TechTarget | SearchVirtual Desktop

E-guide

PRO+ Content

How to Fix 8 Common Remote Desktop Connection Problems

In this e-guide

In this e-guide:

Remote connectivity problems such as network failure and issues with firewalls, expired certificates, failed authentication, and more can wreak havoc in your VDI environment. Luckily, most problems are easily fixed.

Here are some pointers to follow.

In this e-guide

How to fix 8 common remote desktop connection problems

Brien Posey, Microsoft MVP

Remote desktop connectivity is usually reliable, but things can -- and sometimes do -- go wrong.

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 virtual desktop admin, you can prevent and solve these problems using the following pointers on remote desktop troubleshooting.

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 or to the network.

In this e-guide

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.

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 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 port 3389 by default.

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

Some public networks block RDP traffic. This is especially true of the Wi-Fi networks found on cruise ships and in some hotels, airports and coffee shops.

Firewall issues also sometimes come into play when using 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.

In this e-guide

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.

In this e-guide

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. Enter the following command on the client computer to clear the cache and force DNS names to be freshly resolved: **IPConfig /FlushDNS**

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.

Authentication errors

Authentication issues can also arise when accessing a remote system via RDP. Most of the time, such errors occur because the user account does not have the required permissions.

Even if a user can log on locally to a system, it does not mean they will be able to log on remotely. Windows maintains separate permissions for logging on locally and

remotely. You should ensure users have the proper credentials associated with their remote desktop and not just with their local desktop.

Capacity exceeded

You could also experience remote desktop connectivity issues if you exceed infrastructure capacity. In an organization with virtual desktop 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.

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 consuming internet bandwidth.

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.

CredSSP problems

RDP connectivity can sometimes fail due to issues with the Credential Security Support Provider 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 works only 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 have been fully updated.

In this e-guide

You can prevent most of these connection problems with some preplanning, and good remote desktop troubleshooting skills help when other issues come up. Ensure your SSL certificates are updated, configure firewalls correctly and keep an eye on your VDI capacity.

Further reading

In this e-guide

About SearchVirtualDesktop

SearchVirtualDesktop.com features in-depth articles, tips and news around today's evolving desktop virtualization trends and technologies from key experts in the field, including outspoken industry guru Brian Madden.

Take advantage of the countless articles and tips covered on our site across numerous critical VDI topics, such as building and managing virtual desktop infrastructures, cloud-hosted desktops and apps, the VMware vs. Citrix debate, VDI for mobile, and much more.

For further reading, visit us at http://SearchVirtualDesktop.com/

Images; Fotalia