

Creating Custom Environments

In this chapter:

Loopback Processing	440
Terminal Services	444
Group Policy over Slow Links	461
Summary	469

This chapter focuses mainly on modifying the default behavior of Group Policy objects (GPOs) in custom environments, such as when a user's computer is connecting to the network in a unique manner or needs special configurations. We will investigate the GPO settings that allow you to control, secure, and configure these environments to ensure a functional but secure environment.

The scenarios we will examine here may include the use of loopback processing, and this is reviewed first. Loopback processing is a unique and flexible option that allows for control of user settings through computer configurations. You can thus have control over the settings for all users who use a particular computer. We will next discuss Terminal Services sessions, which require special security and functionality control. Finally, we will look at slow link detection and how to control the GPO settings for slow link clients differently from those GPOs that typically affect all computers.

Active Directory Design and Normal GPO Processing

To design and implement custom environments, you need a good understanding of the basics of Group Policy, including how to design Active Directory® to facilitate deploying GPOs. Here are some basic and important concepts to remember with regard to designing Active Directory and deploying GPOs:

- You must design GPOs with consideration of delegation of administration in mind.
- Group Policy applies only to user and computer accounts, not group accounts.
- GPOs affect the container at which they are applied, as well as all subordinate containers through inheritance.

- GPOs affect all objects at the container at which they are deployed, including domain controllers, administrative groups, and administrative user accounts.
- An administrator can limit a GPO's scope of influence by configuring inheritance blocking, security filtering, and WMI filters.
- Keep your (organizational unit) OU structure to a maximum of 10 levels deep.

To design and implement custom environments, you also need a good understanding of how Group Policy is applied. Here is a quick summary of the order and precedence rules for how GPOs are normally processed.

1. When the computer starts, network connectivity also starts.
2. The computer account communicates with DNS and Active Directory.
3. The computer obtains an ordered list of GPOs that apply to the *computer*.
4. Computer policies under Computer Configuration are applied.
5. Computer-based startup scripts run.
6. The user is validated against Active Directory.
7. The user's profile loads.
8. The computer obtains an ordered list of GPOs that apply to the *user*.
9. User policies under User Configuration are applied.
10. User-based logon scripts run.
11. The user is presented with her desktop interface, as configured by Group Policy.

For more information on designing Active Directory and deploying GPOs, see Chapter 4. For more information on how Group Policy is applied, see Chapter 2 and Chapter 13.

Loopback Processing

User Group Policy loopback processing mode is a policy setting you can use to maintain a computer's configuration regardless of who logs on. Loopback processing mode configures the user policy settings based on the computer rather than on the user. When this policy setting is enabled, one set of user settings applies to all users who log on to the computer. Because this policy setting targets computer accounts, it is a powerful tool and ideally suited for closely managed environments such as servers, terminal servers, classrooms, public kiosks, and reception areas.



Note When you enable the policy setting for loopback processing mode, you must ensure that both the computer and user portions of the GPO are enabled.

The loopback policy is set in the Group Policy Object Editor snap-in by using the following policy setting:

Computer Settings\Administrative Templates\System\Group Policy\User Group Policy loopback processing mode

As shown in Figure 12-1, when you enable this policy you can select one of two loopback processing modes: Replace or Merge.

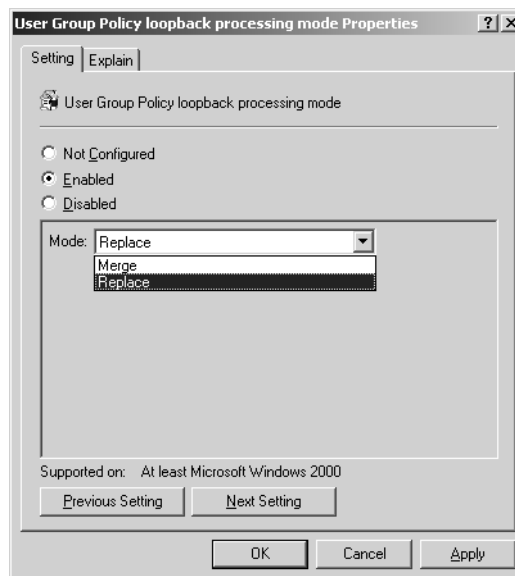


Figure 12-1 The Replace and Merge loopback processing modes

Replace Mode

In Replace mode, the list of GPOs and their settings for the user account is not used. Instead, the GPO list for the user is entirely replaced by the GPO list that was obtained for the computer at startup, and the User Configuration settings from the GPO that has the loopback setting configured are applied to the user account instead. This means that when loopback processing in Replace mode is enabled, policy is processed as follows:

1. The computer settings in the GPOs for the computer account are applied.
2. The user settings in the GPOs for the user account are ignored.
3. The user settings in the GPOs for the computer account are applied.

As a best practice, you might use Replace mode when you have computers that are exposed to the public—for example, if you have a computer that is located in the reception area of your company’s corporate office or a public kiosk that you provide somewhere within your office or company. When the public has access to the computer, you want to lock down the interface completely to ensure that the user cannot run operating system tools or other potentially dangerous applications on the computer.

Here are some best practices when using loopback processing in Replace mode:

- Create Software Restriction Policies that limit available applications to what the public user needs.
- Remove the entire shell except for Microsoft® Internet Explorer.
- Remove the user’s ability to gain access to features and functions by pressing Ctrl+Alt+Del.
- Disable the ability to right-click and access shortcut menus.
- Remove the Shutdown menu option and button.

Merge Mode

In Merge mode, the list of GPOs and settings for the user is gathered during the logon process. Then the list of GPOs and settings for the computer is gathered. Next, the list of GPO settings for the user account that are contained within the GPO with the loopback setting enabled is added to the end of the GPO settings originally compiled for the user account. As a result of this appending of the user settings, the GPO settings that were obtained from the GPO with the loopback setting configured will have higher precedence. Therefore, when loopback processing in Merge mode is enabled, policy is processed as follows:

1. Computer settings in the GPOs for the computer account are applied.
2. User settings in the GPOs for the user account are applied.
3. User settings in the GPOs for the computer account are applied, taking precedence over user settings in the GPOs for the user account.

Although Merge mode offers great control, it still allows many of the individual user GPO settings to affect the logon environment. Merge mode is appropriate for settings such as student labs, Terminal Services sessions, and classrooms. With Merge mode, you can control many of the environment features that are security risks while still providing users with their desktops, applications, and other features that allow them to perform their job functions.

Here are some best practices when using loopback processing in Merge mode:

- Access to Control Panel items

- Access to Add/Remove Programs
- Access to Network Configuration
- Controlling user profiles
- Controlling offline files

Troubleshooting Loopback

When you are testing and validating the use of the loopback feature, it will usually be obvious whether the correct settings are being applied. The difficulty arises when the correct settings are not being applied. Remember that when you are using Replace mode, none of the user settings from the GPOs affecting the user are applied, only user settings in the GPOs affecting the computer. Therefore, if you see any of the user settings coming through that you specifically did not configure in the GPO in which loopback processing has been enabled, the GPO in which loopback processing is enabled is most likely not being applied at all. Here are some possible reasons for this:

- The computer account is not in the correct OU to receive the GPO settings.
- The user or computer (or both) settings have been disabled for the GPO that has the loopback policy configured.
- The GPOs have not replicated properly to all of the domain controllers.
- The GPO containing the loopback policy has been filtered to not include the computer account you are targeting.

Another option for troubleshooting the application of loopback policy is to use the Group Policy Modeling Wizard or the Group Policy Results Wizard in the Group Policy Management Console (GPMC). The Group Policy Modeling Wizard allows you to evaluate a scenario for a particular computer account and user account based on specific GPO settings and criteria. This includes the ability to model the effects of loopback processing, as shown in Figure 12-2.



More Info For more information on how to use the Group Policy Modeling Wizard, see Chapter 3.

The Group Policy Results Wizard offers real-time evaluation of an existing user and computer account. After you run the wizard, you are presented with a summary of the settings that should be applied to both accounts. These results will indicate which policies were applied, the policy setting configuration, and which GPO the policy came from. If you run the wizard and learn that the loopback policy should be applied to the computer but hasn't been, you must evaluate the list of potential problems that are listed above. If the wizard indicates that no loopback setting is configured, you must determine where the GPO is linked and where the computer account is located.

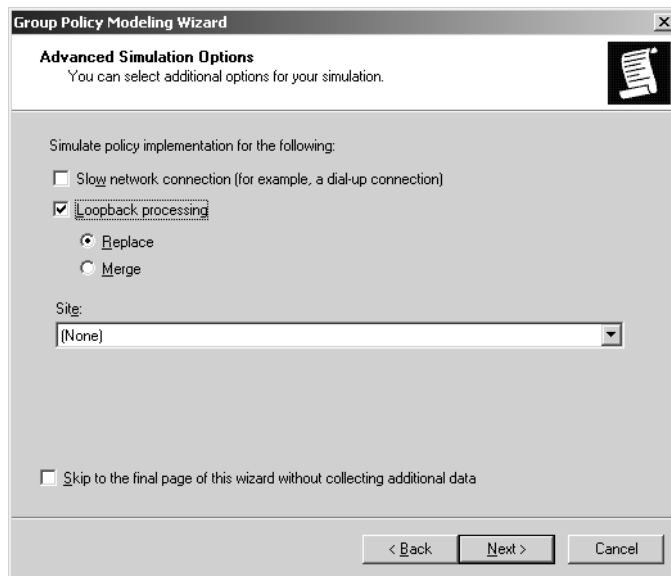


Figure 12-2 Evaluating a scenario by using the Group Policy Modeling Wizard

Terminal Services

If your company relies on Terminal Services for clients to access applications, the network, or resources, you know how important and powerful this technology is. Terminal Services allows a company to provide high-end solutions for legacy operating systems and limited hardware. Without Terminal Services, many companies would be far less productive.

Controlling and limiting Terminal Services sessions can be a full-time job. Terminal server sessions must be protected, along with the servers that run Terminal Services. This is why Microsoft has provided more than 50 Group Policy settings that help control Terminal Services. Many of these settings can be configured to help lock down terminal servers and client sessions.

You can use Group Policy to configure Terminal Services connection settings, set user policies, configure terminal server clusters, and manage Terminal Services sessions. You can enable Group Policy for users of a computer, for individual computers, or for groups of computers belonging to an OU of a domain. To set policies for users of a particular computer, you must be an administrator for that computer. To set policies for an OU in a domain, you must be an administrator for that domain.

Controlling Terminal Services Through Group Policy on an Individual Computer

Sometimes you might need to control the Terminal Services settings for an individual computer. The computer might be a shared computer for which you want to configure

the settings that apply to the computer object. You might also need to configure the Terminal Services settings for the user or users who will use the computer, and in this case you would want to configure the settings that apply to the user object.

You can access Terminal Services settings on a standalone computer by using local Group Policy. The Group Policy Object Editor snap-in allows you to access the Local Group Policy Object (LGPO) on that particular computer. Once you are in the Group Policy Editor, you can view and configure Terminal Services settings under both the Computer Configuration and User Configuration nodes, as shown in Figures 12-3 and 12-4.

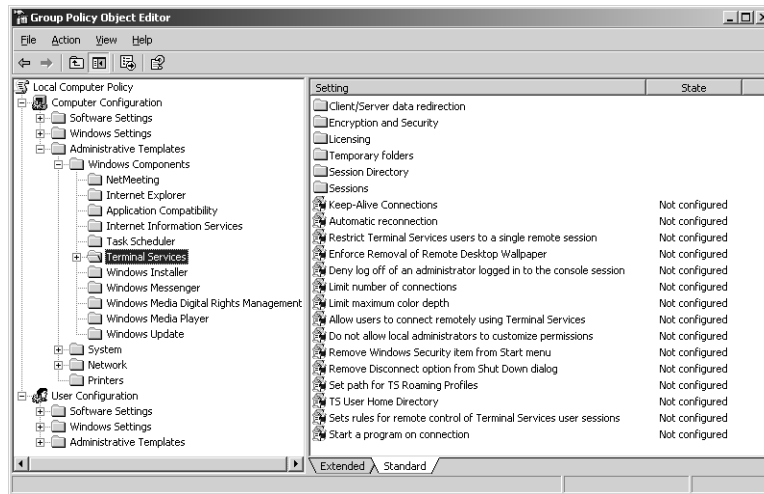


Figure 12-3 Terminal Services GPO settings under Computer Configuration

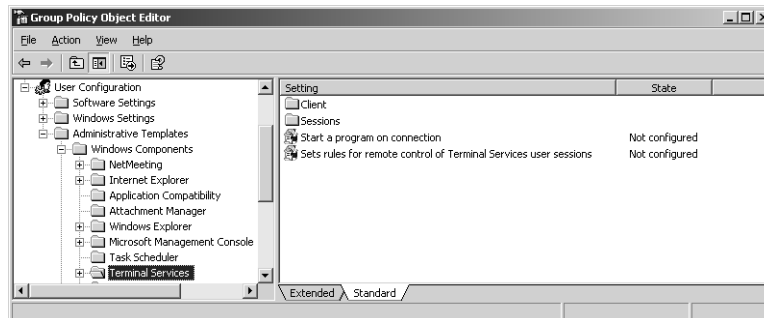


Figure 12-4 Terminal Services GPO settings under User Configuration

Controlling Terminal Services Through Group Policy in a Domain

In Active Directory environments, you may need to lock down several Terminal servers. The policy settings for locking down terminal servers in a domain are similar to those for standalone terminal servers, as shown above. The significant difference is in how you implement Group Policy for terminal servers in a domain.

To configure Terminal Services for multiple computers using Active Directory, you must organize the user and computer accounts into OUs. Then you can configure GPOs that contain the specific Terminal Services settings for those objects.



More Info For more information on how to design and deploy GPOs and Active Directory, see Chapter 4.



Important The Terminal Services Group Policies are geared toward computers running Microsoft Windows® XP and Windows Server™ 2003. If you are running Windows 2000 servers and clients, you cannot use Group Policy settings to control Terminal Services on these computers.

Configuring Order of Precedence

It is possible to make Terminal Services configurations at both the local and Active Directory levels using Group Policy. You can also make configurations within different GPOs at various levels within Active Directory. This is an issue because there is an order of precedence in which the Terminal Services configurations apply. The following is a list of highest to lowest precedence of the locations where Terminal Services settings can be set.

- Computer-level Group Policies (if set)
- User-level Group Policies (if set)
- Local computer configuration set with Terminal Services Configuration tool
- User-level policies set with Local Users and Groups
- Local client settings

Configuring Terminal Services User Properties

When Terminal Services is used in your environment, it is important to configure and control the user environment and properties. If you don't, the user might have too much access or too much flexibility for the sessions that are created on the Terminal Server. This section focuses on some best practices for the general settings related to user properties associated with Terminal Services. It also discusses the GPO settings that can be configured in this area.

Best Practices

Here are some general best practices for establishing user properties for Terminal Services. Your environment might differ slightly, but these suggestions will point you

in the right direction for establishing a secure, stable, and functional Terminal Services environment.

- **Use Terminal Services–specific groups.** Create user groups that are specifically for Terminal Services users. Windows Server 2003 family operating systems contain a default user group called Remote Desktop Users, which is specifically for managing Terminal Services users.
- **Use Terminal Services–specific profiles.** Assign a separate profile for logging on to Terminal Services. Many common options stored in profiles, such as screen savers and animated menu effects, are not needed when users connect through Terminal Services. Assigning a specific profile allows users to get the most out of the system they are working with without requiring additional server resources.
- **Use mandatory profiles.** Use a mandatory Terminal Services profile that was created to suit the needs of all of types of clients and that provides the best server performance. Be aware that 16-bit computers and Windows-based terminals might not support some screen resolutions.
- **Set time limits.** Setting limits on the duration of client connections can improve server performance. You can limit how long a session lasts, how long a disconnected session is allowed to remain active on the server, and how long a session can remain connected yet idle.
- **Use the Starting Program option.** If you have users who need to access only one application on the terminal server, use the Starting Program option. You can do this for all users by using Terminal Services Configuration or you can do it on a per-user basis by using either the Terminal Services Extension to Local Users and Groups or Active Directory Users and Computers.
- **Create preconfigured connection files for users or groups of users.** To make connecting to Terminal Services easier, you can supply users with preconfigured connection files. Collections of connection files can also be made for different departments within your organization or for different job titles. Preconfigured connection files are created using Remote Desktop Connection.

Configuring License Server Using Group Policy Settings

Several GPO settings help you control the terminal server licensing. If you use these settings, you can centrally control and configure license servers and maintain consistency in the environment. You should configure two specific settings to help control the licensing. Both are located under the following path in a default GPO:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Licensing

License Server Security Group

This setting is used to control the Terminal Servers that are issued licenses. In a default configuration, the Terminal Services License Server will issue a license to all computers that request one. When this setting is enabled, the license server responds only to requests from terminal servers that are located in the Terminal Services Computers local group. This is an excellent way to prevent rogue terminal servers from requesting licenses. If you have more than one license server, you can add all of the license servers to the group; this allows the license servers to request licenses on behalf of the terminal servers.

Prevent License Upgrade

A license server attempts to provide the most appropriate client access license (CAL) for a connection. Windows 2000 Terminal Services CAL tokens are provided for Windows 2000 clients. A Windows Server 2003 family Terminal Services CAL is provided when a connection is made to a terminal server running Windows Server 2003. The default behavior is that a Windows 2000 terminal server requests a token, and if the license server does not have any Windows 2000 CALs, it issues a Windows Server 2003 Per-Device token. The Prevent License Upgrade setting can stop this behavior by giving a temporary license to clients connecting to Windows 2000 terminal servers. When the temporary token expires, the connection is refused.

Configuring Terminal Services Connections

Many aspects of the Terminal Services connection can and should be controlled using Group Policy. If these settings are left to individual settings on the Terminal Server or the client, inconsistencies will be introduced throughout the enterprise that waste time, increase help desk calls, and make troubleshooting Terminal Services connection problems more difficult. The following GPO settings can establish a security baseline for the sessions that are running through Terminal Services:

Limit Number Of Connections

The Limit Number Of Connections setting specifies whether Terminal Services limits the number of simultaneous connections to the server. You can use this setting to restrict the number of remote sessions that can be active on a server. If this number is exceeded, additional users who try to connect receive an error message telling them that the server is busy and to try again later. Restricting the number of sessions improves performance because fewer sessions are demanding system resources. By default, terminal servers allow an unlimited number of remote sessions, and Remote Desktop for Administration allows two remote sessions. To use this setting, specify the number of connections you want as the maximum for the server, as shown in Figure 12-5. To specify an unlimited number of connections, type **999999**.

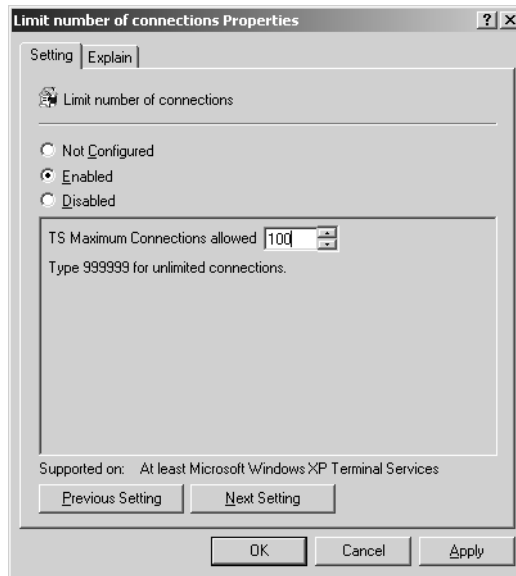


Figure 12-5 The Terminal Services GPO setting that controls the maximum number of connections for a server

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Limit number of connections

When this setting is enabled, you can specify the number of connections in the TS Maximum Connections Allowed box.

Set Client Connection Encryption Level

For Terminal Services connections, using data encryption helps to protect your information on the communications link between the client and the server by preventing unauthorized transmission interception.

The Set Client Connection Encryption Level setting allows you to enforce an encryption level for all data sent between the client and the remote computer during a Terminal Services session, as shown in Figure 12-6.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security\Set client connection encryption level

When this setting is enabled, you can set the encryption level to one of four levels, as described in Table 12-1. By default, Terminal Services connections are encrypted at the highest level of security available (128-bit). However, some earlier versions of the

Terminal Services client do not support this high level of encryption. If your network contains such legacy clients, you can set the encryption level of the connection to send and receive data at the highest encryption level supported by the client.

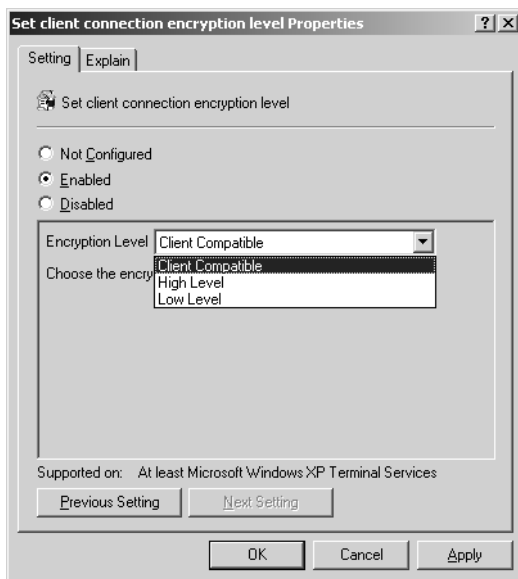


Figure 12-6 The Terminal Services GPO setting that controls client encryption levels

Table 12-1 Client Connection Encryption Levels

Level of Encryption	Description
FIPS Compliant	<p>Encrypts data sent from client to server and from server to client to meet the Federal Information Processing Standard 140-1 (FIPS 140-1), a security implementation designed for certifying cryptographic software. Use this level when Terminal Services connections require the highest degree of encryption. FIPS 140-1–validated software is required by the U.S. government and requested by other prominent institutions.</p> <p>Important: If FIPS compliance has already been enabled by the System Cryptography: Use FIPS Compliant Algorithms For Encryption, Hashing, And Signing Group Policy, administrators cannot change the encryption level for Terminal Services connections by changing the Terminal Services Set Client Connection Encryption Level Group Policy setting or by using Terminal Services Configuration.</p>
High	<p>Encrypts data sent from client to server and from server to client by using strong 128-bit encryption. Use this level when the remote computer is running in an environment containing only 128-bit clients (such as Remote Desktop Connection clients). Clients that do not support this level of encryption cannot connect.</p>

Table 12-1 Client Connection Encryption Levels

Level of Encryption	Description
Client Compatible	Encrypts data sent from client to server and from server to client at the maximum key strength supported by the client. Use this level when the remote computer is running in an environment containing mixed or legacy clients.
Low	Encrypts data sent from the client to the server using 56-bit encryption. Caution: Data sent from the server to the client is not encrypted.

Secure Server (Require Security)

The Secure Server (Require Security) setting specifies whether a Terminal Server requires secure RPC communication with all clients or allows unsecured communication. When this setting is enabled, all RPC communication with clients is more secure because only authenticated and encrypted requests are allowed. The Terminal Server will allow communication only with secure requests and will deny unsecured communication with untrusted clients.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security\RPC Security Policy\Secure Server (Require Security)

Start A Program On Connection

You can use the Start A Program On Connection setting to specify a program to run automatically when a user logs on to a remote computer. By default, Terminal Services sessions provide access to the full Windows desktop unless otherwise specified with this setting. Enabling this setting overrides the Start Program settings set by the server administrator on the Terminal Server or set by the user from the Terminal Services client. When this setting is configured, the Start menu and Windows desktop are not displayed, and when the user exits the program the session is automatically logged off.

To use this setting, you must provide the fully qualified path and file name of the executable file to be run when the user logs on. If necessary, you can also provide the working directory by typing the fully qualified path to the starting directory for the program.



Note If the specified program path, file name, or working directory is not the name of a valid directory, the terminal server connection fails with an error message.



Note The Start A Program On Connection setting appears in both Computer Configuration and User Configuration. If this setting is configured in both places, the Computer Configuration setting takes precedence.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Start a program on connection

When this setting is enabled, you can configure the Program Path And File Name box as well as the Working Directory box, as shown in Figure 12-7.

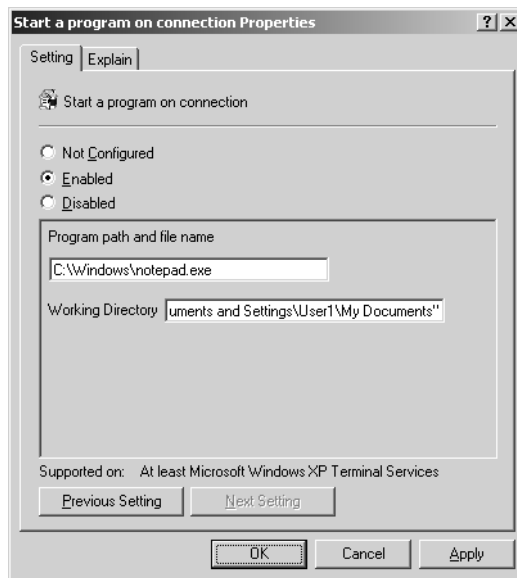


Figure 12-7 Terminal Services GPO settings to start a program on connection



Important These policies affect every client that connects to the terminal server. To specify a program to start on a per-user basis, use the corresponding policy under User Configuration.

Set Rules For Remote Control To Terminal Services User Sessions

You can monitor the actions of a client logged on to a terminal server by remotely controlling the user's session from another session. Remote control allows you to observe or actively control another session. If you choose to actively control a session, you can input keyboard and mouse actions to the session. A message can be displayed on the client session asking permission to view or take part in the session before the session

is remotely controlled. You can use Terminal Services Group Policies to configure remote control settings for a connection and Terminal Services Manager to initiate remote control on a client session.



Tip Windows Server 2003 family operating systems also support Remote Assistance, which allows greater versatility for controlling another user's session. Remote Assistance also provides the ability to chat with the other user.

To access the Set Rules For Remote Control To Terminal Services User Sessions GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Set rules for remote control of Terminal Services user sessions

When this GPO setting is enabled, you can configure the Options setting, which sets the desired remote control permissions. Five permission levels are available, as shown in Figure 12-8.

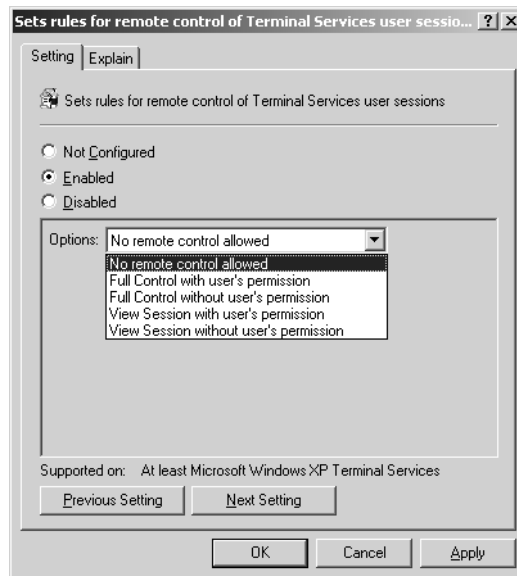


Figure 12-8 Establishing the rules for using remote control over a Terminal Services session



Important These settings affect every client that connects to the Terminal Server. To configure Remote Control on a per-user basis, use the corresponding policy under User Configuration.

Set Time Limit For Disconnected Sessions

For a Terminal Services connection, you can limit the amount of time that active, disconnected, and idle (without client activity) sessions remain on the server. This is useful because sessions that run indefinitely on the server consume valuable system resources. When a session limit is reached for active or idle sessions, you can opt to disconnect the user from the session or end the session. A user who is disconnected from a session can reconnect to the same session later. When a session ends, it is permanently deleted from the server and any running applications are forced to shut down, which can result in loss of data at the client. When a session limit is reached for a disconnected session, the session ends, which permanently deletes it from the server. Sessions can also be allowed to continue indefinitely.

You can use the Set Time Limit For Disconnected Sessions setting to specify the maximum amount of time that a disconnected session is kept active on the server. By default, Terminal Services allows users to disconnect from a remote session without logging off and ending the session.

When a session is in a disconnected state, running programs are kept active even though the user is no longer actively connected. By default, these disconnected sessions are maintained for an unlimited time on the server.

To access the Set Time Limit For Disconnected Sessions setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Sessions\Set time limit for disconnected sessions

When this GPO setting is enabled, you can configure the End A Disconnected Session setting, which specifies when a disconnected session will be ended.



Note The Set Time Limit For Disconnected Sessions setting affects every client that connects to the terminal server. To define Session settings on a per-user basis, use the Sessions policies under User Configuration.



Important The setting does not apply to console sessions such as Remote Desktop sessions with computers running Windows XP Professional. Also note that this setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting takes precedence.

Set Time Limit For Active Terminal Services Sessions

You can use the Set Time Limit For Active Terminal Services Sessions setting to specify the maximum amount of time a Terminal Services session can be active before it is

disconnected. By default, Terminal Services allows sessions to remain active for an unlimited time.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Sessions\Set time limit for active Terminal Services sessions

When this setting is enabled, you can configure the Active Session Limit setting to set the time limit for any Terminal Services session.



Note The Set Time Limit For Active Terminal Services Sessions setting affects every client that connects to the terminal server. To define Session settings on a per-user basis, use the Sessions policies under User Configuration.

This setting appears in both Computer Configuration and User Configuration. If it is configured in both places, the Computer Configuration setting has precedence. Active session limits do not apply to the console session. To specify that user sessions terminate at timeout, enable the Terminate Session When Time Limits Are Reached setting.

Terminate Session When Time Limits Are Reached

You can use the Terminate Session When Time Limits Are Reached setting to direct Terminal Services to terminate a session (that is, the user is logged off and his session is disconnected from the server) after time limits for active or idle sessions are reached. By default, Terminal Services disconnects sessions that reach their time limit.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Sessions\Terminate session when time limits are reached

When this setting is enabled, Terminal Services terminates any session that reaches its timeout limit. This setting exists under both the Computer Configuration and User Configuration. The policy under the Computer Configuration has precedence.

Allow Reconnection From Original Client Only

You can use the Allow Reconnection From Original Client Only setting to configure settings for reconnecting disconnected Citrix ICA sessions. You can prevent Terminal Services users from reconnecting to the disconnected session using a computer other than the client computer from which they originally created the session. By default, Terminal Services allows users to reconnect to disconnected sessions from any client computer.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Sessions\Allow reconnection from original client only

When this setting is enabled, users can reconnect to disconnected sessions only from the original client computer. If a user attempts to connect to the disconnected session from another computer, a new session is created instead.



Tip The Allow Reconnection From Original Client Only setting affects every client that connects to the terminal server. To define Session settings on a per-user basis, use the Sessions policies under User Configuration.



Note The Allow Reconnection From Original Client Only setting is supported only for Citrix ICA clients that provide a serial number when connecting; it is ignored if the user is connecting with a Windows client. Also note that this setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting has precedence.

Managing Drive, Printer, and Device Mappings for Clients

Because client sessions can establish multiple data channels between client and server, users can map to local devices, such as drives and printers. By default, drive and printer mappings that a user sets in a client session are temporary and are not available the next time the user logs on to the server. However, using Terminal Services Configuration, you can specify that client mappings be restored when the user logs on. In addition, you can disable specific client devices so that a user cannot map the device. Users can map the following devices:

- Drives
- Windows printers
- LPT ports
- COM ports
- Smart cards
- Clipboard
- Audio

Whenever possible, use Terminal Services Group Policies to configure the settings described in the following sections.

Allow Audio Redirection

The Allow Audio Redirection setting specifies whether users can choose where to play the remote computer's audio output during a Terminal Services session (audio redirection). Users can use the Remote Computer Sound option on the Local Resources tab of Remote Desktop Connection to specify whether to play the remote audio on the remote computer or on the local computer. Users can also choose to disable the audio.

By default, users cannot apply audio redirection when connecting via Terminal Services to a server running Windows Server 2003. Users connecting to a computer running Windows XP Professional can apply audio redirection by default.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection\Allow audio redirection

Do Not Allow COM Port Redirection

The Do Not Allow COM Port Redirection setting specifies whether to prevent the redirection of data to client COM ports from the remote computer in a Terminal Services session. You can use this setting to prevent users from redirecting data to COM port peripherals or mapping local COM ports while they are logged on to a Terminal Services session. By default, Terminal Services allows this COM port redirection.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection\Do not allow COM port redirection

Do Not Allow Client Printer Redirection

You can use the Do Not Allow Client Printer Redirection setting to prevent users from redirecting print jobs from the remote computer to a printer attached to their local (client) computer. By default, Terminal Services allows this client printer mapping.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection\Do not allow client printer redirection

When this setting is enabled, users cannot redirect print jobs from the remote computer to a local client printer in Terminal Services sessions.

Do Not Allow LPT Port Redirection

The Do Not Allow LPT Port Redirection setting specifies whether to prevent the redirection of data to client LPT ports during a Terminal Services session. You can use this setting to prevent users from mapping local LPT ports and redirecting data from the remote computer to local LPT port peripherals. By default, Terminal Services allows this LPT port redirection.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection\Do not allow LPT port redirection

When this setting is enabled, users in a Terminal Services session cannot redirect server data to the local LPT port.

Do Not Allow Drive Redirection

The Do Not Allow Drive Redirection setting specifies whether to prevent the mapping of client drives in a Terminal Services session (drive redirection). By default, Terminal Services maps client drives automatically upon connection. Mapped drives appear in the session folder tree in Windows Explorer or My Computer in the format *<driveletter> on <computername>*. You can use this setting to override this behavior.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection\Do not allow drive redirection

When this setting is enabled, client drive redirection is not allowed in Terminal Services sessions.

Do Not Set Default Client Printer To Be Default Printer In A Session

The Do Not Set Default Client Printer To Be Default Printer In A Session setting specifies whether the client default printer is automatically set as the default printer in a Terminal Services session. By default, Terminal Services automatically designates the client default printer as the default printer in a Terminal Services session. You can use this setting to override this behavior.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection\Do not set default client printer to be default printer in a session

When this setting is enabled, the default printer is the printer specified on the remote computer.

Controlling Terminal Services Profiles

Each session that is created on a terminal server requires a user profile. As we discussed earlier, you can control this profile if you want it to roam. This option is handy for users who move from computer to computer but want a consistent desktop.

In some cases, you might not want users to download profiles or have profiles stored on certain terminal servers. The following sections offer some suggested settings for controlling these behaviors.

Set Path For TS Roaming Profiles

You can use the Set Path For TS Roaming Profiles setting to specify a network share where the profiles are stored, allowing users to access the same profile for sessions on all terminal servers in the same OU. By default, Terminal Services stores all user profiles locally on the terminal server. This setting allows you to override the setting in the user account on a per-server basis. It also provides an excellent method for specifying a different Terminal Server profile server for groups of terminal servers. If you have server farms that are spread over different locations, you can use this setting to allow users to roam between the servers in the server farms seamlessly.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Set path for TS Roaming Profiles

When this setting is enabled, you type the path to the network share in the form `\\Computersname\Sharename` in the Profile Path box, as shown in Figure 12-9.

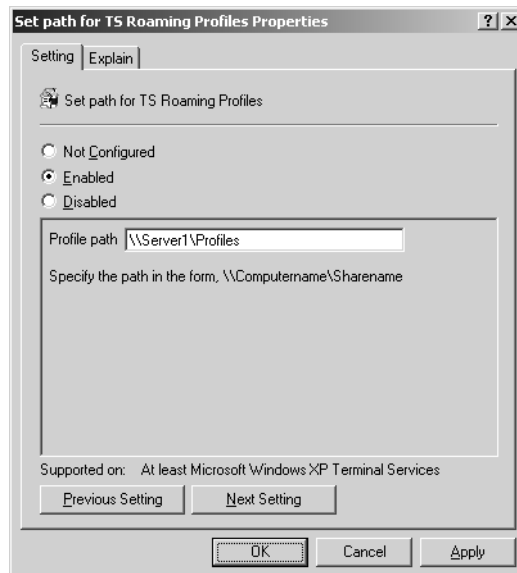


Figure 12-9 The Terminal Services GPO setting that controls the profile path



Caution Do not specify a placeholder for the user alias because Terminal Services automatically appends this at logon. Make sure the specified network share exists; otherwise, Terminal Services will display an error message on the server and will store the user profile locally.

TS User Home Directory

You can use the TS User Home Directory setting to select the location for the home directory for the Terminal Services session. The options are a network share or a local directory. For a network share path, you must type the path in the form `\\Computername\Sharename`. For local directories, you can type the drive letter, followed by the path to the home directory root, such as `C:\users\homedir`. Like the roaming profiles setting, this setting provides an excellent way to configure users' home directories for when they roam between Terminal Server farms throughout the organization.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\TS User Home Directory

When this setting is enabled, you use the Location drop-down list to specify whether the path will be local or on the network, as shown in Figure 12-10. You then type the path to the home directory based on the syntax we discussed earlier. Finally, you specify a drive letter for the home directory, which the user will use to access the home directory on her computer.

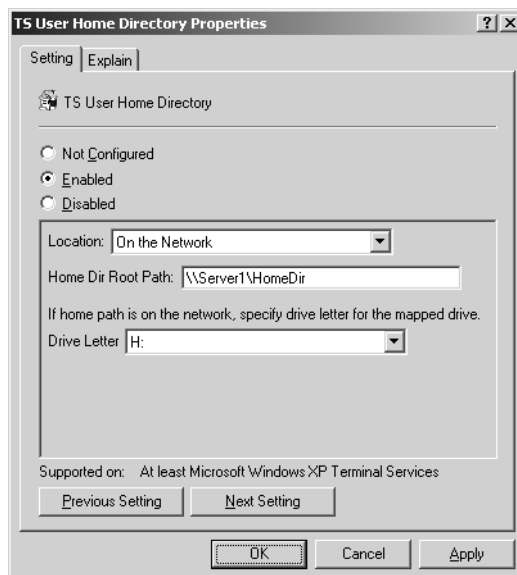


Figure 12-10 The Terminal Services GPO setting that controls the user's home directory

Restrict Terminal Services Users To A Single Remote Session

To control Terminal Services licenses as well as how many Terminal Services sessions a user can start, you can restrict users to a single remote session. The Restrict Terminal Services Users To A Single Remote Session setting restricts users who log on remotely via Terminal Services to a single session on that server. This includes both active and disconnected sessions. This means that if a user disconnects from a session, any attempt to start a new session will fail and will send the user to the disconnected session.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Restrict Terminal Services users to a single remote session

Only Allow Local User Profiles

The Only Allow Local User Profiles setting is not designed for Terminal Services, but it can be used with a Terminal Services session. This setting prevents the roaming user profile from being downloaded, even if the user's account specifies a roaming profile path. This setting is useful if you have terminal servers at different sites and you don't want to maintain profile servers at each site.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\System\User Profiles\Only allow local user profiles

Delete Cached Copies Of Roaming Profiles

Sometimes you will need to free up disk space on terminal servers but also need the users to use their roaming profiles. In this case, you cannot force the user to use a local profile. However, you can use the Delete Cached Copies Of Roaming Profiles setting to configure a different GPO that removes the roaming profile from the server when the user ends the session.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\System\User Profiles>Delete cached copies of roaming profiles

Group Policy over Slow Links

The availability of network bandwidth can affect how Group Policy settings are applied. By default, some policies are not processed across a slow network connection. If the network link speed between a client and the authenticating domain controller falls below the default slow link threshold of 500 kilobits per second (Kbps), only the administrative template (registry-based) settings and security settings are

applied. When the available bandwidth between the client and the domain controller falls below this preset threshold, the client is said to be on a slow link.

If necessary, you can modify the default slow link behavior by using a policy setting that appears under both Computer Configuration and User Configuration in a GPO. You can also adjust the Group Policy extensions that are processed below the slow link threshold. However, depending on your situation, it might be more appropriate to place a local domain controller at a remote location to serve your management requirements.

It is important to have sufficient network bandwidth available between servers and workstations when you deploy roaming user profiles, Offline Files, and Folder Redirection. It is also recommended that the servers to which workstations connect for this data be on a fast network link. Check your network configuration for ways to minimize network routing hops when accessing frequently needed data. Keeping the needed data and the user on the same subnet improves performance.

Default Policy Application over Slow Links

When you want Group Policy to be applied but the network is congested, when you are connecting over slow links, or when you are using a remote access to connect to your network, you might be apprehensive about which portions of the Group Policy to apply because applying many potentially large policies can hurt performance. The behavior of Group Policy application over these slow links is straightforward.

What does Group Policy consider to be a slow link by default? Microsoft has established that a slow link is less than 500 Kbps. Therefore, if you are connecting over your LAN and network congestion slows down your communication with the domain controllers to below 500 Kbps, Group Policy considers this connection to be slow.

In this example, you might not want to have Group Policy consider your connection to be slow. However, in other situations you will want the connection to be considered slow to allow control over which policies are processed. For example, you might want a connection from a branch office that connects over a slow frame-relay link to be considered slow so that you can control whether Microsoft Office will be installed over this small connection. Other situations in which slow link speeds might be a factor include:

- Virtual Private Network (VPN) connections
- Dial-up connections
- Branch offices
- Remote Terminal Services connections
- Wireless connections

Policies That Apply over Slow Links

Let's look at which settings apply over slow links by default. Even if a link is slow, you still want some settings to apply to ensure a secure and functional environment.

Microsoft has thus configured two sections of Group Policy to apply over any link speed: Security and Administrative Templates. Other sections are enabled to apply over slow links but can be turned off. Table 12-2 shows all the GPO sections and their behaviors during slow link application.

Table 12-2 Default Settings for Processing Group Policy over Slow Links

Setting	Default
Security Settings	ON (cannot be turned off)
IP Security	ON
EFS	ON
Software Restriction Policies	ON
Wireless	ON
Administrative Templates	ON (cannot be turned off)
Software Installation	OFF
Scripts	OFF
Folder Redirection	OFF
IE Maintenance	ON

Slow Link Behavior for RAS Connections

A user has two ways to log on to her computer when she plans to use RAS to connect to Active Directory during her session. The choice affects how GPOs are applied for remote access users.

The first option is to select the Logon Using Dial-Up Connection check box, which in essence tells the computer to communicate directly to the RAS server to authenticate the user, bypassing local authentication. This option allows the GPOs (Security Settings and Administrative Templates) to be applied at logon. However, computer-based software installation settings are not processed, nor are computer-based startup scripts executed, because computer policy is normally processed before the logon screen appears.

The second option is to log on locally or with cached credentials. With this option, the domain-based GPOs are not applied, except for what is in the cached profile. When the user connects to the RAS server, she is authenticated to the domain and has access to the remote network resources. However, the GPOs are not applied immediately in this situation—only at the GPO refresh interval.

Slow Link Detection Group Policy Settings

You can configure numerous settings to control how GPO settings react when they are applied over slow links. Not all of the settings are in one location, so it can be confusing to figure out what the settings do, where they are located, and how they are all related.

The following slow link settings are at the core of the slow link detection and Group Policy implementation. You typically begin with these settings as you start to alter the default behavior of how GPOs apply over slow links.

Group Policy Slow Link Detection

The Group Policy Slow Link Detection setting defines a slow connection for purposes of applying and updating Group Policy. If the rate at which data is transferred from the domain controller providing a policy update to the computers in this group is slower than the rate specified by this setting, the system considers the connection to be slow. The default value for this setting is 500 Kbps, which is also what the computer will use if this policy is disabled.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\System\Group Policy\Group Policy slow link detection

When this setting is enabled, as shown in Figure 12-11, you must enter a decimal number between 0 and 4,294,967,200 in the Connection Speed box. The units for this entry are kilobits per second.



Note The User Configuration node in a GPO also has a Group Policy Slow Link Detection setting.

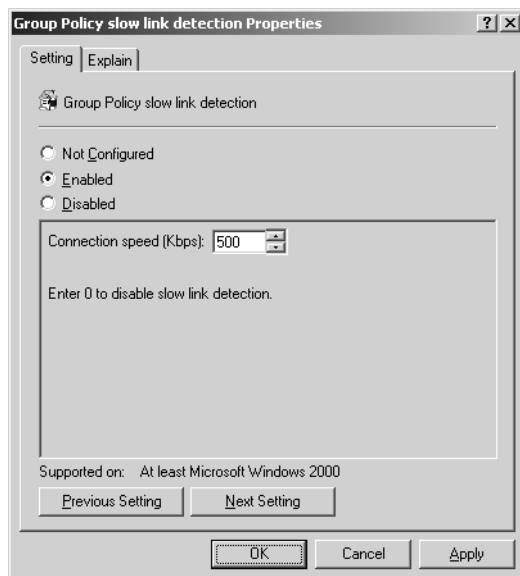


Figure 12-11 Defining a slow link for the application of GPOs over slow network connections

Slow Network Connection Timeout for User Profiles

The Slow Network Connection Timeout for User Profiles setting controls how a slow connection is defined for application of roaming user profiles. If the server on which the user's roaming profile resides takes longer to respond than the thresholds set by this setting, the system considers the connection to the profile to be slow.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\System\User Profiles\Slow network connection timeout for user profiles

When this GPO setting is enabled, as shown in Figure 12-12, you must enter a decimal number between 0 and 4,294,967,200 in the Connection Speed box. The units for this entry are kilobits per second. For non-IP computers, the system measures the responsiveness of the remote server's file system. To set a threshold for this test, in the Time box type a decimal number between 0 and 20,000. The units for this entry are milliseconds.

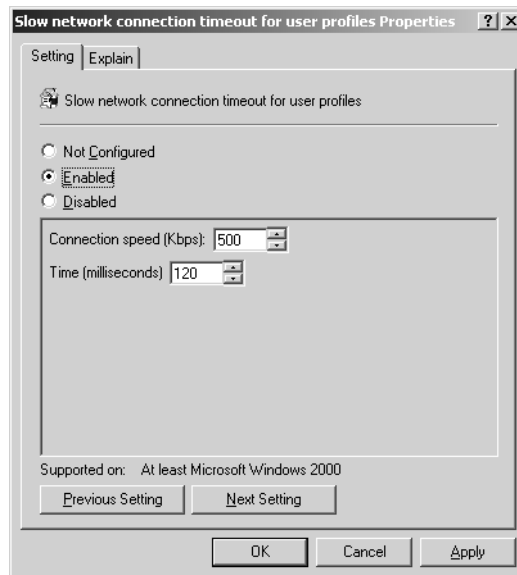


Figure 12-12 Specifying the definition of a slow link

Do Not Detect Slow Network Connections

The Do Not Detect Slow Network Connections setting controls whether user profiles are controlled by the speed of the link. Slow link detection measures the speed of the connection between a user's computer and the remote server that stores the roaming user profile. When the system detects a slow link, the related settings in this folder tell

the system how to respond. When this policy is enabled, the roaming user profile ignores any slow link connection policy settings.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\System\User Profiles\Do not detect slow network connections



Note If the Do Not Detect Slow Network Connections setting is enabled, the Slow Network Connection Timeout For User Profiles setting is ignored.

Prompt User When Slow Link Is Detected

The Prompt User When Slow Link Is Detected setting allows the user to be notified when his roaming profile is slow to load. This gives the user the ability to decide whether to use the local cached copy of his profile or to wait for the roaming user profile.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\System\User Profiles\Prompt user when slow link is detected



Note If the Do Not Detect Slow Network Connections setting is enabled, the Prompt User When Slow Link Is Detected setting is ignored.



More Info For more information on user profiles, see Chapter 7.

Configure Slow Link Speed

When a user uses offline files, it can take a long time to synch the files—with a slow link, it might take hours. When a user is connected over a slow link, you might want to use the Configure Slow Link Speed setting and other settings that control Offline Files behavior.

The Configure Slow Link Speed setting configures the threshold value at which offline files considers a network connection to be slow. If the connection is considered to be slow, the offline files feature adjusts itself to avoid excessive synchronization traffic.

To access this GPO setting, follow this path:

Computer Configuration\Administrative Templates\Network\Offline Files\Configure Slow link speed

When this setting is enabled, as shown in Figure 12-13, you must enter a value in the Value box that defines what offline files will consider to be a slow link. The units for this entry are bits per second divided by 100.

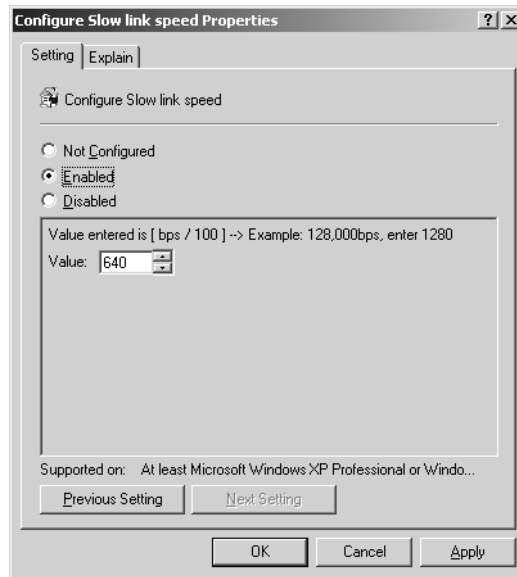


Figure 12-13 Specifying the definition of a slow link for the synchronization of offline files

Additional Slow Link Detection Settings for Client-Side Extensions

Each section of a GPO is controlled by a client-side extension (CSE). Security, administrative templates, and folder redirection are examples of these sections. Most of these CSEs can be controlled when a slow link is detected, to make the connection faster and to reduce the settings that are applied over the slow network connection.

The CSEs that can be controlled when a slow link is detected include:

- Internet Explorer Maintenance policy
- Software Installation policy
- Folder Redirection policy
- Scripts policy
- Security policy
- IP Security policy
- EFS recovery policy
- Wireless policy
- Disk Quota policy

These settings are all in the same location in the GPO and are named accordingly. For example, the policy setting for the Scripts CSE is named Scripts Policy Processing. You can find them at the following path in a GPO:

Computer Configuration\Administrative Templates\System\Group Policy

Once you access the policy you want to control, you will find a specific setting that controls slow network connections, as shown in Figure 12-14. The Allow Processing Across A Slow Network Connection setting controls whether the client-side extension is applied when a slow network connection is detected.



Figure 12-14 The Allow Processing Across A Slow Network Connection setting

The setting specifies whether the client-side extension adheres to slow links. When this setting is enabled for the client-side extension, the policy settings related to this portion of the GPO will apply over a slow link. This is the opposite of the default behavior, which is to not apply policy settings over slow links (except for the few client-side extensions that apply by default over slow links, which were described earlier in this chapter).



More Info For more information on client-side extensions and applying GPOs, see Chapter 13.

Summary

Group Policy can be extended to accommodate almost any network environment. These networks include remote access connections, slow network connections, special security requirements, Terminal Services sessions, and more. When custom scenarios arise, you have great flexibility within Group Policy to meet your needs. Settings such as loopback processing, slow link detection, and Terminal Services settings allow you to easily control almost any environment. These settings should be used only for unique situations, to allow the default Group Policy behavior to work to your advantage when you need to customize a user's environment.