Module 01 : Manage Identity and Access

3 Hr 55 Min Remaining

**Lab 01: Role-Based Access Control**

**Student lab manual**

**Lab scenario**

You have been asked to create a proof of concept showing how Azure users and groups are created. Also, how role-based access control is used to assign roles to groups. Specifically, you need to:

* Create a Senior Admins group containing the user account of Joseph Price as its member.
* Create a Junior Admins group containing the user account of Isabel Garcia as its member.
* Create a Service Desk group containing the user account of Dylan Williams as its member.
* Assign the Virtual Machine Contributor role to the Service Desk group.

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: Create the Senior Admins group with the user account Joseph Price as its member (the Azure portal).
* Exercise 2: Create the Junior Admins group with the user account Isabel Garcia as its member (PowerShell).
* Exercise 3: Create the Service Desk group with the user Dylan Williams as its member (Azure CLI).
* Exercise 4: Assign the Virtual Machine Contributor role to the Service Desk group.

**Exercise 1: Create the Senior Admins group with the user account Joseph Price as its member.**

**Estimated timing: 10 minutes**

In this exercise, you will complete the following tasks:

* Task 1: Use the Azure portal to create a user account for Joseph Price.
* Task 2: Use the Azure portal to create a Senior Admins group and add the user account of Joseph Price to the group.

**Task 1: Use the Azure portal to create a user account for Joseph Price**

In this task, you will create a user account for Joseph Price.

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

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 **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 **Overview** blade of the Azure Active Directory tenant, in the **Manage** section, select **Users**, and then select **+ New user**.
3. On the **New User** blade, ensure that the **Create user** option is selected, and specify the following settings:

| **Setting** | **Value** |
| --- | --- |
| User name | **Joseph** |
| Name | **Joseph Price** |

1. Click on the copy icon next to the **User name** to copy the full user.
2. Ensure that the **Auto-generate** password is selected, select the **Show password** checkbox to identify the automatically generated password. You would need to provide this password, along with the user name to Joseph.
3. Click **Create**.
4. Refresh the **Users | All users** blade to verify the new user was created in your Azure AD tenant.

**Task2: Use the Azure portal to create a Senior Admins group and add the user account of Joseph Price to the group.**

In this task, you will create the *Senior Admins* group, add the user account of Joseph Price to the group, and configure it as the group owner.

1. In the Azure portal, navigate back to the blade displaying your Azure Active Directory tenant.
2. In the **Manage** section, click **Groups**, and then select **+ New group**.
3. On the **New Group** blade, specify the following settings (leave others with their default values):

| **Setting** | **Value** |
| --- | --- |
| Group type | **Security** |
| Group name | **Senior Admins** |
| Membership type | **Assigned** |

1. Click the **No owners selected** link, on the **Add owners** blade, select **Joseph Price**, and click **Select**.
2. Click the **No members selected** link, on the **Add members** blade, select **Joseph Price**, and click **Select**.
3. Back on the **New Group** blade, click **Create**.

Result: You used the Azure Portal to create a user and a group, and assigned the user to the group.

**Exercise 2: Create a Junior Admins group containing the user account of Isabel Garcia as its member.**

**Estimated timing: 10 minutes**

In this exercise, you will complete the following tasks:

* Task 1: Use PowerShell to create a user account for Isabel Garcia.
* Task 2: Use PowerShell to create the Junior Admins group and add the user account of Isabel Garcia to the group.

**Task 1: Use PowerShell to create a user account for Isabel Garcia.**

In this task, you will create a user account for Isabel Garcia by using PowerShell.

1. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select **PowerShell** and **Create storage**.
2. Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.

To paste copied text into the Cloud Shell, right-click within the pane window and select **Pane**. Alternatively, you can use the **Shift+Insert** key combination.

1. In the PowerShell session within the Cloud Shell pane, run the following to create a password profile object:

powershell

$passwordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile

1. In the PowerShell session within the Cloud Shell pane, run the following to set the value of the password within the profile object:

powershell

$passwordProfile.Password = 'Pa55w.rd1234'

1. In the PowerShell session within the Cloud Shell pane, run the following to connect to Azure Active Directory:

powershell

Connect-AzureAD

1. In the PowerShell session within the Cloud Shell pane, run the following to identify the name of your Azure AD tenant:

powershell

$domainName = ((Get-AzureAdTenantDetail).VerifiedDomains)[0].Name

1. In the PowerShell session within the Cloud Shell pane, run the following to create a user account for Isabel Garcia:

powershell

New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@$domainName" -AccountEnabled $true -MailNickName 'Isabel'

1. In the PowerShell session within the Cloud Shell pane, run the following to list Azure AD users (the accounts of Joseph and Isabel should appear on the listed):

powershell

Get-AzureADUser

**Task2: Use PowerShell to create the Junior Admins group and add the user account of Isabel Garcia to the group.**

In this task, you will create the Junior Admins group and add the user account of Isabel Garcia to the group by using PowerShell.

1. In the same PowerShell session within the Cloud Shell pane, run the following to create a new security group named Junior Admins:

powershell

New-AzureADGroup -DisplayName 'Junior Admins' -MailEnabled $false -SecurityEnabled $true -MailNickName JuniorAdmins

1. In the PowerShell session within the Cloud Shell pane, run the following to list the groups in your Azure AD tenant (the list should include the Senior Admins and Junior Admins groups):

powershell

Get-AzureADGroup

1. In the PowerShell session within the Cloud Shell pane, run the following to obtain a reference to the user account of Isabel Garcia:

powershell

$user = Get-AzureADUser -Filter "MailNickName eq 'Isabel'"

1. In the PowerShell session within the Cloud Shell pane, run the following to add the user account of Isabel to the Junior Admins group:

powershell

Add-AzADGroupMember -MemberUserPrincipalName $user.userPrincipalName -TargetGroupDisplayName "Junior Admins"

1. In the PowerShell session within the Cloud Shell pane, run the following to verify that the Junior Admins group contains the user account of Isabel:

powershell

Get-AzADGroupMember -GroupDisplayName "Junior Admins"

Result: You used PowerShell to create a user and a group account, and added the user account to the group account.

**Exercise 3: Create a Service Desk group containing the user account of Dylan Williams as its member.**

**Estimated timing: 10 minutes**

In this exercise, you will complete the following tasks:

* Task 1: Use Azure CLI to create a user account for Dylan Williams.
* Task 2: Use Azure CLI to create the Service Desk group and add the user account of Dylan to the group.

**Task 1: Use Azure CLI to create a user account for Dylan Williams.**

In this task, you will create a user account for Dylan Williams.

1. In the drop-down menu in the upper-left corner of the Cloud Shell pane, select **Bash**, and, when prompted, click **Confirm**.
2. In the Bash session within the Cloud Shell pane, run the following to to identify the name of your Azure AD tenant:

cli

DOMAINNAME=$(az ad signed-in-user show --query 'userPrincipalName' | cut -d '@' -f 2 | sed 's/\"//')

1. In the Bash session within the Cloud Shell pane, run the following to create a user, Dylan Williams. Use *yourdomain*.

cli

az ad user create --display-name "Dylan Williams" --password "Pa55w.rd1234" --user-principal-name Dylan@$DOMAINNAME

1. In the Bash session within the Cloud Shell pane, run the following to list Azure AD user accounts (the list should include user accounts of Joseph, Isabel, and Dylan)

cli

az ad user list --output table

**Task 2: Use Azure CLI to create the Service Desk group and add the user account of Dylan to the group.**

In this task, you will create the Service Desk group and assign Dylan to the group.

1. In the same Bash session within the Cloud Shell pane, run the following to create a new security group named Service Desk.

cli

az ad group create --display-name "Service Desk" --mail-nickname "ServiceDesk"

1. In the Bash session within the Cloud Shell pane, run the following to list the Azure AD groups (the list should include Service Desk, Senior Admins, and Junior Admins groups):

cli

az ad group list -o table

1. In the Bash session within the Cloud Shell pane, run the following to obtain a reference to the user account of Dylan Williams:

cli

USER=$(az ad user list --filter "displayname eq 'Dylan Williams'")

1. In the Bash session within the Cloud Shell pane, run the following to obtain the objectId property of the user account of Dylan Williams:

cli

OBJECTID=$(echo $USER | jq '.[].objectId' | tr -d '"')

1. In the Bash session within the Cloud Shell pane, run the following to add the user account of Dylan to the Service Desk group:

cli

az ad group member add --group "Service Desk" --member-id $OBJECTID

1. In the Bash session within the Cloud Shell pane, run the following to list members of the Service Desk group and verify that it includes the user account of Dylan:

cli

az ad group member list --group "Service Desk"

1. Close the Cloud Shell pane.

Result: Using Azure CLI you created a user and a group accounts, and added the user account to the group.

**Exercise 4: Assign the Virtual Machine Contributor role to the Service Desk group.**

**Estimated timing: 10 minutes**

In this exercise, you will complete the following tasks:

* Task 1: Create a resource group.
* Task 2: Assign the Service Desk Virtual Machine Contributor permissions to the resource group.

**Task 1: Create a resource group**

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Resource groups** and press the **Enter** key.
2. On the **Resource groups** blade, click **+ Add** and specify the following settings:

| **Setting** | **Value** |
| --- | --- |
| Subscription name | the name of your Azure subscription |
| Resource group name | **AZ500Lab01** |
| Location | **East US** |

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

Wait for the resource group to deploy. Use the **Notification** icon (top right) to track progress of the deployment status.

1. Back on the **Resource groups** blade, refresh the page and verify your new resource group appears in the list of resource groups.

**Task 2: Assign the Service Desk Virtual Machine Contributor permissions.**

1. On the **Resource groups** blade, click the **AZ500LAB01** resource group entry.
2. On the **AZ500Lab01** blade, click **Access control (IAM)**.
3. On the **AZ500Lab01 | Access control (IAM)** blade, click **+ Add** and then, in the drop-down menu, click **Add role assignment**.
4. On the **Add role assignment** blade, specify the following settings:

| **Setting** | **Value** |
| --- | --- |
| Role | **Virtual Machine Contributor** |
| Assign access to | **User, group, or service principal** |
| Select | **Service Desk** |

1. Choose **Save** to create the role assignment.
2. From the **Access control (IAM) blade**, select **Check access**.
3. On the **AZ500Lab01 | Access control (IAM)** blade, on the **Check access** tab, in the **Search by name or email address** text box, type **Dylan Williams**.
4. In the list of search results, select the user account of Dylan Williams and, on the **Dylan Williams assignments - AZ500Lab01** blade, view the newly created assignment.
5. Close the **Dylan Williams assignments - AZ500Lab01** blade.
6. Repeat the same last two steps to check access for **Joseph Price**.

Result: You have assigned and checked RBAC permissions.

**Clean up resources**

Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs.

1. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal.
2. In the drop-down menu in the upper-left corner of the Cloud Shell pane, select **PowerShell**, and, when prompted, click **Confirm**.
3. In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:

Remove-AzResourceGroup -Name "AZ500LAB01" -Force -AsJob

1. Close the **Cloud Shell** pane.

**Congratulations!**

You have successfully completed this exercise. Click **Next** to advance to the next **Lab**.

**Lab 02: Azure Policy**

**Student lab manual**

**Lab scenario**

You have been asked to create a proof of concept showing how Azure policy can be used. Specifically, you need to:

* Create an Allowed Locations policy that ensures resource are only created in a specific region.
* Test to ensure resources are only created in the Allowed location

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:

* Exercise 1: Implement Azure Policy.

**Exercise 1: Implement Azure Policy**

**Estimated timing: 20 minutes**

In this exercise, you will complete the following tasks:

* Task 1: Create an Azure resource group.
* Task 2: Create an Allowed Locations policy assignment.
* Task 3: Verify the Allowed Locations policy assignment is working.

**Task 1: Create a resource group for the lab.**

In this task, you will create a resource group for the lab.

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

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.

1. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select **PowerShell** and **Create storage**.
2. Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.
3. In the PowerShell session within the Cloud Shell pane, run the following to create a resource group (verify with your instructor regarding the value of the location parameter):

powershell

New-AzResourceGroup -Name AZ500LAB02 -Location 'East US'

1. In the PowerShell session within the Cloud Shell pane, run the following to list resource groups to verify that the new resource group was created:

powershell

Get-AzResourceGroup | format-table

1. Close the **Cloud Shell**.

**Task 2: Create an Allowed Locations policy assignment.**

In this task, you will create an Allowed Locations policy assignment and specify which Azure regions the policy can use.

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Policy** and press the **Enter** key.
2. On the **Policy** blade, in the **Authoring** section, select **Definitions**.
3. Take a minute to browse the built-in definitions. Use the **Category** drop-down to filter the list of policies.
4. In the **Search** text box, type **Allowed locations**.

The **Allowed locations** policy allows you to restrict location of resources, not resource groups. To restrict locations of resource groups, you can use the **Allowed locations for resource groups** policy.

1. Click the **Allowed locations** policy definition to display its details..

This policy definition takes an array of locations as parameters. A policy rule is an ‘if-then’ statement. The ‘if’ clause checks if the resource location is included in the parameter list, and if not, the ‘then’ clause denies the resource creation or, for existing resources, marks them as non-compliant.

1. On the **Allowed locations** blade, click **Assign**.
2. On the **Basics** tab of the **Allowed locations** blade, click the Ellipsis (…) button next to the **Scope** text box and, on the **Scope** blade, specify the following settings:

| **Setting** | **Value** |
| --- | --- |
| Subscription | the name of you Azure subscription |
| Resource group | **AZ500LAB02** |

1. Click **Select**.
2. On the **Allowed locations** blade, on the **Basics** tab, specify the following settings (leave others with their defualt values):

| **Setting** | **Value** |
| --- | --- |
| Assignment name | **Allow UK South for AZ500LAB02** |
| Description | **Allow resources to be created in UK South Only for AZ500LAB02** |
| Policy enforcement | **Enabled** |

1. Click **Next**.
2. On the **Parameters** tab of the **Allowed locations** blade, in the **Allowed locations** drop-down list, select **UK South** as the only allowed location.

You can select more than one location. If the policy required a different set of parameters, this tab would provide those selections.

1. Click **Review + create**, followed by **Create** to create the policy assignment.

You will see a notification that the assignment was successful, and that the assignment might take around 30 minutes to complete.

The reason the Azure policy assignment might take up to 30 minutes to take effect is that is has to replicate globally. Typically this takes only a few minutes. If the next task fails, simply wait a few minutes and attempt its steps again.

**Task 3: Test the Allowed Locations policy assignment**

In this task, you will test the Allowed Locations policy assignment.

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Virtual networks** and press the **Enter** key.
2. On the **Virtual Networks** blade, click **+ Add**.

First, you will try to create a virtual network in East US. Since this is not an allowed location, the request should be blocked.

1. On the **Basics** tab of the **Create virtual network** blade, specify the following settings (leave others with their defualt values):

| **Setting** | **Value** |
| --- | --- |
| Resource group | **AZ500LAB02** |
| Name | **myVnet** |
| Region | **(US) East US** |

1. Click **Review + create**.
2. On the **Review + create** tab of the **Create virtual network** blade note the **Validation failed** message.

If the **Validation Failed** warning does not appear, click **Previous** and wait a few more minutes.

1. Click the error message to open the **Errors** blade. You will see the detailed error message stating that the deployment of the resource **myVnet** was disallowed by policy.
2. Close the **Errors** blade, on the **Create virtual network** blade, click the **Basics** tab, and, in the **Region** drop-down list, select **(Europe) UK South**.
3. Click **Review + create**, verify that validation passed, click **Create**, and verify that the virtual network was created successfully.

Exercise results: In this exercise, you learned to apply an Azure policy by selecting a built-in policy definitions and assigning it to a resource group.

**Clean up resources**

Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs.

1. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, click **Reconnect**.
2. In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:

powershell

Remove-AzResourceGroup -Name "AZ500LAB02" -Force -AsJob

1. Close the **Cloud Shell** pane.

**Congratulations!**

You have successfully completed this exercise. Click **Next** to advance to the next **Lab**.

Module 01 : Manage Identity and Access

2 Hr 35 Min Remaining

**Lab 04: MFA, Conditional Access and AAD Identity Protection**

**Student lab manual**

**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

**Lab files:**

* **\Allfiles\Labs\04\az-500-04\_azuredeploy.json**
* **\Allfiles\Labs\04\az-500-04\_azuredeploy.parameters.json**

**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/**.

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 **custom template** and select **Deploy a custom template** under the list of **Services**.

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**.

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**.

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):

| **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 | **Pa55w.rd1234** |
| Virtual Network Name | **az500-04-vnet1** |

1. To identify Azure regions where you can provision Azure VMs, refer to https://azure.microsoft.com/en-us/regions/offers
2. Click **Review + create**, and then click **Create**.

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 **+ Create a tenant**.
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. Record the initial domain name. You will need it later in this lab.
2. Click **Review + Create** and then click **Create**.

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**.

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

1. On the **AdatumLab500-04** Azure Active Directory 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. 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. 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. 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. Record the full user name and the password.
2. On the **New user** blade, click **Create**.

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**.
3. In the **Settings** section, in the **Usage location** drop down list, select the **United States** entry and click **Save**.
4. Navigate back to the **AdatumLab500-04** Azure Active Directory blade and, in the **Manage** section, click **Licenses**.
5. On the **Licenses | Overview** blae, click **All products**, select the **Azure Active Directory Premium P2** checkbox, and click **+ Assign**.
6. On the **Assign licenses** blade, click **Users**.
7. On the **Users** blade, select **aaduser1**, **aaduser2**, **aaduser3**, and your user account and click **Select**.
8. Back on the **Assign licenses** blade, click **Assignment options**, ensure that all options are enabled, and click **OK**.
9. Back on the **Assign licenses** blade, click **Assign**.
10. 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.

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.

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.

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.

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**

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**.

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.

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**.

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

1. In the **Step 1: How should we contact you?** section, note that you need to set up one of the following options:
   * **Authentication phone**
   * **Mobile app**
2. Ensure that the **Authentication phone** entry appears in the drop-down list and the **Send me a code by text message** option is selected.
3. In the **Step 1: How should we contact you?** section, in the drop-down list, select your country or region, provide your mobile phone number in the empty text box, and click **Next**.
4. Provide your phone number, click **Next**, in the text box, type the code you received in the text message on your mobile phone, and click **Verify**.
5. On the **Additional security verification** page, review instructions provided in **Step 3: Keep using your existing applications**, 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**.
5. On the **New** blade, configure the following settings:
   * In the **Name** text box, type **AZ500Policy1**
   * Click **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**.

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 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**.

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**.

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.

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**.

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/**.

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 **Protect**, **Report**, and **Notify** options.

**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**, click **Select**, 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 adVM via Remote Desktop. When prompted to authenticate, provide the following credntials:

| **Setting** | **Value** |
| --- | --- |
| User name | **Student** |
| Password | **Pa55w.rd1234** |

1. Wait for the Remote Desktop session and **Server Manager** to load.
2. 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.

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** to sign in as **aaduser1** account you created and configured for multi-factor authentication earlier in this lab.

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.

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 **Reports** 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**

Do not remove any resources provisioned in this lab, since the PIM lab has a dependency on them.

**Congratulations!**

You have successfully completed this exercise. Click **Next** to advance to the next **Lab**.

Module 01 : Manage Identity and Access

3 Hr 47 Min Remaining

**Lab 04: MFA, Conditional Access and AAD Identity Protection**

**Student lab manual**

**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

**Lab files:**

* **\Allfiles\Labs\04\az-500-04\_azuredeploy.json**
* **\Allfiles\Labs\04\az-500-04\_azuredeploy.parameters.json**

**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/**.

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 **custom template** and select **Deploy a custom template** under the list of **Services**.

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**.

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**.

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):

| **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 | **Pa55w.rd1234** |
| Virtual Network Name | **az500-04-vnet1** |

1. To identify Azure regions where you can provision Azure VMs, refer to https://azure.microsoft.com/en-us/regions/offers
2. Click **Review + create**, and then click **Create**.

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 **+ Create a tenant**.
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. Record the initial domain name. You will need it later in this lab.
2. Click **Review + Create** and then click **Create**.

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**.

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

1. On the **AdatumLab500-04** Azure Active Directory 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. 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. 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. 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. Record the full user name and the password.
2. On the **New user** blade, click **Create**.

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**.
3. In the **Settings** section, in the **Usage location** drop down list, select the **United States** entry and click **Save**.
4. Navigate back to the **AdatumLab500-04** Azure Active Directory blade and, in the **Manage** section, click **Licenses**.
5. On the **Licenses | Overview** blae, click **All products**, select the **Azure Active Directory Premium P2** checkbox, and click **+ Assign**.
6. On the **Assign licenses** blade, click **Users**.
7. On the **Users** blade, select **aaduser1**, **aaduser2**, **aaduser3**, and your user account and click **Select**.
8. Back on the **Assign licenses** blade, click **Assignment options**, ensure that all options are enabled, and click **OK**.
9. Back on the **Assign licenses** blade, click **Assign**.
10. 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.

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.

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.

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.

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**

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**.

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.

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**.

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

1. In the **Step 1: How should we contact you?** section, note that you need to set up one of the following options:
   * **Authentication phone**
   * **Mobile app**
2. Ensure that the **Authentication phone** entry appears in the drop-down list and the **Send me a code by text message** option is selected.
3. In the **Step 1: How should we contact you?** section, in the drop-down list, select your country or region, provide your mobile phone number in the empty text box, and click **Next**.
4. Provide your phone number, click **Next**, in the text box, type the code you received in the text message on your mobile phone, and click **Verify**.
5. On the **Additional security verification** page, review instructions provided in **Step 3: Keep using your existing applications**, 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**.
5. On the **New** blade, configure the following settings:
   * In the **Name** text box, type **AZ500Policy1**
   * Click **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**.

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 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**.

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**.

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.

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**.

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/**.

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 **Protect**, **Report**, and **Notify** options.

**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**, click **Select**, 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 adVM via Remote Desktop. When prompted to authenticate, provide the following credntials:

| **Setting** | **Value** |
| --- | --- |
| User name | **Student** |
| Password | **Pa55w.rd1234** |

1. Wait for the Remote Desktop session and **Server Manager** to load.
2. 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.

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** to sign in as **aaduser1** account you created and configured for multi-factor authentication earlier in this lab.

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.

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 **Reports** 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**

Do not remove any resources provisioned in this lab, since the PIM lab has a dependency on them.

**Congratulations!**

You have successfully completed this exercise. Click **Next** to advance to the next **Lab**.

Module 01 : Manage Identity and Access

1 Hr 46 Min Remaining

**Lab 06: Implement Directory Synchronization**

**Student lab manual**

**Lab scenario**

You have been asked to create a proof of concept demonstrating how to integrate on-premises Active Directory Domain Services (AD DS) environment with an Azure Active Directory (Azure AD) tenant. Specifically, you want to:

* Implement a single-domain AD DS forest by deploying an Azure VM hosting an AD DS domain controller
* Create and configure an Azure AD tenant
* Synchronize the AD DS forest with the Azure AD tenant

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 hosting an Active Directory domain controller
* Exercise 2: Create and configure an Azure Active Directory tenant
* Exercise 3: Synchronize Active Directory forest with an Azure Active Directory tenant

**Exercise 1: Deploy an Azure VM hosting an Active Directory domain controller**

**Estimated timing: 10 minutes**

In this exercise, you will complete the following tasks:

* Task 1: Identify an available DNS name for an Azure VM deployment
* Task 2: Use an ARM template to deploy an Azure VM hosting an Active Directory domain controller

**Task 1: Identify an available DNS name for an Azure VM deployment**

In this task, you will identify a DNS name for your Azure VM deployment.

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

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.

1. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, click **PowerShell** and **Create storage**.
2. Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.
3. In the PowerShell session within the Cloud Shell pane, run the following to identify an available DNS name you can use for an Azure VM deployment in the next task of this exercise:

powershell

Test-AzDnsAvailability -DomainNameLabel <custom-label> -Location '<location>'

Replace the (custom-label) placeholder with a valid DNS name that is likely to be globlly unique. Replace the (location) placeholder with the name of the region into which you want to deploy the Azure VM that will host the Active Directory domain controller you will use in this lab.

To identify Azure regions where you can provision Azure VMs, refer to https://azure.microsoft.com/en-us/regions/offers

1. Verify that the command returned **True**. If not, rerun the same command with a different value of the (custom-label) until the command returns **True**.
2. Record the value of the (custom-label) that resulted in the successful outcome. You will need it in the next task.
3. Close the Cloud Shell.

**Task 2: Use an ARM template to deploy an Azure VM hosting an Active Directory domain controller**

In this task, you will deploy an Azure VM that will host an Active Directory domain controller

1. Open another browser tab in the same browser window and navigate to the https://github.com/Azure/azure-quickstart-templates/tree/master/active-directory-new-domain.
2. On the **Create a new Windows VM and create a new AD Forest, Domain and DC** page, click **Deploy to Azure**. This will automatically redirect the browser to the **Create an Azure VM with a new AD Forest** blade in the Azure portal.
3. On the **Create an Azure VM with a new AD Forest** blade, click **Edit parameters**.
4. On the **Edit parameters** blade, click **Load file**, in the **Open** dialog box, click **\\AllFiles\Labs\06\active-directory-new-domain\azuredeploy.parameters.json**, click **Open**, and then click **Save**.
5. On the **Create an Azure VM with a new AD Forest** blade, specify the following settings (leave others with their existing values):

| **Setting** | **Value** |
| --- | --- |
| Subscription | the name of you Azure subscription |
| Resource group | click **Create new** and type the name **AZ500LAB06** |
| Region | the Azure region you identified in the previous task |
| Admin Username | **Student** |
| Admin Password | **Pa55w.rd1234** |
| Domain Name | **adatum.com** |
| Dns Prefix | the DNS hostname you identified in the previous task |
| VM Size | **Standard\_D2s\_v3** |

1. On the **Create an Azure VM with a new AD Forest** blade, click **Review + create**, and then click **Create**.

Do not wait for the deployment to complete but instead proceed to the next exercise. The deployment might take about 15 minutes. You will use the virtual machine deployed in this task in the third exercise of this lab.

Result: After you completed this exercise, you have initiated deployment of an Azure VM that will host an Active Directory domain controller by using an Azure Resource Manager template

**Exercise 2: Create and configure an Azure Active Directory tenant**

**Estimated timing: 20 minutes**

In this exercise, you will complete the following tasks:

* Task 1: Create an Azure Active Directory (AD) tenant
* Task 2: Add a custom DNS name to the new Azure AD tenant
* Task 3: Create an Azure AD user with the Global Administrator role

**Task 1: Create an Azure Active Directory (AD) tenant**

In this task, you will create a new Azure AD tenant to use in this lab.

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 **+ Create a tenant**.
3. On the **Basics** tab of the **Create a directory** blade, ensure that the option **Azure Active Directory** is selected and click **Next: Configuration >**.
4. On the **Configuration** tab of the **Create a directory** blade, specify the following settings:

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

1. Record the initial domain name. You will need it later in this lab.
2. The green check mark in the **Initial domain name** text box will indicate whether the domain name you typed in is valid and unique. (Record your initial domain name for later use).
3. Click **Review + create** and then click **Create**.

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

**Task 2: Add a custom DNS name to the new Azure AD tenant**

In this task, you will add your custom DNS name to the new Azure AD tenant.

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, **AdatumSync**.

You may need to refresh the browser window if the **AdatumSync** entry does not appear in the **Directory + subscription** filter list.

1. On the **AdatumSync** blade, in the **Manage** section, click **Custom domain names**.
2. On the **AdatumSync | Custom domain names** blade, click **+ Add custom domain**.
3. On the **Custom domain name** blade, in the **Custom domain name** text box, type **adatum.com** and click **Add Domain**.
4. On the **adatum.com** blade, review the information necessary to perform verification of the Azure AD domain name.

You will not be able to complete the validation process because you do not own the **adatum.com** DNS domain name. This will not prevent you from synchronizing the **adatum.com** AD DS domain with the Azure AD tenant. You will use for this purpose the initial DNS name of the Azure AD tenant (the name ending with the **onmicrosoft.com** suffix), which you identified in the previous task. However, keep in mind that, as a result, the DNS domain name of the AD DS domain and the DNS name of the Azure AD tenant will differ. This means that Adatum users will need to use different names when signing in to the AD DS domain and when signing in to Azure AD tenant.

**Task 3: Create an Azure AD user with the Global Administrator role**

In this task, you will add a new Azure AD user and assign them to the Global Administrator role.

1. On the **AdatumSync** Azure AD tenant blade, 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, specify the following settings (leave all others with their default values) and click **Create**:

| **Setting** | **Value** |
| --- | --- |
| User name | **syncadmin** |
| Name | **syncadmin** |
| 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. 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. Record the user's password. You will need this later in this lab.
3. An Azure AD user with the Global Administrator role is required in order to implement Azure AD Connect.
4. Open an InPrivate browser window.
5. Navigate to the Azure portal and sign in using the **syncadmin** user account. When prompted, change the password you recorded earlier in this task to **Pa55w.rd1234**.

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

1. Sign out as **syncadmin** and close the InPrivate browser window.

**Result**: After you completed this exercise, you have created an Azure AD tenant, added a custom DNS name to the new Azure AD tenant, and created an Azure AD user with the Global Administrator role.

**Exercise 3: Synchronize Active Directory forest with an Azure Active Directory tenant**

**Estimated timing: 20 minutes**

In this exercise, you will complete the following tasks:

* Task 1: Prepare AD DS for directory synchronization
* Task 2: Install Azure AD Connect
* Task 3: Verify directory synchronization

**Task 1: Prepare AD DS for directory synchronization**

In this task, you will connect to the Azure VM running AD DS domain controller and create a directory synchronization account.

Before you start this task, ensure that the template deployment you started in the first exercise of this lab has completed.

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 Azure VM in the first exercise of this lab.
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 **adVM** entry.
4. On the **adVM** blade, click **Connect** and, in the drop down menu, click **RDP**.
5. Change the **IP Address** to the **Load balancer public IP address**.
6. In the **IP address** parameter, select **Load balancer public IP address**, then click **Download RDP File** and use it to connect to the **adVM** Azure VM via Remote Desktop. When prompted to authenticate, provide the following credntials:

| **Setting** | **Value** |
| --- | --- |
| User name | **Student** |
| Password | **Pa55w.rd1234** |

1. Wait for the Remote Desktop session and **Server Manager** to load.
2. The following steps are performed in the Remote Desktop session to the **adVM** 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. In **Server Manager**, click **Tools** and, in the drop-down menu, click **Active Directory Administrative Center**.
6. In **Active Directory Administrative Center**, click **adatum (local)**, in the **Tasks** pane, click **New**, and, in the cascading menu, click **Organizational Unit**.
7. In the **Create Organizational Unit** window, in the **Name** text box, type **ToSync** and click **OK**.
8. Double-click the newly crated **ToSync** organizational unit such that its content appears in the details pane of the Active Directory Administrative Center console.
9. In the **Tasks** pane, within the **ToSync** section, click **New**, and, in the cascading menu, click **User**.
10. In the **Create User** window, create a new user account with the following settings (leave others with their existing values) and click **OK**:

| **Setting** | **Value** |
| --- | --- |
| Full Name | **aduser1** |
| User UPN logon | **aduser1** |
| User SamAccountName logon | **aduser1** |
| Password | **Pa55w.rd1234** |
| Other password options | **Password never expires** |

**Task 2: Install Azure AD Connect**

In this task, you will install AD Connect on the virtual machine.

1. Within the Remote Desktop session to **adVM**, start Internet Explorer, navigate to the https://portal.azure.com, and sign in by using the **syncadmin** user account you created the previous exercise. When prompted, specify the full user name you recorded and the **Pa55w.rd1234** password.
2. 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.
3. In the Azure portal, on the **AdatumSync | Overview** blade, click **Azure AD Connect**.
4. On the **AdatumSync | Azure AD Connect** blade, click the **Download Azure AD Connect** link. You will be redirected to the **Microsoft Azure Active Directory Connect** download page.
5. On the **Microsoft Azure Active Directory Connect** download page, click **Download**.
6. When prompted, click **Run** to start the **Microsoft Azure Active Directory Connect** wizard.
7. On the **Welcome to Azure AD Connect** page of the **Microsoft Azure Active Directory Connect** wizard, click the checkbox **I agree to the license terms and privacy notice** and click **Continue**.
8. On the **Express Settings** page of the **Microsoft Azure Active Directory Connect** wizard, click the **Customize** option.
9. On the **Install required components** page, leave all optional configuration options deselected and click **Install**.
10. On the **User sign-in** page, ensure that only the **Password Hash Synchronization** is enabled and click **Next**.
11. On the **Connect to Azure AD** page, authenticate by using the credentials of the **syncadmin** user account you created in the previous exercise and click **Next**.
12. On the **Connect your directories** page, click the **Add Directory** button to the right of the **adatum.com** forest entry.
13. In the **AD forest account** window, ensure that the option to **Create new AD account** is selected, specify the following credentials, and click **OK**:

| **Setting** | **Value** |
| --- | --- |
| User Name | **ADATUM\Student** |
| Password | **Pa55w.rd1234** |

1. Back on the **Connect your directories** page, ensure that the **adatum.com** entry appears as a configured directory and click **Next**
2. On the **Azure AD sign-in configuration** page, note the warning stating **Users will not be able to sign-in to Azure AD with on-premises credentials if the UPN suffix does not match a verified domain name**, enable the checkbox **Continue without matching all UPN suffixes to verified domain**, and click **Next**.

As explained earlier, this is expected, since you could not verify the custom Azure AD DNS domain **adatum.com**.

1. On the **Domain and OU filtering** page, click the option **Sync selected domains and OUs**, clear all checkboxes, click only the checkbox next to the **ToSync** OU, and click **Next**.
2. On the **Uniquely identifying your users** page, accept the default settings, and click **Next**.
3. On the **Filter users and devices** page, accept the default settings, and click **Next**.
4. On the **Optional features** page, accept the default settings, and click **Next**.
5. On the **Ready to configure** page, ensure that the **Start the synchronization process when configuration completes** checkbox is selected and click **Install**.

Installation should take about 2 minutes.

1. Review the information on the **Configuration complete** page and click **Exit** to close the **Microsoft Azure Active Directory Connect** window.

**Task 3: Verify directory synchronization**

In this task, you will verify that directory synchronization is working.

1. Within the Remote Desktop session to **adVM**, in the Internet Explorer window displaying the Azure portal, navigate to the **Users - All users** blade of the Adatum Lab Azure AD tenant.
2. On the **Users | All users** blade, note that the list of user objects includes the **aduser1** account.
3. Select the **aduser1** account and, in the **Profile > Identity** section, note that the **Source** attribute is set to **Windows Server AD**.

You might have to wait a few minutes and select **Refresh** for the **aduser1** user account to appear.

1. On the **Users | All users** blade, select the **aduser1** entry.
2. On the **aduser1 | Profile** blade, in the **Job info** section, note that the **Department** attribute is not set.
3. Within the Remote Desktop session to **adVM**, switch to **Active Directory Administrative Center**, select the **aduser1** entry in the list of objects in the **ToSync** OU, and, in the **Tasks** pane, in the **ToSync** section, select **Properties**.
4. In the **aduser1** window, in the **Organization** section, in the **Department** text box, type **Sales**, and select **OK**.
5. Within the Remote Desktop session to **adVM**, start **Windows PowerShell**.
6. From the **Administrator: Windows PowerShell** console, run the following to start Azure AD Connect delta synchronization:

powershell

Import-Module -Name 'C:\Program Files\Microsoft Azure AD Sync\Bin\ADSync\ADSync.psd1'

Start-ADSyncSyncCycle -PolicyType Delta

1. Switch to the Internet Explorer window displaying the **aduser1 | Profile** blade, refresh the page and note that the **Department** property is set to **Sales**.

You might need to wait for another minute and refresh the page again if the **Department** attribute remains not set.

**Result**: After you completed this exercise, you have prepared AD DS for directory synchronization, installed Azure AD Connect, and verified directory synchronization.

**Clean up resources**

Start by disabling Azure AD synchronization

1. Within the Remote Desktop session to **adVM**, start Windows PowerShell as Administrator.
2. From the Windows PowerShell console, install the MsOnline PowerShell module by running the following (when prompted, in the NuGet provider is required to continue dialog box, type **Yes** and hit Enter.):

powershell

[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12

Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force

Install-Module MsOnline -Force

1. From the Windows PowerShell console, connect to the AdatumSync Azure AD tenant by running the following (when prompted, sign in with the **syncadmin** credentials):

powershell

Connect-MsolService

1. From the Windows PowerShell console, disable the Azure AD Connect synchronization by running the following:

powershell

Set-MsolDirSyncEnabled -EnableDirSync $false -Force

1. From the Windows PowerShell console, verify that the operation was successful by running the following:

powershell

(Get-MSOLCompanyInformation).DirectorySynchronizationEnabled

The result should be False. If that is not the case, wait a minute and re-run the command.

Next, remove the Azure resources

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 **adVM** Azure VM.
2. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal.
3. In the drop-down menu in the upper-left corner of the Cloud Shell pane, select **PowerShell**, and, when prompted, click **Confirm**.
4. In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:

powershell

Remove-AzResourceGroup -Name "AZ500LAB06" -Force -AsJob

1. Close the **Cloud Shell** pane.

Finally, remove the Azure AD tenant

1. Back in the Azure portal, use the **Directory + subscription** filter to switch to the **AdatumSync** Azure Active Directory tenant.
2. In the Azure portal, navigate to the **Users - All users** blade, click the entry representing the **syncadmin** user account, on the **syncadmin - Profile** blade click **Delete**, and, when prompted to confirm, click **OK**.
3. Repeat the same sequence of steps to delete the **aduser1** user account.
4. Navigate to the **AdatumSync - Overview** blade of the Azure AD tenant, click **Delete tenant**, on the **Delete directory 'AdatumSync'** blade, click the **Get permission to delete Azure resources** link, on the **Properties** blade of Azure Active Directory, set **Access management for Azure resources** to **Yes** and click **Save**.
5. Sign out from the Azure portal and sign in back.
6. Navigate back to the **Delete directory 'AdatumSync'** blade and click **Delete**.

For any additional information regarding this task, refer to (<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-delete-howto>

Module 02: Implement Platform Protection

4 Hr 21 Min Remaining

# Lab 08: Azure Firewall

# Student lab manual

## Lab scenario

You have been asked to install Azure Firewall. This will help your organization control inbound and outbound network access which is an important part of an overall network security plan. Specifically, you would like to create and test the following infrastructure components:

* A virtual network with a workload subnet and a jump host subnet.
* A virtual machine is each subnet.
* A custom route that ensures all outbound workload traffic from the workload subnet must use the firewall.
* Firewall Application rules that only allow outbound traffic to www.bing.com.
* Firewall Network rules that allow external DNS server lookups.

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 exercise:

* Exercise 1: Deploy and test an Azure Firewall

## Lab files:

* **\Allfiles\Labs\08\template.json**

### Exercise 1: Deploy and test an Azure Firewall

### Estimated timing: 40 minutes

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

In this exercise, you will complete the following tasks:

* Task 1: Use a template to deploy the lab environment.
* Task 2: Deploy an Azure firewall.
* Task 3: Create a default route.
* Task 4: Configure an application rule.
* Task 5: Configure a network rule.
* Task 6: Configure DNS servers.
* Task 7: Test the firewall.

#### Task 1: Use a template to deploy the lab environment.

In this task, you will review and deploy the lab environment.

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/**.

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.

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** and press the **Enter** key.
2. On the **Custom deployment** blade, click the **Build your own template in the editor** option.
3. On the **Edit template** blade, click **Load file**, locate the **\Allfiles\Labs\08\template.json** file and click **Open**.

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

| **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 **AZ500LAB08** |
| Location | **(US) East US** |

1. To identify Azure regions where you can provision Azure VMs, refer to https://azure.microsoft.com/en-us/regions/offers/
2. Click **Review + create**, and then click **Create**.

Wait for the deployment to complete. This should take about 2 minutes.

#### Task 2: Deploy the Azure firewall

In this task you will deploy the Azure firewall into the virtual network.

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Firewalls** and press the **Enter** key.
2. On the **Firewalls** blade, click **+ Add**.
3. On the **Basics** tab of the **Create a firewall** blade, specify the following settings (leave others with their default values):

| **Setting** | **Value** |
| --- | --- |
| Resource group | **AZ500LAB08** |
| Name | **Test-FW01** |
| Region | **(US) East US** |
| Choose a virtual network | click the **Use existing** option and, in the drop-down list, select **Test-FW-VN** |
| Public IP address | clck **Add new** and type the name **TEST-FW-PIP** and click **OK** |

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

Wait for the deployment to complete. This should take about 5 minutes.

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Resource groups** and press the **Enter** key.
2. On the **Resource groups** blade, in the list of resource group, click the **AZ500LAB08** entry.

On the **AZ500LAB08** resource group blade, review the list of resources. You can sort by **Type**.

1. In the list of resources, click the entry representing the **Test-FW01** firewall.
2. On the **Test-FW01** blade, identify the **Private IP** address that was assigned to the firewall.

You will need this information in the next task.

#### Task 3: Create a default route

In this task, you will create a default route for the **Workload-SN** subnet. This route will configure outbound traffic through the firewall.

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Route tables** and press the **Enter** key.
2. On the **Route tables** blade, click **+ Add**.
3. On the **Create route table** blade, specify the following settings:

| **Setting** | **Value** |
| --- | --- |
| Name | **Firewall-route** |
| Resource group | **AZ500LAB08** |
| Region | **East US** |

1. Click **Review + create**, then click **Create**, and wait for the provisioning to complete.
2. On the **Route tables** blade, click **Refresh**, and, in the list of route tables, click the **Firewall-route** entry.
3. On the **Firewall-route** blade, in the **Settings** section, click **Subnets** and then, on the **Firewall-route | Subnets** blade, click **+ Associate**.
4. On the **Associate subnet** blade, specify the following settings:

| **Setting** | **Value** |
| --- | --- |
| Virtual network | **Test-FW-VN** |
| Subnet | **Workload-SN** |

1. Ensure the **Workload-SN** subnet is selected for this route, otherwise the firewall won't work correctly.
2. Click **OK** to associate the firewall to the virtual network subnet.
3. Back on the **Firewall-route** blade, in the **Settings** section, click **Routes** and then click **+ Add**.
4. On the **Add route** blade, specify the following settings:

| **Setting** | **Value** |
| --- | --- |
| Route name | **FW-DG** |
| Address prefix | **0.0.0.0/0** |
| Next hop type | **Virtual appliance** |
| Next hop address | the private IP address of the firewall that you identified in the previous task |

1. Azure Firewall is actually a managed service, but virtual appliance works in this situation.
2. Click **OK** to add the route.

#### Task 4: Configure an application rule

In this task you will create an application rule that allows outbound access to www.bing.com.

1. In the Azure portal, navigate back to the **Test-FW01** firewall.
2. On the **Test-FW01** blade, in the **Settings** section, click **Rules**.
3. On the **Test-FW01 | Rules** blade, click the **Application rule collection** tab, and then click **+ Add application rule collection**.
4. On the **Add application rule collection** blade, specify the following settings (leave others with their default values):

| **Setting** | **Value** |
| --- | --- |
| Name | **App-Coll01** |
| Priority | **200** |
| Action | **Allow** |

1. On the **Add application rule collection** blade, create a new entry in the **Target FQDNs** section with the following settings (leave others with their default values):

| **Setting** | **Value** |
| --- | --- |
| name | **AllowGH** |
| Source type | **IP Address** |
| Source | **10.0.2.0/24** |
| Protocol port | **http:80, https:443** |
| Target FQDNS | **www.bing.com** |

1. Click **Add** to add the Target FQDNs-based application rule.

Azure Firewall includes a built-in rule collection for infrastructure FQDNs that are allowed by default. These FQDNs are specific for the platform and can't be used for other purposes.

#### Task 5: Configure a network rule

In this task, you will create a network rule that allows outbound access to two IP addresses on port 53 (DNS).

1. In the Azure portal, navigate back to the **Test-FW01 | Rules** blade.
2. On the **Test-FW01 | Rules** blade, click the **Network rule collection** tab and then click **+ Add network rule collection**.
3. On the **Add network rule collection** blade, specify the following settings (leave others with their default values):

| **Setting** | **Value** |
| --- | --- |
| Name | **Net-Coll01** |
| Priority | **200** |
| Action | **Allow** |

1. On the **Add network rule collection** blade, create a new entry in the **IP Addresses** section with the following settings (leave others with their default values):

| **Setting** | **Value** |
| --- | --- |
| Name | **AllowDNS** |
| Protocol | **UDP** |
| Source type | **IP address** |
| Source Addresses | **10.0.2.0/24** |
| Destination type | **IP address** |
| Destination Address | **209.244.0.3,209.244.0.4** |
| Destination Ports | **53** |

1. Click **Add** to add the network rule.

The destination addresses used in this case are known public DNS servers.

#### Task 6: Configure the virtual machine DNS servers

In this task, you will configure the primary and secondary DNS addresses for the virtual machine. This is not a firewall requirement.

1. In the Azure portal, navigate back to the **AZ500LAB08** resource group.
2. On the **AZ500LAB08** blade, in the list of resources, click the **Srv-Work** virtual machine.
3. On the **Srv-Work** blade, in the **Settings** section, click **Networking**.
4. On the **Srv-Work | Networking** blade, click the link next to the **Network interface** entry.
5. On the network interface blade, in the **Settings** section, click **DNS servers**, select the **Custom** option, add the two DNS servers referenced in the network rule: **209.244.0.3** and **209.244.0.4**, and click **Save** to save the change.
6. Return to the **Srv-Work** virtual machine page.

Wait for the update to complete.

Updating the DNS servers for a network interface will automatically restart the virtual machine to which that interface is attached, and if applicable, any other virtual machines in the same availability set.

#### Task 7: Test the firewall

In this task, you will test the firewall to confirm that it works as expected.

1. In the Azure portal, navigate back to the **AZ500LAB08** resource group.
2. On the **AZ500LAB08** blade, in the list of resources, click the **Srv-Jump** virtual machine.
3. On the **Srv-Jump** blade, click **Connect** and, in the drop down menu, click **RDP**.
4. Click **Download RDP File** and use it to connect to the **Srv-Jump** Azure VM via Remote Desktop. When prompted to authenticate, provide the following credntials:

| **Setting** | **Value** |
| --- | --- |
| User name | **localadmin** |
| Password | **Pa55w.rd1234** |

1. The following steps are performed in the Remote Desktop session to the **Srv-Jump** Azure VM.
2. You will connect to the **Srv-Work** virtual machine. This is being done so we can test the ability to access the bing.com website.
3. Within the Remote Desktop session to **Srv-Jump**, right-click **Start**, in the right-click menu, click **Run**, and, from the **Run** dialog box, run the following to connect to **Srv-Work**.

mstsc /v:Srv-Work

1. When prompted to authenticate, provide the following credentials:

| **Setting** | **Value** |
| --- | --- |
| User name | **localadmin** |
| Password | **Pa55w.rd1234** |

1. Wait for the Remote Desktop session to be established and the Server Manager interface to load.
2. Within the Remote Desktop session to **Srv-Work**, in **Server Manager**, click **Local Server** and then click **IE Enhanced Security Configuration**.
3. In the **Internet Explorer Enhanced Security Configuration** dialog box, set both options to **Off** and click **OK**.
4. Within the Remote Desktop session to **Srv-Work**, start Internet Explorer and browse to **https://www.bing.com**.

The website should successfully display. The firewall allows you access.

1. Browse to **http://www.microsoft.com/**

Within the browser page, you should receive a message with text resembling the following: HTTP request from 10.0.2.4:xxxxx to microsoft.com:80. Action: Deny. No rule matched. Proceeding with default action. This is expected, since the firewall blocks access to this website.

1. Terminate both Remote Desktop sessions.

Result: You have successfully configured and tested the Azure Firewall.

**Clean up resources**

Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs.

1. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, click **PowerShell** and **Create storage**.
2. Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.
3. In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:

powershell

Remove-AzResourceGroup -Name "AZ500LAB08" -Force -AsJob

1. Close the **Cloud Shell** pane.

### Congratulations!

You have successfully completed this exercise. Click **Next** to advance to the next **Lab**.