Lab - Configure Conditional Access policies for AVD (AD DS)

Student lab manual

Lab dependencies

- An Azure subscription
- A Microsoft account or a Microsoft Entra account with the Global Administrator role in the Microsoft Entra tenant associated with the Azure subscription and with the Owner or Contributor role in the Azure subscription
- The completed lab **Prepare for deployment of Azure Virtual Desktop (AD DS)**
- The completed lab **Deploy host pools and session hosts by using the Azure portal (AD DS)**

Estimated Time

60 minutes

Lab scenario

You need to control access to a deployment of Azure Virtual Desktop in an Active Directory Domain Services (AD DS) environment by using Microsoft Entra conditional access.

Objectives

After completing this lab, you will be able to:

- Prepare for Microsoft Entra-based Conditional Access for Azure Virtual Desktop
- Implement Microsoft Entra-based Conditional Access for Azure Virtual Desktop

Lab files

- None

Instructions

> **Important**: Microsoft renamed **Azure Active Directory** (**Azure AD**) to **Microsoft Entra ID**. For details regarding this change, refer to New name for Azure Active Directory. This is an ongoing effort, so you might still encounter instances where there is a mismatch between the lab instruction and the elements of the interface as you step through individual exercises. Take this into considerations (in particular, in this lab, the **Microsoft Entra Connect** designates the new name of **Azure Active Directory Connect** and the term **Azure Active Directory** is still used when configuring the service connection point in task 4 of exercise 1).

> **Important**: Activating a Microsoft Entra ID P2 trial requires providing credit card information. For this reason, this exercise is entirely optional. Instead, course instructors might choose to demonstrate this

> functionality to students.

Exercise 1: Prepare for Microsoft Entra-based Conditional Access for Azure Virtual Desktop

The main tasks for this exercise are as follows:

1. Configure Microsoft Entra Premium P2 licensing
2. Configure Microsoft Entra Multi-Factor Authentication (MFA)
3. Register a user for Microsoft Entra MFA
4. Configure hybrid Microsoft Entra join
5. Trigger Microsoft Azure Active Directory Connect delta synchronization

Task 1: Configure Microsoft Entra Premium P2 licensing

> **Note**: Premium P1 or P2 licensing of Microsoft Entra is required in order to implement Microsoft Entra Conditional Access. You will use a 30-day trial for this lab.

1. From your lab computer, start a web browser, navigate to the Azure portal, and sign in by providing a Microsoft Entra credentials of a user account with the Owner role in the subscription you will be using in this lab and the Global Administrator role in the Microsoft Entra tenant associated with that subscription.

   > **Important**: Ensure that you are using a work or school account, **not** a Microsoft account.

2. In the Azure portal, search for and select **Azure Active Directory** to navigate to the Microsoft Entra tenant associated with the Azure subscription you are using for this lab.

3. On the Azure Active Directory blade, in the vertical menu bar on the left side, in the **Manage** section, click **Users**.

4. On the **Users | All users (Preview)** blade, select **aduser5**.

5. On the **aduser5 | Profile** blade, in the toolbar, click **Edit**, in the **Settings** section, in the **Usage location** dropdown list, select country where the lab environment is located and, in the toolbar, click **Save**.

6. On the **aduser5 | Profile** blade, in the **Identity** section, identify the user principal name of the **aduser5** account.

   > **Note**: Record this value. You will need it later in this lab.

7. On the **Users | All users (Preview)** blade, select the user account you used to sign at the beginning of this task and repeat the previous step in case your account does not have the **Usage location** assigned.

   > **Note**: The **Usage location** property must be set in order to assign an Microsoft Entra Premium P2 licenses to user accounts.

8. On the **Users | All users (Preview)** blade, select the **aadsyncuser** user account and identify its user principal name.

   > **Note**: Record this value. You will need it later in this lab.

9. In the Azure portal, navigate back to the **Overview** blade of the Microsoft Entra tenant and, in the vertical menu bar on the left side, in the **Manage** section, click **Licenses**.
10. On the **Licenses | Overview** blade, in the vertical menu bar on the left side, in the **Manage** section, click **All products**.
11. On the **Licenses | All products** blade, in the toolbar, click **+ Try/Buy**.
12. On the **Activate** blade, click **Free trial** in the **MICROSOFT ENTRA ID P2** section and then click **Activate** and follow prompts to complete the activation process.
13. On the **Licenses - All products** blade, select the **Enterprise Mobility + Security E5** entry.
14. On the **Enterprise Mobility + Security E5** blade, in the toolbar, click **+ Assign**.
15. On the **Assign license** blade, click **Add users and groups**, on the **Add users and groups** blade, select **aduser5** and your user account, and click **Select**.
16. Back on the **Assign license** blade, click **Assignment options**, on the **Assignment options** blade, verify that all options are enabled, click **Review + assign**, click **Assign**.

Task 2: Configure Microsoft Entra Multi-Factor Authentication (MFA)

1. On your lab computer, in the web browser displaying the Azure portal, navigate back to the **Overview** blade of the Microsoft Entra tenant and, in the vertical menu on the left side, in the **Manage** section, click **Security**.
2. On the **Security | Getting started** blade, in the vertical menu on the left side, in the **Protect** section, click **Identity Protection**.
3. On the **Identity Protection | Overview** blade, in the vertical menu on the left side, in the **Protect** section, click **Multifactor authentication registration policy** (if necessary, refresh the web browser page).
4. On the **Identity Protection | Multifactor authentication registration policy** blade, in the **Assignments** section of the **Multi-factor authentication registration policy**, click **All users**, on the **Include** tab, click the **Select individuals and groups** option, on the **Select users**, click **aduser5**, click **Select**, at the bottom of the blade, set the **Enforce policy** switch to **On**, and click **Save**.

Task 3: Register a user for Microsoft Entra MFA

1. On your lab computer, open an **InPrivate** web browser session, navigate to the Azure portal, and sign in by providing the **aduser5** user principal name you identified earlier in this exercise and the password you set when creating this user account.
2. When presented with the message **More information required**, click **Next**. This will automatically redirect your browser to the **Microsoft Authenticator** page.
3. On the **Additional security verification** page, in the **Step 1: How should we contact you?** section, select your preferred authentication method and follow instructions to complete the registration process.
4. On the Azure portal page, in the upper right corner, click the icon representing the user avatar, click **Sign out**, and close the **In private** browser window.

Task 4: Configure hybrid Microsoft Entra join

> **Note**: This functionality can be leveraged to implement additional security when setting up Conditional Access for devices based on their Microsoft Entra join status.

1. On the lab computer, in the web browser displaying the Azure portal, search for and select **Virtual machines** and, from the **Virtual machines** blade, select **az140-dc-vm11**.
2. On the **az140-dc-vm11** blade, select **Connect**, in the drop-down menu, select **Connect via Bastion**.
3. When prompted, provde the following credentials and select **Connect**:

Setting	Value
User Name	**Student**
Password	**Pa55w.rd1234**

4. Within the Bastion session to **az140-dc-vm11**, in the **Start** menu, expand the **Azure AD Connect** folder and select **Azure AD Connect**.

   > **Note** If you receive a failure error window that the Sync Service is not running, go to PowerShell command window and enter **Start-Service "ADSync"**, and then try the previous step again.

5. On the **Welcome to Azure AD Connect** page of the **Microsoft Azure Active Directory Connect** window, select **Configure**.
6. On the **Additional tasks** page in the **Microsoft Azure Active Directory Connect** window, select **Configure device options** and select **Next**.
7. On the **Overview** page in the **Microsoft Azure Active Directory Connect** window, review the information regarding **Hybrid Microsoft Entra join** and **Device writeback** and select **Next**.
8. On the **Connect to Microsoft Entra** page in the **Microsoft Azure Active Directory Connect** window, authenticate by using the credentials of the **aadsyncuser** user account you created in an earlier lab and select **Next**.
9. On the **Device options** page in the **Microsoft Azure Active Directory Connect** window, ensure that the **Configure Hybrid Azure AD join** option is selected and select **Next**.
10. On the **Device operating systems** page in the **Microsoft Azure Active Directory Connect** window, select the **Windows 10 or later domain-joined devices** checkbox and select **Next**.
11. On the **SCP configuration** page in the **Microsoft Azure Active Directory Connect** window, select the checkbox next to the **adatum.com** entry, in the **Authentication Service** drop-down list, select the **Azure Active Directory** entry, and select **Add**.
12. When prompted, in the **Enterprise Admin Credentials** dialog box, specify the following credentials, and select **OK**:

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

13. Back on the **SCP configuration** page in the **Microsoft Azure Active Directory Connect** window, select **Next**.

14. On the **Ready to configure** page in the **Microsoft Azure Active Directory Connect** window, select **Configure** and, once the configuration completes, select **Exit**.

15. Within the Bastion session to **az140-dc-vm11**, start **Windows PowerShell ISE** as administrator.

16. Within the Bastion session to **az140-dc-vm11**, from the **Administrator: Windows PowerShell ISE** console, run the following to move the **az140-cl-vm11** computer account to the **WVDClients** organizational unit (OU):

    ```
    Move-ADObject -Identity "CN=az140-cl-vm11,CN=Computers,DC=adatum,DC=com" -
    TargetPath "OU=WVDClients,DC=adatum,DC=com"
    ```

17. Within the Bastion session to **az140-dc-vm11**, in the **Start** menu, expand the **Azure AD Connect** folder and select **Azure AD Connect**.

18. On the **Welcome to Azure AD Connect** page of the **Microsoft Azure Active Directory Connect** window, select **Configure**.

19. On the **Additional tasks** page in the **Microsoft Azure Active Directory Connect** window, select **Customize synchronization options** and select **Next**.

20. On the **Connect to Microsoft Entra** page in the **Microsoft Azure Active Directory Connect** window, authenticate by using the credentials of the **aadsyncuser** user account you created in the previous exercise and select **Next**.

21. On the **Connect your directories** page in the **Microsoft Azure Active Directory Connect** window, select **Next**.

22. On the **Domain and OU filtering** page in the **Microsoft Azure Active Directory Connect** window, ensure that the option **Sync selected domains and OUs** is selected, expand the **adatum.com** node, ensure that the checkbox next to the **ToSync** OU is selected, select the checkbox next to the **WVDClients** OU, and select **Next**.

23. On the **Optional features** page in the **Microsoft Azure Active Directory Connect** window, accept the default settings, and select **Next**.

24. On the **Ready to configure** page in the **Microsoft Azure Active Directory Connect** window, ensure that the checkbox **Start the synchronization process when configuration completes** is selected and select **Configure**.

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

Task 5: Trigger Microsoft Azure Active Directory Connect full synchronization

1. From your lab computer, in the Azure portal, search for and select **Virtual machines** and, from the **Virtual machines** blade, select the **az140-cl-vm11** entry. This will open the **az140-cl-vm11** blade.
2. Within the **az140-cl-vm11** blade, select **Restart** and then wait until the **Successfully restarted virtual machine** notification appears.
3. Within the Bastion session to **az140-dc-vm11**, switch to the **Administrator: Windows PowerShell ISE** window.
4. Within the Bastion session to **az140-dc-vm11**, from the **Administrator: Windows PowerShell ISE** console pane, run the following to trigger Microsoft Azure Active Directory Connect full synchronization:

```
Import-Module -Name "C:\Program Files\Microsoft Azure AD Sync\Bin\ADSync"
Start-ADSyncSyncCycle -PolicyType Initial
```

5. Within the Bastion session to **az140-dc-vm11**, start Microsoft Edge and navigate to the Azure portal. When prompted, sign in by using the Microsoft Entra credentials of the user account with the Global Administrator role in the Microsoft Entra tenant associated with the Azure subscription you are using in this lab.
6. Within the Bastion session to **az140-dc-vm11**, in the Microsoft Edge window displaying the Azure portal, search for and select **Microsoft Entra ID** to navigate to the Microsoft Entra tenant associated with the Azure subscription you are using for this lab.
7. On the Microsoft Entra ID blade, in the vertical menu bar on the left side, in the **Manage** section, click **Devices**.
8. On the **Devices | All devices** blade, review the list of devices and verify that the **az140-cl-vm11** device is listed with the **Microsoft Entra hybrid joined** entry in the **Join type** column.

> **Note**: You might have to wait a few minutes for the synchronization to take efect before the device appears in the Azure portal.

Exercise 2: Implement Microsoft Entra-based Conditional Access for Azure Virtual Desktop

The main tasks for this exercise are as follows:

1. Create an Microsoft Entra-based Conditional Access policy for all Azure Virtual Desktop connections
2. Test the Microsoft Entra-based Conditional Access policy for all Azure Virtual Desktop connections
3. Modify the Microsoft Entra-based Conditional Access policy to exclude hybrid Microsoft Entra joined computers from the MFA requirement
4. Test the modified Microsoft Entra-based Conditional Access policy

Task 1: Create an Microsoft Entra-based Conditional Access policy for all Azure Virtual Desktop connections

> **Note**: In this task, you will configure an Microsoft Entra-based Conditional Access policy that requires MFA to sign in to a Azure Virtual Desktop session. The policy will also enforce reauthentication after

> the first 4 hours following a successful authentication.

1. On your lab computer, in the web browser displaying the Azure portal, navigate back to the **Overview** blade of the Microsoft Entra tenant and, in the vertical menu on the left side, in the **Manage** section, click **Security**.

2. On the **Security | Getting started** blade, in the vertical menu on the left side, in the **Protect** section, click **Conditional Access**.

3. On the **Conditional Access | Policies** blade, in the toolbar, click **+ New policy**.

4. On the **New** blade, configure the following settings:

    - In the **Name** text box, type **az140-31-wvdpolicy1**
    - In the **Assignments** section, select the **Users or workload identities** option, in the **What does this policy apply to?** drop-down list, ensure that **Users and groups** is selected, in the **Select Users and groups** section, select the **Users and groups** checkbox, on the **Select** blade, click **aduser5**, and then click **Select**.
    - In the **Assignments** section, click **Cloud apps or actions**, ensure that in the **Select what this policy applies to** switch, the **Cloud apps** option is selected, click the **Select apps** option, on the **Select** blade, in the **Search** textbox, enter **Azure Virtual Desktop**, in the listing of results, select the checkbox next to the **Azure Virtual Desktop** entry, in the **Search** textbox, enter **Microsoft Remote Desktop**, select the checkbox next to the **Microsoft Remote Desktop** entry, and click **Select**.

    > **Note**: Azure Virtual Desktop (app ID 9cdead84-a844-4324-93f2-b2e6bb768d07) is used when the user subscribes to a feed and authenticates to the Azure Virtual Desktop Gateway during a connection. Microsoft Remote Desktop (app ID a4a365df-50f1-4397-bc59-1a1564b8bb9c) is used when the user authenticates to the session host when single sign-on is enabled.

    - In the **Assignments** section, click **Conditions**, click **Client apps**, on the **Client apps** blade, set the **Configure** switch to **Yes**, ensure that both the **Browser** and **Mobile apps and desktop clients** checkboxes are selected, and click **Done**.
    - In the **Access controls** section, click **Grant**, on the **Grant** blade, ensure that the **Grant access** option is selected, select the **Require multi-factor authentication** checkbox and click **Select**.
    - In the **Access controls** section, click **Session**, on the **Session** blade, select the **Sign-in frequency** checkbox, in the first textbox, type **4**, in the **Select units** dropdown list, select **Hours**, leave the **Persistent browser session** checkbox cleared, and click **Select**.
    - Set the **Enable policy** switch to **On**.

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

Task 2: Test the Microsoft Entra-based Conditional Access policy for all Azure Virtual Desktop connections

1. On the lab computer and, in the web browser window displaying the Azure portal, open the **PowerShell** shell session within the **Cloud Shell** pane.

2. From the PowerShell session in the Cloud Shell pane, run the following to start the Azure Virtual Desktop session host Azure VMs you will be using in this lab:

```
Get-AzVM -ResourceGroup 'az140-21-RG' | Start-AzVM
```

> **Note**: Wait until the command completes and all the Azure VMs in the **az140-21-RG** resource group are running.

3. On your lab computer, open an **InPrivate** web browser session, navigate to the Azure portal, and sign in by providing the **aduser5** user principal name you identified earlier in this exercise and the password you set when creating this user account.

> **Note**: Verify that you are not prompted to authenticate via MFA.

4. In the **InPrivate** web browser session, navigate to the Azure Virtual Desktop HTML5 web client page at https://rdweb.wvd.microsoft.com/arm/webclient.

> **Note**: Verify that this will automatically trigger authentication via MFA.

5. In the **Enter code** pane, type the code from the text message or authenticator app that you registered and select **Verify**.

6. On the **All Resources** page, click **Command Prompt**, on the **Access local resources** pane, clear the **Printer** checkbox, and click **Allow**.

7. When prompted, in the **Enter your credentials**, in the **User name** textbox type the user principal name of **aduser5** and, in the **Password** textbox, type the password you set when creating this user account and click **Submit**.

8. Verify that the **Command Prompt** Remote App was launched successfully.

9. In the **Command Prompt** Remote App window, at the command prompt, type **logoff** and press the **Enter** key.

10. Back on the **All Resources** page, in the upper right corner, click **aduser5**, in the dropdown menu, click **Sign Out**, and close the **InPrivate** web browser window.

Task 3: Modify the Microsoft Entra-based Conditional Access policy to exclude hybrid Microsoft Entra joined computers from the MFA requirement

> **Note**: In this task, you will modify the Microsoft Entra-based Conditional Access policy that requires MFA to sign in to a Azure Virtual Desktop session such that connections originating from Microsoft Entra joined computers will not require MFA.

1. On your lab computer, in the browser window displaying the Azure portal, on the **Conditional Access | Policies** blade, click the entry representing the **az140-31-wvdpolicy1** policy.
2. On the **az140-31-wvdpolicy1** blade, in the **Access controls** section, click **Grant**, on the **Grant** blade, select the **Require multi-factor authentication** and **Require Hybrid Microsoft Entra joined device** checkboxes, ensure that the **Require one of the selected controls** option is enabled, and click **Select**.
3. On the **az140-31-wvdpolicy1** blade, click **Save**.

> **Note**: It might take a few minutes for the policy to take effect.

Task 4: Test the modified Microsoft Entra-based Conditional Access policy

1. On your lab computer, in the browser window displaying the Azure portal, search for and select **Virtual machines** and, on the **Virtual machines** blade, select the **az140-cl-vm11** entry.
2. On the **az140-cl-vm11** blade, select **Connect**, in the drop-down menu, select **Bastion**, on the **Bastion** tab of the **az140-cl-vm11 | Connect** blade, select **Use Bastion**.
3. When prompted, provde the following credentials and select **Connect**:

Setting	Value
User Name	**Student@adatum.com**
Password	**Pa55w.rd1234**

4. Within the Bastion session to **az140-cl-vm11**, start Microsoft Edge and navigate to navigate to the Azure Virtual Desktop HTML5 web client page at https://rdweb.wvd.microsoft.com/arm/webclient.

> **Note**: Verify that this time you will not be prompted to authenticate via MFA. This is because **az140-cl-vm11** is Hybrid Microsoft Entra-joined.

5. On the **All Resources** page, double-click **Command Prompt**, on the **Access local resources** pane, clear the **Printer** checkbox, and click **Allow**.
6. When prompted, in the **Enter your credentials**, in the **User name** textbox type the user principal name of **aduser5** and, in the **Password** textbox, type the password you set when creating this user account and click **Submit**.
7. Verify that the **Command Prompt** Remote App was launched successfully.
8. In the **Command Prompt** Remote App window, at the command prompt, type **logoff** and press the **Enter** key.
9. Back on the **All Resources** page, in the upper right corner, click **aduser5**, in the dropdown menu, click **Sign Out**.
10. Within the Bastion session to **az140-cl-vm11**, click **Start**, in the vertical bar directly above the **Start** button, click the icon representing the signed in user account, and, in the pop-up menu, click **Sign out**.

Exercise 3: Stop and deallocate Azure VMs provisioned and used in the lab

The main tasks for this exercise are as follows:

1. Stop and deallocate Azure VMs provisioned and used in the lab

> **Note**: In this exercise, you will deallocate the Azure VMs provisioned and used in this lab to minimize the corresponding compute charges

Task 1: Deallocate Azure VMs provisioned and used in the lab

1. Switch to the lab computer and, in the web browser window displaying the Azure portal, open the **PowerShell** shell session within the **Cloud Shell** pane.

2. From the PowerShell session in the Cloud Shell pane, run the following to list all Azure VMs created and used in this lab:

```
Get-AzVM -ResourceGroup 'az140-21-RG'
```

3. From the PowerShell session in the Cloud Shell pane, run the following to stop and deallocate all Azure VMs you created and used in this lab:

```
Get-AzVM -ResourceGroup 'az140-21-RG' | Stop-AzVM -NoWait -Force
```

> **Note**: The command executes asynchronously (as determined by the -NoWait parameter), so while you will be able to run another PowerShell command immediately afterwards within the same PowerShell session, it will take a few minutes before the Azure VMs are actually stopped and deallocated.