General Remote Desktop connection troubleshooting

Article • 04/04/2022 • 8 minutes to read

Try our Virtual Agent - It can help you quickly identify and fix common RD Sessions connectivity issues

Use these steps when a Remote Desktop client can't connect to a remote desktop but doesn't provide messages or other symptoms that would help identify the cause.

Check the status of the RDP protocol

Check the status of the RDP protocol on a local computer

To check and change the status of the RDP protocol on a local computer, see How to enable Remote Desktop.

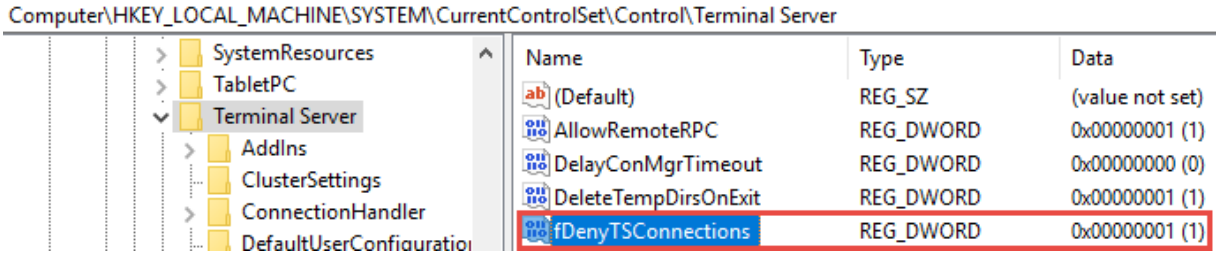
> **Note**
>
> If the remote desktop options are not available, see **Check whether a Group Policy Object is blocking RDP**.

Check the status of the RDP protocol on a remote computer

> **Important**
>
> Follow this section's instructions carefully. Serious problems can occur if the registry is modified incorrectly. Before you start modifying the registry, **back up the registry** so you can restore it in case something goes wrong.

To check and change the status of the RDP protocol on a remote computer, use a network registry connection:

1. First, go to the **Start** menu, then select **Run**. In the text box that appears, enter **regedt32**.
2. In the Registry Editor, select **File**, then select **Connect Network Registry**.
3. In the **Select Computer** dialog box, enter the name of the remote computer, select **Check Names**, and then select **OK**.
4. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server** and to **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services**.



   - If the value of the **fDenyTSConnections** key is **0**, then RDP is enabled.
   - If the value of the **fDenyTSConnections** key is **1**, then RDP is disabled.

5. To enable RDP, change the value of **fDenyTSConnections** from **1** to **0**.

Check whether a Group Policy Object (GPO) is blocking RDP on a local computer

If you can't turn on RDP in the user interface or the value of **fDenyTSConnections** reverts to **1** after you've changed it, a GPO may be overriding the computer-level settings.

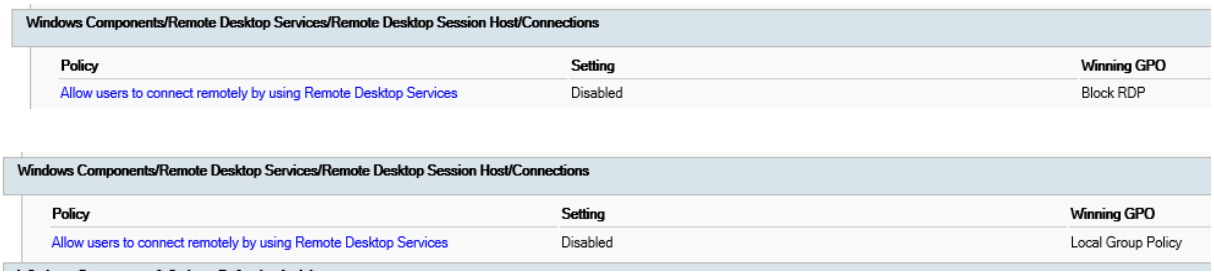
To check the group policy configuration on a local computer, open a Command Prompt window as an administrator, and enter the following command:

Windows Command Prompt

```
gpresult /H c:\gpresult.html
```

After this command finishes, open gpresult.html. In **Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections**, find the **Allow users to connect remotely by using Remote Desktop Services** policy.

- If the setting for this policy is **Enabled**, Group Policy is not blocking RDP connections.
- If the setting for this policy is **Disabled**, check **Winning GPO**. This is the GPO that is blocking RDP connections.



Windows Components/Remote Desktop Services/Remote Desktop Session Host/Connections		
Policy	**Setting**	**Winning GPO**
Allow users to connect remotely by using Remote Desktop Services	Disabled	Block RDP

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Connections		
Policy	**Setting**	**Winning GPO**
Allow users to connect remotely by using Remote Desktop Services	Disabled	Local Group Policy

Check whether a GPO is blocking RDP on a remote computer

To check the Group Policy configuration on a remote computer, the command is almost the same as for a local computer:

Windows Command Prompt

```
gpresult /S <computer name> /H c:\gpresult-<computer name>.html
```

The file that this command produces (**gpresult-<computer name>.html**) uses the same information format as the local computer version (**gpresult.html**) uses.

Modifying a blocking GPO

You can modify these settings in the Group Policy Object Editor (GPE) and Group Policy Management Console (GPM). For more information about how to use Group Policy, see Advanced Group Policy Management.

To modify the blocking policy, use one of the following methods:

- In GPE, access the appropriate level of GPO (such as local or domain), and navigate to **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections** > **Allow users to connect remotely by using Remote Desktop Services**.

    1. Set the policy to either **Enabled** or **Not configured**.
    2. On the affected computers, open a command prompt window as an administrator, and run the **gpupdate /force** command.

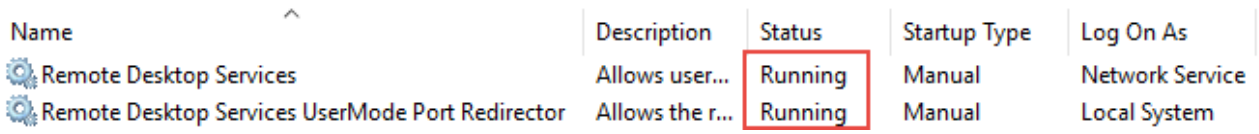
- In GPM, navigate to the organizational unit (OU) in which the blocking policy is applied to the affected computers and delete the policy from the OU.

Check the status of the RDP services

On both the local (client) computer and the remote (target) computer, the following services should be running:

- Remote Desktop Services (TermService)
- Remote Desktop Services UserMode Port Redirector (UmRdpService)

You can use the Services MMC snap-in to manage the services locally or remotely. You can also use PowerShell to manage the services locally or remotely (if the remote computer is configured to accept remote PowerShell cmdlets).



On either computer, if one or both services are not running, start them.

> **Note**
>
> If you start the Remote Desktop Services service, click **Yes** to automatically restart the Remote Desktop Services UserMode Port Redirector service.

Check that the RDP listener is functioning

> **Important**
>
> Follow this section's instructions carefully. Serious problems can occur if the registry is modified incorrectly. Before you starty modifying the registry, **back up the registry** so you can restore it in case something goes wrong.

Check the status of the RDP listener

For this procedure, use a PowerShell instance that has administrative permissions. For a local computer, you can also use a command prompt that has administrative permissions. However, this procedure uses PowerShell because the same cmdlets work both locally and remotely.

1. To connect to a remote computer, run the following cmdlet:

```
PowerShell

Enter-PSSession -ComputerName <computer name>
```

2. Enter **qwinsta**.

```
[rdwagw01]: PS C:\> qwinsta
 SESSIONNAME       USERNAME                 ID  STATE   TYPE        DEVICE
>services                                    0  Disc
 console                                     1  Conn
 31c5ce94259d4...                        65536  Listen
 rdp-tcp                                 65537  Listen
```

3. If the list includes **rdp-tcp** with a status of **Listen**, the RDP listener is working. Proceed to Check the RDP listener port. Otherwise, continue at step 4.

4. Export the RDP listener configuration from a working computer.
   a. Sign in to a computer that has the same operating system version as the affected computer has, and access that computer's registry (for example, by using Registry Editor).
   b. Navigate to the following registry entry: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp**
   c. Export the entry to a .reg file. For example, in Registry Editor, right-click the entry, select **Export**, and then enter a filename for the exported settings.
   d. Copy the exported .reg file to the affected computer.

5. To import the RDP listener configuration, open a PowerShell window that has administrative permissions on the affected computer (or open the PowerShell window and connect to the affected computer remotely).

   a. To back up the existing registry entry, enter the following cmdlet:

```
PowerShell

cmd /c 'reg export "HKLM\SYSTEM\CurrentControlSet\Control\Terminal
```

```
Server\WinStations\RDP-tcp" C:\Rdp-tcp-backup.reg'
```

b. To remove the existing registry entry, enter the following cmdlets:

```
PowerShell

Remove-Item -path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-tcp' -Recurse -Force
```

c. To import the new registry entry and then restart the service, enter the following cmdlets:

```
PowerShell

cmd /c 'regedit /s c:\<filename>.reg'
Restart-Service TermService -Force
```

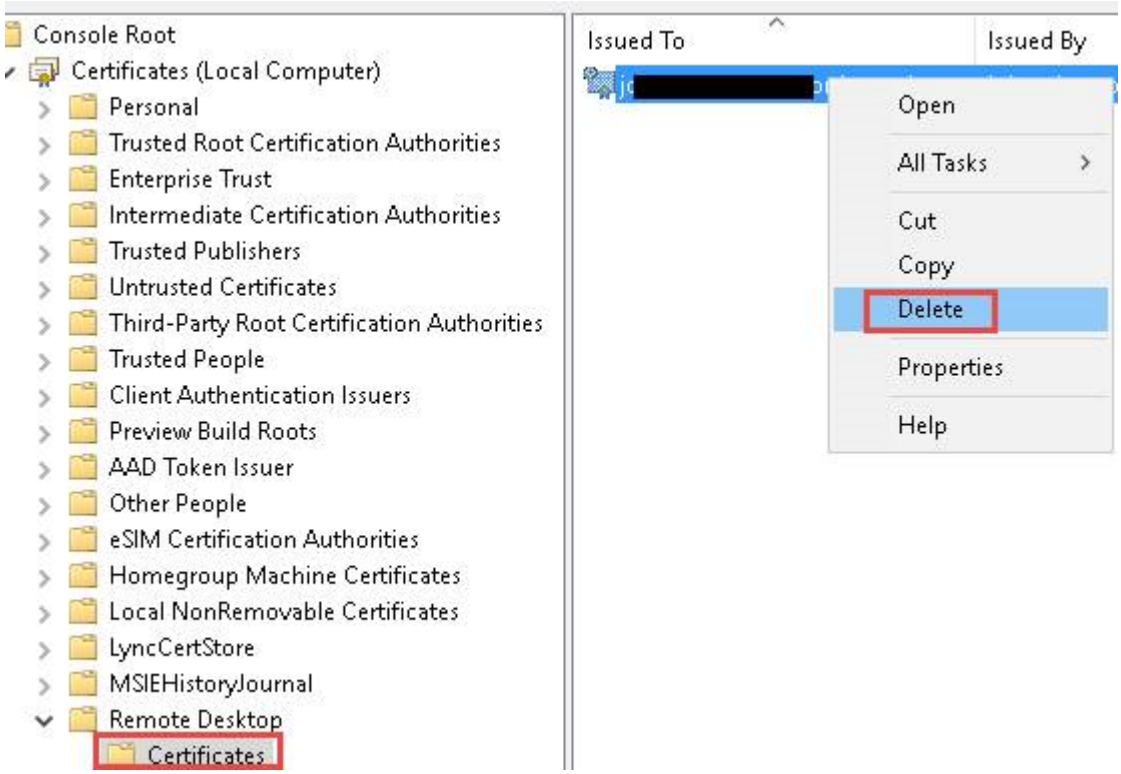
Replace <filename> with the name of the exported .reg file.

6. Test the configuration by trying the remote desktop connection again. If you still can't connect, restart the affected computer.

7. If you still can't connect, check the status of the RDP self-signed certificate.

Check the status of the RDP self-signed certificate

1. If you still can't connect, open the Certificates MMC snap-in. When you are prompted to select the certificate store to manage, select **Computer account**, and then select the affected computer.
2. In the **Certificates** folder under **Remote Desktop**, delete the RDP self-signed certificate.



3. On the affected computer, restart the Remote Desktop Services service.
4. Refresh the Certificates snap-in.
5. If the RDP self-signed certificate has not been recreated, check the permissions of the MachineKeys folder.

Check the permissions of the MachineKeys folder

1. On the affected computer, open Explorer, and then navigate to **C:\ProgramData\Microsoft\Crypto\RSA**.
2. Right-click **MachineKeys**, select **Properties**, select **Security**, and then select **Advanced**.
3. Make sure that the following permissions are configured:

   - Builtin\Administrators: Full control
   - Everyone: Read, Write

Check the RDP listener port

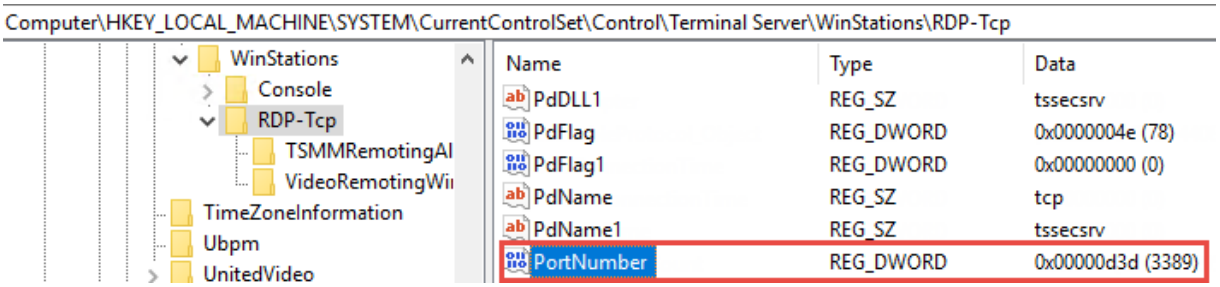
On both the local (client) computer and the remote (target) computer, the RDP listener should be listening on port 3389. No other applications should be using this port.

> **Important**

> Follow this section's instructions carefully. Serious problems can occur if the registry is modified incorrectly. Before you starty modifying the registry, **back up the registry** so you can restore it in case something goes wrong.

To check or change the RDP port, use the Registry Editor:

1. Go to the Start menu, select **Run**, then enter **regedt32** into the text box that appears.
   - To connect to a remote computer, select **File**, and then select **Connect Network Registry**.
   - In the **Select Computer** dialog box, enter the name of the remote computer, select **Check Names**, and then select **OK**.
2. Open the registry and navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\<listener>**.



3. If **PortNumber** has a value other than **3389**, change it to **3389**.

> **ⓘ Important**
>
> You can operate Remote Desktop services using another port. However, we don't recommend you do this. This article doesn't cover how to troubleshoot that type of configuration.

4. After you change the port number, restart the Remote Desktop Services service.

Check that another application isn't trying to use the same port

For this procedure, use a PowerShell instance that has administrative permissions. For a local computer, you can also use a command prompt that has administrative permissions. However, this procedure uses PowerShell because the same cmdlets work locally and remotely.

1. Open a PowerShell window. To connect to a remote computer, enter **Enter-PSSession -ComputerName <computer name>**.

2. Enter the following command:

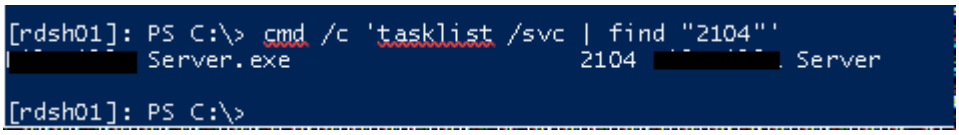
```
PowerShell
cmd /c 'netstat -ano | find "3389"'
```

3. Look for an entry for TCP port 3389 (or the assigned RDP port) with a status of **Listening**.

> **Note**
>
> The process identifier (PID) for the process or service using that port appears under the PID column.

4. To determine which application is using port 3389 (or the assigned RDP port), enter the following command:

```
PowerShell
cmd /c 'tasklist /svc | find "<pid listening on 3389>"'
```



5. Look for an entry for the PID number that is associated with the port (from the **netstat** output). The services or processes that are associated with that PID appear on the right column.

6. If an application or service other than Remote Desktop Services (TermServ.exe) is using the port, you can resolve the conflict by using one of the following methods:

   - Configure the other application or service to use a different port (recommended).

- Uninstall the other application or service.
- Configure RDP to use a different port, and then restart the Remote Desktop Services service (not recommended).

Check whether a firewall is blocking the RDP port

Use the **psping** tool to test whether you can reach the affected computer by using port 3389.

1. Go to a different computer that isn't affected and download **psping** from https://live.sysinternals.com/psping.exe .
2. Open a command prompt window as an administrator, change to the directory in which you installed **psping**, and then enter the following command:

```
psping -accepteula <computer IP>:3389
```

3. Check the output of the **psping** command for results such as the following:
   - **Connecting to <computer IP>**: The remote computer is reachable.
   - **(0% loss)**: All attempts to connect succeeded.
   - **The remote computer refused the network connection**: The remote computer is not reachable.
   - **(100% loss)**: All attempts to connect failed.
4. Run **psping** on multiple computers to test their ability to connect to the affected computer.
5. Note whether the affected computer blocks connections from all other computers, some other computers, or only one other computer.
6. Recommended next steps:
   - Engage your network administrators to verify that the network allows RDP traffic to the affected computer.
   - Investigate the configurations of any firewalls between the source computers and the affected computer (including Windows Firewall on the affected computer) to determine whether a firewall is blocking the RDP port.