# Remote Access

Remote access refers to the ability to access a computer, such as a home computer or an office network computer, from a remote location. This allows employees to work offsite, such as at home or in another location, while still having access to a distant computer or network, such as the office network.

**Remote access**  Connection to a data-processing system from a remote location, for example, through a remote desktop or [telnet](https://en.wikipedia.org/wiki/Telnet) services

TELNET

Developed in 1969, telnet enabled access to the command-line interface (CLI) of remote hosts. Telnet uses the client/server model, where the host you want to access remotely is configured as the server, allowing remote clients to control its CLI. The telnet protocol uses TCP and has port 23 defined as its standard by IANA.

On the 5thof March, 1973, the telnet standard was defined with the release of The Telnet Protocol Specification (RFC 8541) and the Telnet Option Specifications (RFC 8552

). These documents are referred as STD 8, meaning that it was one of the first Internet Standards defined by the Internet Engineering Task Force (IETF) and that it is compatible with the TCP/IP stack.When using the telnet protocol all information is transferred as plain-text in ASCII-format. The output on the CLI will therefore be presented identical on the client, as it would on a monitor directly connected to the host.

## Telnet Server

Telnet Server hosts the remote sessions for Telnet clients. When Telnet Server is running on a computer, users can connect to the server with a Telnet client from a remote computer. Telnet Server is implemented in Windows as a service that can be configured to always run, even when no one is logged on to the server.

When a Telnet client connects to a computer running Telnet Server, the remote user is asked to enter a user name and password. The user name and password combination must be one that is valid on the Telnet Server. Telnet Server on Windows supports two types of authentication: NTLM and Password (or plaintext).

Once logged on, a user is presented with a command prompt that can be used as if it had been started locally on the server console. Commands that you type at the Telnet client command prompt are sent to the Telnet Server and executed there, as though you were locally logged on to a command prompt session at the server. Output from the commands you run are sent back to the Telnet client where they are displayed for you to view.

Telnet does not support applications that require a graphical user interface. However, Telnet Server and Telnet Client understand special character sequences that provide some level of formatting and cursor positioning within the Telnet client window. Telnet Server and Telnet Client support the emulation of four types of terminals: ANSI, VT-100, VT-52, and VT-NT.

## Installing Telnet Server

On Windows Server 2008, you can install Telnet Server by using the Add Features Wizard in Server Manager. Although Server Manager opens by default when a member of the Administrators group logs on to the computer, you can also open Server Manager by using commands on the **Start** menu in **Administrative Tools**, and by opening **Programs**in **Control Panel**. On Windows Vista and later versions, you can install Telnet Server (and Telnet client) by opening **Control Panel**, then **Programs**, and then **Turn Windows features on or off**.

MICROSOFT RDP (REMOTE DESKTOP PROTOCOL)

RDP is Microsoft’s proprietary remote desktop offering. The first version of RDP was version 4.0 andwas introduced by Microsoft in 1998 as part of a special version of the Windows NT server OS. Although based on the ITU (International Telecommunication Union) T.120 series of protocols, RDP has been extended with a great range of features that is only support by the official application itself. Still, an open alternative based on RDP 5.0 (released in 2000) called Free RDP is available for download

Windows Server 2008 Remote Desktop Administration

Windows Server 2008 is, as the name suggests, a server operating system. In the real world this means that systems running Windows Server 2008 will most likely be located in large rack systems in a server room. As such, it is highly unlikely that system administrators are going to want to have to physically visit each of these servers to perform routine administrative tasks such as system configuration and monitoring. A far preferable scenario involves these administrators remotely logging into the servers from their own desktop systems to perform administrative tasks. Fortunately Windows Server 2008 provides precisely this functionality through Remote Desktop and the remote administration features of the Machine Management Console (MMC). In this chapter we will look at the steps necessary to remotely administer Windows Server 2008 systems using Remote Desktop.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | | |

What is Remote Desktop?

Remote Desktop allows the graphical interface of a remote Windows system to be displayed over a network onto a local system. In addition, keyboard and mouse events on the local system are transmitted to the remote system enabling the local user to perform tasks on the remote system as if they were physically sitting at the remote system. Conversely, resources (such as printers and disk drives) on the local system can be made available to the remote system for the duration of the connection. This remote control can be established in a number of ways, including over wide area networks (WAN), local area networks (LAN) or over the internet.

In the case of Windows Server 2008, this service is provided by *Terminal Services* running on the remote systems and the *Remote Desktop Connection* (RDC) client on the local system.

Terminal Services run in two different modes, *Administration* and *Virtual Session*. Remote Desktop for Administration provides full administration functionality to the remote administrator (including access to the console session and visibility of notification messages). Remote Desktop for Administration is the equivalent to working directly at the remote system's console. In virtual session mode the user is subject to some limitations such as the ability to install applications and view console notification messages.

Windows Server 2008 imposes some administrator logon restrictions. Specifically, a maximum of two administrators may be logged on at any one time, either two logged on remotely, or one local and one remote administrator. This assumes, however, that different accounts are being used to log on. In other words, the same user may not log on locally and remotely simultaneously.

Enabling Remote Desktop Administration on the Remote Server

As mentioned previously, remote desktop functionality on the server is provided by Terminal Services. It is important to note, however, that Terminal Services do not have to be explicitly enabled on the server in order to support Remote Desktop Administration. In fact, all that needs to be done is to enable Remote Desktop Administration. This is configured by opening the Control Panel from the Start menu and selecting the *System* icon (if the Control Panel is in *Control Panel Home* mode this is located under *System and Maintenance*). In the *Task* section in the top left hand corner of the System page select *Remote settings* to display the following properties window:

The Remote properties dialog provides a number of options. The default setting is to disallow remote connections to the computer system. The second option allows remote desktop connections from any version of the Remote Desktop client. The third, and most secure option, will only allow connections from Remote Desktop clients with Network Level Authentication support. This typically will only allow access to systems providing secure network authentication such as Windows Vista and Windows Server 2008.

If the Windows Firewall is active, the act of enabling Remote Desktop administration also results in the creation of a firewall exception allowing Remote Desktop Protocol (RDP) traffic to pass through on TCP port 3389. This default port can be changed by changing this setting in the Registry key HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-tcp\PortNumber. The easiest way to locate this registry key value is to execute *regedit* from the *Run* window or a command prompt, select *Edit - > Find* and enter *RDP-tcp*.

Controlling Remote Desktop Access

The default configuration for Remote Desktop is to allow all members of the Administration group to connect remotely. Active Directory also contains a *Remote Desktop Users* group to which users may be added to provide Remote Desktop access privileges. To provide users with remote desktop access, open the *Control Panel -> System and Maintenance -> System -> Remote settings* and click on the *Select Users* button to invoke the *Remote Desktop Users* dialog illustrated in the following figure:

Note that users with administrative privileges do not need to be added to this list; by default they already have Remote Desktop access. To add additional users click on the *Add...* button to display the *Select Users* dialog. Enter the name of the user in the text box entitled *Enter object names to select* and click on *Check names* to list names that match the name entered. Select the appropriate name from the list. The following example shows user *Bill* on server *winserver-2*:Click on *OK* to apply the change. The new user will now appear in the list of users with Remote Desktop access on the *Remote Users* screen. Click *OK* to close this screen and click on *Apply* in the System Settings screen. The specified user will now have remote desktop access to the system.

Remote Desktop Group Policy

A vast array of configuration options for Terminal Services is available through the Group Policy settings. To access these values start the Group Policy Object Editor (open the Start menu and enter*gpedit.msc* into the Search box). In the Group Object Policy Editor navigate to Computer Configuration\Administrative Templates\Windows Components\Terminal Services or User Configuration\Administrative Templates\Windows Components\Terminal Services to access the range of policy settings available.

Policy options include, amongst other options, items such as control over resource redirection (printers, audio etc), setting session time limits and security settings. A complete overview of all the settings is beyond the scope of this book but almost without exception the various settings are largely self-explanatory.

Starting the Remote Desktop Client

With the appropriate configuration tasks completed on the remote system the next step is to launch the Remote Desktop Client on the local system. The client can be run in either *administration mode* which provides full integration with the console of the remote server, or *virtual session mode* which provides some administrative privileges but does not provide console access or allow applications to be installed.

To invoke the Remote Desktop Client in virtual session mode either select *Start -> All Programs -> Accessories -> Remote Desktop Connection* or enter the following in the Run dialog or at a command prompt:

mstsc

To start the Remote Desktop Client in administrator mode run the following command:

mstsc /admin

In either case the following initial screen will appear requesting details of computer to which the client is to connect:

This can either be an IP address or a computer name. If previous connections have been established the *User name* field will be populated with the user name used in the preceding session. If you need to log in as a different user this option will be provided on the next screen which appears after the *Connect* button is pressed:

In this screen enter the password for the selected user (note that remote desktop access is only available for user accounts which are password protected). If a user other than the one displayed is required, simply click on the *Use another account* link and enter the necessary details. Click on OK to establish the connection. After a short delay the remote desktop will appear on the local computer screen.

Remote Desktop Client Configuration Options

The *Options>>* button displayed on the initial screen of the Remote Desktop Client provides six tabs, each containing a range of configuration options:

* **General** - Allows login credentials to be configured and session information to be saved.
* **Display** - Configures the resolution and color settings to be used when displaying the remote desktop on the local system.
* **Local Resources** - Specifies which local resources (sound, disk drives, printers etc) are to be made accessible to the remote system during the Remote Desktop session. This page also provides options to control the situations under which special key combinations such as Ctrl-Alt-Del are interpreted by the local or remote systems.
* **Programs** - Allows specified programs to be automatically invoked each time a remote sessions is established.
* **Experience** - Controls which desktop features are enabled or disabled for the Remote Desktop session. For example, over a slow dial-up connection it is unwise to have the desktop background displayed and font smoothing enabled. Either select the connection type and speed to see recommended settings, or use *Custom* to configure your own settings. This particular screen also provides the option to have the connection automatically re-established in the event that a session is dropped.
* **Advanced** - Enables and disables remote server verification. This ensures that the remote server to which you are connected is indeed the server you wanted. Also available are TS Gateway settings. By default the Remote Desktop Client is configured to automatically detect TS Gateway settings.