Designing Terminal Server Connection Configurations

Use the following guidelines to design the configuration of the connections to your terminal servers. If you are using TSCC to configure a single server, you can use the Terminal Services Connection Wizard to configure these settings when you create a new connection. For more information about configuring Terminal Server with TSCC when you create a new connection, see "Make a new connection" in Help and Support Center for Windows Server 2003. You can also use Group Policy or WMI to configure the connections to many terminal servers. For a job aid to assist you in recording your Terminal Server Group Policy configuration decisions, see "Group Policy Configuration Worksheet" (SDCTS_2.xls) on the *Windows Server 2003 Deployment Kit* companion CD (or see "Group Policy Configuration Worksheet" on the Web at http://www.microsoft.com/reskit).

Data Encryption

You can assign data transfer encryption levels between the Remote Desktop client and Terminal Server by using either Group Policy or TSCC. The default RDP encryption level is **Client Compatible**. You can choose one of the following possible choices for encryption:

- **FIPS Compliant.** Encrypts traffic between client and server to meet the Federal Information Processing Standard 140-1 (FIPS 140-1). Use this level when Terminal Services connections require the highest degree of encryption, such as those required by the U.S. federal government.
- **Client Compatible.** With Client Compatible encryption, traffic between the client and the server is encrypted using the RC4 algorithm and the strongest key the client supports (40-bit, 56-bit, or 128 bit). The server negotiates with the client to determine the key strength on connection, however the server does not accept non-encrypted client connections.
- **High.** Traffic in both directions is encrypted using the RC4 algorithm and a 128-bit key only. If a client does not support 128-bit encryption, it is not permitted to connect.
- **Low.** Traffic from the client to the server only is encrypted, at the strongest key that the client supports. This can improve performance on the client because the client does not have to decrypt the screen update data coming from the server. The client still encrypts the keystroke and mouse data that it sends to the server. This also allows you to use products to improve performance over a WAN, for example to use between a branch and a home office. Use this setting only if you are planning to use these products. A malicious user can monitor documents and data coming from the server over the link if this setting is used.

On the **General** tab of TSCC or on the Data Encryption property page of the Terminal Services Connection Wizard, the **Use standard Windows authentication** check box is cleared by default. If you select this check box, lower security authentication mechanisms are permitted.

Logon Settings

By default, users are allowed access to the terminal server using the information that they provided to log on to their remote desktop client. For a more secure system, you can require users to provide logon credentials to access the terminal server.

You can allow access to the server based on the credentials provided here by clicking the **Always use the following logon information** radio button on the **Logon Settings** tab of TSCC or by enabling the **Always prompt client for password upon connection** Group Policy setting located in the Encryption and Security folder under Terminal Services in Computer Configuration. Use one of these options only if you are hosting an application that requires a password for access. For more information, see "Planning Terminal Server User Rights and Logon" earlier in this chapter.

Remote Procedure Call (RPC) Security Policy

You can enable this Group Policy setting to allow Terminal Server to accept only authenticated and encrypted requests. It is recommended that you enable this setting for increased security.

Sessions

You can set Terminal Server time-out and reconnection settings on the server to help manage the number of sessions held by a terminal server at any one time, to help manage unreliable connections for remote users, or to reduce the impact on the CPU of many users logging on to the server at the same time. You can set most of these settings by using TSCC or Group Policy. Exceptions are noted.

Note

- You can also set these settings per user through Group Policy User Configuration and through Active Directory Users and Computers user properties. However, the Group Policy computer settings listed here take precedence over user settings.

End a disconnected session

You can set a limit on the time that a disconnected session continues to exist on the server. There can be many reasons why a session becomes disconnected, for example if a user's computer fails or if the user places the session into a disconnected state in order to access the same session from another location. The programs and processes that the user had running before the disconnection continue to run during a disconnected session. Because a user can have a disconnected session running on the server without realizing it, it is best to set a limit on how long disconnected sessions continue to run on the server. However, by setting this as high as possible you can achieve better server performance by reducing the additional CPU usage needed when a user reconnects to the server.

Active session limit

You can set a limit on how long a user can maintain an active session with the server. If you choose **Never**, the server allows an active session to continue forever.

Idle session limit

You can set a limit on how long an idle session remains open. An idle session occurs if there has been no mouse or keyboard activity for a certain period of time. This can indicate that the user has stepped away from the computer, presenting someone else with the opportunity to use his or her session. When a session has been idle for more time than you have specified, the user is notified and given two minutes to place the session back into an active state. If the two minutes elapse, the server disconnects or ends the session, depending on the settings you choose. Just as with choosing a timeframe for ending a disconnected session, it is important to understand users' work patterns and needs when choosing a limit for idle sessions.

Note

- In a load-balanced farm, an idle session cannot be moved to a different server within the farm.

Session reconnection

By default, users can reconnect to a disconnected session from a computer other that the one from which they originally connected to the session. However, if a user connects from a Citrix ICA client, you can restrict the user to reconnecting only from the computer that originally connected to the session. This setting does not apply to Windows clients.

Session limit behavior

If you choose to enforce session limits for your users, you can ensure that users do not choose to have their sessions end when the connection to the server is broken for whatever reason. This way, you can be sure that all users can pick up where they left off in the event of a server failure, thereby reducing the loss of work and helpdesk incidents. If you choose to have sessions disconnect, you can use TSCC or Group Policy to specify the amount of time the session remains in a disconnected state.

Shut down options

You can use the following two Group Policy settings, found in the Terminal Services folder under Computer Configuration/Administrative Templates/Windows Components, to remove items from the **Start** menu and **Shut Down** dialog box so that users cannot use certain methods to disconnect or log off from their session:

- Enable the **Remove Windows Security item from the Start menu** policy to prevent users from unintentionally logging off of Terminal Server.
- Enable the **Remove Disconnect option from Shut Down dialog** policy to prevent users from using this method to disconnect from Terminal Server.

Automatic reconnection

You can allow a session to automatically reconnect to Terminal Server if the network connection is lost.

User Environment

Use the following settings to control the users' desktop environment.

Launch application on connection

If you are hosting a single application with Terminal Server, for example a line-of-business application or an application for task workers who use the server for only one thing, you can have that application start automatically when the user logs on. This eliminates the possibility of the user running unauthorized applications on the server or accessing other parts of the server or the network through the server. For information about how to start an application on connection, see "Specify a program to start when the user logs on" in Help and Support Center for Windows Server 2003. For more information about automatic logon, see "Planning Terminal Server User Rights and Logon" earlier in this chapter. You can configure this setting by using Group Policy (which you can apply to both computers and users), TSCC, and for users through the Remote Desktop Connection tool.

Desktop wallpaper

By default, sessions connecting to Windows Server 2003 Terminal Server do not display desktop wallpaper. For sessions connecting to servers running previous versions of Windows server operating systems and clients running Windows XP Professional or earlier, you can accomplish this by using Group Policy. For more information, see "Enforce removal of Remote Desktop wallpaper" in Help and Support Center for Windows Server 2003.

Note

- In Windows 2000 you can disable desktop wallpaper on the client from the **Environment** tab of the Terminal Services Connection Configuration tool.

Remote Control

You can use Remote Control to control or troubleshoot a user's session from a remote location. You can configure this setting by using Group Policy settings (which you can apply to both computers and users) or TSCC. If you choose to enable this in your organization, you can configure this setting in the following ways:

- Full Control with user's permission
- Full Control without user's permission
- View Session with user's permission
- View Session without user's permission

It is recommended that you configure this setting so that the user's permission is required to allow another person to access their computer through Remote Control. Keep in mind that even if you require a user to give permission, the user can choose to allow anyone who has acquired the correct permissions to access his or her computer. Also, some countries and regions have laws that do not allow the **View Session with user's permission** setting. If your organization has offices in several countries and regions, check the local laws before configuring Remote Control in this way. For more information about configuring sessions for Remote Control, see "Configure remote control settings" in Help and Support Center for Windows Server 2003.

Client Settings

You can use the settings discussed in this section to control certain aspects of the user experience and allow users to perform certain operations through their desktop computer rather than through the server.

Client/Server data redirection

You can use data redirection with Terminal Server to enable users to access and use resources from their desktop computers rather than from the terminal server. The most notable of these resources is printing, but you can also enable drive, audio, smart card, and clipboard redirection to the client computer. In general, restricting user's options to only those required to do their jobs can minimize the likelihood of introducing a vulnerability to the system. You can configure most of these settings through Group Policy (which you can apply to computers only) or TSCC. Exceptions are noted.

Note

- You can also configure redirection for disk drives, printer, and serial ports by using the Remote Desktop Connection tool on the client. For more information, see "Configuring Remote Desktop Connection" later in this chapter.

Table 4.3 summarizes the data redirection settings.

Table 4.3 Data Redirection Settings

Data redirection type	Characteristics
Time zone	Only configurable by using Group Policy. By default the session time zone is the same as the time zone of the terminal server. This can be an issue if you are using Terminal Server for remote or mobile users, especially when your line-of-business applications (for example, financial applications) have time dependencies.
Clipboard	By default, you can copy and paste between the terminal server and the Remote Desktop client. Disable this ability if you have sensitive data on the terminal server that should not be shared outside of the application in which it is used.
Smart card	Only configurable by using Group Policy. By default the ability to log on to the Remote Desktop client is allowed. For more information about using smart card with Terminal Server, see the "Planning Network Security Components" earlier in this chapter.
Audio	By default, users cannot play audio on the Remote Desktop client. The sound plays on the server rather than the client computer. If you enable this setting, users can specify on the Remote Desktop Connection tool whether to play audio at their computer or the server, or to not have the sound play at all.
Serial port	By default, Terminal Server allows users to redirect data to peripherals attached to the serial (COM) port. Disable this capability unless there is a requirement for it. This prevents users from printing or copying sensitive data stored on the terminal server, and reduces vulnerabilities to security threats that could access your computer through these ports.
Client printer	By default, users can redirect print jobs to a printer attached to their client computer. Unless users need to print to a local printer, disable this capability so that users cannot print or copy sensitive data stored on the terminal server.
Parallel port	By default, Terminal Server allows users to redirect data to peripherals attached to the parallel (LPT) port. Disable this capability unless there is a requirement for it. This prevents users from printing or copying sensitive data stored on the terminal server, and reduces vulnerabilities to security threats that could access your computer through these ports.
Drive	By default, Terminal Server allows users to redirect data to the drives on the client computer. Unless there is a requirement for this, you should disable this capability so that users cannot copy sensitive data stored on the terminal server onto their local computer.
Default printer	By default, Terminal Server designates the client default printer as the default printer in a session. Unless users need to be able to print to a local printer, disable this capability so that users cannot print or copy sensitive data stored on the terminal server.

Color depth

You can reduce or increase the maximum color depth depending on your bandwidth and fidelity requirements (greater color depth requires more bandwidth and resources on the terminal server).

Number of connections

By default, an unlimited number of sessions are permitted on the terminal server. Restricting the number of sessions improves the performance of Terminal Server because fewer sessions are demanding system resources.

You can configure this setting in the Terminal Services folder of the Group Policy Object Editor. In TSCC, you can configure the number of settings on the **Network Adapter** tab. You can also select the network adapter you want to use for the RDP connection traffic.

Permissions

You can use TSCC to change your permissions lists by adding and removing users and groups. You can also customize the permissions for users or groups on a per-connection basis. It is recommended that you give permissions to as few users and groups as is necessary, and to give those users and groups the lowest level permissions necessary for them to do their jobs. For more information about how to set permissions, see the topics under "Managing permissions on connections" in Help and Support Center for Windows Server 2003.