

12.6.3 Remote Desktop Facts

Remote Desktop lets you access your computer from a remote location over a network connection.

The quickest way to access Remote Desktop settings is to type **Allow remote access to your computer** in the search box on the taskbar.

With Remote Desktop:

- The remote host (called the server) is left running in a state ready to accept a connection.
- The remote client (running on a different computer) establishes the connection and logs on to the remote host.
- The client computer can then run programs, make configuration changes, or access data on the host computer.

Keep in mind the following details when working with Remote Desktop:

- The Remote Desktop service is supported only on Professional, Business, Enterprise, and Ultimate editions of Windows. It is supported only on Professional and Enterprise for Windows 10.
- The Remote Desktop client software is available on all editions of Windows.
- By default, the Remote Desktop feature is not enabled at installation. Edit the System properties to enable Remote Desktop.
- By default, Administrators have the ability to log on remotely. You can also allow other users to connect to the system by making them members of the Remote Desktop Users group.
- The user account that is used to authenticate through the Remote Desktop connection must have a password assigned. If one is not set, the connection cannot be established.
- Firewalls must be configured to allow Remote Desktop traffic through them. This is done by opening TCP port 3389 (by default). This port is opened automatically on the Remote Desktop host when remote connections are enabled.
- As you make the connection, you can configure the connection to redirect devices on the host device to the client device. For example, Remote Desktop can:
 - Play sound from the remote computer through the local computer's speakers.
 - Connect a printer on the local computer to the remote computer. When printing from an application on the remote computer, the print job is redirected through the Remote Desktop connection to the local printer.
 - Map local drives to the remote computer. This allows access to local drives from the remote computer. It also makes it easy to share files between the remote and local computers.

In addition to Remote Desktop, you can use the following protocols for remote access administration:

- Telnet opens a plain-text, unsecured, remote console connection. Telnet uses TCP port 23.
- Secure Shell (SSH) provides the same capabilities as Telnet, but encrypts the data being transferred. SSH uses TCP port 22.

These protocols are typically used to manage Linux and Macintosh computer systems. While they can also be configured on Windows, Remote Desktop is the preferred solution.

TestOut Corporation All rights reserved.