policies
* Exercise 4: Implement Azure AD Identity Protection

MFA - Conditional Access - Identity Protection diagram

[](https://user-images.githubusercontent.com/91347931/157518628-8b4a9efe-0086-4ec0-825e-3d062748fa63.png)

Instructions

Lab files:

* **Download file az-500-04\_azuredeploy.json and az-500-04\_azuredeploy.parameters.json from here** [**https://github.com/nivedv/SC-300/blob/main/AllFiles/az-500-04\_labfiles.zip**](https://github.com/nivedv/SC-300/blob/main/AllFiles/az-500-04_labfiles.zip) **. Unzip both the files in the same folder on your laptop/desktop and follow the instruction later in the lab.**

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

Estimated timing: 10 minutes

In this exercise, you will complete the following tasks:

* Task 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.

1. Sign-in to the Azure portal **https://portal.azure.com/**.

**Note**: Sign in to the Azure portal using an account that has the Owner or Contributor role in the Azure subscription you are using for this lab and the Global Administrator role in the Azure AD tenant associated with that subscription.

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Deploy a custom template**.

**Note**: You can also select **Template Deployment (deploy using custom templates)** from the **Marketplace** list.

1. On the **Custom deployment** blade, click the **Build your own template in the editor** option.
2. On the **Edit template** blade, click **Load file**, locate the **\Allfiles\Labs\04\az-500-04\_azuredeploy.json** file and click **Open**.

**Note**: Review the content of the template and note that it deploys an Azure VM hosting Windows Server 2019 Datacenter.

1. On the **Edit template** blade, click **Save**.
2. Back on the **Custom deployment** blade, click **Edit parameters**.
3. On the **Edit parameters** blade, click **Load file**, locate the **\Allfiles\Labs\04\az-500-04\_azuredeploy.parameters.json** file and click **Open**.

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

1. On the **Edit parameters** blade, click **Save**.
2. On the **Custom deployment** blade, ensure that the following settings are configured (leave any others with their default values):

**Note**: You will need to create a unique password that will be used for creating VMs (virtual machines) for the rest of the course. The password must be at least 12 characters long and meet the defined complexity requirements (Password must have 3 of the following: 1 lower case character, 1 upper case character, 1 number, and 1 special character). [VM password requirements](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/faq#what-are-the-password-requirements-when-creating-a-vm-). Please make a note of the password.

| Setting | Value |
| --- | --- |
| Subscription | the name of the Azure subscription you will be using in this lab |
| Resource group | click **Create new** and type the name **AZ500LAB04** |
| Location | **(US) East US** |
| Vm Size | **Standard\_D2s\_v3** |
| Vm Name | **az500-04-vm1** |
| Admin Username | **Student** |
| Admin Password | **Please create your own password and record it for future reference. You will be prompted for this password for the required lab access.** |
| Virtual Network Name | **az500-04-vnet1** |

CodeCopy

>**\*\*Note\*\***: To identify Azure regions where you can provision Azure VMs, refer to [\*\*https://azure.microsoft.com/en-us/regions/offers/\*\*](https://azure.microsoft.com/en-us/regions/offers/)

1. Click **Review + create**, and then click **Create**.

**Note**: Do not wait for the deployment to complete but proceed to the next exercise. You will use the virtual machine included in this deployment in the last exercise of this lab.

Result: You have initiated a template deployment of an Azure VM **az500-04-vm1** that you will use in the last exercise of this lab.

Exercise 2: Implement Azure MFA

Estimated timing: 30 minutes

In this exercise, you will complete the following tasks

* 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: Create a new Azure AD tenant

In this task, you will create a new Azure AD tenant.

1. 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.
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:

| Setting | Value |
| --- | --- |
| Organization name | **AdatumLab500-04** |
| Initial domain name | a unique name consisting of a combination of letters and digits |
| Country or region | **United States** |

1. **Note**: Record the initial domain name. You will need it later in this lab.
2. Click **Review + Create** and then click **Create**.
3. Add Captcha code on **Help us prove you’re not a robot** blade and then click on **Submit** button.

**Note**: Wait for the new tenant to be created. Use the **Notification** icon to monitor the deployment status.

Task 2: Activate Azure AD Premium P2 trial

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

**Note**: You may need to refresh the browser window if the **AdatumLab500-04** entry does not appear in the **Directory + subscription** filter list.

1. 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**.
2. On the **Licenses | Overview** blade, in the **Manage** section, click **All products** and then click **+ Try / Buy**.
3. On the **Activate** blade, in the Azure AD Premium P2 section, click **Free Trial** and then click **Activate**.

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.

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**:

| Setting | Value |
| --- | --- |
| User name | **aaduser1** |
| Name | **aaduser1** |
| Password | ensure that the option **Auto-generate password** is selected and click **Show Password** |
| Groups | **0 groups selected** |
| Roles | click **User**, then click **Global administrator**, and click **Select** |
| Usage Location | **United States** |

1. **Note**: Record the full user name. You can copy its value by clicking the **Copy to clipboard** button on the right hand side of the drop-down list displaying the domain name.
2. **Note**: Record the user’s password. You will need this later in this lab.
3. Back on the **Users | All users** blade, click **+ New User**.
4. 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):

| Setting | Value |
| --- | --- |
| User name | **aaduser2** |
| Name | **aaduser2** |
| Password | ensure that the option **Auto-generate password** is selected and click **Show Password** |
| Groups | **0 groups selected** |
| Roles | **User** |
| Usage Location | **United States** |

1. **Note**: Record the full user name and the password.
2. Back on the **Users | All users** blade, click **+ New User**.
3. Click **New User**,complete the new user configuration settings, and then click **Create**.

| Setting | Value |
| --- | --- |
| User name | **aaduser3** |
| Name | **aaduser3** |
| Password | ensure that the option **Auto-generate password** is selected and click **Show Password** |
| Groups | **0 groups selected** |
| Roles | **User** |
| Usage Location | **United States** |

1. **Note**: Record the full user name and the password.
2. **Note**: 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

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

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.

**Note**: 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.

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

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

1. On the **AdatumLab500-04** Azure Active Directory tenant blade, in the **Manage** section, click **Security**.
2. On the **Security | Getting started** blade, in the **Manage** section, click **MFA**.
3. On the **Multi-Factor Authentication | Getting started** blade, click the **Additional cloud-based MFA settings** link.

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

1. 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**.
2. Switch to the **users** tab, click **aaduser1** entry, click the **Enable** link, and, when prompted, click **enable multi-factor auth**.
3. Notice the **Multi-Factor Auth status** column for **aaduser1** is now **Enabled**.
4. Click **aaduser1** and notice that, at this point, you also have the **Enforce** option.

**Note**: Changing the user status from Enabled to Enforced impacts only legacy Azure AD integrated apps which do not support Azure MFA and, once the status changes to Enforced, require the use of app passwords.

1. 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.
   * Restore multi-factor authentication on all remembered devices.
2. Click **Cancel** and switch back to the browser tab displaying the **Multi-Factor Authentication | Getting started** blade in the Azure portal.
3. In the **Settings** section, click **Fraud alert**.
4. On the **Multi-Factor Authentication | Fraud alert** blade, configure the following settings:

| Setting | Value |
| --- | --- |
| Allow users to submit fraud alerts | **On** |
| Automatically block users who report fraud | **On** |
| Code to report fraud during initial greeting | **0** |

1. Click **Save**

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

1. 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 Conditonal Access** as the reason and and then click **Save**.

**Note**: Ensure that you are signed-in to the **AdatumLab500-04** Azure AD tenant. You can use the **Directory + subscription** filter to switch between Azure AD tenants. Ensure you are signed in as a user with the Global Administrator role in the Azure AD tenant.

Task 6: Validate MFA configuration

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

1. Open an InPrivate browser window.
2. Navigate to the Azure portal and sign in using the **aaduser1** user account.

**Note**: To sign in you will need to provide a fully qualified name of the **aaduser1** user account, including the Azure AD tenant DNS domain name, which you recorded earlier in this lab. This user name is in the format aaduser1@<your\_tenant\_name>.onmicrosoft.com, where <your\_tenant\_name> is the placeholder representing your unique Azure AD tenant name.

1. When prompted, in the **More information required** dialog box, click **Next**.

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

1. On the **Keep your account secure** page, select the **I want to set up a different method** link, in the **Which method would you like to use?** drop-down list, select **Phone**, and select **Confirm**.
2. On the **Keep your account secure** page, 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**.
3. On the **Keep your account secure** page, type the code you received in the text message on your mobile phone, and click **Next**.
4. On the **Keep your account secure** page, ensure that the verification was successful and click **Next**.
5. On the **Keep your account secure** page, click **I want to use a different method**, select **Email** from the drop down list, click **Confirm**, provide the email address you intend to use, and click **Next**. Once you receive the corresponding email, identify the code in the email body, provide it, and then click **Done**.
6. When prompted, change your password. Make sure to record the new password.
7. Verify that you successfully signed in to the Azure portal.
8. Sign out as **aaduser1** and close the InPrivate browser window.

Result: 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

Estimated timing: 15 minutes

In this exercise, you will complete the following tasks

* Task 1: Configure a conditional access policy.
* Task 2: Test the conditional access policy.

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.

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**.

**Note**: Review the warning that this policy impacts access to the Azure Portal.

* + 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**.

1. On the **New** blade, click **Create**.

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

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.

1. Open an InPrivate Microsoft Edge window.
2. In the new browser window, navigate to the Azure portal and sign in with the **aaduser2** user account.
3. When prompted, in the **More information required** dialog box, click **Next**.

**Note**: The browser seesion will be redirected to the **Keep your account secure** page.

1. On the **Keep your account secure** page, select the **I want to set up a different method** link, in the **Which method would you like to use?** drop-down list, select **Phone**, and select **Confirm**.
2. On the **Keep your account secure** page, 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**.
3. On the **Keep your account secure** page, type the code you received in the text message on your mobile phone, and click **Next**.
4. On the **Keep your account secure** page, ensure that the verification was successful and click **Next**.
5. On the **Keep your account secure** page, click **Done**.
6. When prompted, change your password. Make sure to record the new password.
7. Verify that you successfully signed in to the Azure portal.
8. Sign out as **aaduser2** and close the InPrivate browser window.

**Note**: You have now verified that the newly created conditional access policy enforces MFA when aaduser2 signs into the Azure portal.

1. Back in the browser window displaying 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 the ellipsis next to **AZ500Policy1**, click **Delete**, and, when prompted to confirm, click **Yes**.

**Note**: Result: In this exercise you implement a conditional access policy to require MFA when a user signs into the Azure portal.

Result: You have configured and tested Azure AD conditional access.

Exercise 4: Implement Azure AD Identity Protection

Estimated timing: 30 minutes

In this exercise, you will complete the following tasks

* Task 1: View Azure AD Identity Protection options in the Azure portal
* Task 2: Configure a user risk policy
* Task 3: Configure a sign-in risk policy
* Task 4: Simulate risk events against the Azure AD Identity Protection policies
* Task 5: Review the Azure AD Identity Protection reports

Task 1: Enable Azure AD Identity Protection

In this task, you will view the Azure AD Identity Protection options in the Azure portal.

1. If needed, sign-in to the Azure portal **https://portal.azure.com/**.

**Note**: Ensure that you are signed-in to the **AdatumLab500-04** Azure AD tenant. You can use the **Directory + subscription** filter to switch between Azure AD tenants. Ensure you are signed in as a user with the Global Administrator role in the Azure AD tenant.

1. On the **AdatumLab500-04** blade, in the **Manage** section, click **Security**.
2. On the **Security | Getting started** blade, in the **Protect** section, click **Identity Protection**.
3. 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: Configure a user risk policy

In this task, you will create 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: Configure sign-in risk policy

In this task, you will configure a 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**.

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

Before you start this task, ensure that the template deployment you started in Exercise 1 has completed. The deployment includes an Azure VM named **az500-04-vm1**.

1. In the Azure portal, set the **Directory + subscription** filter to the 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 **Connect** and, in the drop down menu, click **RDP**.
5. Click **Download RDP File** and use it to connect to the **az500-04-vm1** Azure VM via Remote Desktop. When prompted to authenticate, provide the following credntials:

| Setting | Value |
| --- | --- |
| User name | **Student** |
| Password | **Please use your personal password created in Lab 04 > Exercise 1 > Task 1 > Step 9.** |

1. **Note**: Wait for the Remote Desktop session and **Server Manager** to load.
2. **Note**: The following steps are performed in the Remote Desktop session to the **az500-04-vm1** Azure VM.
3. In **Server Manager**, click **Local Server** and then click **IE Enhanced Security Configuration**.
4. In the **Internet Explorer Enhanced Security Configuration** dialog box, set both options to **Off** and click **OK**.
5. Start **Internet Explorer**, click the cog wheel icon in the toolbar, in the drop-down menu, click **Safety** and then click **InPrivate Browsing**.
6. In the InPrivate Internet Explorer window, navigate to the ToR Browser Project at **https://www.torproject.org/projects/torbrowser.html.en**.
7. Download and install the Windows version of the ToR Browser with the default settings.
8. Once the installation completes, start the ToR Browser, use the **Connect** option on the initial page, and browse to the Application Access Panel at **https://myapps.microsoft.com**.
9. When prompted, attempt to sign in with the **aaduser3** account.

**Note**: You will be presented with the message **Your sign-in was blocked**. This is expected, since this account is not configured with multi-factor authentication, which is required due to increased sign-in risk associated with the use of ToR Browser.

1. Use the **Sign out and sign in with a different account option** or select the back arrow to sign in as **aaduser1** account you created and configured for multi-factor authentication earlier in this lab.

**Note**: This time, you will be presented with the **Suspicious activity detected** message. Again, this is expected, since this account is configured with multi-factor authentiation. Considering the increased sign-in risk associated with the use of ToR Browser, you will have to use multi-factor authentication.

1. Use the **Verify** option and specify whether you want to verify your identity via text or a call.
2. Complete the verification and ensure that you successfully signed in to the Application Access Panel.
3. Close your RDP session.

**Note**: At this point, you attempted two different sign ins. Next, you will review the Azure Identity Protection reports.

Task 5: Review the Azure AD Identity Protection reports

In this task, you will review the Azure AD Identity Protection reports generated from the ToR browser logins.

1. Back in the Azure portal, use the **Directory + subscription** filter to switch to the **AdatumLab500-04** Azure Active Directory tenant.
2. On the **AdatumLab500-04** blade, in the **Manage** section, click **Security**.
3. On the **Security | Getting started** blade, in the **Report** section, click **Risky users**.
4. Review the report and identify any entries referencing the **aaduser3** user account.
5. On the **Security | Getting started** blade, in the **Reports** section, click **Risky sign-ins**.
6. Review the report and identify any entries corresponding to the sign-in with the **aaduser3** user account.
7. Under **Reports** click **Risk detections**.
8. Review the report and identify any entries representing the sign-in from anonymous IP address generated by the ToR browser.

**Note**: It may take 10-15 minutes to risks to show up in reports.

**Result**: 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.

**Clean up resources**

We need to remove identity protection resources that you no longer use.

Use the following steps to disable the identity protection policies in the **AdatumLab500-04** Azure AD tenant.

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 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**