Activate and configure Remote Desktop for Administration on Windows Server 2003

On Windows operating systems, there is a built-in Remote Desktop function that allows users to access and access remote systems via an intranet or Internet. Assuming that in case you are far away but need to access the server in the company to work, you just need to activate and configure Remote Desktop.

On Windows operating systems, there is a built-in Remote Desktop function that allows users to access and access remote systems via an intranet or Internet. Assuming that in case you are far away but need to access the server in the company to work, you just need to activate and configure Remote Desktop.

In the following article, Network Administrator will guide you how to enable and configure Remote Desktop for Administration in Microsoft Windows Server 2003. After activation and configuration, you can access the server anywhere. have Internet connection as if using it directly on the computer.

1. Windows Server 2003 Terminal Services

Windows Server 2003 Terminal Services consists of two components:

1. ***Remote Desktop for Administration*** (***Remote computer administration*** tool)

   With Remote Desktop for Administration, administrators can remotely manage Microsoft Windows 2000-based and Windows Server 2003-based servers from any Terminal Services client. For presentation and collaboration purposes, two administrators can share a session. In addition, the administrator can remotely connect to the real console of a server using the **-console** command.

   Note :
   1. You do not need a license to access the Client Terminal Server when using Remote Desktop for Administration. However, only members of the administrative group can access the server.
   2. By default Remote Desktop for Administration is installed at the same time as Windows Server 2003, but is left inactive for a number of security reasons.
2. ***Terminal Server***

   Terminal Server allows multiple remote clients to simultaneously access the Windows-based programs running on the server at the same time. This is the usual form of Terminal Server deployment.

   When using a Terminal Server model, many concurrent connections that users do not belong to the administrator group will still be accepted. You can also install Terminal Services Licesing service on any member server. However, you must configure a copyrighted server on all destination servers. This server must contact copyright servers that do not have a domain controller but are configured as a domain name

server. Enterprise domain license servers are deployed on non-domain controllers that are detected automatically.

Before using Windows Server 2003 Terminal Services, you should review some of the following terms:

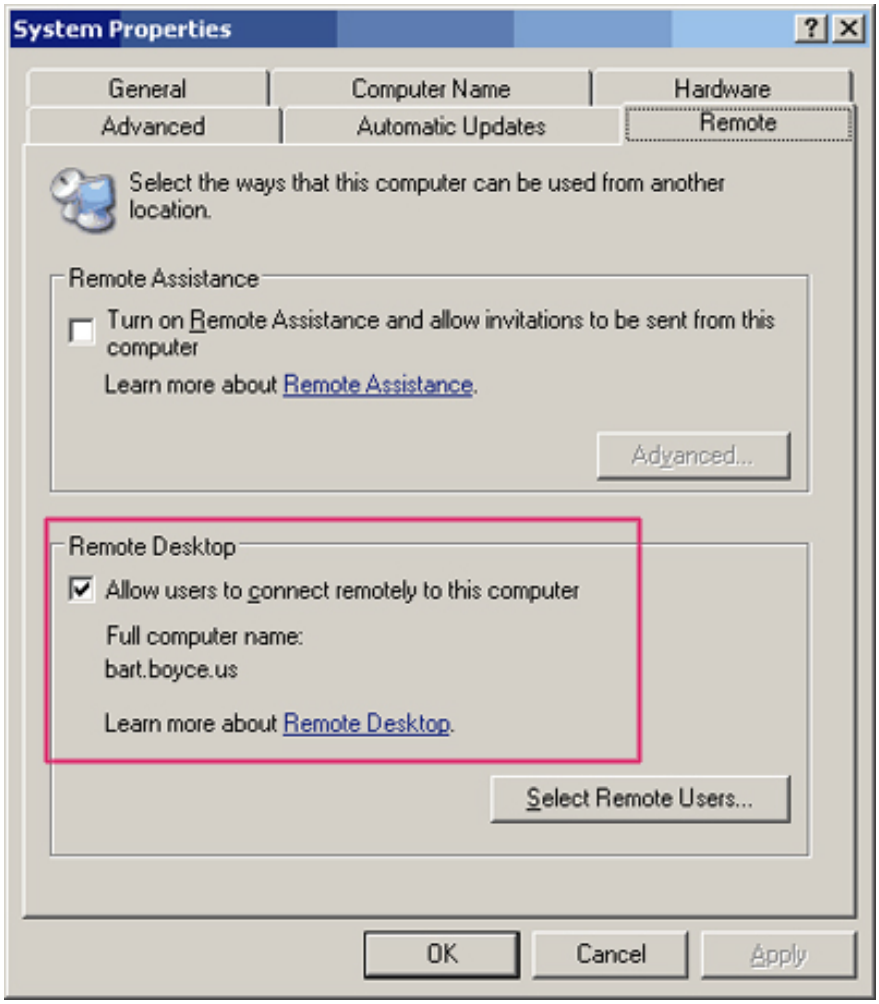
1. **Server** (server)
   Server is the server, which contains most computer resources. Server used in Terminal Services network environment. The server receives and executes information from the keyboard and mouse at the client. Then display the screen and the programs running on the server in a window on the client.
2. **Messaging** (messenger)
   Messaging is the activity of communicating between the server (server) and client (client) via Remote Desktop Protocol (RDP) 5.2. RDP is a protocol layer based on TCP / IP.
3. **Client** (client)
   The remote desktop running on the server is displayed in a window on the client. When starting a program on the client, these programs are actually running on the server. Remote Desktop Connection is the name given to the Terminal Services client in Windows 2000. Remote Desktop Connection uses the latest enhancements of RDP 5.2, providing significant enhancements over previous versions. Remote Desktop Connection can be used to connect to older versions of Terminal Services.

2. Use Remote Desktop for Administration

2.1. Activate Remote Desktop for Administration

By default, Remote Desktop for Administration is disabled. So if you want to use Remote Desktop you must enable this feature. To activate Remote Desktop, follow these steps:

1. ***Go to Start*** > ***Control Panel*** > ***System*** .
2. Click the ***Remote*** tab, select ***Allow users to connect to your computer*** (***Allow users to connect to your computer*** remotely) and click ***OK*** .



Note : You do not need to have a Terminal Server client access license when using Remote Desktop for Administration. The maximum number of two concurrent connections is allowed automatically on the last server when Remote Desktop for Administration operates.

2.2. Change the session encryption level

By default, the encryption level of Terminal Services sessions is set for Client Compantible to provide the highest level of encryption supported by the client. Other possible settings are:

1. ***High*** - this setting provides two-way security using 128-bit encryption.
2. ***Low*** - this setting uses 56 bit encryption.
3. ***FIPS Compliant*** : all data is encrypted using valid methods Federal Information Processing Standard 140-1.

To check the encryption level, follow these steps:

1. ***Go to Start*** > ***All Programs*** > ***Administrative Tools*** > ***Terminal Services Configuration*** .
2. In the left pane, click ***Connections*** .
3. In the right pane, right-click ***RDP-tcp*** and select ***Properties*** .
4. Select the ***General*** tab, select the encryption level you want in the ***Encryption*** list and click ***OK*** .

3. Debug and repair

If Terminal Services is not stable, please check your IP address. Issues may appear when you provide an invalid IP address. If a program runs unexpectedly, you can consider the following issues:

1. Programs with locked files or DLLs do not run correctly. This problem occurs when many users use a program at the same time.
2. Programs that use computer names or IP addresses for testing purposes may experience problems. This problem occurs when many users run the program at the same time when using the same computer name or IP address.

For more information about Windows Server 2003 Terminal Services, you can look in Help and Support Center, using the "Terminal Services" keyword.

4. Enable or disable Remote Desktop

4. Using Group Policies

To enable or disable Remote Desktop with Group Policies, follow the steps below:

1. Open Group Policy.

2. On Group Policy interface, navigate by **Computer Configuration, Administrative Templates, Windows Components, Terminal Services** , then find and double-click **Allow users to connect using Terminal Services.**

3. Take one of the steps below:

- To activate Remote Desktop, click **Enabled.**

- To disable Remote Desktop, click **Disabled.**

If Remote Desktop is disabled while the user connects to the destination computer, the computer still maintains the current connection but does not accept any other new connections.

Important note:

When you enable Remote Desktop on your computer, you can enable other users or groups to log on to the remote computer. However, you should consider allowing users who can log in to the remote computer and then add those users to the Remote Desktop Users group.

Some other notes:

- To perform the above steps, you must be a member of the Admin group in the local computer system (Local Computer) or you are granted a license. If your computer joins a Domain, members of the Domain Admin group have the right to do this.

- Follow the steps above to configure the internal Group Policy. To change a Policy for a Domain (domain) or a certain organizational unit, you must log in to the Primary Domain Controller under Admin. Then open Group

Policy using the Active Directory Users and Computers snap-in.

- Be aware of security issues when logging in remotely. Users who log in remotely can perform some unauthorized behavior. Therefore, you should create a firewall to protect the server.

- Requires all users to connect remotely to use a strong password.

- Remote Desktop is disabled on Windows Server 2003 operating system by default.

4. 2. Use System Properties

1. Open **System** on Control Panel.

2. On the **Remote** tab, select or deselect the option **Enable Remote Desktop on this computer** and then click **OK.**

Important note:

When you enable Remote Desktop on your computer, you can enable other users or groups to log on to the remote computer. However, you should consider allowing users who can log in to the remote computer and then add those users to the Remote Desktop Users group.

Some other notes:

- You must log in as a member of the Admin group to enable or disable Remote Desktop.

- To open Control Panel, click **Start** , then click **Control Panel** , then double click on the Control Panel icon.

- When using System properties, any settings configured Group Policy will override the default configuration.

- Be aware of security issues when logging in remotely. Users who log in remotely can perform some unauthorized behavior. Therefore, you should create a firewall to protect the server.

- Requires all users to connect remotely to use a strong password.

- Remote Desktop is disabled on Windows Server 2003 operating system by default.

On Windows operating system, there is a built-in Remote Desktop function that allows users to access remote systems via local network or Internet.

Refer to some of the following articles:

1. Set up and use Remote Desktop application in Windows 8

1. Setting up and connecting Remote Desktop in Windows 7

1. Instructions on how to login to your computer when you forget your password

Good luck!

and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.