TIP

How to fix 8 common remote desktop connection problems

When the connection between a desktop and its host fails, it's time to do some remote desktop troubleshooting. Check firewalls, security certificates and more if a remote desktop is not working.

Brien Posey

Published: **11 Dec 2020**

There are many remote desktop connection problems that administrators may encounter, including network failure, Secure Sockets Layer certificate issues, authentication troubles and capacity limitations.

As a desktop admin, you can prevent and solve common remote desktop problems by using these tips.

1. Network failure

A lack of a valid communications path can prevent a client from connecting to a remote desktop session. The easiest way to diagnose this issue is through the process of elimination.

First, try to establish a session from a client that has been able to successfully connect in the past. The goal is to find out if the problem is specific to an individual client, the network or a terminal server/Windows server.

If you suspect the network might be to blame, try to narrow down the scope of the issue to find the root cause. In doing so, you might discover that the problem affects wireless connections but not wired ones. Likewise, you may discover the problem is unique to VPN traffic or a particular subnet.

> **Some organizations configure their corporate firewall to block outbound RDP traffic, thereby preventing connectivity to remote systems.**

2. Firewall problems

It's easy to dismiss the notion that a firewall could contribute to a remote desktop not working, but it's quite common. To avoid firewall problems, ensure that the port your remote desktop software uses is open on any firewalls residing between client computers and the server they connect to. Remote Desktop Protocol (RDP)-based tools use RDP port 3389 by default.

You may need to configure multiple firewalls. For example, the client and the server may both run Windows Defender Firewall, and there will probably be one or more hardware firewalls between the two systems.

Some public networks block RDP traffic. This setting is especially common for Wi-Fi networks found in some hotels, airports and coffee shops.

Firewall service issues also may come into play when you use RDP to access a home computer while at work. Some organizations configure their corporate firewall to block outbound RDP traffic, thereby preventing connectivity to remote systems.

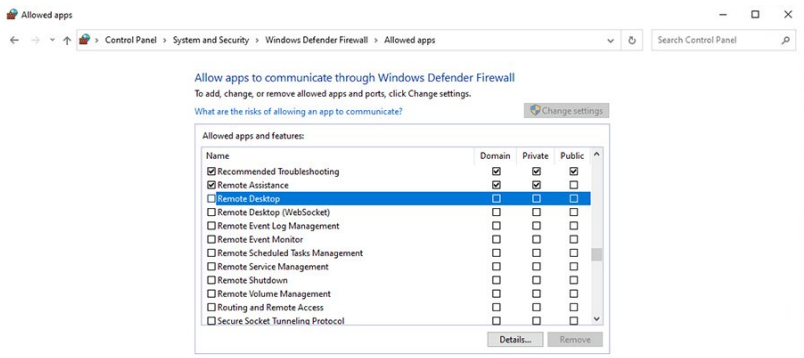
1. Open the **Control Panel** by entering Control at the Windows Run prompt
2. Click **System and Security**
3. Click **Windows Defender Firewall**
4. Click **Allow an App** or **Feature Through Windows Defender Firewall**
5. Select the **Remote Desktop** option
6. Click **OK**

Up Next

How to fix 8 common remote c connection problems

When the connection between a desktop a fails, it's time to do some remote desktop t Check firewalls, security certificates and r

BRIEN POSEY



The Control Panel setting that shows Windows Defender Firewall allowing RDP traffic on port 3389

3. SSL certificate issues

Security certificates can also cause remote desktop connection problems. Many VDI products use Secure Sockets Layer (SSL) encryption for users that access VDI sessions outside the network perimeter. But SSL encryption requires the use of certificates, which creates two problems that can cause a remote desktop to not work.

First, if remote desktops are going to connect properly, client computers must trust the certificate authority that issued the certificate. This isn't usually a problem for organizations that purchase certificates from large, well-known authorities, but clients won't always trust the certificates an organization generates in-house. Use a reliable certificate authority to ensure that clients establish remote desktop connectivity.

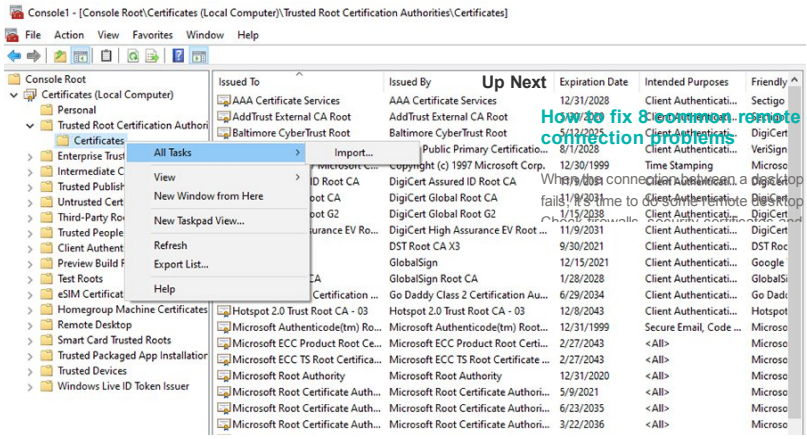
If you're using a certificate provided by an enterprise certificate authority, it is important to note that network clients do not automatically trust the certificate. You will need to download a copy of the certificate authority's root certificate and add it to the client's certificate store in a way that allows it to trust the certificate authority associated with the certificate.

The client must also be able to verify the certificate the server uses. The verification process can break down if the certificate has expired or if the name on the certificate doesn't match the name of the server using it.

To check if your network endpoint trusts your certificate authority and import any required certificates, complete these steps:

1. Enter the MMC command at the Windows Run prompt
2. Select the **Add / Remove Snap-In Command** from the File menu
3. Choose **Certificates** from the list of available snap-ins and click **Add**
4. When prompted, choose the **Computer Account** option and click **Next**
5. Choose the **Local Computer** option and click **Finish**
6. Click **OK**
7. Navigate through the console tree to Certificates (Local Computer) \ Trusted Root Certification Authorities \ Certificates
8. Browse the list of certification authorities to make sure that your certificate authority is listed. If not, right-click on the **Certificates** container and choose the **All Tasks | Import** options

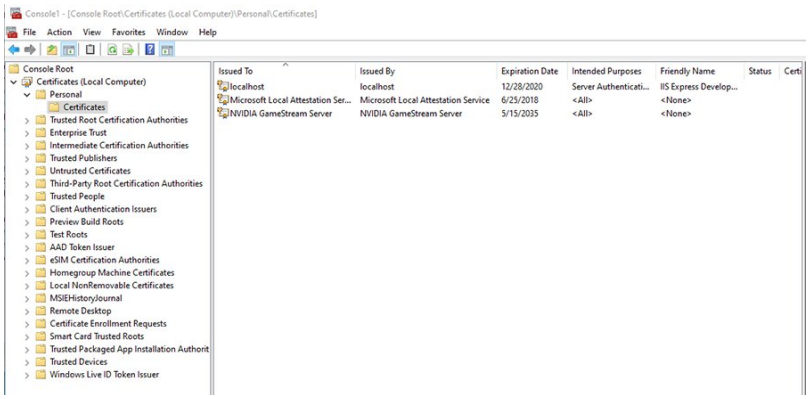
BRIEN POSEY



The option to import a root certificate that you need your endpoints' firewall(s) to trust

1. After verifying -- and importing, if necessary -- the root certificate that will allow Windows to trust the SSL certificate, it is necessary to check for the existence of the SSL certificate. Navigate through the console tree to Certificates (Local Computer) | Personal | Certificates
2. If the SSL certificate does not exist or has expired, right-click on the **Certificates** container and choose the **All Tasks | Import** commands from the shortcut menus
3. Follow the prompts to import the certificate

BRIEN POSEY



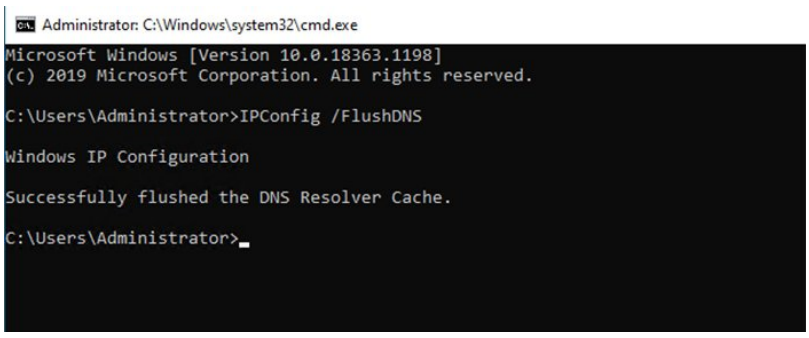
The list of trusted SSL certificates for the firewall

4. DNS problems

Many remote desktop connectivity problems can be traced to DNS issues. If an admin changed a host's IP address, then clients might not be able to connect to the host until the client's DNS resolver cache expires. To expire a DNS resolver cache, follow these steps:

1. Open an elevated **Command Prompt** window by entering the CMD command at the Windows Run prompt.
2. Enter the **IPConfig /FlushDNS** command.

BRIEN POSEY



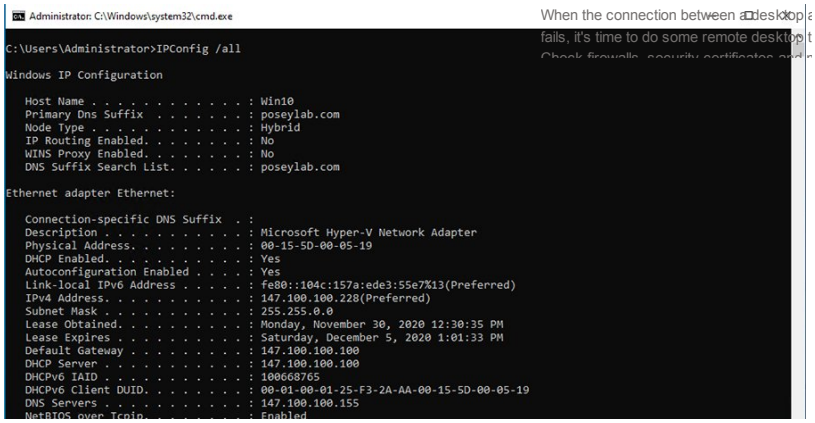
The process for resolving the DNS cache

Clients may also have trouble connecting to a host if they use an external DNS server that is unable to resolve hosts on the organization's private network. The fix for this problem is to modify the client's IP address settings so it uses one of the organization's DNS servers rather than an external DNS.

As an alternative, you may be able to connect to a remote system by specifying its IP address rather than a host name. To determine whether an

1. Open a **Command Prompt** window by entering the CMD command at the Windows Run prompt
2. Enter the **IPConfig /all** command
3. Verify that the correct DNS server is being used with the Preferred network adapter. If the DNS server listed is incorrect, then you can manually specify a different DNS server in the PC's IP address properties or configure the PC to use a DHCP server

BRIEN POSEY



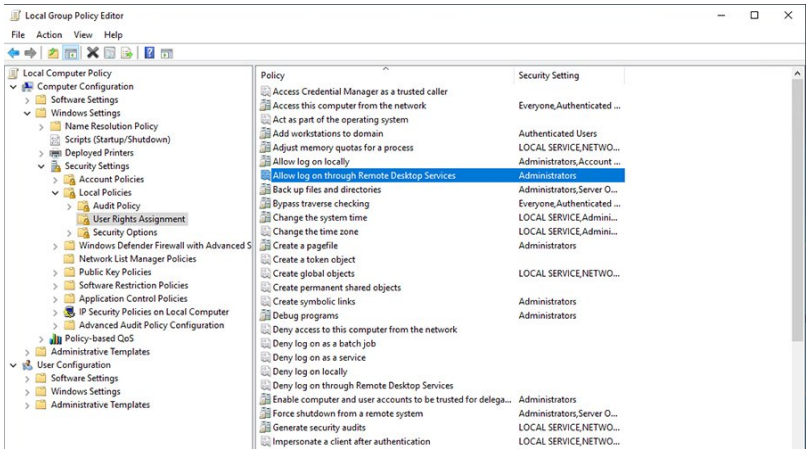
The process to verify that a PC is pointed to the proper DNS server

5. Insufficient permissions

For users to access a remote resource through the Remote Desktop Services, formerly known as Terminal Services, you must assign them the Logon Through Remote Desktop Services right. Otherwise, the users will receive an error when they try to connect to the remote resource. To make sure you have the proper permissions assigned, complete these steps on the remote server:

1. Open the **Group Policy Object Editor** by entering the GPEdit.msc command at the Windows Run prompt
2. Navigate through the console tree to Computer Configuration \ Windows Settings \ Security Settings \ Local Policies \ User Rights Assignment
3. Double-click on **Allow log on through Remote Desktop Services**
4. Add the necessary groups and click **OK**

BRIEN POSEY



Verifying that the endpoint has the right permissions to access Remote Desktop Services

6. Capacity exceeded

You could also experience remote desktop connectivity issues if you exceed infrastructure capacity. In an organization with virtual desktops or VDI, for example, clients may be unable to connect if the available licenses have been depleted. Some VDI implementations also refuse client connections if the server is too busy or if launching another virtual desktop session would weaken the performance of existing sessions.

7. Dropped connections

Sometimes the client can establish an RDP session, but the available bandwidth is inadequate to support the session's requirements. Depending on the RDP client used, this problem can manifest itself in a variety of ways.

The session may appear to freeze, or you might see a black screen. In some cases, the client may drop the connection and display a message that says 'Reconnecting.' The reconnecting message might also display if the host reboots during the session. This could occur if you have recently installed a Windows update.

If you suspect there might not be enough bandwidth to support the RDP session, try closing any applications that may be consuming bandwidth. If users are working from home, they should consider shutting down any other devices -- for example, someone streaming Netflix in another room -- that may be

You can adjust the RDP client to use a lower display resolution or color depth and disable visual features such as font smoothing or the Windows background. To reduce the bandwidth consumption of the native Windows RDP client, follow these steps:

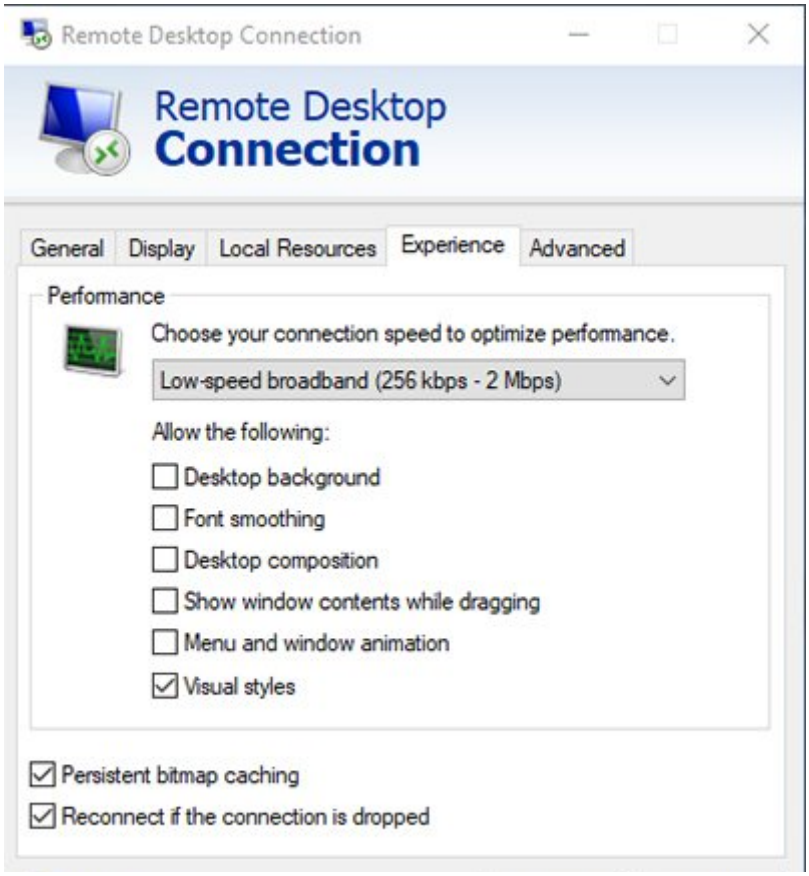
Up Next

How to fix 8 common remote d connection problems

When the connection between a desktop a fails, it's time to do some remote desktop t

1. Open the **RDP client**
2. Expand the console by clicking on the **Show Options** link
3. Select the **Experience** tab
4. Select the **Low-speed broadband** option from the drop-down menu
5. Click **Connect**

BRIEN POSEY



The remote desktop session Windows with the low-speed broadband option selected

8. CredSSP problems

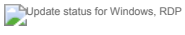
RDP connectivity can sometimes fail due to issues with the Credential Security Support Provider (CredSSP) protocol. The CredSSP provides a means of sending user credentials from a client computer to a host computer when an RDP session is in use.

In 2018, Microsoft updated the CredSSP to fix a security vulnerability. Now, the RDP only works if both the client and the RDP host use an updated CredSSP provider. If a system does not include an up-to-date CredSSP provider, the client will typically display an authentication error. Depending on which RDP client you use, this error may even indicate that the issue was caused by CredSSP.

The best way to fix this is to ensure that both the client and the host are running supported Windows versions and both systems are fully updated. You can access Windows Update by:

1. Click on **Settings**
2. Click **Updates & Security**
3. Select the **Windows Update** tab
4. Click **Check for updates**

BRIEN POSEY



Verifying that the RDP server and the users' Windows 10 systems are fully up to date.

You can prevent most of these connection problems from persisting with some preplanning, and good remote desktop troubleshooting skills.

Understanding remote desktop connection management tools

How to fix a remote desktop microphone that's not working

Up Next

How to fix 8 common remote d connection problems

When the connection between a desktop a fails, it's time to do some remote desktop t Check firewalls, security certificates and r

Dig Deeper on Virtual desktop delivery tools

Fixing issues with a computer mouse on a remote desktop

By: Brien Posey

How to configure multiple monitors for remote desktop use

By: Chris Twiest

6 steps for when remote desktop credentials are not working

By: Brien Posey

Remote Desktop Connection Manager (RDCMan)

By: Alexander Gillis

Enterprise Desktop

PC sales head south as users look for reasons to buy

PC sales continue to sag as business users and consumers remain conservative in spending and wait to see if the macroeconomic ...

Comparing enabled and enforced MFA in Microsoft 365

When managing Microsoft 365 authentication, IT admins may encounter the distinction between enabled and enforced MFA. Find out ...

Up Next

How to fix 8 common remote c connection problems

When the connection between a desktop fails, it's time to do some remote desktop t Check firewalls, security certificates and r