

AZ-140 Agenda

Learning Path 1

1. Azure Virtual Desktop Architecture
2. Design the Azure Virtual Desktop architecture
3. Design for user identities and profiles


Learning Path 2

4. Implement and manage networking for AVD
5. Implement and manage storage for AVD
6. Create and configure host pools and session hosts for AVD
7. Create and manage session host image for AVD

Learning Path 3

8. Manage access for AVD
9. Manage security for AVD

Learning Path 4

10. Implement and manage FSLogix 
11. Configure user experience settings
12. Install and configure apps on a session host

Learning Path 5

13. Monitor and manage performance and health
14. Plan and implement updates, backups, and disaster recovery

Configure user experience settings



Introduction

After completing this module, you'll be able to:

- Connect to Azure Virtual Desktop with the Remote Desktop client for Windows
- Configure session timeout properties
- Configure user settings through group policies
- Implement the Start Virtual Machine on Connect feature
- Configure Universal Print
- Configure device redirections
- Troubleshoot Azure Virtual Desktop clients

Remote Desktop Client

Connect to Azure Virtual Desktop with the Remote Desktop client for Windows



Connect to Azure Virtual Desktop with the Remote Desktop client for Windows

Microsoft Remote Desktop client is used to connect to Azure Virtual Desktop to access desktops and applications.

There are three versions of the Remote Desktop client for Windows, which are all supported for connecting to Azure Virtual Desktop:

- **Standalone** download as an MSI installer.
- **Azure Virtual Desktop app** from the Microsoft Store. This is a preview version of the Remote Desktop client for Windows.
- **Remote Desktop app** from the Microsoft Store. This version is no longer being developed.

You can also connect to Azure Virtual Desktop with Windows App, a single app to securely connect you to Windows devices and apps from Azure Virtual Desktop, Windows 365, Microsoft Dev Box, Remote Desktop Services, and remote PCs.

Configure session timeout properties

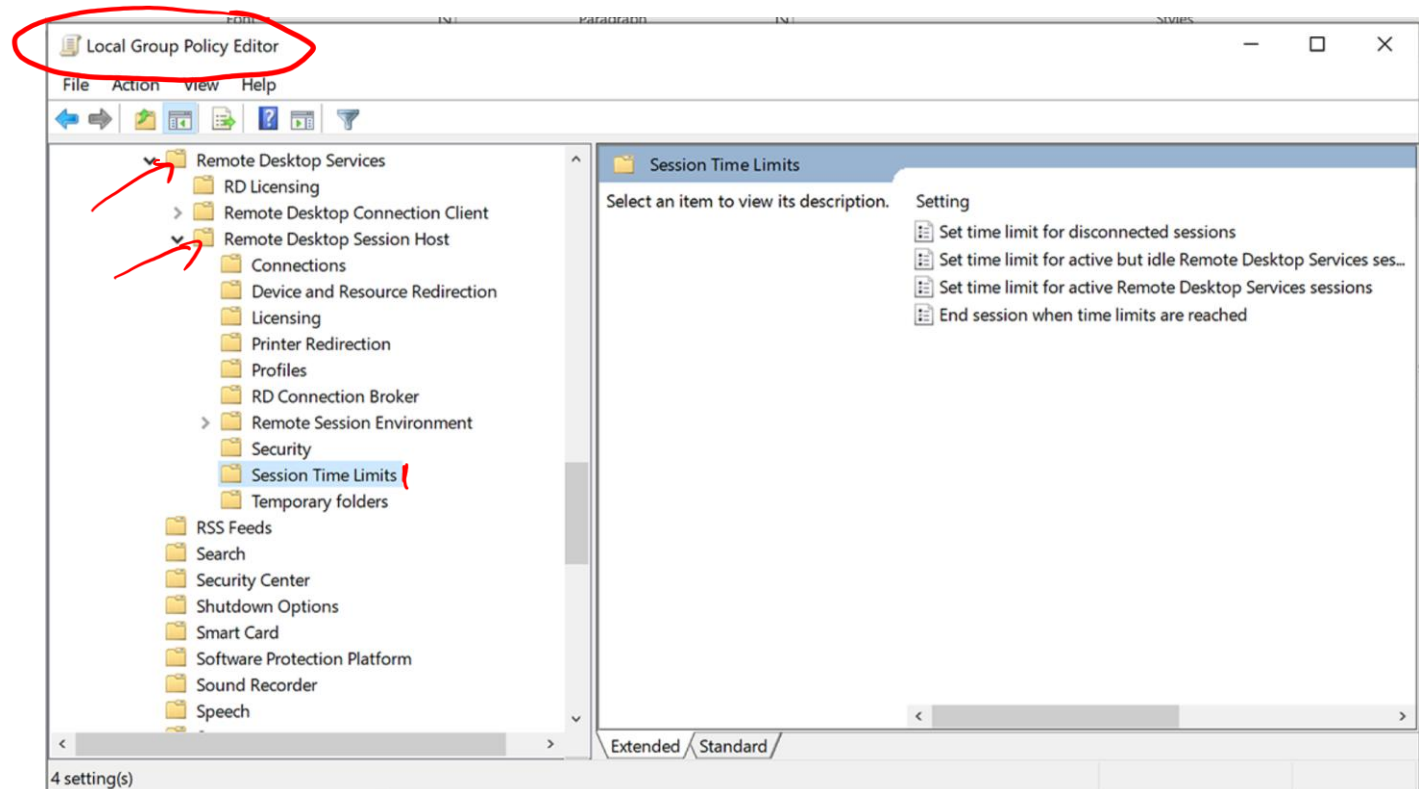


Configure session timeout properties

- Signing users out when they're inactive preserves resources and prevents access by unauthorized users.
- We recommend that timeouts balance user productivity and resource usage.
- For users that interact with stateless applications, consider more aggressive policies that turn off machines and preserve resources.


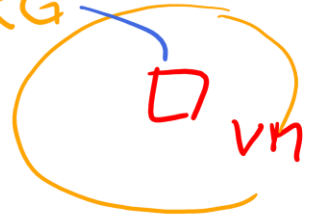
The timeout options for RDP are set on the servers in the Local Group Policy.

- Set time limit for disconnected sessions.
- Set time limit for active but idle Remote Desktop Services sessions.
- Set time limit for active Remote Desktop Services sessions.
- End Session when time limits are reached.



Implement the Start Virtual
Machine on Connect feature



AUD SP  — Role "VM start.." RG  VM = SH

Implement the Start Virtual Machine on Connect feature



Start VM on Connect lets you reduce costs by enabling end users to power on the virtual machines (VMs) used as session hosts only when they're needed. You can then power off VMs when they're not needed.



For personal host pools, **Start VM on Connect** only powers on an existing session host VM that is already assigned or can be assigned to a user.



For pooled host pools, **Start VM on Connect** only powers on a session host VM when none are turned on and more VMs are only be turned on when the first VM reaches the session limit.



The time it takes for a user to connect to a remote session on a session host that is powered off (deallocated) increases because the VM needs time to power on again.



You can enable **Start VM on Connect** for session hosts on Azure and Azure Stack HCI in personal or pooled host pools using the Azure portal, Azure PowerShell, or Azure CLI. Start VM on Connect is configured per host pool.

Configure Universal Print



Configure Universal Print

Universal Print runs entirely on Microsoft Azure. When it's deployed with Universal Print-compatible printers, it doesn't require any on-premises infrastructure.

Printers are installed as part of the user profile

Instead of printers being installed as a machine-wide resource (that is, all installed printers are visible to all users who sign in to the VM), each user sees only the printers they install.

Printers roam with user profiles

When user profiles are configured to roam, printers that the user installs on one VM will be automatically installed on other VMs the user signs into. This behavior also works when users remove printers from their profile.

Location-based printer search the local device location

Instead of finding printers close to the location of the VM where the user is signed in, location-based printer search will find printers based on the device the user is connecting from. This requires the location override functionality to be enabled.

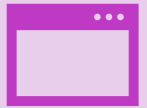
Configure device
redirections



Configure device redirections



Configuring device redirection for your Azure Virtual Desktop environment allows you to use printers, USB devices, microphones, and other peripheral devices in the remote session.



Some device redirections require changes to both Remote Desktop Protocol (RDP) properties and Group Policy settings.

Audio input (microphone) redirection

Set the following RDP property to configure audio input redirection:

- `audiocapturemode:i:1` enables audio input redirection.
- `audiocapturemode:i:0` disables audio input redirection.

Audio output (speaker) redirection

Set the following RDP property to configure audio output redirection:

- `audiomode:i:0` enables audio output redirection.
- `audiomode:i:1` or `audiomode:i:2` disable audio output redirection.

Camera redirection

Set the following RDP property to configure camera redirection:

- `camerastoredirect:s:*` redirects all cameras.
- `camerastoredirect:s:` disables camera redirection.

Troubleshoot Azure Virtual Desktop clients



Troubleshoot Azure Virtual Desktop clients

You don't see the expected resources

If you don't see the remote resources you're expecting to see in the app, check the account you're using. If you've already signed in with a different account than the one you want to use for Azure Virtual Desktop, you should first sign out, then sign in again with the correct account.

If you're using the correct account, make sure your application group is associated with a workspace.

The user name or password is incorrect

If you can't sign in and keep receiving an error message that says your credentials are incorrect, first make sure you're using the right credentials.

If you keep seeing error messages:

- Have you assigned the Virtual Machine User Login role-based access control (RBAC) permission to the virtual machine (VM) or resource group for each user?
- Does your Conditional Access policy exclude multifactor authentication requirements for the Azure Windows VM sign-in cloud application?

The logon attempt failed

Verify the following:

- You're using a device that is Microsoft Entra joined or Microsoft Entra hybrid joined to the same Microsoft Entra tenant as the session host.
- The PKU2U protocol is enabled on both the local PC and the session host.
- Per-user multifactor authentication is disabled for the user account as it's not supported for Microsoft Entra joined VMs.

The sign-in method you're trying to use isn't allowed

Try a different sign-in method or contact your system administrator, you have Conditional Access policies restricting access. Follow the instructions in [Enforce Microsoft Entra multifactor authentication for Azure Virtual Desktop using Conditional Access to enforce Microsoft Entra multifactor authentication for your Microsoft Entra joined VMs](#).

A specified logon session does not exist. It may already have been terminated.

It may already have been terminated, verify that you properly created and configured the Kerberos server object when configuring single sign-on.

Knowledge check



Knowledge check

An IT professional is tasked with managing the desktops and applications made available to them by their admin through Azure Virtual Desktop. They need to ensure that the workspace content updates automatically and regularly. What should they do to achieve this?

Choices:

1. Manually update the workspace content every time they start the client
2. Unsubscribe and then resubscribe to the workspace
3. Subscribe to a workspace

Knowledge check

A system administrator needs to configure device redirection for an Azure Virtual Desktop environment. They need to enable USB device redirection for all supported devices on the client. Which RDP property should they set?

Choices:

1. `audiocapturemode` i 1
2. `redirectclipboard` i 1
3. `usbdevicestoredirect` s

Knowledge check

A user is trying to connect to Azure Virtual Desktop but keeps receiving an error message that says the credentials are incorrect. What should the user check first?

Choices:

1. Check if the Remote Desktop client is updated to the latest version
2. Check if the user has assigned the Virtual Machine User Login role based access control (RBAC) permission to the virtual machine (VM) or resource group for each user
3. Ensure the right credentials are being used

Knowledge check

A system administrator is tasked with setting up a corporate Microsoft Virtual Desktop Infrastructure (VDI) environment. They have installed a reference image of Windows 10 1607 version 10.0.1393 on a virtual machine. What should be their next step?

Choices:

1. Install the base OS using Express Settings
2. Enable all background services and tasks
3. Adjust settings during installation in Customize settings

Summary



Summary



What you learned:

- Connect to Azure Virtual Desktop with the Remote Desktop client for Windows
- Configure session timeout properties
- Configure user settings through group policies
- Implement the Start Virtual Machine on Connect feature
- Configure Universal Print
- Configure device redirections
- Troubleshoot Azure Virtual Desktop clients