1. **What is AVD (Azure Virtual Desktop)?**  
   Azure Virtual Desktop is a desktop and app virtualization service that runs on the cloud.  
   Here's what you can do when you run Azure Virtual Desktop on Azure:

* Set up a multi-session Windows 11 or Windows 10 deployment that delivers a full Windows experience with scalability.
* Present Microsoft 365 Apps for enterprise and optimize it to run in multi-user virtual scenarios.
* Provide Windows 7 virtual desktops with free Extended Security Updates
* Bring your existing Remote Desktop Services (RDS) and Windows Server desktops and apps to any computer.
* Virtualize both desktops and apps.
* Manage desktops and apps from different Windows and Windows Server operating systems with a unified management experience.

Key capabilities  
With Azure Virtual Desktop, you can set up a scalable and flexible environment:

* Create a full desktop virtualization environment in your Azure subscription without running any gateway

servers.

* Publish host pools as you need to accommodate your diverse workloads.
* Bring your own image for production workloads or test from the Azure Gallery.
* Reduce costs with pooled, multi-session resources. With the new Windows 11 and Windows 10 Enterprise

multi-session capability, exclusive to Azure Virtual Desktop and Remote Desktop Session Host (RDSH) role

on Windows Server, you can greatly reduce the number of virtual machines and operating system overhead

while still providing the same resources to your users.

* Provide individual ownership through personal (persistent) desktops.
* Use autoscale to automatically increase or decrease capacity based on time of day, specific days of the week,or as demand changes, helping to manage cost.

**You can deploy and manage virtual desktops:**

* Use the Azure portal, Azure CLI, PowerShell and REST API to configure the host pools, create app groups,

assign users, and publish resources.

Next steps

* Publish full desktop or individual remote apps from a single host pool, create individual app groups for

different sets of users, or even assign users to multiple app groups to reduce the number of images.

* As you manage your environment, use built-in delegated access to assign roles and collect diagnostics to

understand various configuration or user errors.

* Use the new Diagnostics service to troubleshoot errors.
* Only manage the image and virtual machines, not the infrastructure. You don't need to personally manage

the Remote Desktop roles like you do with Remote Desktop Services, just the virtual machines in your Azure subscription.

**You can also assign and connect users to your virtual desktops:**

* Once assigned, users can launch any Azure Virtual Desktop client to connect to their published Windows

desktops and applications. Connect from any device through either a native application on your device or the Azure Virtual Desktop HTML5 web client.

* Securely establish users through reverse connections to the service, so you don't need to open any inbound
* ports.

**Prerequisite: -**

* An Azure account with an active subscription
* An identity provider
* A supported operating system
* Appropriate licenses
* Network connectivity
* A Remote Desktop client  
    
    
  **Note: -**

If you're planning on using Azure AD only with FSLogix Profile Container, you will need to store profiles on Azure Files, which is currently in public preview. In this scenario, user accounts must be hybrid identities, which means you'll also need AD DS and Azure AD Connect. You must create these accounts in AD DS and synchronize them to Azure AD. The service

doesn't currently support environments where users are managed with Azure AD and synchronized to Azure AD DS.  
 **IMPORTANT: -**

The account you use for joining a domain can't have multi-factor authentication (MFA) enabled. When joining an Azure AD DS domain, the account you use must be part of the Azure AD DC administrators’ group.

Azure Virtual Desktop doesn't support 32-bit operating systems or SKUs not listed in the previous table. In addition, Windows 7 doesn't support any VHD or VHDX-based profile solutions hosted on managed Azure Storage due to a sector size limitation.

Azure Virtual Desktop extended support for Windows 7 session host VMs ends on January 10, 2023.

Ephemeral OS disks for Azure VMs are not supported.

Operating Systems and License: -

|  |  |
| --- | --- |
| * Windows Server 2022 * Windows Server 2019 * Windows Server 2016 * Windows Server 2012 R2 | License entitlement:  Remote Desktop Services (RDS) Client Access License (CAL) with Software Assurance (per-user or per device), or RDS User Subscription Licenses  Note:-Per-user access pricing is not available for Windows Server  operating systems. |

|  |  |
| --- | --- |
| * Windows 11 Enterprise multi-session * Windows 11 Enterprise * Windows 10 Enterprise multi-session, version 1909 and later * Windows 10 Enterprise, version 1909 and later * Windows 7 Enterprise | * License entitlement: * Microsoft 365 E3, E5, A3, A5, F3, Business Premium, Student Use Benefit * Windows Enterprise E3, E5 * Windows VDA E3, E5 * Windows Education A3, A5   External users can use per-user access pricing instead of license entitlement. |

* You can use operating system images provided by Microsoft in the Azure Marketplace, or your own custom images stored in an Azure Compute Gallery, as a managed image, or storage blob. To learn more about how to create custom images, see:

Store and share images in an Azure Compute Gallery.

Create a managed image of a generalized VM in Azure.

Prepare a Windows VHD or VHDX to upload to Azure.  
  
**Network**  
There are several network requirements you'll need to meet to successfully deploy Azure Virtual Desktop. This lets users connect to their virtual desktops and remote apps while also giving them the best possible user experience.

Users connecting to Azure Virtual Desktop securely establish a reverse connection to the service, which means you don't need to open any inbound ports. Transmission Control Protocol (TCP) on port 443 is used by default, however RDP Shortpath can be used for managed networks and public networks that establishes a direct User Datagram Protocol (UDP)-based transport.

To successfully deploy Azure Virtual Desktop, you'll need to meet the following network requirements:

* You'll need a virtual network for your session hosts. If you create your session hosts at the same time as a host pool, you must create this virtual network in advance for it to appear in the drop-down list. Your virtual network must be in the same Azure region as the session host.
* Make sure this virtual network can connect to your domain controllers and relevant DNS servers if you're using AD DS or Azure AD DS, since you'll need to join session hosts to the domain.
* Your session hosts and users need to be able to connect to the Azure Virtual Desktop service. These connections also use TCP on port 443 to a specific list of URLs. For more information, see Required URL list. You must make sure these URLs aren't blocked by network filtering or a firewall in order for your deployment to work properly and be supported. If your users need to access Microsoft 365, make sure your session hosts can connect to Microsoft 365 endpoints.

Also consider the following:

* Your users may need access to applications and data that is hosted on different networks, so make sure your session hosts can connect to them.
* Round-trip time (RTT) latency from the client's network to the Azure region that contains the host pools should be less than 150 ms. Use the Experience Estimator to view your connection health and recommended Azure region. To optimize for network performance, we recommend you create session hosts in the Azure region closest to your users.
* Use Azure Firewall for Azure Virtual Desktop deployments to help you lock down your environment and filter outbound traffic.

targetisaadjoined:i:1;

Diagram

Description automatically generated

## Workspaces

A workspace is a logical grouping of application groups in Azure Virtual Desktop.  
Each Azure Virtual Desktop application group must be associated with a workspace for users to see the remote apps and desktops published to them.

## App groups

An app group is a logical grouping of applications installed on session hosts in the host pool.

**HOST POOL -**   
Host pools are a collection of one or more identical virtual machines (VMs), also known as "session hosts," within Azure Virtual Desktop environments. Each host pool can contain an app group that users can interact with as they would on a physical desktop.  
Host pool: - host pool will be **Personal** or **Pooled**.  
  
Load balancing algorithm for Pooled, choose either **breadth-first** or **depth-first**, based on your usage

Pattern: -

* **Breadth-first** load balancing allows you to evenly distribute user sessions across the session hosts in a host pool.
* **Depth-first** load balancing allows you to saturate a session host with user sessions in a host pool. Once the first session host reaches its session limit threshold, the load balancer directs any new user connections to the next session host in the host pool until it reaches its limit, and so on.  
    
  **Host Pool Type - Personal**  
     
  **Automatic assignment** – The service will select an available host and assign it to an user

**Direct assignment** – Admin selects a specific host to assign to an user

M A N A G E D B Y M IC R O SO F T M A N A G E D B Y C U STO M E R

Load balancer Network

Session broker Session hosts

Gateway Storage

Diagnostics User profile data

Cloud identity platform  
RD WEB,RD Broker, RD Gateway Identity

Start Menu  
File Path

MSIX Package  
  
**Validation Environment: -**  
  
Validation host pool allows you to test service changes before they are deployed to production.

**Preferred App Group type- Desktop and Remote App (RAIL)**  
Set the preferred app group type for this host pool. If an end user has both RemoteApp and Desktop apps published to them on this host pool they will only see the selected app type in their feed.  
  
Graphical user interface, text, application, email

Description automatically generated  
Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

**Start VM on Connect** - Enable Start VM on connect to allow users to start the virtual machine from a deallocated state. Important: Custom RBAC role required to power manage VMs. [Learn more](https://go.microsoft.com/fwlink/?linkid=2153218)

Graphical user interface, text, application

Description automatically generated

**MSIX App:-**  
  
Create a MSIX Package and then Mount it into VHD or VHDX or CIM FILE

* MSIX Packaging Tool - This tool help you to Create MSIX Package.
* User needs to have file share NTFS read only permission on container which hold MSIX app.
* Session host need to have storage file data SMB contributor role on Container which hold MSIX app. We can provide this permission by the help of Group.
* Need to install same certificate (it could be self-signed, form your CA authority or from Public CA) on Session host(in Trusted People Grp) and assign that certificate to package for trust.  
  In each session host, install the certificate that you signed the MSIX package with. Make sure to store the certificates in the folder named **Trusted People**.
* Create a VHDX with NTFS file system in which we unzip the MSIX Package.

## MSIXMGR TOOL – this tool help us to unzip MSIX package into VHD(x). Requirements

Before you can follow the instructions in this article, you'll need to do the following things:

* [Download the MSIXMGR tool](https://aka.ms/msixmgr)
* Get an MSIX-packaged application (.MSIX file)
* Get administrative permissions on the machine where you'll create the MSIX image

**Create an MSIX image**

Expansion is the process of taking an MSIX packaged application (.MSIX) and unzipping it into a MSIX image (.VHD(x) or .CIM file).

To expand an MSIX file:

1. [Download the MSIXMGR tool](https://aka.ms/msixmgr) if you haven't already.
2. Unzip MSIXMGR.zip into a local folder.
3. Open a command prompt in elevated mode.
4. Find the local folder from step 2.
5. Run the following command in the command prompt to create an MSIX image.

Windows Command PromptCopy

msixmgr.exe -Unpack -packagePath <path to package> -destination <output folder> [-applyacls] [-create] [-vhdSize <size in MB>] [-filetype <CIM | VHD | VHDX>] [-rootDirectory <rootDirectory>]

Remember to replace the placeholder values with the relevant values. For example:

Windows Command PromptCopy

msixmgr.exe -Unpack -packagePath "C:\Users\%username%\Desktop\packageName\_3.51.1.0\_x64\_\_81q6ced8g4aa0.msix" -destination "c:\temp\packageName.vhdx" -applyacls -create -vhdSize 200 -filetype "vhdx" -rootDirectory apps

1. Now that you've created the image, go to the destination folder and make sure you successfully created the MSIX image (.VHDX).
   * Select the **Registration type** you want to use. Which one you use depends on your needs:
   * **On-demand registration** postpones the full registration of the MSIX application until the user starts the application. This is the registration type we recommend you use.
   * **Log on blocking** only registers while the user is signing in. We don't recommend this type because it can lead to longer sign-in times for users.
2. For **State**, select your preferred state.
   * The **Active** status lets users interact with the package.
   * The **Inactive** status causes Azure Virtual Desktop to ignore the package and not deliver it

**FSLOGIX -**  
  
With the acquisition of FSLogix, eligible clients will get access to the following three core pieces of technology.

*Profile Container*: Replacement for roaming profiles and folder redirection, which dramatically speeds up login and launch times, including Office 365 container, which roams Office cache data.

*App Mask Imaging*: Minimise the number of gold images creating a single image with all applications. Excellent app compatibility with no packaging, sequencing, backend infrastructure, or virtualisation.

*Java Redirection*: Helps protect the enterprise from vulnerabilities of multiple installed versions of Java by mapping specific versions to individual apps or websites.

**Prepare the virtual machine to act as a file share for user profiles**

The following are general instructions about how to prepare a virtual machine to act as a file share for user profiles:

1. Add the Azure Virtual Desktop Active Directory users to an [Active Directory security group](https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups/). This security group will be used to authenticate the Azure Virtual Desktop users to the file share virtual machine you just created.
2. [Connect to the file share virtual machine](https://learn.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal#connect-to-virtual-machine).
3. On the file share virtual machine, create a folder on the **C drive** that will be used as the profile share.
4. Right-click the new folder, select **Properties**, select **Sharing**, then select **Advanced sharing...**.
5. Select **Share this folder**, select **Permissions...**, then select **Add...**.
6. Search for the security group to which you added the Azure Virtual Desktop users, then make sure that group has **Full Control**.
7. After adding the security group, right-click the folder, select **Properties**, select **Sharing**, then copy down the **Network Path** to use for later.

## Configure the FSLogix profile container

To configure FSLogix profile container, do the following on each session host registered to the host pool:

1. [Connect to the virtual machine](https://learn.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal#connect-to-virtual-machine) with the credentials you provided when creating the virtual machine.
2. Launch an internet browser and [download the FSLogix agent](https://aka.ms/fslogix_download).
3. Open the downloaded .zip file, navigate to either **Win32\Release** or **x64\Release** (depending on your operating system) and run **FSLogixAppsSetup** to install the FSLogix agent. To learn more about how to install FSLogix, see [Download and install FSLogix](https://learn.microsoft.com/en-us/fslogix/install-ht/).
4. Navigate to **Program Files** > **FSLogix** > **Apps** to confirm the agent installed successfully.
5. From the start menu, run **regedit** as an administrator. Navigate to **Computer\HKEY\_LOCAL\_MACHINE\Software\FSLogix**.
6. Create a key named **Profiles**.
7. Create the following values for the **Profiles** key (replacing **\\hostname\share** with your real path):

| **Name** | **Type** | **Data/Value** |
| --- | --- | --- |
| Enabled | DWORD | 1 |
| VHDLocations | Multi-String Value | \\hostname\share |

### **MS Teams -** Install Remote Desktop WebRTC Redirector Service and make below changes in registry to Use MS Team. Enable media optimization for Teams

To enable media optimization for Teams, set the following registry key on the host VM:

1. From the start menu, run **Registry Editor** as an administrator. Go to HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Teams. Create the Teams key if it doesn't already exist.
2. Create the following value for the Teams key:

| **Name** | **Type** | **Data/Value** |
| --- | --- | --- |
| IsWVDEnvironment | DWORD | 1 |

### New-Item -Path "HKLM:\SOFTWARE\Microsoft\Teams" -Force

### New-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Teams" -Name IsWVDEnvironment -PropertyType DWORD -Value 1 -Force

## Default RDP file properties

RDP files have the following properties by default:

| **RDP property** | **For both Desktop and RemoteApp** |
| --- | --- |
| Multi-monitor mode | Enabled |
| Redirections enabled | Drives, clipboard, printers, COM ports, smart cards, devices, usbdevicestore, and WebAuthn |
| Remote audio mode | Play locally |
| VideoPlayback | Enabled |
| EnableCredssp | Enabled |

## Screen capture protection in Azure Virtual Desktop

# Screen capture protection, alongside [watermarking](https://learn.microsoft.com/en-us/azure/virtual-desktop/watermarking), helps prevent sensitive information from being captured on client endpoints. When you enable screen capture protection, remote content will be automatically blocked or hidden in screenshots and screen shares. Also, the Remote Desktop client will hide content from malicious software that may be capturing the screen. **RDP Shortpath for Azure Virtual Desktop**

Connections to Azure Virtual Desktop use Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). RDP Shortpath is a feature of Azure Virtual Desktop that establishes a direct UDP-based transport between a supported Windows Remote Desktop client and session host. Remote Desktop Protocol (RDP) by default uses a TCP-based reverse connect transport as it provides the best compatibility with various networking configurations and has a high success rate for establishing RDP connections. However, if RDP Shortpath can be used instead, this UDP-based transport offers better connection reliability and more consistent latency.

RDP Shortpath can be used in two ways:

* **Managed networks**, where direct connectivity is established between the client and the session host when using a private connection, such as a virtual private network (VPN).

**Public networks**, where direct connectivity is established between the client and the session host through a NAT gateway, provided as part of the Azure Desktop service, when using a public connection.  
  
**RDP SHORTPATH**

## Reverse connect transport

Azure Virtual Desktop is using reverse connect transport for establishing the remote session and for carrying RDP traffic. Unlike the on-premises Remote Desktop Services deployments, reverse connect transport doesn't use a TCP listener to receive incoming RDP connections. Instead, it is using outbound connectivity to the Azure Virtual Desktop infrastructure over the HTTPS connection.

The transport used for RDP Shortpath is based on the [Universal Rate Control Protocol (URCP)](https://www.microsoft.com/research/publication/urcp-universal-rate-control-protocol-for-real-time-communication-applications/). URCP enhances UDP with active monitoring of the network conditions and provides fair and full link utilization. URCP operates at low delay and loss levels as needed.

## Key benefits

Using RDP Shortpath has the following key benefits:

* Using URCP to enhance UDP achieves the best performance by dynamically learning network parameters and providing the protocol with a rate control mechanism.
* The removal of extra relay points reduces round-trip time, which improves connection reliability and user experience with latency-sensitive applications and input methods.
* In addition, for managed networks:
  + RDP Shortpath brings support for configuring Quality of Service (QoS) priority for RDP connections through Differentiated Services Code Point (DSCP) marks.
  + The RDP Shortpath transport allows limiting outbound network traffic by specifying a throttle rate for each session.

Public Networks - RDP Shortpath uses Simple Traversal Underneath NAT (STUN) protocol to discover the external IP address of the NAT router.

Both Client and Session Host connect update and share candidate list (from STUN with Public ip and port number) each other and try to establish Connection.  
  
After the initial packet exchange, the client and session host may establish one or many data flows. From these data flows, RDP chooses the fastest network path. The client then establishes a secure TLS connection with the session host and initiates RDP Shortpath transport.

After RDP establishes the RDP Shortpath transport, all Dynamic Virtual Channels (DVCs), including remote graphics, input, and device redirection move to the new transport.

**Managed Network** **-**  
  
You can achieve the direct line of sight connectivity required to use RDP Shortpath with managed networks using the following methods. Having direct line of sight connectivity means that the client can connect directly to the session host without being blocked by firewalls.

1. The session host sends the list of its IPv4 and IPv6 addresses to the client.
2. The client starts the background thread to establish a parallel UDP-based transport directly to one of the session host's IP addresses.
3. While the client is probing the provided IP addresses, it continues to establish the initial connection over the reverse connect transport to ensure there's no delay in the user connection.
4. If the client has a direct connection to the session host, the client establishes a secure TLS connection.
5. After establishing the RDP Shortpath transport, all Dynamic Virtual Channels (DVCs), including remote graphics, input, and device redirection, are moved to the new transport. However, if a firewall or network topology prevents the client from establishing direct UDP connectivity, RDP continues with a reverse connect transport.

## Error: Session host VMs are stuck in Unavailable or Upgrading state

If the status listed for session hosts in your host pool always says **Unavailable** or **Upgrading**, the agent or stack didn't install successfully.

To resolve this issue, first reinstall the side-by-side stack:

1. Sign in to your session host VM as an administrator.
2. From an elevated PowerShell prompt run qwinsta.exe and make note of the version number that appears next to **rdp-sxs** in the SESSIONNAME column. If the STATE column for **rdp-tcp** and **rdp-sxs** entries isn't **Listen**, or if **rdp-tcp** and **rdp-sxs** entries aren't listed at all, it means that there's a stack issue.
3. Run the following command to stop the RDAgentBootLoader service:

PowerShellCopy

Stop-Service RDAgentBootLoader

1. Go to **Control Panel** > **Programs** > **Programs and Features**, or on Windows 11 go to the **Settings App > Apps**.
2. Uninstall the latest version of the **Remote Desktop Services SxS Network Stack** or the version listed in Registry Editor in **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations** under the value for **ReverseConnectionListener**.
3. Back at the PowerShell prompt, run the following commands to add the file path of the latest installer available on your session host VM for the side-by-side stack to a variable and list its name:

PowerShellCopy

$sxsMsi = (Get-ChildItem "$env:SystemDrive\Program Files\Microsoft RDInfra\" | ? Name -like SxSStack\*.msi | Sort-Object CreationTime -Descending | Select-Object -First 1).FullName

$sxsMsi

1. Install the latest installer available on your session host VM for the side-by-side stack by running the following command:

PowerShellCopy

msiexec /i $sxsMsi

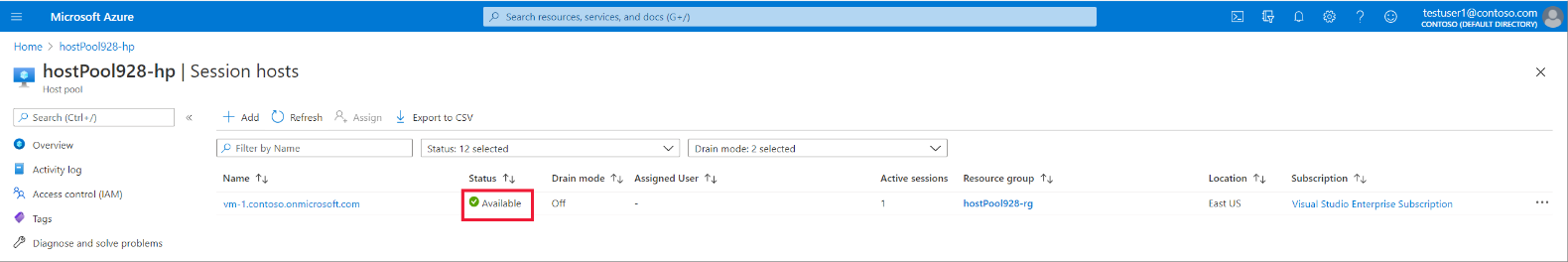
1. Restart your session host VM.
2. From a command prompt run qwinsta.exe again and verify the STATE column for **rdp-tcp** and **rdp-sxs** entries is **Listen**. If not, you will need to [re-register your VM and reinstall the agent](https://learn.microsoft.com/en-us/azure/virtual-desktop/troubleshoot-agent#your-issue-isnt-listed-here-or-wasnt-resolved) component.

## Error: NAME\_ALREADY\_REGISTERED

The name of your session host VM has already been registered and is probably a duplicate.

To resolve this issue:

1. Follow the steps in the [Remove the session host from the host pool](https://learn.microsoft.com/en-us/azure/virtual-desktop/troubleshoot-agent#step-2-remove-the-session-host-from-the-host-pool) section.
2. [Create another VM](https://learn.microsoft.com/en-us/azure/virtual-desktop/expand-existing-host-pool#add-virtual-machines-with-the-azure-portal). Make sure to choose a unique name for this VM.
3. Go to the [Azure portal](https://portal.azure.com/) and open the **Overview** page for the host pool your VM was in.
4. Open the **Session Hosts** tab and check to make sure all session hosts are in that host pool.
5. Wait for 5-10 minutes for the session host status to say **Available**.



## Your issue isn't listed here or wasn't resolved

If you can't find your issue in this article or the instructions didn't help you, we recommend you uninstall, reinstall, and re-register the Azure Virtual Desktop Agent. The instructions in this section will show you how to reregister your session host VM to the Azure Virtual Desktop service by:

1. Uninstalling all agent, boot loader, and stack components
2. Removing the session host from the host pool
3. Generating a new registration key for the VM
4. Reinstalling the Azure Virtual Desktop Agent and boot loader.

Follow these instructions in this section if one or more of the following scenarios apply to you:

* The state of your session host VM is stuck as **Upgrading** or **Unavailable**.
* Your stack listener isn't working and you're running on Windows 10 version 1809, 1903, or 1909.
* You're receiving an **EXPIRED\_REGISTRATION\_TOKEN** error.
* You're not seeing your session host VMs show up in the session hosts list.
* You don't see the **Remote Desktop Agent Loader** service in the Services console.
* You don't see the **RdAgentBootLoader** component as a running process in Task Manager.
* You're receiving a **Connection Broker couldn't validate the settings** error on custom image VMs.
* Previous sections in this article didn't resolve your issue.

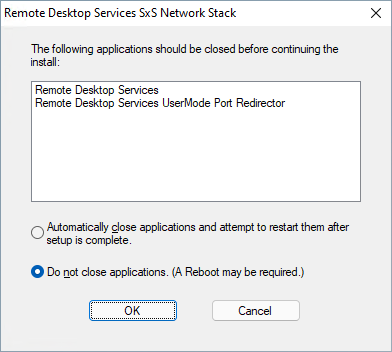
### Step 1: Uninstall all agent, boot loader, and stack component programs

Before reinstalling the agent, boot loader, and stack, you must uninstall any existing components from your VM. To uninstall all agent, boot loader, and stack component programs:

1. Sign in to your session host VM as an administrator.
2. Go to **Control Panel** > **Programs** > **Programs and Features**, or on Windows 11 go to the **Settings App > Apps**.
3. Uninstall the following programs, then restart your session host VM:

**Caution**

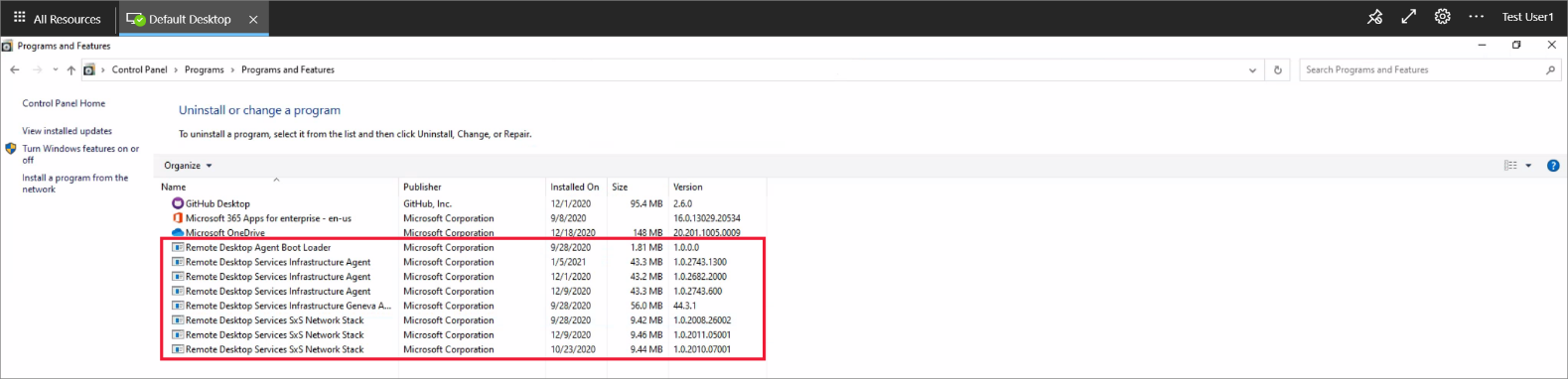
When uninstalling **Remote Desktop Services SxS Network Stack**, you'll be prompted that Remote Desktop Services and Remote Desktop Services UserMode Port Redirector should be closed. If you're connected to the session host VM using RDP, select **Do not close applications** then select **OK**, otherwise your RDP connection will be closed.



* + Remote Desktop Agent Boot Loader
  + Remote Desktop Services Infrastructure Agent
  + Remote Desktop Services Infrastructure Geneva Agent
  + Remote Desktop Services SxS Network Stack

**Note**

You may see multiple instances of these programs. Make sure to remove all of them.



### Step 2: Remove the session host from the host pool

When you remove the session host from the host pool, the session host is no longer registered to that host pool. This acts as a reset for the session host registration. To remove the session host from the host pool:

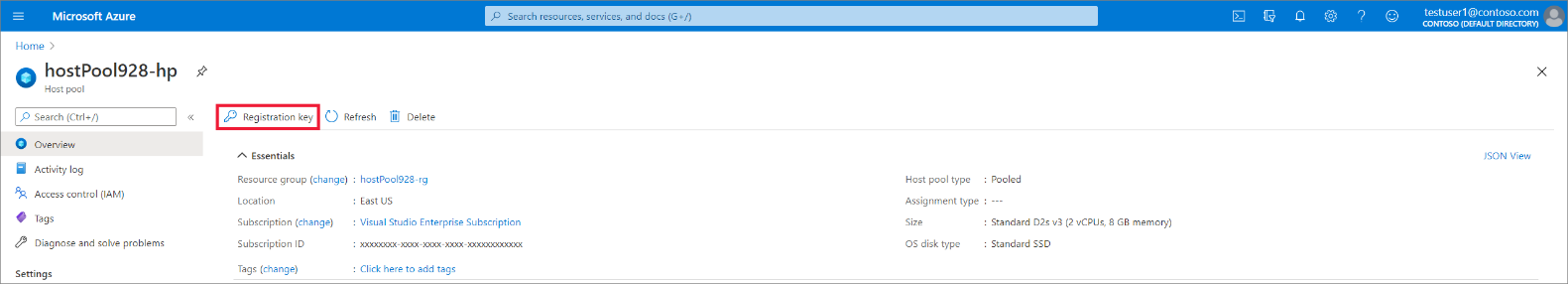
1. Sign in to the [Azure portal](https://portal.azure.com/).
2. In the search bar, type Azure Virtual Desktop and select the matching service entry.
3. Select **Host pools** and select the name of the host pool that your session host VM is in.
4. Select **Session Hosts** to see the list of all session hosts in that host pool.
5. Look at the list of session hosts and tick the box next to the session host that you want to remove.
6. Select **Remove**.



### Step 3: Generate a new registration key for the VM

You must generate a new registration key that is used to re-register your session VM to the host pool and to the service. To generate a new registration key for the VM:

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. In the search bar, type Azure Virtual Desktop and select the matching service entry.
3. Select **Host pools** and select the name of the host pool that your session host VM is in.
4. On the **Overview** blade, select **Registration key**.



1. Open the **Registration key** tab and select **Generate new key**.
2. Enter the expiration date and then select **Ok**.

**Note**

The expiration date can be no less than an hour and no longer than 27 days from its generation time and date. Generate a registration key only for as long as you need.

1. Copy the newly generated key to your clipboard or download the file. You'll need this key later.

### Step 4: Reinstall the agent and boot loader

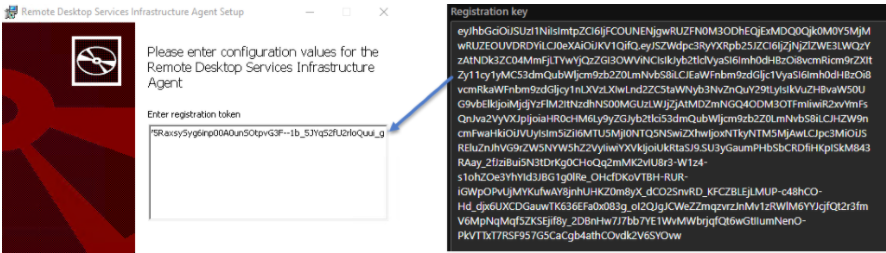
By reinstalling the most updated version of the agent and boot loader, the side-by-side stack and Geneva monitoring agent automatically get installed as well. To reinstall the agent and boot loader:

1. Sign in to your session host VM as an administrator and run the agent installer and bootloader for your session host VM:
   * [Azure Virtual Desktop Agent](https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWrmXv)
   * [Azure Virtual Desktop Agent Bootloader](https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWrxrH)

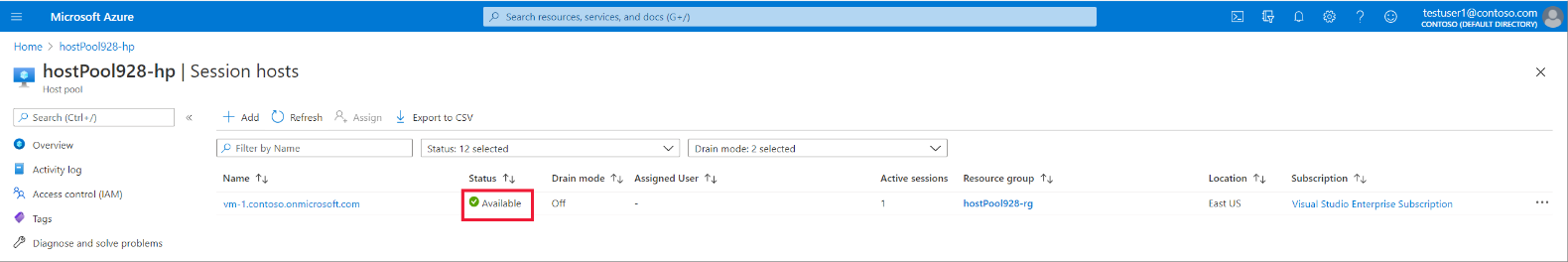
**Tip**

For each of the the agent and boot loader installers you downloaded, you may need to unblock them. Right-click each file and select **Properties**, then select **Unblock**, and finally select **OK**.

1. When the installer asks you for the registration token, paste the registration key from your clipboard.



1. Run the boot loader installer.
2. Restart your session VM.
3. Sign in to the [Azure portal](https://portal.azure.com/).
4. In the search bar, enter **Azure Virtual Desktop** and select the matching service entry.
5. Select **Host pools** and select the name of the host pool that your session host VM is in.
6. Select **Session Hosts** to see the list of all session hosts in that host pool.
7. You should now see the session host registered in the host pool with the status **Available**.



**SYSPREP – TO Generalize or Specialize Image :-**  
  
Graphical user interface, text, application

Description automatically generated