# Lab - Connect to session hosts (Entra ID)

# Student lab manual

## Lab dependencies

- An Azure subscription you will be using in this lab.
- A Microsoft Entra user account with the Owner or Contributor role in the Azure subscription you will be using in this lab and with the permissions sufficient to join devices to the Entra tenant associated with that Azure subscription.
- The lab *Deploy host pools and session hosts by using the Azure portal (Entra ID)* completed
- The lab *Manage host pools and session hosts by using the Azure portal (Entra ID)* completed

## Estimated Time

20 minutes

## 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

After completing this lab, you will be able to:

- 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 files

- None

## 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 a 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 the lab computer, start a web browser, navigate to the Azure portal and sign in by providing credentials of a user account with the Owner role in the subscription you will be using in this lab.

   > **Note**: Use the credentials of the `User1-` account listed on the Resources tab on the right side of the lab session window.

2. In the web browser displaying the Azure portal, on the **az140-21-hp1** page, in the in the vertical menu bar, in the **Settings** section, select the **RDP Properties** entry.

3. On the **az140-21-hp1|RDP Properties** page, select the **Advanced** tab.

4. On the **Advanced** tab of the **az140-21-hp1|RDP Properties** page, 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 preceeds 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):

   ```
   enablerdsaadauth:i:value
   ```

6. On the **az140-21-hp1|Properties** page, select **Save**.

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

1. From the lab 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.

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 a Azure Virtual Desktop workspace**

1. On the lab computer, switch to the **Remote Desktop** client window, select **Subscribe** and, when prompted, sign in with the credentials of the `User1` Entra ID user account which you can locate on the **Resources** tab in the right pane of the lab interface window.

> **Note**: Select the user account which is the member of the Entra group with the **AVD-DAG** prefix.

> **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 (Entra ID)* to the auto-generated **az140-21-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. 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.

12. Back in the **Remote Desktop** window, select the ellipsis (. . .) icon to the right of the **az140-21-ws1** workspace entry, select **Unsubscribe** and, when prompted to confirm, select **Continue**.

13. In the **Remote Desktop** client window, select **Subscribe** and, when prompted, sign in with the credentials of the second Entra ID user account which you can locate on the **Resources** tab in the right pane of the lab interface window.

> **Note**: Select the user account which is the member of the Entra group with the **AVD-RemoteApp** prefix.

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 **az140-21-hp1-Office365-RAG** and **az140-21-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 **hostname** and press the **Enter** key to display the name of the computer on which the Command Prompt is running.

> **Note**: Verify that the displayed name starts with the **sh-** prefix.

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.

21. Close each session window.