Seneca

CPO550 - Lab 08:

Configure Conditional Access policies for AVD

Student Lab Manual

Fall 2026

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 ID (Microsoft Entra) conditional access.

Objectives

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

Lab requirements

- **Lab 01:** Deploy host pools and session hosts by using the Azure portal

Submission Requirements

Take a screenshot whenever you see the camera icon ( ) alongside task instructions. For better visibility, don't take screenshots in the dark mode.
Compile all screenshots into a single Word (.docx) or PDF file in the order of each task and provide a brief explanation of the significance of each screenshot. Underline or highlight all important information as shown in the provided sample screenshots at the end of this lab manual. Ensure your Odl_user account is clearly visible and underlined in every screenshot. Do not include the lab instructions in your submission.

Important: Use the provided template in the Blackboard to submit your lab reports.

Instructions

Exercise 1: Prepare and Implement 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. Create a Microsoft Entra-based Conditional Access policy for all Azure Virtual Desktop connections
5. Test the Microsoft Entra-based Conditional Access policy for all Azure Virtual Desktop connections
6. Summary Questions

Task 1: Configure Microsoft Entra Premium P2 licensing

Note: Premium P1 or P2 licensing of Microsoft Entra is required to implement Microsoft Entra Conditional Access. P2 license should be active on your account before attempting this lab.

1. From your local computer, start a web browser, navigate to the Azure portal, and sign in by providing your **Odl_user** credentials.

2. In 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.

3. On the Microsoft Entra ID blade, in the vertical menu bar on the left side, in the **Manage** section, click **Users**.

4. On the **Users** blade, select **cpoF67-User2**.

5. On the **cpoF67-User2** blade, in the toolbar, click **Edit Properties**, select the **Settings** tab, in the **Usage location** dropdown list, select country where the lab environment is located and, in the toolbar, click **Save**.

6. On the **cpoF67-User2** blade, in the **Overview**|**Basic info** section, identify the user principal name of the **cpoF67-User2** account.

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

7. On the **Users | All users** blade, select your **ODL_User...** account 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 a Microsoft Entra Premium P2 licenses to user accounts.

8. 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**.

9. On the **Licenses | Overview** blade, in the vertical menu bar on the left side, in the **Manage** section, click **All products**.

10. On the **Licenses | All products** blade, under manage, in the toolbar select **All products**.

Note: The Microsoft Entra P2 license will be available in your Odl account during the second half of the semester. I will provide more information about this in class.

11. For adding, removing, and reprocessing licensing assignments go to Microsoft 365 Admin Center. M365 Admin Center

12. On the **Microsoft 365 Admin Center** blade click **Microsoft Entra ID P2**. Select your **ODL_User account** and from the top menue select **Unassign lincenses.**

13. On the same page click **+ Assign licenses.** From the **Assign licenses to users** select and assign **cpoF67-User2.**

14. Back on the **License details** blade, click on **cpoF67-User2**, verify that all options are enabled.

15. From the All users blade, click on cpoF67-User2 and from the licenses tab verify the license **state** is **Acitve**.

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

1. From 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 | Dashboard** blade, in the vertical menu on the left side, in the **Protect** section, click **MFA registration policy** (if necessary, refresh the web browser page).
4. On the **Identity Protection | MFA registration policy** blade, in the **Assignments** section click **All users**, on the **Include** tab, click the **Select individuals and groups** option, on the **Select users**, click **cpoF67-User2**, 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 local computer, open an **InPrivate** web browser session, navigate to the Azure portal, and sign in by providing the **cpoF67-User2** 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: Create a Microsoft Entra-based Conditional Access policy for all Azure Virtual Desktop connections

Note: In this task, you will configure a Microsoft Entra-based Conditional Access policy that requires MFA to sign in to an Azure Virtual Desktop session. The policy will also enforce reauthentication after the first 4 hours following a successful authentication.

1. On your local 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**.

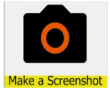
2. On the **Security | Getting started** blade, in the vertical menu on the left side, in the **Protect** section, click **Conditional Access**.

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

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

    - In the **Name** text box, type **<studentID>-F67-avdpolicy1**
    - In the **Assignments** section, select the **Users or agents** 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 **cpoF67-User2**, and then click **Select**.
    - In the **Assignments** section, click **Target resources**, ensure that in the Select **what this policy applies to**, the **Resources (formerly Cloud apps)** option is selected, click the **Select resources** option, on the **Select specific resource** blade, in the **Search** textbox, enter **Azure Virtual Desktop**, in the listing of results, select the checkbox next to the **Azure Virtual Desktop** entry, and then in the **Search** textbox, enter **Microsoft Remote Desktop**, select the checkbox next to the **Microsoft Remote Desktop** entry, and click **Select**.
    - 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 5: Test the Microsoft Entra-based Conditional Access policy for all Azure Virtual Desktop connections

1. On the local 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 AVD session hosts:

```
Get-AzVM -ResourceGroup <sName> -cpoF67-21e-RG' | Start-AzVM
```

Note: Wait until the command completes and all the Azure VMs are running.

3. On your local computer, open an **InPrivate** web browser session. 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.

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

5. On the **<sName>-cpoF67-21-ws1** page, 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 **cpoF67-User2** and its **Password.**

7. Verify that the **Command Prompt** Remote App was launched successfully. Type **whoami** and press the **Enter** key. Now type **hostname** and press the **Enter** key. Take your screenshot.

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

9. Back on the **<sName>-cpoF67-21-ws1** page, in the upper right corner, click **cpoF67-User2**, in the dropdown menu, click **Sign Out**, and close the **InPrivate** web browser window.

Review Questions:

Please answer the following questions in your own words and submit with your lab report:

1. Why is assigning a **Microsoft Entra Premium P2 license** necessary before configuring Conditional Access policies, and what limitations would you face without it?

2. In this lab, Multi-Factor Authentication (MFA) was enforced for Azure Virtual Desktop access. How does MFA improve security specifically in a remote desktop environment, and what types of attacks does it help prevent?

3. During testing, you verified that MFA was triggered when accessing the AVD web client. If MFA did **not** trigger as expected, what are two possible misconfigurations you would investigate, and why?

Course Labs Reflection: *(Note: Answer based on your own personal experience doing the lab; do not use general or textbook statements)*

4. **Question 1:** After completing all Azure Virtual Desktop labs in this course, reflect on your overall experience with the AVD service. What are the most important concepts or skills you gained from these labs, and how do you think they would apply in a real-world cloud or IT environment?

Important: Lab Cleanup Instructions

Congratulations on completing your final lab for this course!

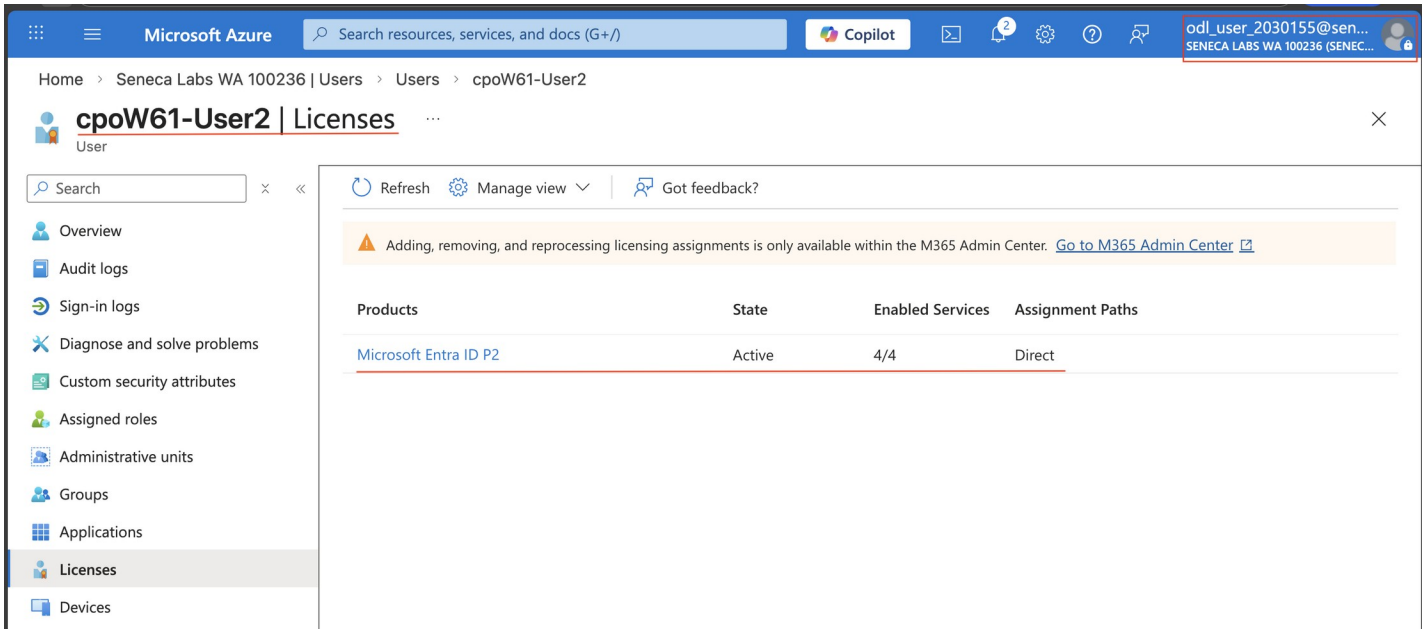
To minimize charges against your Azure credits, please ***delete all your resources***. You can do this efficiently by deleting your individual Resource Groups.

Note: Do NOT delete the default resource group: **ODL-seneca-lab**.

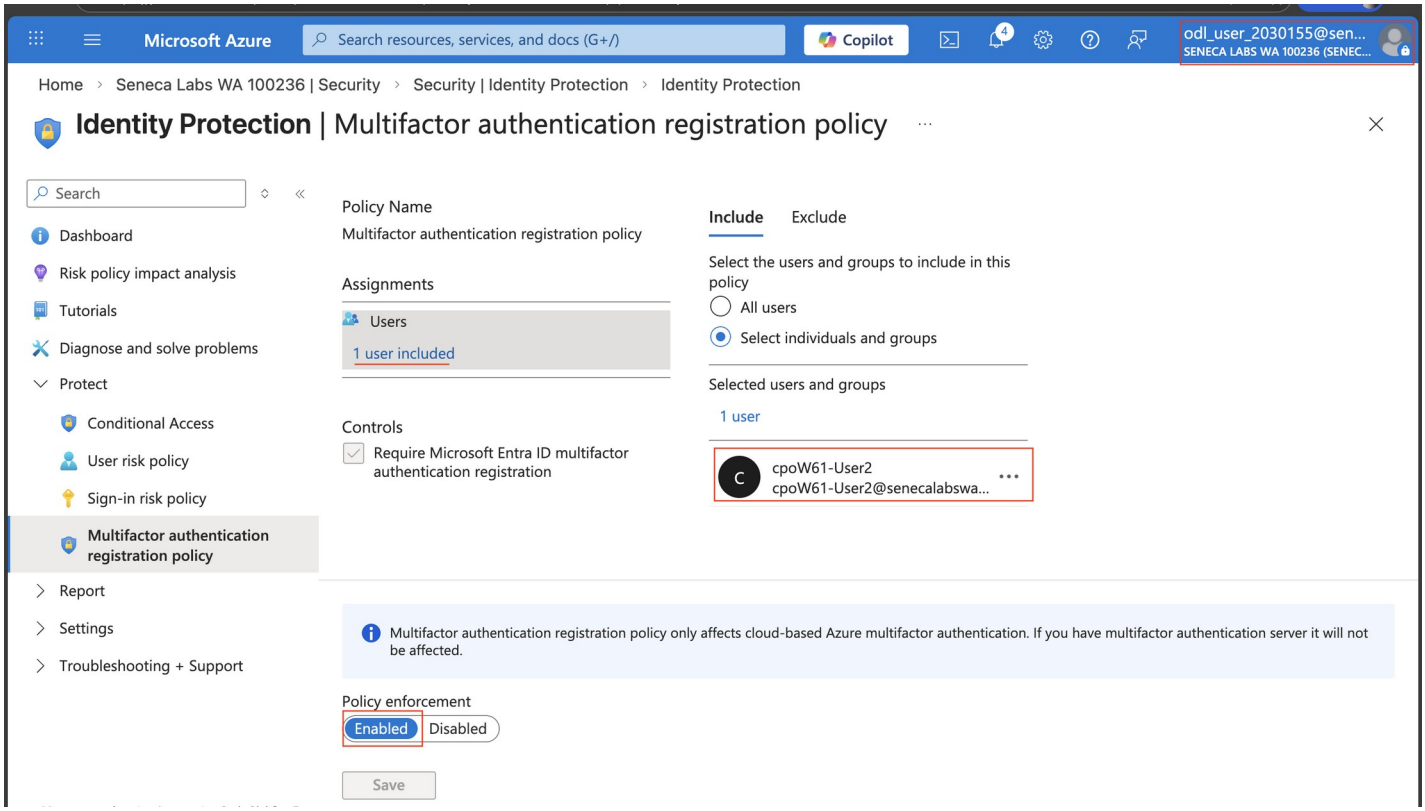
Sample Screenshots

Please ensure that all marked information in the samples is included, clearly visible, and underlined in your screenshots.

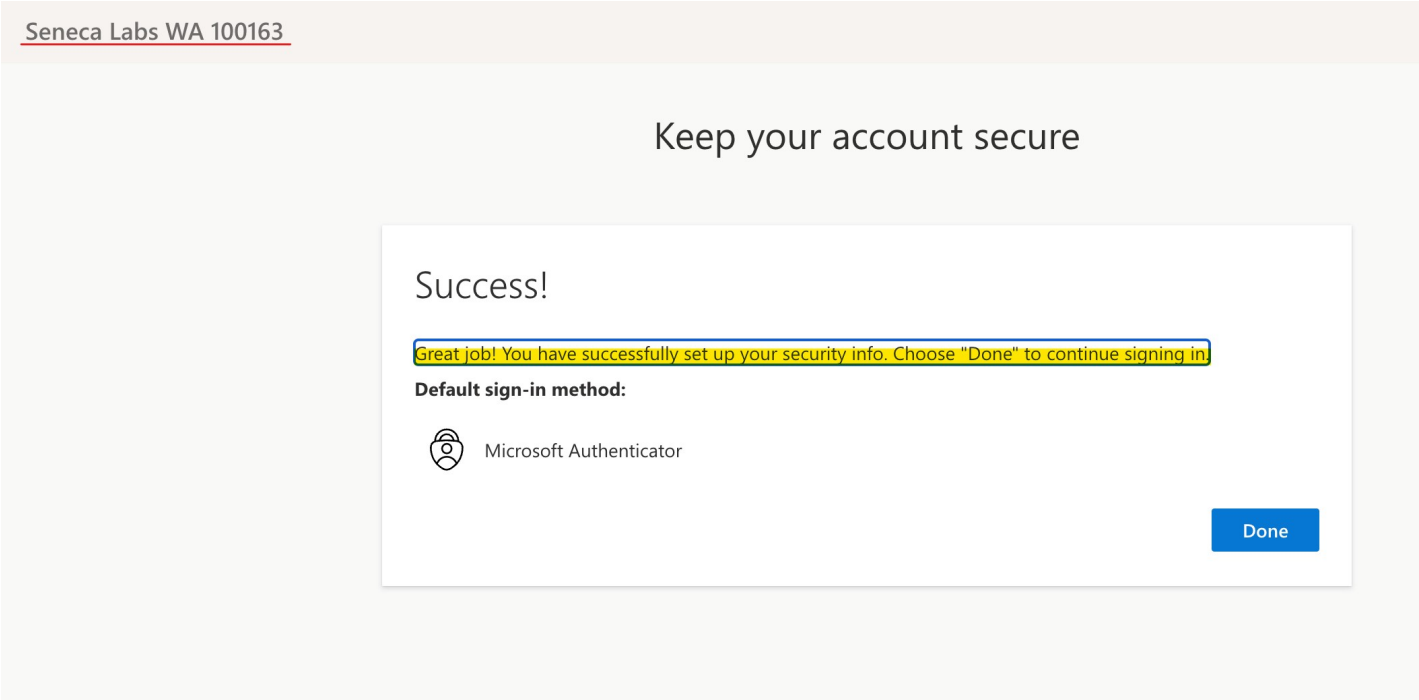
Task 1:



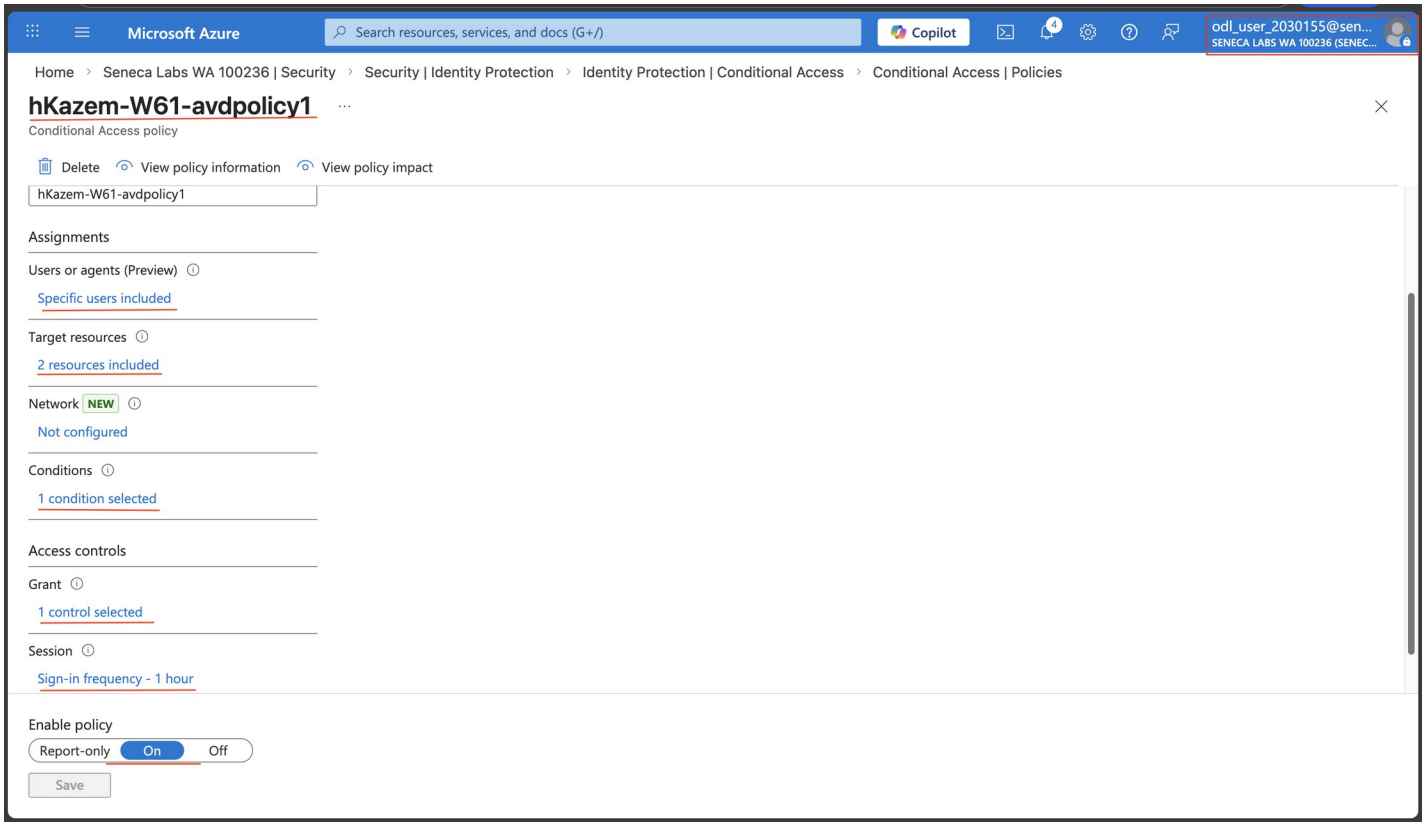
Task 2:



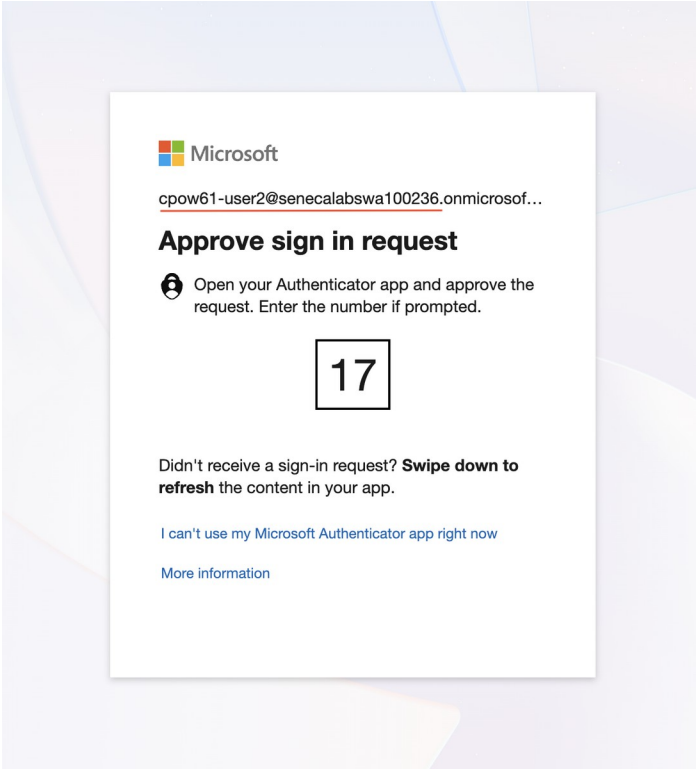
Task 3:


Seneca Labs WA 100163
Keep your account secure
Success!
Great job! You have successfully set up your security info. Choose "Done" to continue signing in.
Default sign-in method:
Microsoft Authenticator
Done

Task 4:


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
odl_user_2030155@sen...
SENECA LABS WA 100236 (SENEC...
Home
Seneca Labs WA 100236 | Security
Security | Identity Protection
Identity Protection | Conditional Access
Conditional Access | Policies
hKazem-W61-avdpolicy1
Conditional Access policy
Delete
View policy information
View policy impact
hKazem-W61-avdpolicy1
Assignments
Users or agents (Preview)
Specific users included
Target resources
2 resources included
Network NEW
Not configured
Conditions
1 condition selected
Access controls
Grant
1 control selected
Session
Sign-in frequency - 1 hour
Enable policy
Report-only
On
Off
Save

Task 5(s3):



Task 5(s7):