



CPO550 - Lab 04:

Connect to Azure Virtual Desktop Session Hosts

Student Lab Manual

Fall 2026

Lab scenario

You have an existing Azure Virtual Desktop environment containing Entra joined session hosts. You need to validate their functionality by connecting to them from a Windows 11 client which is not Microsoft Entra-joined or registered.

Objectives

- Validate the functionality of Microsoft Entra joined Azure Virtual Desktop session hosts by connecting to them from a Windows client which is not Microsoft Entra-joined or registered.

Lab requirements

- The lab 01: *Deploy host pools and session hosts by using the Azure portal* completed.
- The lab 02: *Manage host pools and session hosts by using the Azure portal* completed.

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: Validate the functionality of Microsoft Entra joined Azure Virtual Desktop session hosts by connecting to them from a Windows 11 client

The main tasks for this exercise are as follows:

1. Adjust RDP properties of the Azure Virtual Desktop host pool
2. Install Microsoft Remote Desktop client on a Windows 11 computer
3. Subscribe to an Azure Virtual Desktop workspace
4. Test Azure Virtual Desktop apps

Task 1: Adjust RDP properties of the Azure Virtual Desktop host pool

Note: The RDP settings you implemented in the previous lab provide the optimal user experience (via support for single sign-on), however, this requires additional changes described in [Configure single sign-on for Azure Virtual Desktop using Microsoft Entra ID authentication](#). Without these changes, by default, authentication is supported providing that the client computer satisfies one of the following criteria:

- It is Microsoft Entra joined to the same Microsoft Entra tenant as the session host
- It is Microsoft Entra hybrid joined to the same Microsoft Entra tenant as the session host
- It is Microsoft Entra registered to the same Microsoft Entra tenant as the session host

Since none of these criteria apply to the lab computer, it is necessary to add `targetisaadjoined:i:1` as a custom RDP property to the host pool.

1. If needed, 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 web browser displaying the Azure portal, on the **•sName• -cpoF67-hp1** Azure Virtual Desktop host pool page, in the vertical menu bar, in the **Settings** section, select the **RDP Properties** entry.
3. On the **•sName• -cpoF67-hp1 | RDP Properties** page, select the **Advanced** tab.
4. On the **Advanced** tab, in the **RDP Properties** text box, append the following string to the existing content (make sure to add a leading semicolon character (;) if needed to separate this string from the one which proceeds it:

```
targetisaadjoined:i:1
```

5. In the **RDP Properties** text box, remove the following string (if present) from the existing content (with its trailing semicolon character):

```
enablerdsaauth:i:value (for example: enablerdsaauth:i:1;)
```

6. On the **•sName• -cpoF67-hp1 | RDP Properties** page, select **Save**.



Task 2: Install Microsoft Remote Desktop client on a Windows 11 computer

Note: If you don't have a Windows 10/11 on your local computer, you can create a Virtual Machine (i.e. Client-VM) in a separate resource group (i.e. clientDemo-RG) and a separate Virtual Network (i.e. clientDemo-Vnet) and follow the instructions on the newly created Client-VM.

1. From your local computer, start a web browser, navigate to the [Connect to Azure Virtual Desktop with the Remote Desktop client for Windows](#) page, scroll down to the section **Download and install the Remote Desktop client (MSI)**, and select the [Windows 64-bit](#) link.

Note: If you're using a macOS device, then use **Windows App**.

2. Open File Explorer, navigate to the **Downloads** folder, and launch the installation of the newly downloaded MSI file.
3. In the **Remote Desktop Setup** window, when prompted, accept the terms of the licensing agreement and choose the option to **Install for all users of this machine**. If prompted, accept the User Account Control prompt to proceed with the installation.
4. Once the installation completes, ensure that the **Launch Remote Desktop when setup exits** checkbox is selected and select **Finish** to start the Microsoft Remote Desktop client.

Note: The [Remote Desktop Store app](#) for Windows doesn't support connecting to Microsoft Entra-joined session hosts.



Task 3: Subscribe to an AVD workspace and test Azure Virtual Desktop apps

1. On the lab computer, from the **Remote Desktop** client window, select **Subscribe** and, when prompted, sign in with your **cpoF67-User1@senecalabs.wa** credentials.

Note: Alternatively, in the **Remote Desktop** client window, select **Subscribe with URL**, in the **Subscribe to a Workspace** pane, in the **Email or Workspace URL**, type <https://client.wvd.microsoft.com/api/arm/feeddiscovery>, select **Next**, and, once prompted, sign in with the Microsoft Entra credentials.

2. Ensure that the **Remote Desktop** page displays only the **SessionDesktop** icon.

Note: This is expected, because the Microsoft Entra user account you selected was assigned in the first lab *Deploy host pools and session hosts by using the Azure portal* to the auto-generated **sName-cpoF67-hp1-DAG** desktop application group.

3. On the **Remote Desktop** page, right-click the **SessionDesktop** icon and, in the pop-up menu, select **Settings**.
4. In the **SessionDesktop** pane, turn off the **Use default settings** switch.
5. In the **Display settings** section, in the drop-down menu, select the entry **Select displays** and choose the displays you want to use for the session.
6. In the **SessionDesktop** pane, review the remaining options, including **Maximize to current displays**, **Single display when in windowed mode** and **Fit session to window**, without making any changes.

7. Close the **SessionDesktop** pane.
8. On the **Remote Desktop** page, double-click the **SessionDesktop** icon.
9. When prompted to sign in, in the **Windows Security** dialog box, enter the password of the first Microsoft Entra user account, which you used in this task to connect to the target Azure Virtual Desktop environment.

Note: Azure Virtual Desktop doesn't support signing in to Microsoft Entra ID with one user account, then signing in to Windows with a separate user account. Signing in with two different accounts at the same time can lead to users reconnecting to the wrong session host, incorrect or missing information in the Azure portal, and error messages appearing while using app attach or MSIX app attach.

Note: You will be automatically presented with the **SessionDesktop** window.

10. In the Remote Desktop session window, verify that you have full administrative access within the session (for example, select the **Windows** logo icon in the taskbar and then select the **Windows PowerShell(Admin)** item from the pop-up menu.



11. In the Command Prompt window, type **whoami /upn** and press the enter key. Then, type **ipconfig /all** and press the enter key.
12. Within the Remote Desktop session window, select the Windows logo icon in the taskbar, select the avatar icon representing the Microsoft Entra user account you used to sign in and, in the pop-up menu, select **Sign out**.

Note: This will automatically terminate the Remote Desktop session.

13. Back in the **Remote Desktop** window, select the ellipsis (...) icon to the right of **Title** select **Subscribe** when prompted, sign in with the credentials of the **cpoF67-User2@senecalabswa** account.
14. Ensure that the **Remote Desktop** page displays four icons, including Command Prompt, Microsoft Word, Microsoft Excel, Microsoft PowerPoint.

Note: This is expected, because the Microsoft Entra user account you selected was assigned in the first lab *Deploy host pools and session hosts by using the Azure portal (Entra ID)* to the **•sName• - cpoF67-hp1-Office365-RAG** and **•sName• - cpoF67-hp1-Utilities-RAG** application groups.

15. Double-click the Command Prompt icon.
16. When prompted to sign in, in the **Windows Security** dialog box, enter the password of the second Microsoft Entra user account you used to connect to the target Azure Virtual Desktop environment.
17. Verify that a **Command Prompt** window appears shortly afterwards.
18. In the Command Prompt window, type **whoami /upn** and press the enter key. Then, type **ipconfig /all** and press the enter key.
19. At the Command Prompt, type **logoff** and press the **Enter** key to log off from the current Remote App session.
20. Double-click the remaining icons on the **Remote Desktop** page to launch Microsoft Word, Microsoft Excel, and Microsoft PowerPoint making sure they all work properly.
21. Close each session window.
22. Back in the **Remote Desktop** window, select the ellipsis (...) icon to the right of each **user (user1 & user2)** workspace entry, select **Unsubscribe** and, when prompted to confirm, select **Continue**.



Task 4: Summary Questions

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

Question 1: Why is it important for an administrator to be able to validate access to Microsoft Entra joined session hosts from a client that is not Entra-joined, hybrid-joined, or registered? Describe at least two real-world scenarios where this capability matters?

Question 2: During the lab, you connected with two different Entra user accounts and saw different published resources (full desktop vs. specific apps). What does this teach you about how application group assignments can be used to design secure and flexible user experiences in Azure Virtual Desktop?

Question 3: In Task 3 you connected as two different Entra users and ran `whoami /upn` and `ipconfig /all` inside the session. Describe what information these commands reveal and why both users were connected to the same session host?

Lab Reflection

Question 4: Describe one moment in this lab where you felt your understanding of Azure Virtual Desktop “clicked” (for example, around RDP properties, workspace subscriptions, or app/desktop assignments), and explain how this insight would change the way you design or troubleshoot a real AVD deployment in the future.

Important Lab Cleanup Instructions

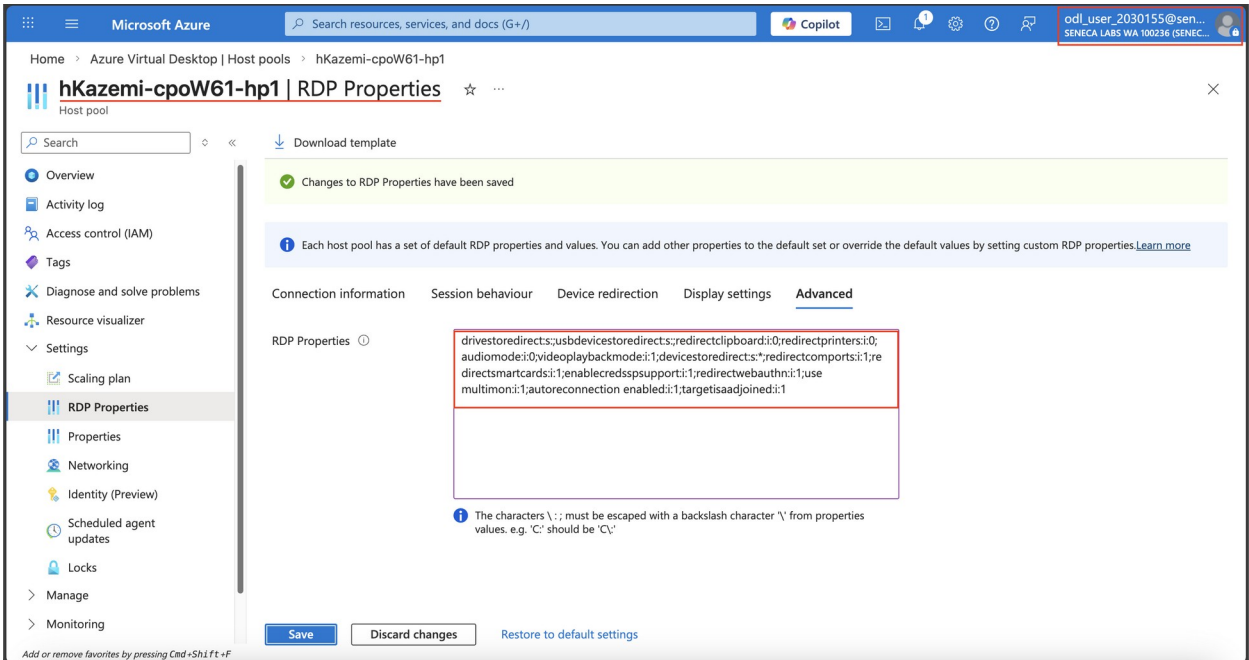
Do **NOT** delete any resources created in this lab. They are required for subsequent labs.

To minimize costs, stop all virtual machines (VMs) immediately. Restart them only when beginning the next lab.

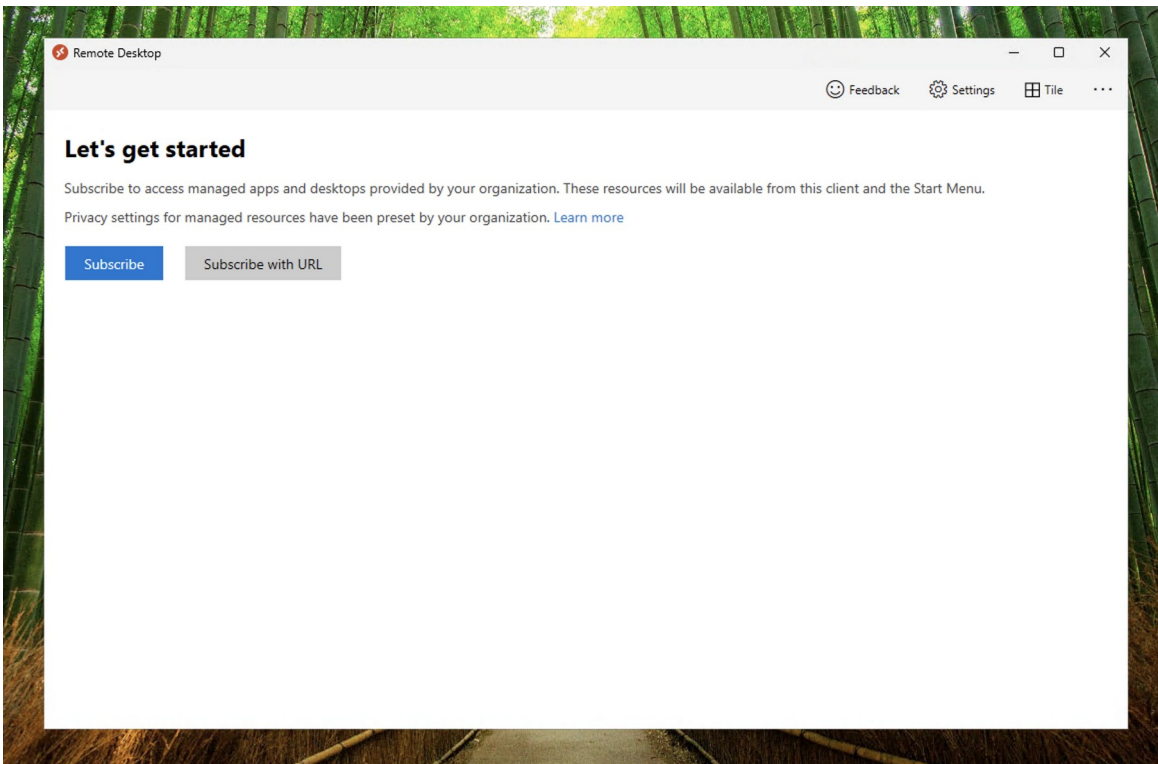
Sample Screenshots

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

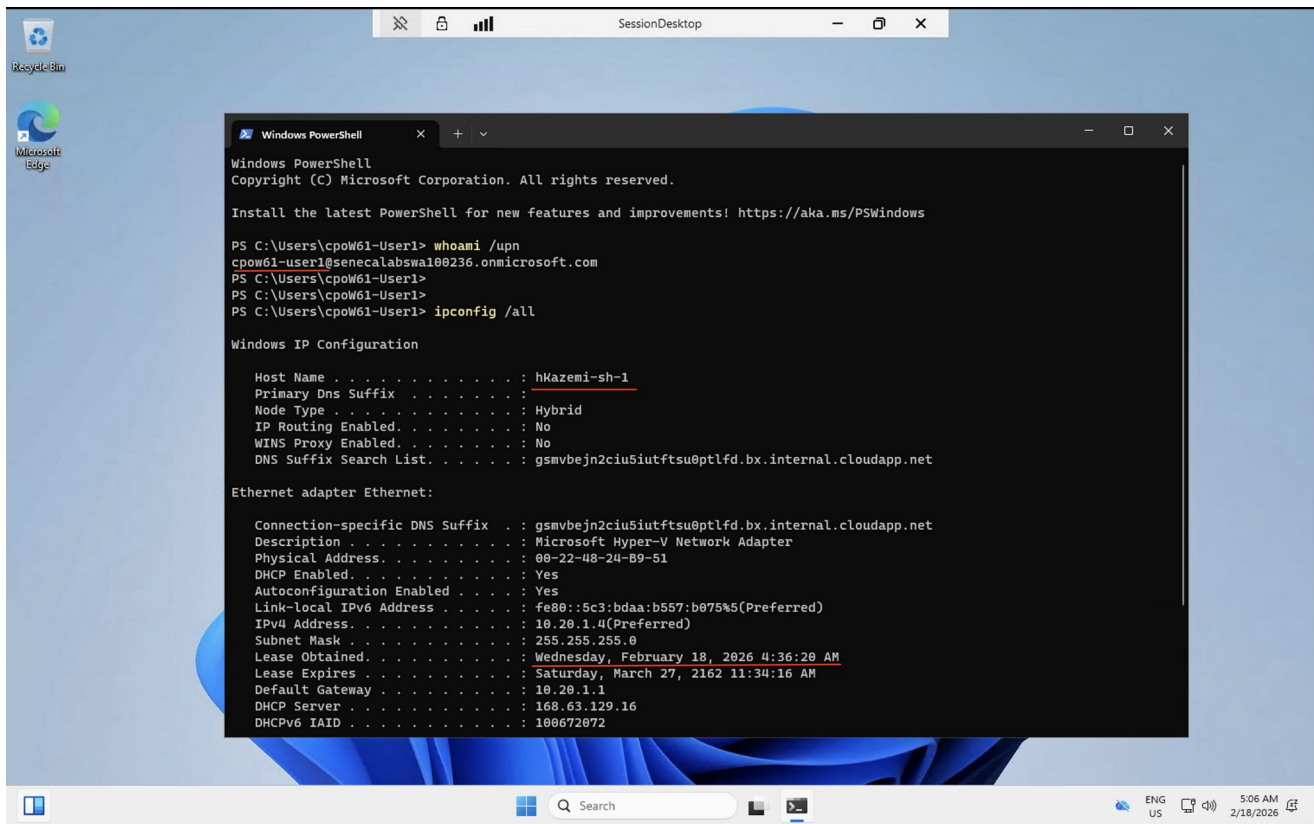
Task 1:



Task 2:



Task 3(10):



Task 3(18):

