KB001279: TESTING REMOTE DESKTOP CONNECTIVITY FOR CLOUD-HOSTED ENVIRONMENTS PROVIDED BY K2

NEIL MAARTENS, K2 LEARNING

5/3/2016

Contents

OVERVIEW

K2 may provide online, cloud-hosted virtual K2 environments for training events, product evaluation, product testing or other short-term requirements ("events"). These K2-provided virtual environments are hosted on a cloud service (Microsoft Azure) which is reachable via the internet. Users normally access these hosted virtual environments using the Microsoft Remote Desktop connection tool.

This knowledge base article describes how you can test whether a computer and the underlying network infrastructure is configured correctly to allow the remote desktop connection tool to work with these cloud-hosted environments. K2 provides a dedicated cloud environment that is used exclusively for testing Remote Desktop connectivity, and you will be connecting to this Test environment to perform the tests.

IMPORTANT NOTES ABOUT THE TESTS YOU ARE ABOUT TO PERFORM

1) These tests will only verify that the computer and network are set up correctly for Remote Desktop Connections to work with the infrastructure used for the K2-provided virtual environments. You will be connecting to a dedicated Test-only environment to perform the tests. The virtual environment used during the event is a different environment, and may not be available until that event starts. You will receive the connection information to connect to your dedicated virtual environment before the event starts.

2) Your virtual environment will have a different IP address and DNS name than the Test environment used to perform these connectivity tests. If your network administrator needs to make firewall exceptions based on IP address or DNS name, please ask them to review the Network Administrator Notes section of this document.

3) If you use a different computer or different network during the event, you may need to perform these tests again to verify that the other computer/network can connect.

4) We will use Microsoft Remote Desktop Connection to connect to the virtual environment, both for the tests and during the event. You should have Remote Desktop Connection installed and operational on your computer before attempting these tests. If you are not using Microsoft Windows, you may need to download an appropriate Remote Desktop client application for your operating system. Note that the Remote Desktop Connection tool is not provided or supported by K2.

5) The Screenshots provided may not exactly match the screens on your machine, but the steps should be the same

QUICK TEST

Start with the Quick Test steps as described below:

1) To test whether a computer will be able to connect to a K2-provided, cloud-hosted instance on the internet, please download the ***K2RDPTest.rdp*** connection file in the ***Download*** link on the right-hand side of the http://help.k2.com/en/kb001279.aspx KB article, or download the file directly from the following location: http://help.k2.com/files/4247.

> **Note** If file downloads or .rdp files are prohibited in your environment, please follow the instructions under the **Manual Test** heading

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

2) When downloading the .rdp file, you will be prompted to save the file or open the file. You may select either option: “Open With” will automatically open the connection, or alternatively you may save the file to a location on your computer, and then double-click the saved .rdp file to open the Remote Desktop Connection.

3) After opening the RDP file, you may see a login dialog box. If the security dialog box is shown, you may log on to the test environment using the following credentials:

Username	Denallix\K2RDPTest
Password (case sensitive)	K2pass!

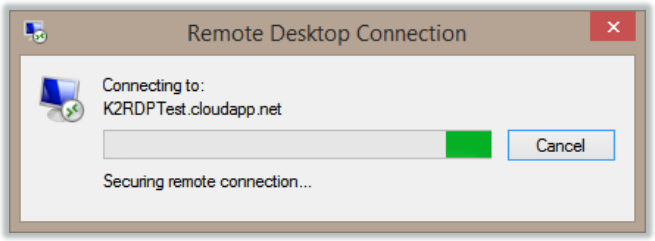
4) Once the .rdp file is opened, you will be prompted to connect to the environment. Click ***Connect*** or ***OK*** to connect the remote server.

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

Note

You may be presented with security warning dialog boxes similar to the ones below. You may click **Connect** to accept the security warning (The hosted environment is perfectly safe to use)

5) Your computer will attempt to connect to the remote server



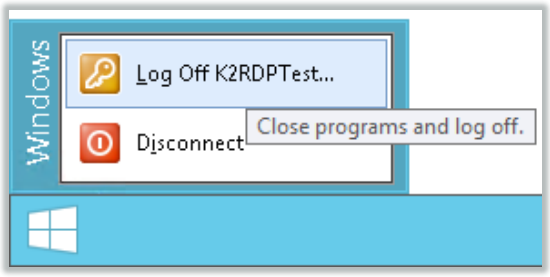
6) You should not need to provide the credentials again to log in to the Test environment, but if required, you may log on to the test environment using the same credentials as before:

Username	Denallix\K2RDPTest
Password (case sensitive)	K2pass!

7) If the connection was successful, you should see a confirmation message on the remote desktop, similar to the screenshot below:

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

8) If you can see this screen, the connection test was successful and you have verified that Remote Desktop Connection will work on the current computer and network during the Event. Please log off from the remote desktop environment by clicking the Start button (windows logo) and selecting ***Log Off K2RDPTest*.**



If the test was successful you can stop here. Remember that you will use a different hosted environment during the event itself, and you will receive the details for your dedicated virtual environment once your dedicated environment has been provisioned.

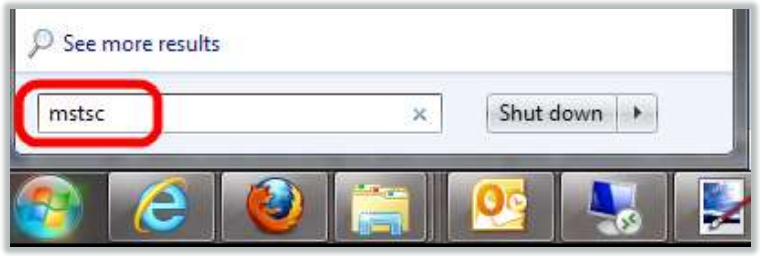
MANUAL TEST

If file downloads or .rdp file types are disabled in your environment because of security policies, or if you were not able to download the .rdp file in the Quick Test, please follow these steps to test the RDP connection manually:

1) On your computer, open the Windows ***Start*** Menu, click on ***All Programs***, then ***Accessories*** and then select ***Remote Desktop Connection***, or alternatively click in the ***Run*** textbox and type

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

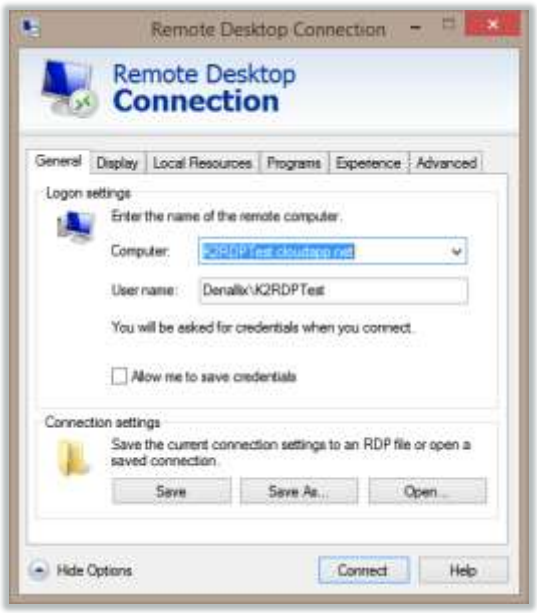
mstsc to launch Remote Desktop.

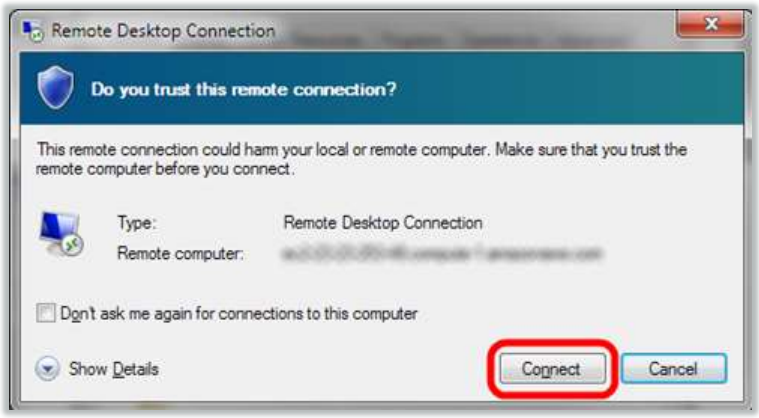


2) Once the Remote Desktop Connection application has opened, use the following credentials to connect to the Test Environment:

Computer Name	K2RDPTest.cloudapp.net
Username	Denallix\K2RDPTest
Password (case sensitive)	K2pass!
Remote Gateway *(this is only necessary if port 3389 is blocked by your firewall. Please see **Network Administrator Notes** for more information)*	awsrdg01.k2.com

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.



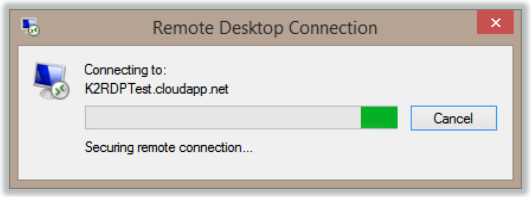


Note

You may be presented with security warning dialog boxes similar to the ones below. You may click **Connect** to accept the security warning (The hosted environment is perfectly safe to use)

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

3) Your computer will attempt to connect to the remote server

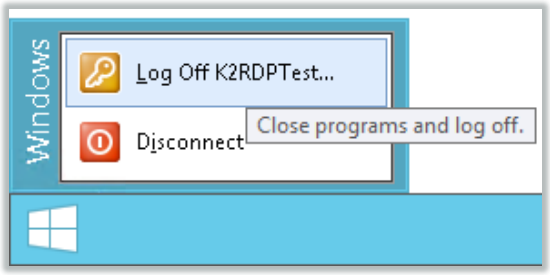


4) You should not need to provide the credentials again to log in to the Test environment, but if required, you may log on to the test environment using the same credentials as before:

Username	Denallix\K2RDPTest
Password (case sensitive)	K2pass!

5) If the connection was successful, you should see a confirmation message on the remote desktop, similar to the screenshot below:

9) If you can see this screen, the connection test was successful and you have verified that Remote Desktop Connection will work on the current computer and network during the Event. Please log off from the remote desktop environment by clicking the Start button (windows logo) and selecting ***Log Off K2RDPTest*.**



6) If the test was successful you can stop here. Remember that you will use a different hosted environment during the event itself, and you will receive the details for your dedicated virtual environment once it has been provisioned. You may need to connect manually to the Test Environment as described in this manual test, however.

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

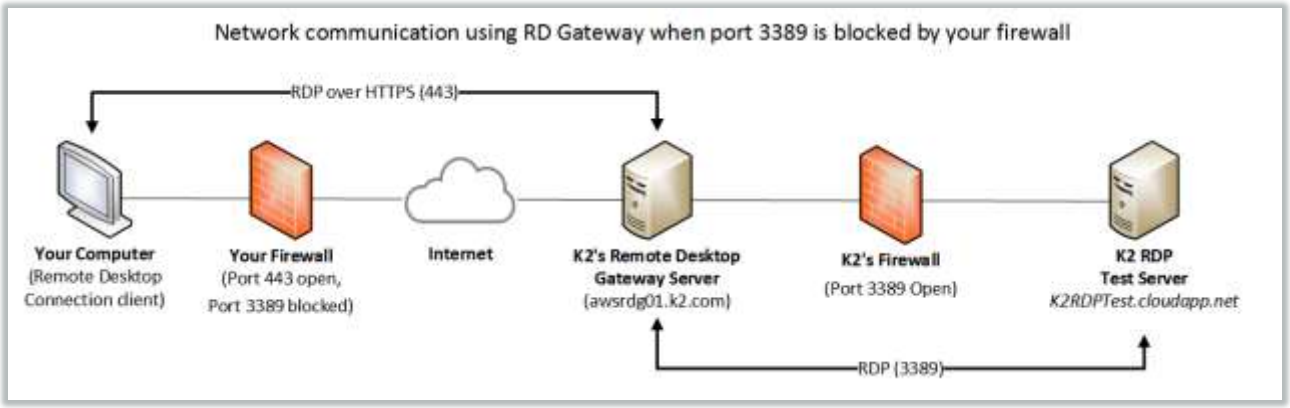
NETWORK ADMINISTRATOR NOTES

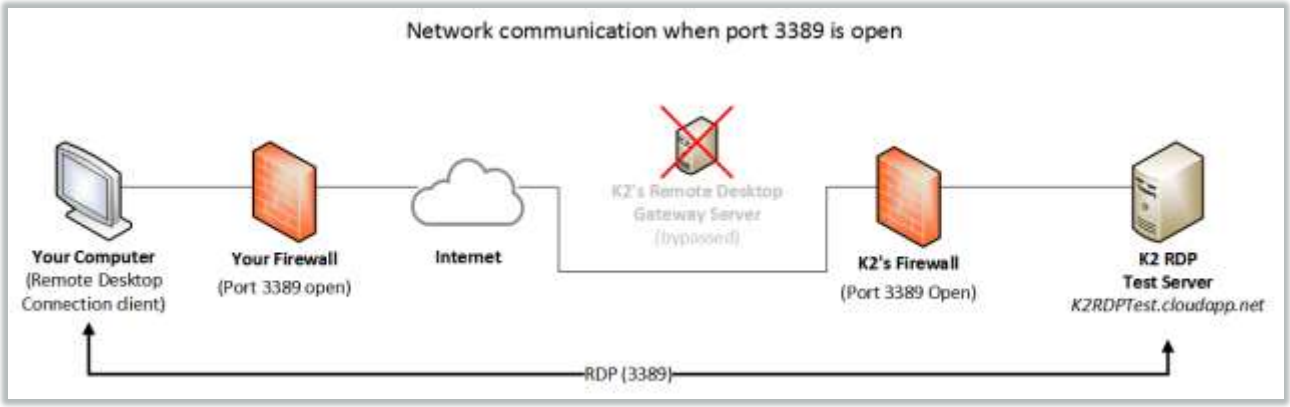
The following notes may help your network administrator configure Remote Desktop Connectivity for the Event

REMOTE DESKTOP GATEWAY

The K2 hosted instances do not require that port 3389 (RDP) is opened on firewalls to allow RDP traffic to pass through. If communication over port 3389 is blocked by your firewall, the K2-provided remote desktop connection file will automatically and transparently revert to a Remote Desktop Gateway server called *awsrdg01.k2.com* which will perform the necessary communication over port 443, just like normal HTTPS traffic. The Remote Desktop Gateway server will then connect to the test environment through the usual 3389 RDP port.

The diagrams below may help to illustrate the differences between using RDP (port 3389) or RDP over HTTPS (port 443).





Note

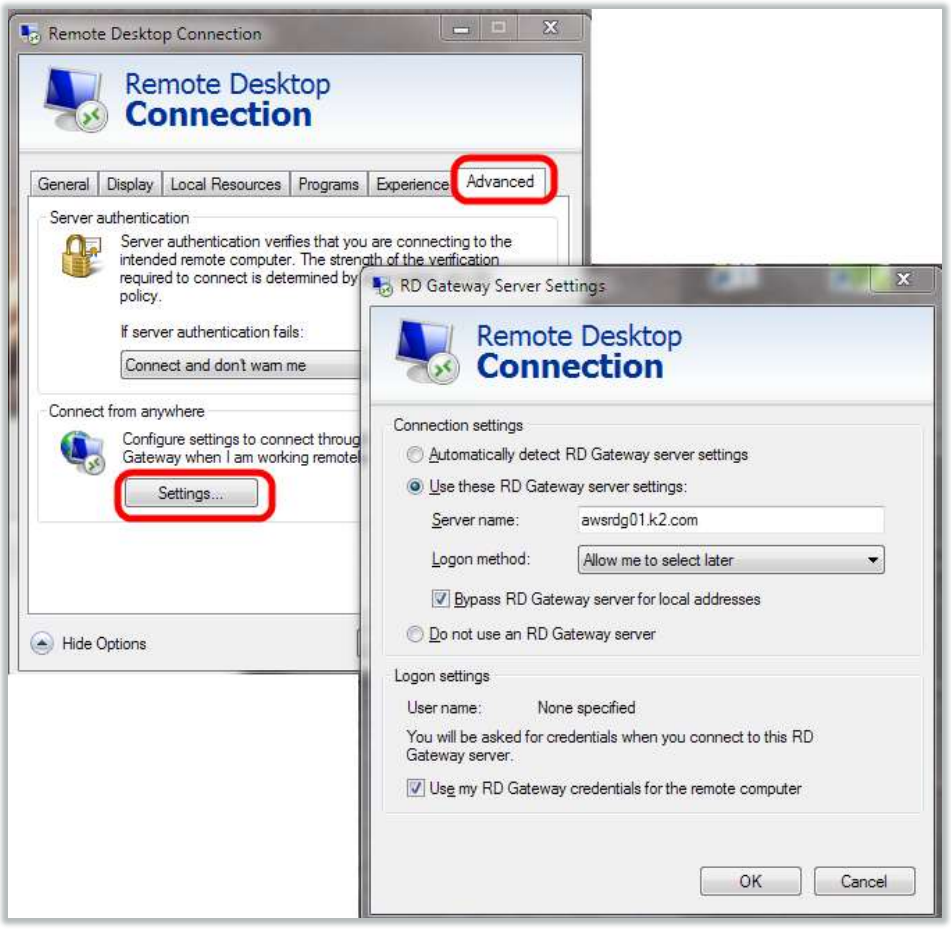
Not all client operating systems support the use of the Remote Desktop Gateway. At time of writing (May 2016), Windows XP can use gateway with version 6.1 of Remote Desktop Connector. Windows 2008, Vista, 2008 R2, 7, 8, 8.1, 10, 2012 all support RDGateway natively. There is no Macintosh client (both Microsoft's client and CoRD lack this capability) nor is there a Unix Remote Desktop client with Gateway connectivity. On the iPad, PocketCloud and iTap should work with the Remote Desktop Gateway

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

Note

While it is not required to open port 3389, opening this port can improve performance and provide a better user experience since the Remote Desktop Gateway server will be bypassed.

The setting to use the Remote Desktop gateway can be found in the .rdp file, under "Settings" > "Advanced Settings"

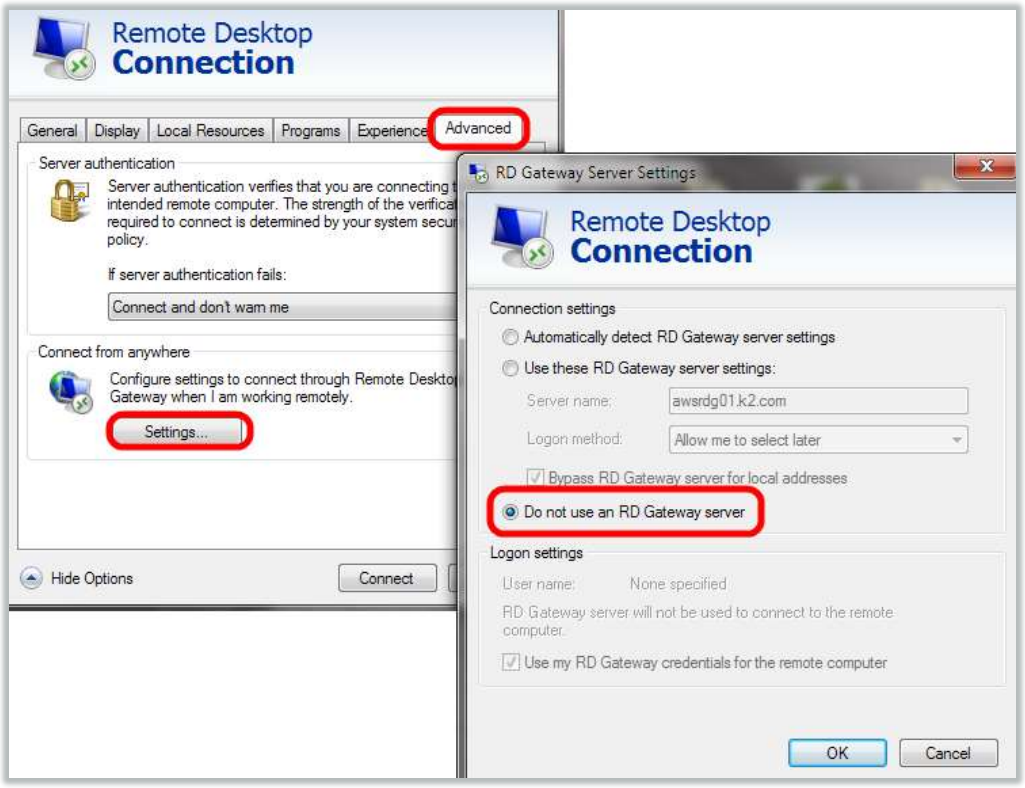


Disabling the Remote Desktop Gateway setting

To disable the Remote Desktop Gateway setting, edit the downloaded .rdp file, then go to the ***Advanced*** tab, click ***Settings*** and then select the ***Do not use RD Gateway Server*** option. This has worked for some computers that cannot work through a Remote Desktop Gateway, or that have

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

security issues with the certificates.



IP ADDRESSES AND DNS NAMES

While the Test environment used for these tests has a static IP address and DNS name, please be aware that the virtual environment(s) provided for the event will have different DNS names and IP addresses. Since these DNS names and IP addresses are dynamically determined when the environments are provisioned, it is not possible to provide an IP address range or predict the exact DNS names that will be used. We can only predict that the DNS names will exist in the format **.cloudapp.net.*

Depending on your organization's security policies, you may need to define a blanket exception for these instances, or use an alternative approach if it is not possible to open port 3389 or port 443 for the hosted virtual environments.

Warning	The virtual environments' IP addresses will change if the environments are shut down or restarted. This behaviour is outside of K2's control and you should cater for this known behaviour as part of your exception rule, perhaps by adding a wildcard to the target domain (cloudapp.net) if possible. The machines' DNS names (e.g. C-999-AAAAAAAAA.cloudapp.net) will not change between restarts or when the machine is shut down, only the IP address will change.

NETWORK BANDWIDTH AND RDP PERFORMANCE

The virtual environments used for the event will be geographically located on the East Coast of the USA, mainland Europe or Japan, depending on the region where the event is being hosted. Once a virtual environment has been provisioned in one of these regions it is not possible to move it to

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

another environment. Historically, the performance of the underlying cloud infrastructure has not resulted in bottlenecks and any performance-related issues were normally due to bandwidth limitations. There may be some settings you can change on your network infrastructure to improve RDP performance, and you may want to review the notes in this Microsoft article.

You can tweak some of the .rdp file settings such as connecting to local resources or the color-bit depth for the remote session that may help to improve performance, but at the cost of some functionality or fidelity. See the section tweaking RDP settings for more information.

If your location has a very slow internet connection (e.g. 56kbps dial-up), you may need to revert to one of the alternative approaches to ensure an acceptable user experience during the event.

PROXY SERVER RESTRICTIONS

Your ISA or Proxy server may be restricting access to the Test environment or to the Remote Desktop Gateway server (awsrdg01.k2.com). You may need to temporarily disable the rules or modify the configuration of your Proxy or ISA server to allow connections to the Test environment and then to the dedicated environments for the duration of the event. If this is not possible, you may need to use one of the alternative options as described in the Alternative Approaches section of this document

SECURITY CERTIFICATE ISSUES

Client machines may report that the publisher of the remote connection cannot be identified, or that there are issues with the certificate for the remote machine. This is because the remote connections file has not been signed with a public certificate: you may read more about this warning in this Microsoft Article.

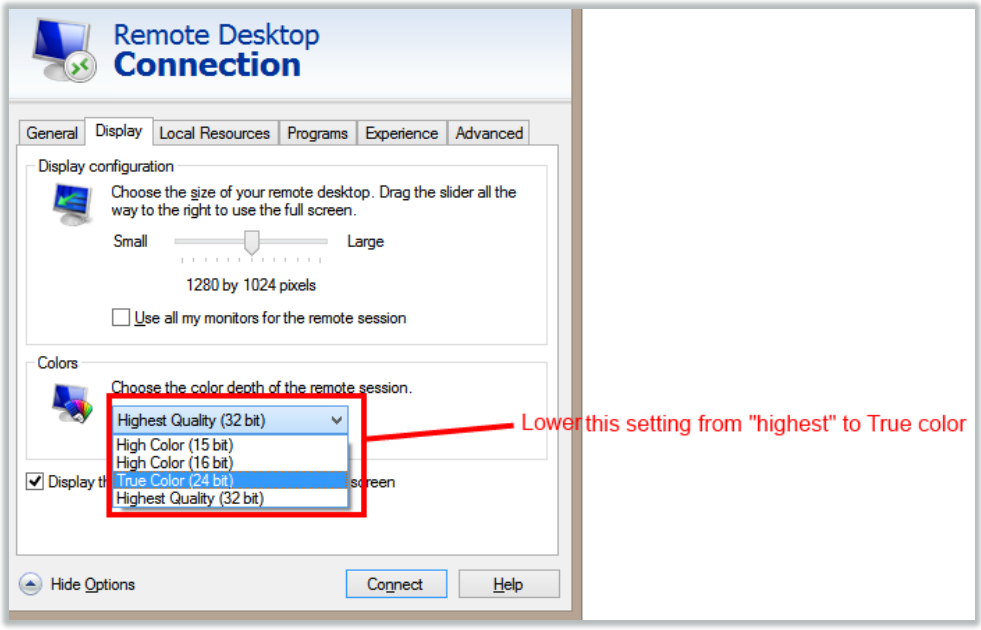
It is safe to connect to both the RD Gateway and the virtual environments, but if your organization has very strict security policies and cannot accept this restriction, you may need to use one of the Alternative Approaches.

TWEAKING RDP SETTINGS FOR BETTER PERFORMANCE

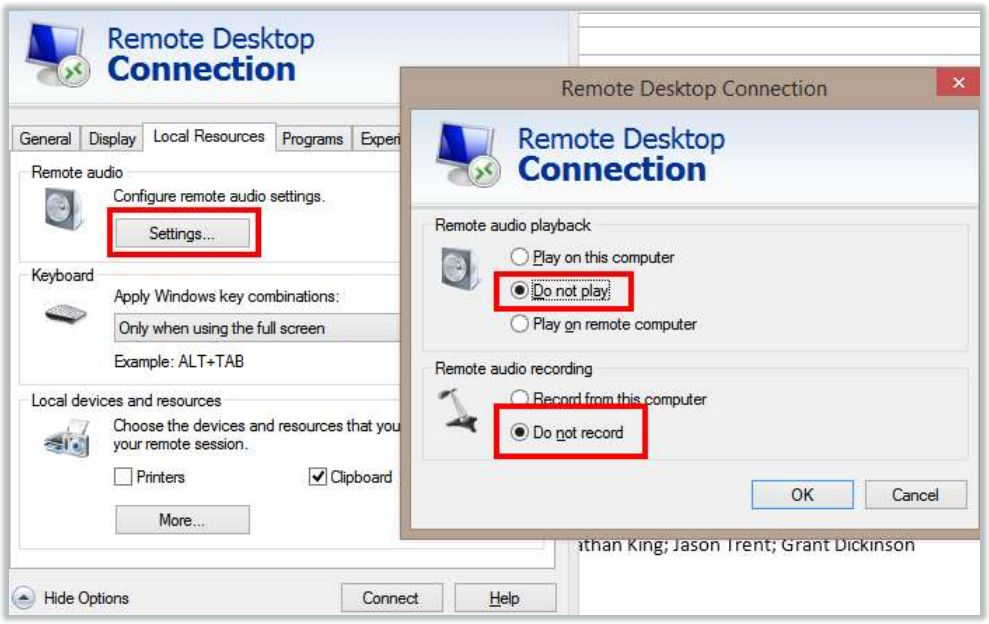
For environments with lower bandwidth, or if the user experience in the Virtual Environment is unacceptably slow, you can tweak some of the settings in the downloaded RDP file to try and improve the performance, but potentially at the cost of some functionality or fidelity.

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

1. Lower the screen **color depth**

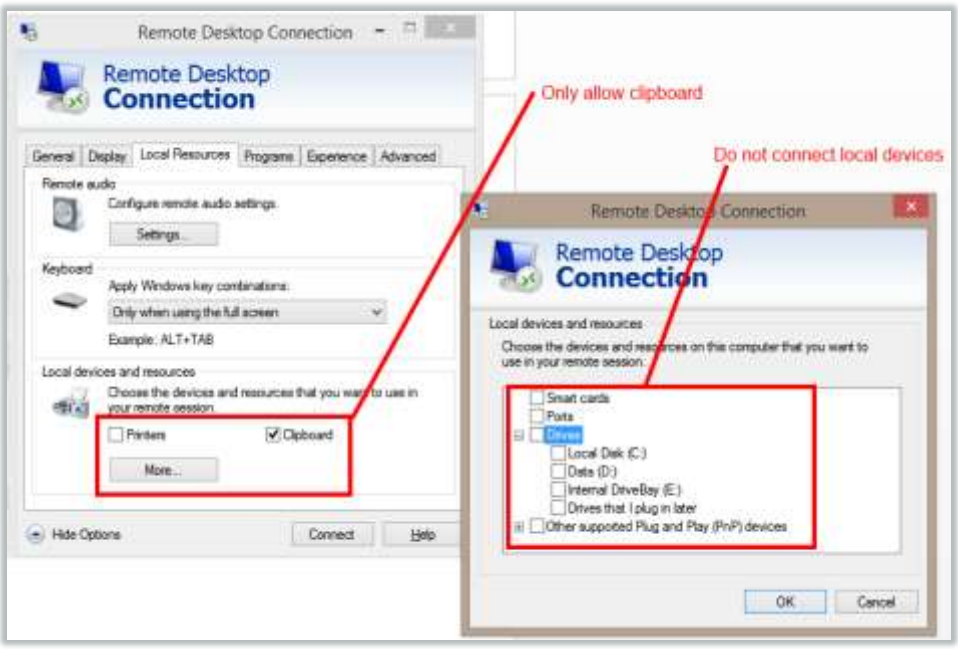


2. Disable **Remote Audio** settings

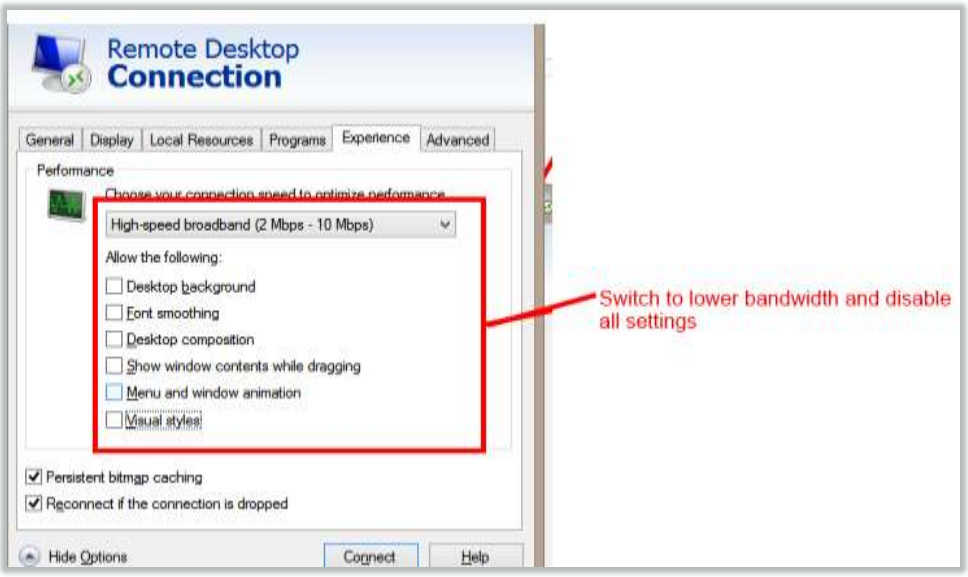


© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

3. Do not connect any **Local Resources**, apart from the clipboard



4. Switch to lower **Experience** settings, and disable all **Allow the following** settings in the Experience tab



5. Disable the Remote Desktop Gateway setting.

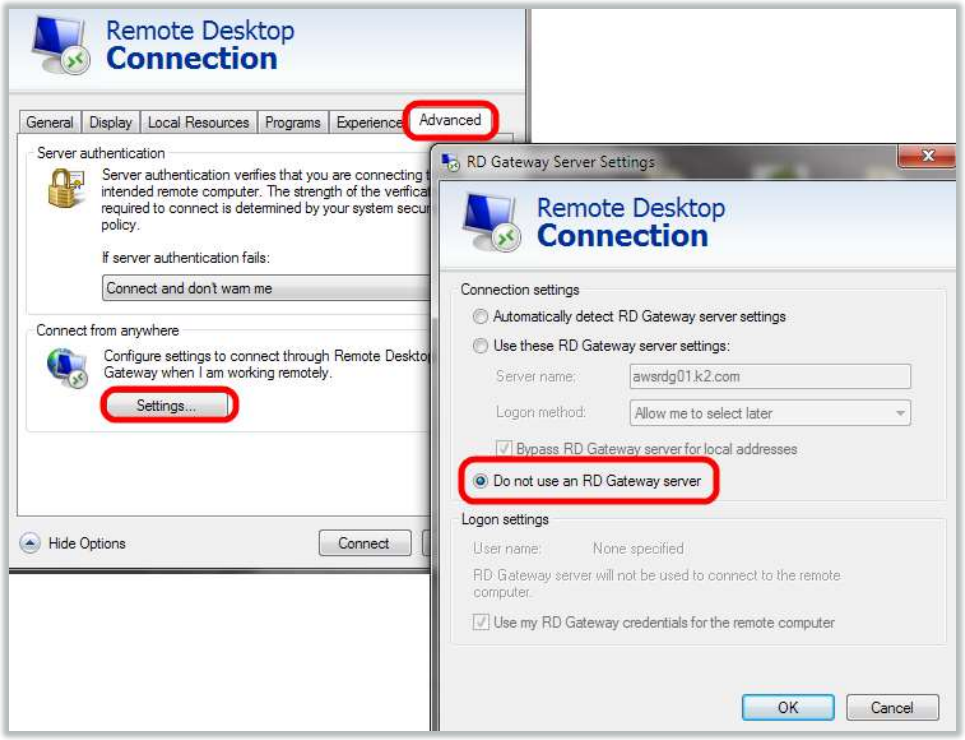
Warning

Changing this option might cause your connection to stop working, depending on you network's configuration. If you change this setting and are no longer able to connect, please revert back to the original setting that uses the *awsrdg01.k2.com* Remote Desktop Gateway.

In the **Advanced** tab, click **Settings** and then select the **Do not use RD Gateway Server**

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

option.



6. If you still experience a slow interface, use the built-in Windows Performance Monitor on the virtual machine to determine whether the virtual environment is running out of memory or CPU resources.

TROUBLESHOOTING

If you have trouble testing the connection, you may try the following troubleshooting steps:

1) Remote Desktop connection may not be installed or configured, in which case you may need to ask your IT department for assistance. Note that you may need to download a Remote Desktop Connection client if you are using a non-Windows operating system like Mac. Microsoft provides a Mac client for remote desktop connection. You must have access to the Remote Desktop Client to use the virtual environment.

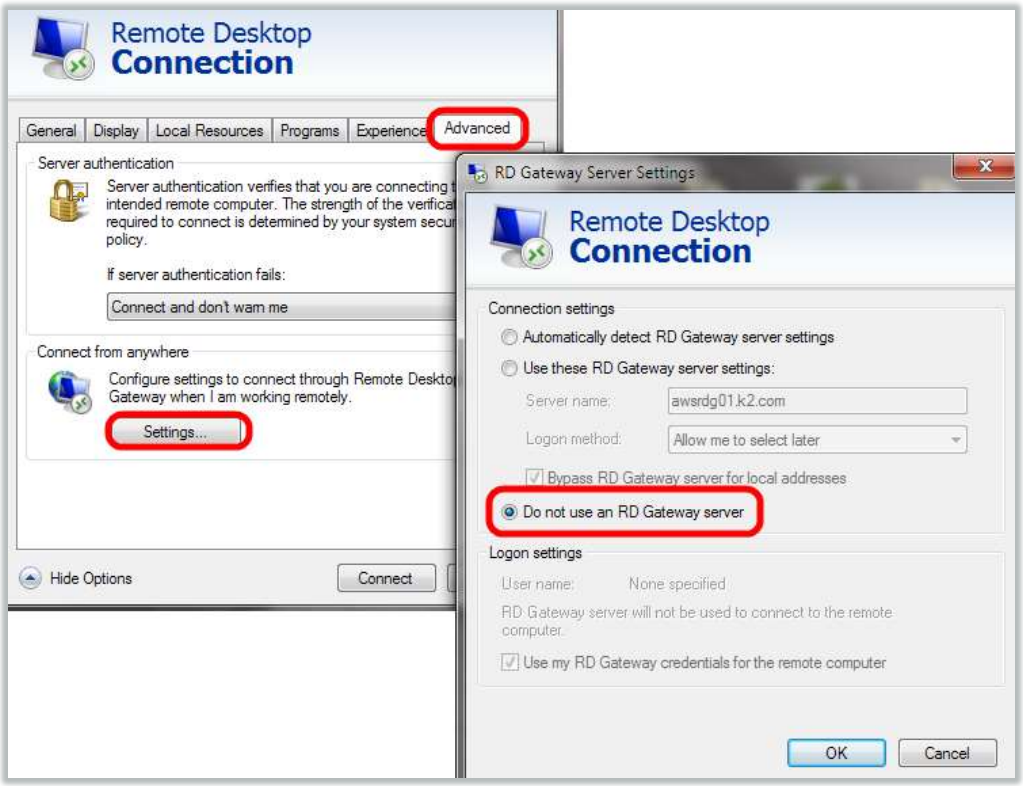
2) Your anti-virus software or software restriction policies may prevent you from downloading or opening an .rdp file. In this case, please try to connect manually as described in the **Manual Test** section of this document. If this is the case, note that you will need to repeat the same manual connection steps with your dedicated virtual environment, since that environment will use an .rdp file as well.

3) If you receive an error message while downloading the .rdp file or while connecting, wait a few minutes and then repeat the connection download/manual connection steps. Sometimes, the remote server may be too busy serving other Test connections, or the .rdp file may not have downloaded successfully.

4) Try to disable the option to use a Remote Desktop Gateway. Edit the downloaded .rdp file, then go to the ***Advanced*** tab, click ***Settings*** and then select the ***Do not use RD Gateway Server*** option. This has worked for some computers that cannot work through a Remote Desktop Gateway, or

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

that have security issues with the certificates.



5) Verify whether your computer can reach the hosted virtual server environment. To test this, use a tool like PSPing to ping the RDP server on the RDP port (3389)
psping K2rdptest.cloudapp.net:3389

You should see a set of responses like the ones shown below:

```
C:\Temp>psping k2rdptest.cloudapp.net:3389

PsPing v2.01 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to 13.92.97.135:3389:
5 iterations (warmup 1) connecting test:
Connecting to 13.92.97.135:3389 (warmup): 51.23ms
Connecting to 13.92.97.135:3389: 53.31ms
Connecting to 13.92.97.135:3389: 39.02ms
Connecting to 13.92.97.135:3389: 43.18ms
Connecting to 13.92.97.135:3389: 41.20ms

TCP connect statistics for 13.92.97.135:3389:
  Sent = 4, Received = 4, Lost = 0 (0% loss),
  Minimum = 39.02ms, Maximum = 53.31ms, Average = 44.18ms
```

If you do not get any responses (e.g. "Request Timed out" or "Ping request could not find host…"), it may mean that the K2 Test environment is offline, or another problem may be preventing communication. Please try step 6) before contacting your K2 representative for assistance, and check with your network administrator whether there are any security policies or restrictions in place that would prevent your computer from reaching the test server.

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

Note

The standard Ping.exe tool will not work, since the ICMP protocol is blocked by routing rules on the Azure infrastructure and cannot be enabled. See https://blogs.msdn.microsoft.com/mast/2014/06/22/use-port-pings-instead-of-icmp-to-test-azure-vm-connectivity/ for more information.

6) Use a different computer and, if possible, a different network to test the connection. Try the same test from another user's computer to verify whether this problem is isolated to your own computer. If the other user's computer can connect, you may need to enlist the help of your IT department to troubleshoot your computer, because it is possible that Remote Desktop is not installed or configured correctly on your machine.

   If the other computer cannot connect, try to use a different network connection to run the test again, if another network is available. Perhaps your organization has a "Guest" wireless network that you can connect to, or perhaps you can try the same test from your home network connection. If the connection is successful on the alternate network, the problem is likely a security restriction on your primary network. Please check with your network administrator what your options are: they may be able to temporarily remove the security restriction for the duration of the event, or perhaps you may need to use the alternate network for the duration of the event.

7) The virtual environments may take up to 20 minutes to start up and be available for accepting RDP connections. If you just started up your virtual environment from the control panel and are unable to connect to the environment, please wait for a maximum of 15 minutes before trying again.

8) Your or your IT department may refer to the following Microsoft articles which describe some more troubleshooting steps you can follow to resolve Remote Desktop connection issues:
   - http://azure.microsoft.com/en-us/documentation/articles/virtual-machines-troubleshoot-remote-desktop-connections/
   - http://support.microsoft.com/kb/187628
   - http://technet.microsoft.com/en-us/library/cc780927%28WS.10%29.aspx

9) If you experience a slow interface after tweaking the RDP settings, use the built-in Windows Performance Monitor on the virtual machine to determine whether the virtual environment is running out of memory or CPU resources.

ALTERNATIVE APPROACHES

If the troubleshooting section has not resolved your issue, here are some alternative approaches to allow users to use the virtual K2 environments. Please note that the alternative approaches may not be provided by K2 and you should clarify with your K2 representative whether your organization or K2 will be providing the alternative. Also clarify with your IT department whether a particular approach will be allowed based on your organization's security policies.

Suggestion	Notes
Open port 3389 or port 443 on your firewalls for the duration of the event	The easiest option is to enable port 3389 (or at least port 443) for the hosted environments for the duration of the event.
Define temporary exception rules on your firewall/proxy server for the duration of the event	Network administrator could define temporary exception rules on the firewall and/or proxy server to allow the remote desktop connectivity to work. Please refer to the Network Administrator Notes for more information. Remember that the virtual environments will have different IP addresses each time they are

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

	restarted.
Use an alternate network connection to connect to the internet	Your organization may have a guest network that the users can use for the duration of the event, or perhaps you can create a temporary network without the security restrictions for the duration of the event.
Use a temporary network connection (outside of your network infrastructure) to connect to the internet	If your security policy allows users to use their computers on a non-organization network, you could use a temporary network connection option like a Mobile Wi-Fi hotspot ("tethering") through a suitably equipped and enabled mobile phone, or a commercial product like MiFi to establish a temporary network connection that does not rely on your organization's network infrastructure. Performance-wise, a smart phone with its Wi-Fi hotspot enabled can connect several concurrent users to hosted environments with RDP and achieve reasonably good performance over both 3G and 4G networks. Most mobile service providers offer the service (sometimes at an additional charge) and many provide the service for a limited time or once-off charge
Allow users to attend the training event from their homes and use their home networks	For online or self-study training, it may be easier to allow users to attend the training from home and use their home internet connections to connect to the training session and the hosted environments. In this case, please ask each user to perform the test mentioned in this article to verify that their home network is configured correctly for Remote Desktop connectivity
Rent computers and/or internet connections for the duration of the event	If your organization has very strict security polices and it is not possible to make any changes to the client computers and/or network infrastructure, consider renting computers with a temporary internet connection solution like a MiFi device for the duration of the training event
Use an off-site training facility with computers and internet access for the training event	You may use an off-site training location that provides computers and internet connectivity for the duration of the training event. Some high-security customers prefer this approach since it completely isolates the training environment from their own network infrastructure and devices. Users will still have access to the training materials after the training event is completed, and since the temporary virtual environments are decommissioned after the event anyway, they do not need to (and cannot) connect to the virtual environments after the event has completed
Install the K2 virtual environment on each computer and run the virtual environment locally	K2 can provide the same virtual environment used for online hosted instances as a Microsoft Virtual Server (.vhd) image. Users can copy this image to their local machines and run the virtual server on their own computers. See the K2 KB article KB001397: K2 Virtual Machine Options and Prerequisites for information on downloading the vhd images. In this scenario, internet access is only required for the participants to be able to download the training material from a location on the internet. (If internet connectivity is not permitted at all, the instructor can provide the materials on a USB memory stick) Note that setting up the environment on local machines is a time-consuming process and is usually not a trivial exercise. If this approach is necessary, the time allocated for training should be adjusted so that the users' machines can be set up before training starts. We highly recommend arranging the logistics for this locally-run option ahead of time to ensure that the required resources are available and that the training plan caters for the additional set-up time. In addition, the local virtual environment option has a high level of minimum requirements for the user's computer (for example: a 64-bit host operating system, Virtualization software capable of running the Windows Server 2008 R2 64-bit operating system, 120GB free disc space, 16GB of RAM minimum, 18GB or more recommended). This is because the virtual environment used is essentially a full installation of several server technologies such as Active Directory, SQL Server, SharePoint, Exchange Server, CRM, K2 and others.
Other options	K2 may be able to provide alternative suggestions or alternative approaches for your specific environment or requirements. Please contact your K2 representative to discuss your options if the tests were not successful and if the alternative approaches do not work for your organization

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.

© 2016 SOURCECODE TECHNOLOGY HOLDINGS, INC.