Report Number: C4-023R-01

Guide to Securing Microsoft Windows 2000® Terminal Services

Network Security Evaluations and Tools Division
of the
Systems and Network Attack Center (SNAC)

Authors:
Vincent J. DiMaria
James F. Barnes
CDR Jerry L. Birdsong
Kathryn A. Merenyi

Updated: July 2, 2001
Version 1.0

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704

W2kguides@nsa.gov

This Page Intentionally Left Blank

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- The security changes described in this document only apply to Microsoft Windows 2000 systems and should not be applied to any other Windows 2000 versions or operating systems.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- This document is current as of July 2, 2001. See Microsoft's web page http://www.microsoft.com/ for the latest changes or modifications to the Windows 2000 operating system.

This Page Intentionally Left Blank

Acknowledgements

The authors would like to acknowledge Julie Haney, Paul Bartock, Stephen Dhanraj and Donald Simard for their encouragement and help reviewing the document.

Trademark Information

Table of Contents

Table of Figures

Table of Tables

This Page Intentionally Left Blank

Introduction

The purpose of this guide is to provide the reader with security guidance to support the design and implementation of Windows 2000 Terminal Services (WTS). This guide provides step-by-step instructions to perform many of the tasks recommended to secure WTS. Because WTS implementations will vary, system administrators and network managers should choose appropriate security settings for their environment.

The *Guide to Securing Microsoft Windows 2000 Terminal Services* presents detailed information on how to secure this service in a network environment.

WARNING: This guide does not address security issues for the Microsoft Windows 2000 operating system that are not specifically related to the Windows 2000 Terminal Service and its implementation.

This document is intended for Windows 2000 network administrators, but is beneficial to anyone involved or interested in Windows 2000 or network security.

Getting the Most from this Guide

The following list contains suggestions to successfully secure the Windows 2000 Terminal Service according to this guide:

WARNING: This list does not address site-specific issues and every setting in this book should be tested on a non-operational network.

- Read the document in its entirety. Omitting or deleting steps can potentially lead to an unstable system and/or network that will require reconfiguration and reinstallation of software.
- Be aware that while most of the security guidance applies to WTS in application sharing mode and in remote administration mode, there is some guidance that is unique to each mode. Care must be taken to ensure the correct guidance is applied.
- Perform pre-configuration recommendations:

  If not using a new server, perform a complete backup of your server before implementing any of the recommendations in this guide.

  Ensure that the latest Windows 2000 service pack and hotfixes are available to be installed. At a minimum, this includes Microsoft Windows 2000 Service Pack 2. For further information on critical Windows 2000 updates, see the Windows Update for Windows 2000 web page http://www.microsoft.com/windows2000/downloads/default.asp.

About the Guide to Securing Microsoft Windows 2000 Terminal Services

This document consists of the following:

Chapter 1, "Windows 2000 Terminal Services," introduces Windows Terminal Services (WTS) and describes three potential operational scenarios for WTS. The three scenarios include using WTS to support application sharing on an internal network (Intranet), using WTS to support remote administration of Windows 2000 servers, and

using WTS to support application sharing on the Internet. Chapter 1 also describes the test network configuration that was used to develop the security guidance in this document.

Chapter 2, "Security Guidance for Windows 2000 Terminal Services," provides security guidance for implementing Windows 2000 Terminal Services (WTS). Guidance is provided for WTS when it is used for sharing applications on an internal network (Intranet) and when it is used for remote administration of Windows 2000 servers on an internal network (Intranet). The guidance covers WTS installation, configuration, file permissions, auditing, and router/firewall settings.

Appendix A, "Limiting Access to Applications," provides security guidance on restricting user access to applications when using WTS for sharing applications on an Intranet.

Appendix B, "Windows 2000 Terminal Services Default User Settings," identifies the default settings that Windows 2000 assigns to a WTS user.

Appendix C, "Windows 2000 Terminal Services Security Guidance Troubleshooting," contains a list of common problems that can occur, when implementing WTS with the security guidance specified in this document, and potential solutions to those problems.

Appendix D, "References," is a list of references used in developing the WTS security guidance.

Chapter

1

Windows 2000 Terminal Services

The Microsoft Windows 2000 Terminal Service (WTS) is a useful capability that can satisfy a variety of needs. WTS permits a user on a client computer to use WTS client software to initiate and control actions on a WTS server. The "keystrokes" and "mouse clicks" of the user are sent to the server, the server takes the appropriate action (for example, starts an application) and then sends a "monitor update" back to the user so they can see the consequence of the action. The processing power, operating system, application software, network bandwidth, etc, are all supplied by the server and remotely controlled by the user.

Windows 2000 Terminal Services (WTS) Operational Scenarios

There are several generic operational scenarios for Windows 2000 Terminal Services (WTS) as shown in Figure 1 and described in additional detail below.

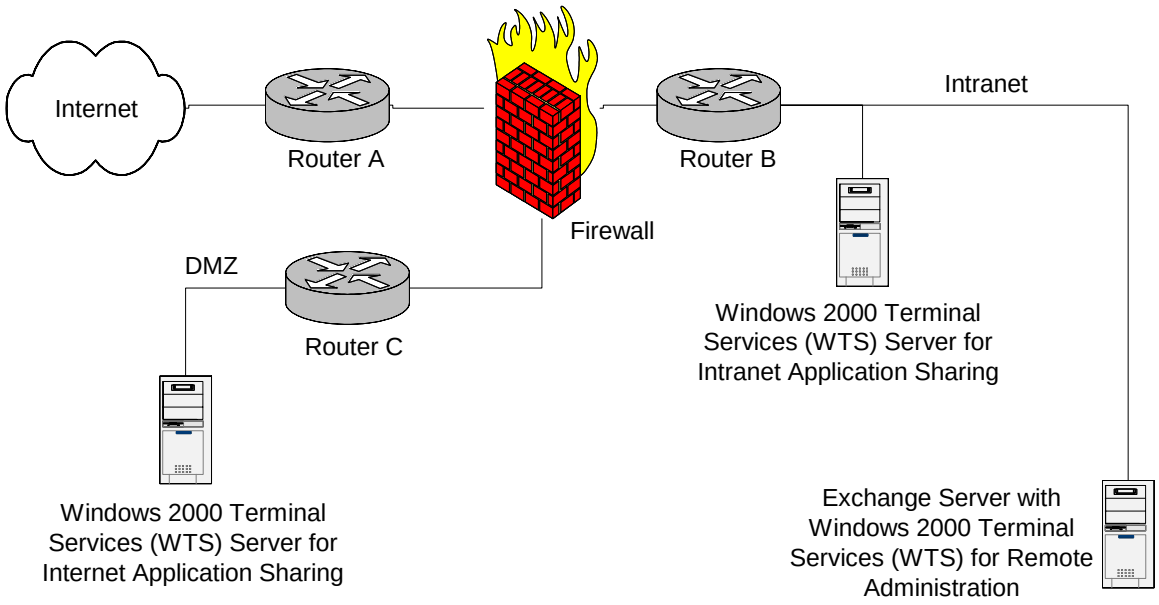

Figure 1 Operational Scenarios for Windows 2000 Terminal Services

WTS for Intranet Application Sharing

This operational scenario for WTS is a situation where you have one or more Windows applications that you want internal users (e.g., employees) to be able to use via an internal network, the corporate Intranet. The "Windows 2000 Terminal Services (WTS)

Server for Intranet Application Sharing" in the figure above represents this scenario. For example, an organization may have a personnel department that has purchased or developed a Windows application for supervisors to use for personnel transactions. Distributing the application to each user's computer is troublesome because the application is frequently being changed and it isn't practical to maintain compatibility between newer and older versions. WTS offers the personnel department the option of installing the application just once on a WTS server and then permitting users to access the application via the Intranet. Under this scenario, users can potentially execute software of their choosing on the server itself, which is typically not the case on Windows networks where administrators control what software is executing on the server. Appendix A contains guidance on restricting the applications that a user can run on the server in this scenario.

WTS for Remote Administration

In this operational scenario, various Windows 2000 servers such as Domain Controllers, Exchange servers, etc, use WTS to provide an administrator the ability to manage that server from any computer on the corporate Intranet. The "Exchange Server with Windows 2000 Terminal Services (WTS) for Remote Administration" in the figure above represents this scenario. For example, an administrator may be at a user's computer troubleshooting an e-mail problem and want to run the Exchange administrator tool (which isn't installed on the user's computer). If the Exchange server has WTS for remote administration implemented, the administrator can remotely run the Exchange administrator tool that is installed on the Exchange server from the user's computer.

WTS for Internet Application Sharing

This operational scenario for WTS is a situation where you have a Windows application that you want external users (customers, non-employees) to be able to use via the Internet. The "Windows 2000 Terminal Services (WTS) Server for Internet Application Sharing" in the figure above represents this scenario. For example, a bank may have a "loan calculator" Windows application that they want to make available to potential customers via the Internet. By implementing WTS for application sharing with an Internet Connector license, and placing the WTS in a DMZ with the appropriate protection measures (see the *Microsoft Windows 2000 Network Architecture Guide*), the loan calculator application can be made available for potential customers to use via their Web browser and Internet connection. Of the three operational scenarios defined, this scenario has the highest security risk. Security guidance for this operational scenario is not provided in this document, however, it is expected that the security guidance will be provided in a future version.

Configuration of WTS Test Network

To better understand some of the information provided in this document, it is necessary to understand the configuration that was used for generating the included figures.

An Active Directory domain named "CAR" was established. Within the CAR domain, a member server named "LINCOLN" was established. Windows 2000 Terminal Services were installed on LINCOLN. A local group named "WTS Users" was created on LINCOLN. A Global Security Group was created in the CAR domain and appropriate user accounts (users that are being granted permission to use WTS) were made members of the Global Security Group. The Global Security Group was then made a member of the local group "WTS Users" on LINCOLN. Permissions were assigned to the local user group, which were then applied to the members of that group. Members of the local Administrators group on LINCOLN are administrators that are being granted

permission to administer WTS on LINCOLN. Permissions were assigned to the local administrator group, which were then applied to the members of that group.

Windows 2000 allows policy to be set in a variety of ways. The WTS test network used for developing this guidance did not apply group policy at the domain, site or Organizational Unit (OU) level. The only policy imposed on the WTS server (LINCOLN) was at the local group policy object level.

This Page Intentionally Left Blank

Chapter

2

Security Guidance for Windows 2000 Terminal Services

This chapter provides security guidance for Windows 2000 Terminal Services (WTS) in the two most widely used operational scenarios: Intranet Application Sharing and Remote Administration

WTS can be used to make Windows applications available to users on an internal network (Intranet). In this Intranet Application Sharing scenario, the application runs on the server but is controlled by the user from the client computer.

WTS can also be used to facilitate remote administration of Windows 2000 servers via an internal network (Intranet). In this Remote Administration scenario, the application, such as Active Directory Users and Computers, runs on the server but is controlled by an administrator from their client computer.

WTS has several options that help to secure the implementation. These options focus on areas such as how users are authenticated, the confidentiality of the information exchanged between the client and the server, and maintaining the integrity of the server.

Guidance for WTS Implementation Planning

The following items should be considered during the initial planning stages of a WTS for Intranet Application Sharing or Remote Administration implementation.

- WTS for application sharing should not be implemented on a Domain Controller to prevent giving WTS users the “log on locally” permission to all Domain Controllers.
- It is best to limit an application-sharing WTS server to providing a single application on each server. For example, if an organization wants to make a personnel tool available to supervisors and a training tool available to engineers, it is best to have one WTS server providing the personnel tool and a second WTS server providing the training tool. This takes advantage of WTS’s ability to restrict the client to accessing a single application on the server. Allowing users to run applications of their choosing on the server can be a security risk. If it is not practical to limit the server to one application, Appendix A contains guidance on limiting the applications a user can run on the server.
- Whenever possible, do not enable the remote control feature of WTS. The remote control feature allows a second user to view or interact with the original user’s WTS session and possibly use the original user’s permissions to perform actions.
- When multiple servers will be using WTS to provide application sharing, consider placing all the WTS application-sharing servers in a single OU (Organizational Unit) to facilitate the application of Group Policies.

- Do not implement WTS for application sharing on a server if using WTS for remote administration will satisfy the primary needs. WTS for application sharing places the server at a greater security risk than WTS for remote administration.
- If protection of the information exchanged between the client and the WTS server is a high priority, consider implementing an IPSEC VPN between the WTS server and the client as a layer of protection in addition to the protection provided by WTS itself.
- Limit which users are permitted to establish a WTS session with a server to only those requiring the service. For example, if making an application such as a personnel tool available to supervisors, limit which users can use WTS to establish an application sharing session with the WTS server to only supervisors vice all domain users.
- WTS does not support the use of smart cards for authentication. For example, if administrators are normally required to use smart cards to authenticate, they will not be able to use them to initiate a WTS session.
- A limitation of WTS for Remote Administration is that only two concurrent sessions are permitted. No client access licenses are required to support this capability.

Guidance for WTS Installation

Install the Windows 2000 Server operating system, the latest service pack (Service Pack 2 as a minimum), and applicable hotfixes.

Apply the Windows 2000 security guidance as documented in the *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set* guide.

To install Windows 2000 Terminal Services:

- **Start → Settings → Control Panel → Add/Remove Programs**
- Click **Add/Remove Windows Components** to start the **Windows Components Wizard**
- Select **Terminal Services**
- Click **Next**

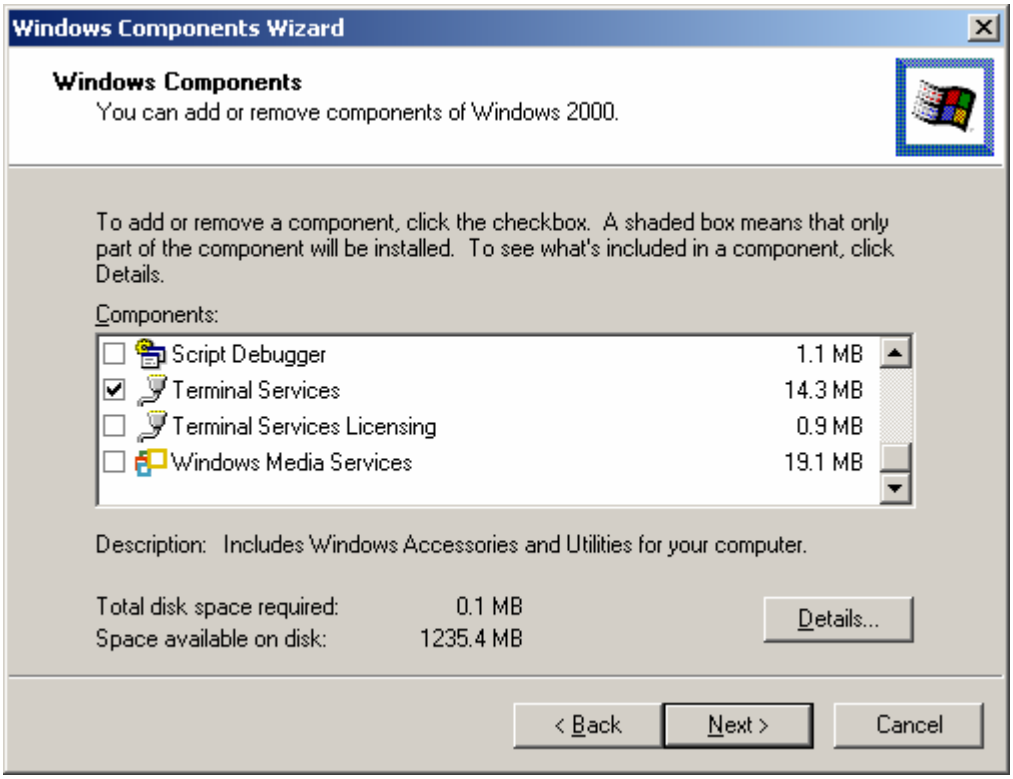

Figure 2 Windows Components Wizard

- Select **Application server mode** for the Intranet Application Sharing operational scenario or **Remote administration mode** for the Remote Administration operational scenario.
- Click **Next**
- If the window shown in Figure 3 appears, select **Permissions compatible with Windows 2000 Server**, (NOT the default **Permissions compatible with Terminal Server 4.0 users** which would give users undesirable permissions).
- Click **Next**. Windows Terminal Services will be installed.

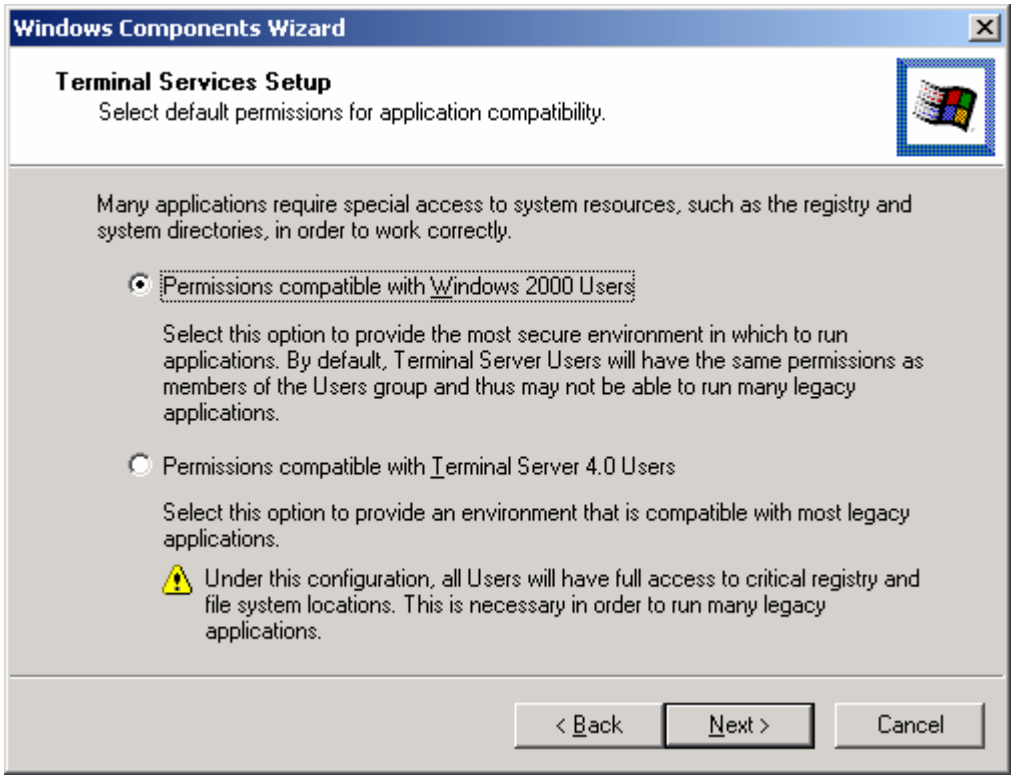

Figure 3 WTS Permissions Compatibility

The user group that should be granted access to WTS on the server needs to be given the **Log on locally** permission normally assigned only to the Administrators group per the *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set*. One option for assigning the **Log on locally** right to the WTS user group is using a security template and applying it via a Group Policy. This is especially convenient if there are multiple servers and the servers are in the same Organizational Unit (OU). A second option, described below, applies to a single server and assigns the necessary permissions using the Local Security Policy tool to edit the Local Group Policy object.

NOTE: Group Policy will override Local Security Policy.

To give the appropriate user group the **Log on locally** right:

- **Start → Programs → Administrative Tools → Local Security Policy** to start the **Local Security Settings** tool
- **Local Policies → User Rights Assignments**
- Double click **Log on locally** in the right pane
- Click **Add**, and then select the appropriate user group.
- Click **Add**
- Click **OK → OK**
- Close the **Local Security Settings** tool.

If after closing the Local Security Settings tool, it is opened again, the figure below reflects the proper settings (note that until the tool is closed and reopened, the effective policy settings may not appear correctly).

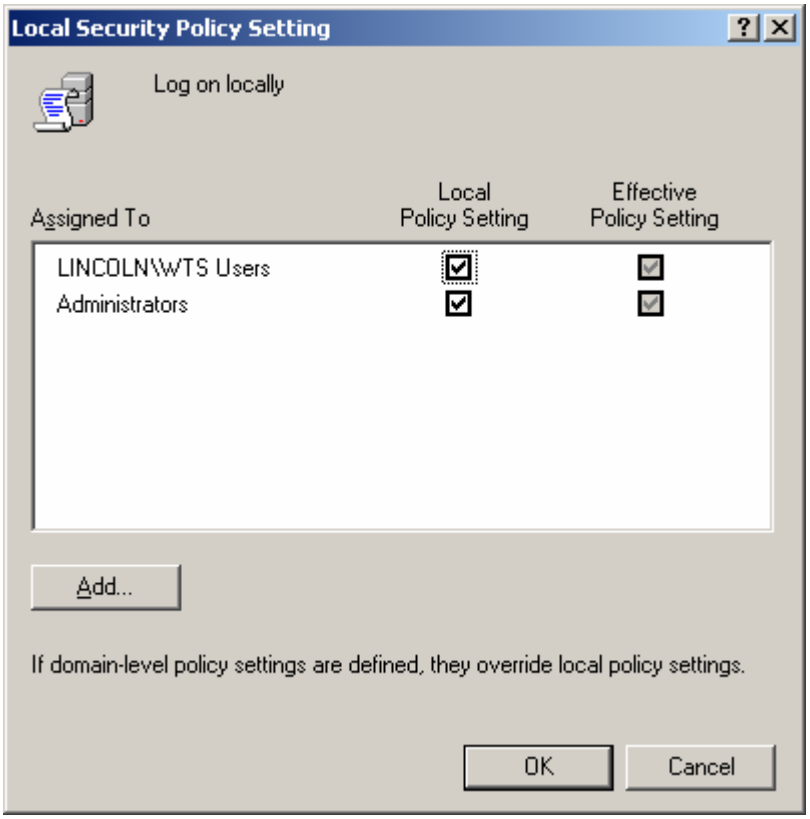

Figure 4 Log On Locally Permissions

Additional permissions associated with the **Permissions compatible with Terminal Server 4.0 Users** option should be removed. The `nottsid.inf` security template is the recommended means for removing the additional permissions. To apply the security template, run the included `notssid.bat` program, or take the following steps:

- At a command prompt, type `cd /d %systemroot%\security\templates`
- Type `secedit /configure /db notssid.sdb /cfg notssid.inf /log notssid.log /verbose`
- View the `notssid.log` file in the `%systemroot%\security\templates\` directory to ensure the security template was applied successfully.

Guidance for WTS Configuration

The following guidance can be applied to the WTS server via the Terminal Services Configuration tool.

- **Start → Programs → Administrative Tools → Terminal Services Configuration** to run the tool
- Select **Connections** under **Terminal Services Configuration**
- Double click the **RDP-TCP** entry under **Connection** to display the properties for that connection

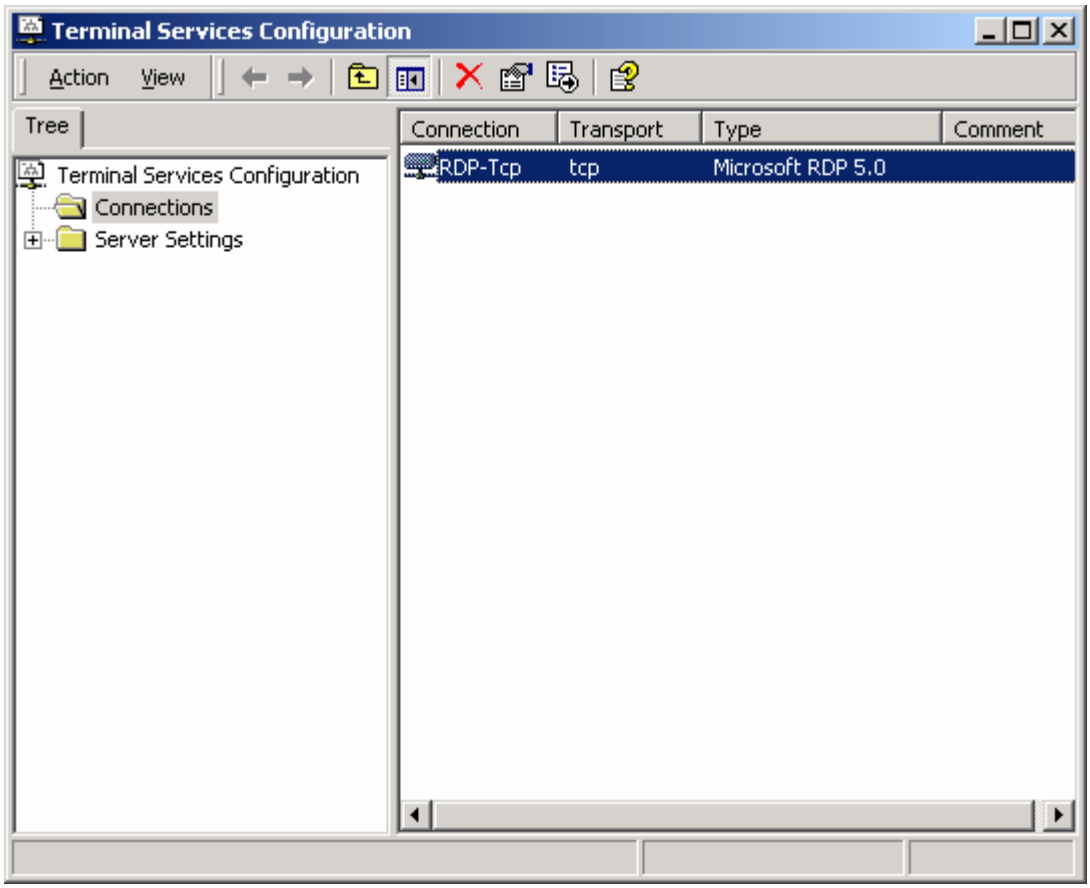

Figure 5 WTS Configuration Tool

General Settings

Available settings under the **General** tab for **RDP-TCP Properties** are shown in **Figure 6. Table 1** gives the recommended settings.

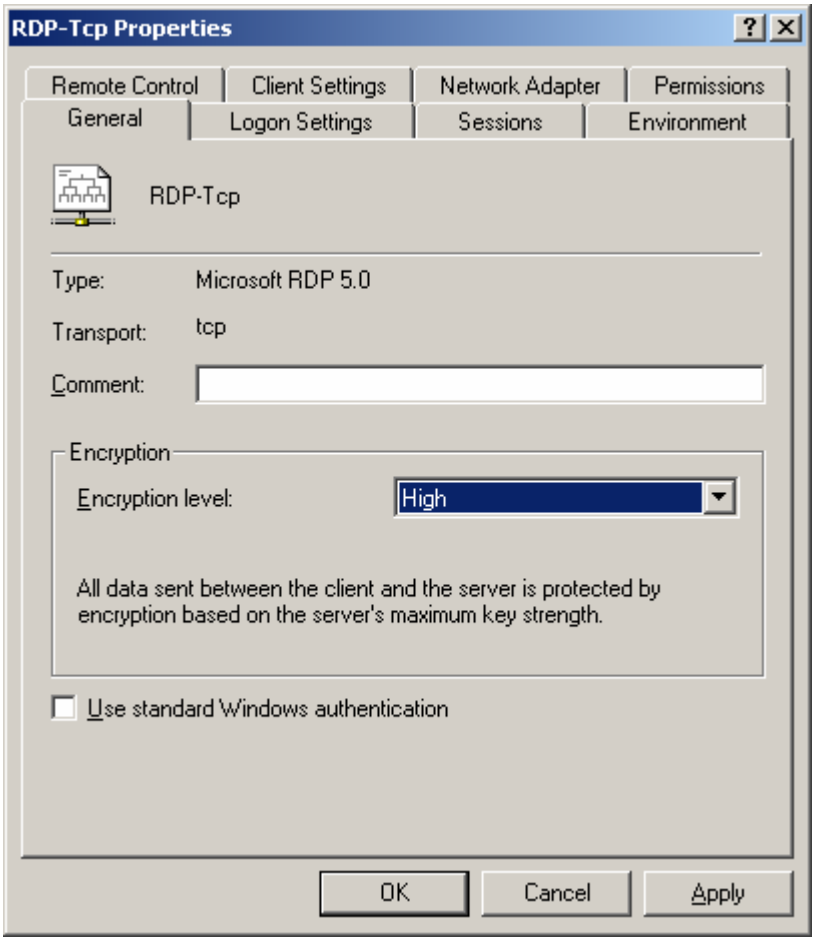

Figure 6 General Tab for RDP-TCP Properties

General Settings for RDP-TCP Properties	Recommended Settings
Encryption Level Sets the encryption parameters for communications between the WTS client and server. There are three choices: Low, Medium, and High. All three choices use RC4 as the encryption algorithm. Low encrypts only the data sent from the client to the server and not the data sent from the server to the client. Medium and High encrypt the data in both directions, but High uses a 128 bit key vice the 40 or 56 bit key used for Medium and Low. A user's computer must be running the 128-bit WTS client software in order to establish a session with a server that is using 128-bit encryption. Looking at the "About" information for the WTS client will identify whether the client software is 56 or 128 bits. Default is Medium.	High
Use standard Windows authentication If selected, permits lower security authentication mechanisms to be used. Default is Not Selected.	Not Selected

Table 1 General Settings for RDP-TCP Properties

Logon Settings

Available settings under the **Logon Settings** tab for **RDP-TCP Properties** are shown in **Figure 7**. **Table 2** gives the recommended settings.

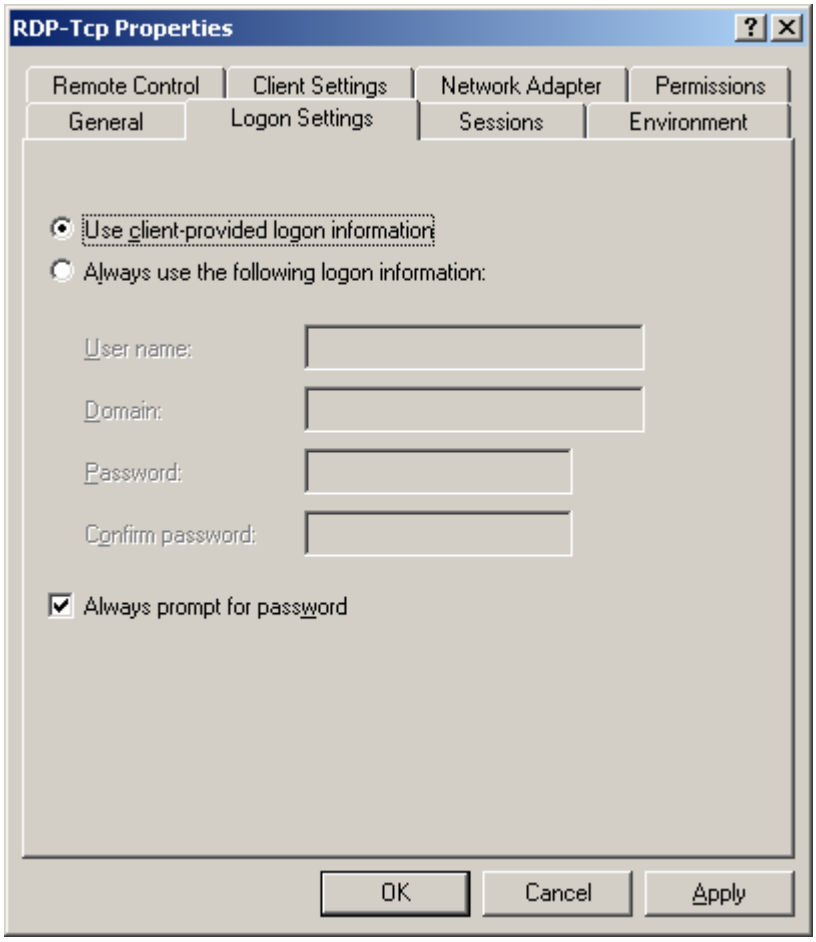

Figure 7 Logon Settings Tab for RDP-TCP Properties

Logon Settings for RDP-TCP Properties	Recommended Settings
Use client-provided logon information When a user wants to establish a WTS session, they are required to provide account name and password that are permitted for access to WTS. Default is Selected.	Selected
Allows use the following logon information Anyone that attempts to establish a WTS session with the server would be granted a session based on the account name and password entered here. Default is Not Selected.	Not Selected
Always prompt for password Requires user to provide a password to establish a WTS session with the server. Prevents use of an embedded password by the user. Default is Selected.	Selected

Table 2 Logon Settings for RDP-TCP Properties

Sessions Settings

Available settings under the **Sessions** tab for **RDP-TCP Properties** are shown in **Figure 8** and **Figure 9**. **Table 3** gives the recommended settings.

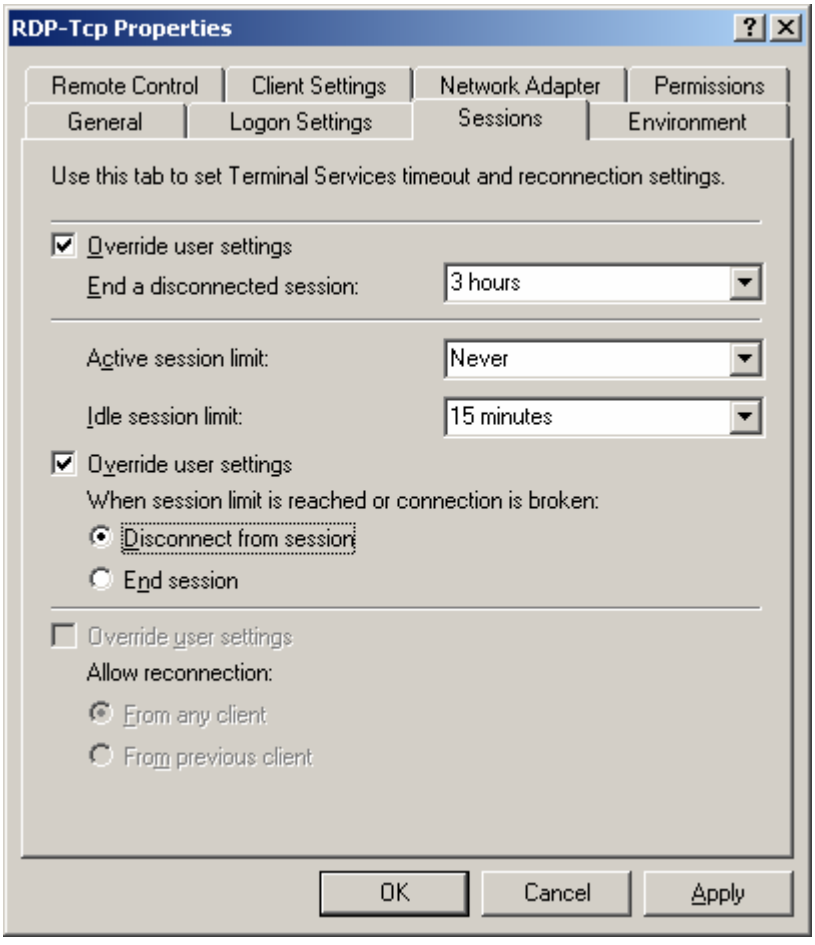

Figure 8 Sessions Tab for Intranet Application Sharing for RDP-TCP Properties

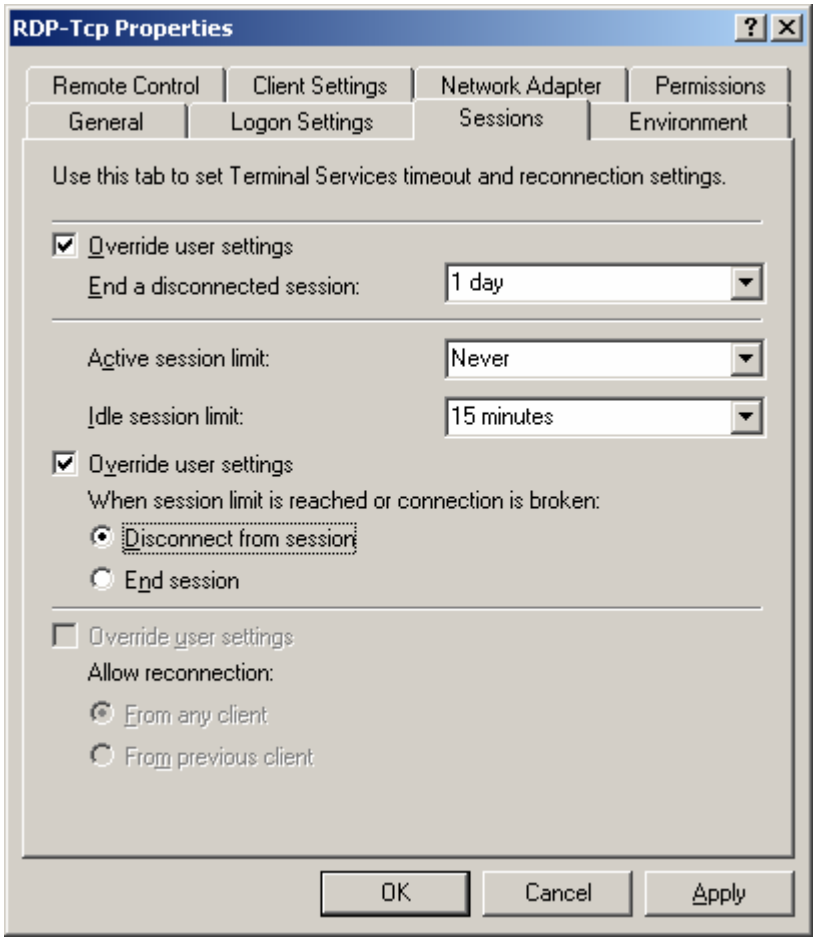

Figure 9 Sessions Tab for Remote Administration for RDP-TCP Properties

Sessions Settings for RDP-TCP Properties	Recommended Settings
Override user settings for session limits When selected, allows the server administrator to control the settings vice allowing the user to control the settings. Default is Not Selected.	Selected
End a disconnected session Limits how long a disconnected session can exist before it is closed. A disconnected session happens when a user has established a session with the server, but then the session/connection is disconnected. This can have many causes, for example, a user's computer crashes, or the user places the session into a disconnected state so they can access the same session from another location. During a disconnected session, the programs/processes the user had running on the server before the disconnection will continue to run even though the session/communications with the client have been lost. Since a user can possibly have a disconnected session running on the server without realizing it, it is best to limit how long that session stays running on the server. Default is Not Selected.	3 hours for Intranet Application Sharing 1 day for Remote Administration
Active session limit Limits how long a user can maintain an active session with the server. If set to "Never" the server will allow an active session to continue forever. Default is Not Selected	Never
Idle session limit Limits how long an idle session is kept open and not disconnected. An idle session may indicate that the user has stepped away from their computer, presenting someone else with the opportunity to use their session. Default is Not Selected	15 minutes
Override user settings for action when session limit is reached When selected, allows the server administrator to control the settings vice allowing the user to control the settings. Default is Not Selected.	Selected
Disconnect from session When selected will put a user session into a "disconnect" state when a session limit is reached or the client/server connection is broken. Default is Not Selected	Selected
End session When selected will end a user's session when a session limit is reached or the client/server connection is broken. If selected, a user will not be able to put their session into a disconnected state. If disconnecting a session is not required then selecting this option will prevent it from occuring. Default is Not Selected	Not Selected

Table 3 Sessions Settings for RDP-TCP Properties

When a session has been idle for more than fifteen minutes, the user is notified and given two minutes to take some action and place the session back into an "active" state. If the two minutes elapse, the server places the session into a disconnected state where the user's desktop, processes, etc are retained on the server. If the user doesn't connect to the session within the next three hours (one day is recommended for remote administration), the user is logged out, and the session is closed.

Environment Settings

Available settings under the **Environment** tab for **RDP-TCP Properties** are shown in **Figure 10** and **Figure 11**. **Table 4** gives the recommended settings.

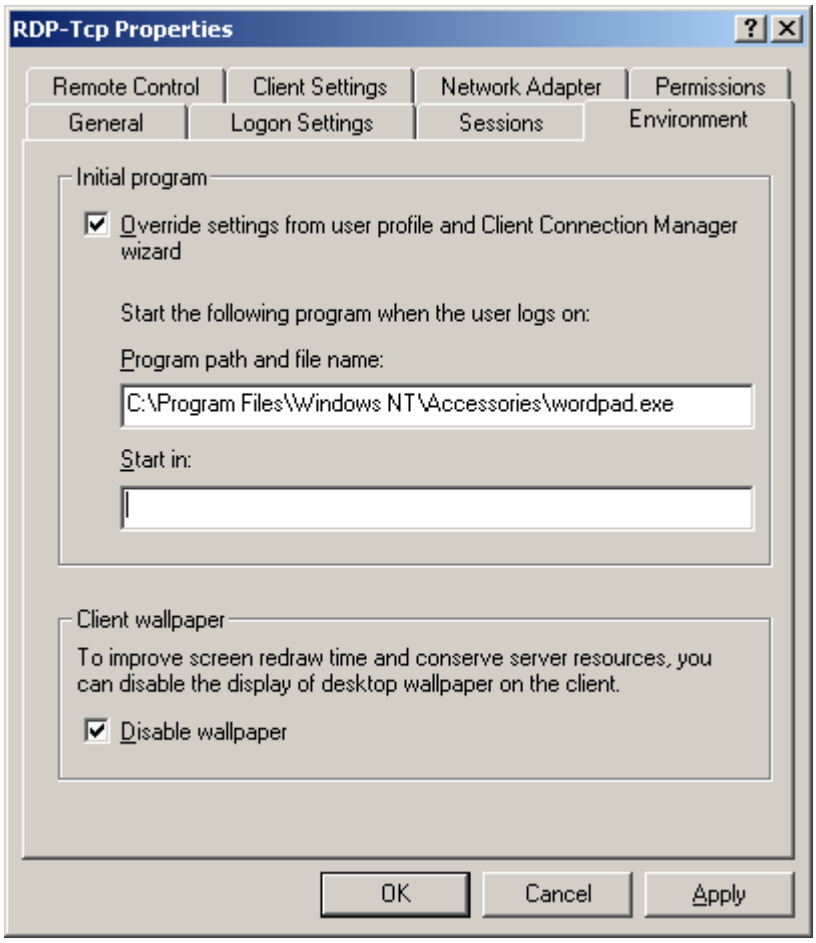

Figure 10 Environment Tab for Intranet Application Sharing for RDP-TCP Properties

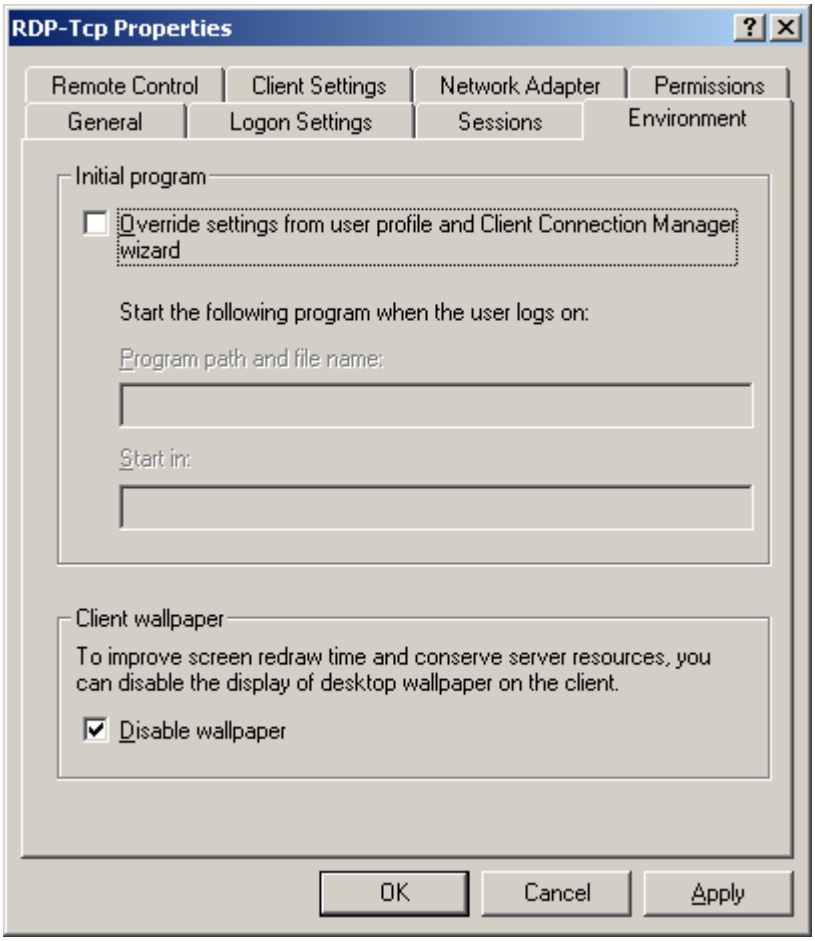

Figure 11 Environment Tab for Remote Administration for RDP-TCP Properties

Environment Settings for RDP-TCP Properties	Recommended Settings
Override settings from user profile and Client Connection Manager wizard When selected, allows the server administrator to control what application users will be provided via WTS. Can only be used when recommendation to limit a WTS application server to providing a single application is acceptable. In some cases, may not be practical for WTS for Intranet application sharing scenario and the guidance in Appendix A should be used to limit user access to applications. Not Selected is recommendation for WTS for remote administration scenario since administrators would be expected to require access to more than one application on the server. Default is Not Selected.	Selected for Intranet Application Sharing Not Selected for Remote Administration
Program path and file name Specifies the application that users will be provided via WTS. When a user starts a WTS session with the server, this application will start automatically. When the user closes the application, the WTS session with the server will end. The user will not have "Start", a taskbar, or other means to start other applications. Note that users must have the Query Information permission; otherwise the user will not be limited to this application and will be able to run other applications. See Appendix A for additional guidance on limiting a user's access to applications. A user may be able to run unintended applications. Thorough testing to identify the applications and restrict them is recommended. Default is Blank.	Full path of the application that will be provided to WTS users for Intranet Application Sharing Blank for Remote Administration
Start in Specifies a default directory. Default is Blank.	As applicable
Disable wallpaper When selected, disables the display of desktop wallpaper on the client thereby improving performance especially over low bandwidth connections such as dial-in (RAS). Either option is acceptable. The choice depends on the environment. Default is Selected	Environment Specific

Table 4 Environment Settings for RDP-TCP Properties

Remote Control Settings

Available settings under the **Remote Control** tab for **RDP-TCP Properties** are shown in **Figure 12**. **Table 5** gives the recommended settings.

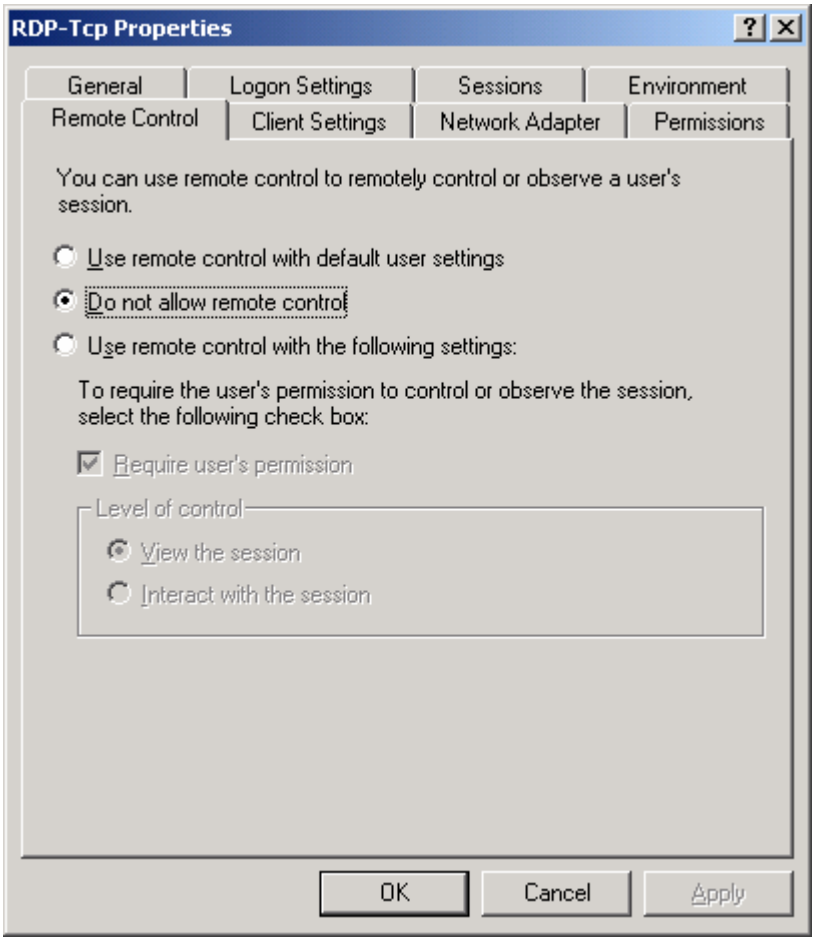

Figure 12 Remote Control Tab for RDP-TCP Properties

Remote Control Settings for RDP-TCP Properties	Recommended Settings
Use remote control with default user settings Permits the use of remote control and allows the user to control the settings. Remote control enables users that have the privilege enabled to take control of another user's WTS session and possibly perform actions under that user's account. Remote control is not recommended. If it is required that remote control be permitted, it is recommended that the "Use remote control with the following settings" be selected instead of this option. Default is Selected.	Not Selected
Do not allow remote control This is the recommended option since it disables the ability for one user to remotely control another user's session. Default is Not Selected.	Selected
Use remote control with the following settings: If it is required that remote control be permitted, the recommendation is that this option be Selected and that "Require user's permission" also be Selected. 'View the session" should be Selected unless it is essential that the user exercising their remote control privilege over another user's session also be able to perform actions under that user's account. Default is Not Selected.	Not Selected

Table 5 Remote Control Settings for RDP-TCP Properties

Client Settings

Available settings under the **Client Settings** tab for **RDP-TCP Properties** are shown in **Figure 13**. **Table 6** gives the recommended settings.

The recommendations are to restrict the user's options to those required to meet the operational needs in order to minimize the likelihood of introducing a vulnerability to the system. When an operational need exists, for example, using a local printer from within the WTS session, the recommendation is to add the fewest capabilities necessary to meet the need. For example, to allow a user to print from within a session to a local printer requires that the client settings below be changed to **Select** for **Connect client printers at log on** and that **(Disable) Windows printer mapping** be **Not Selected**.

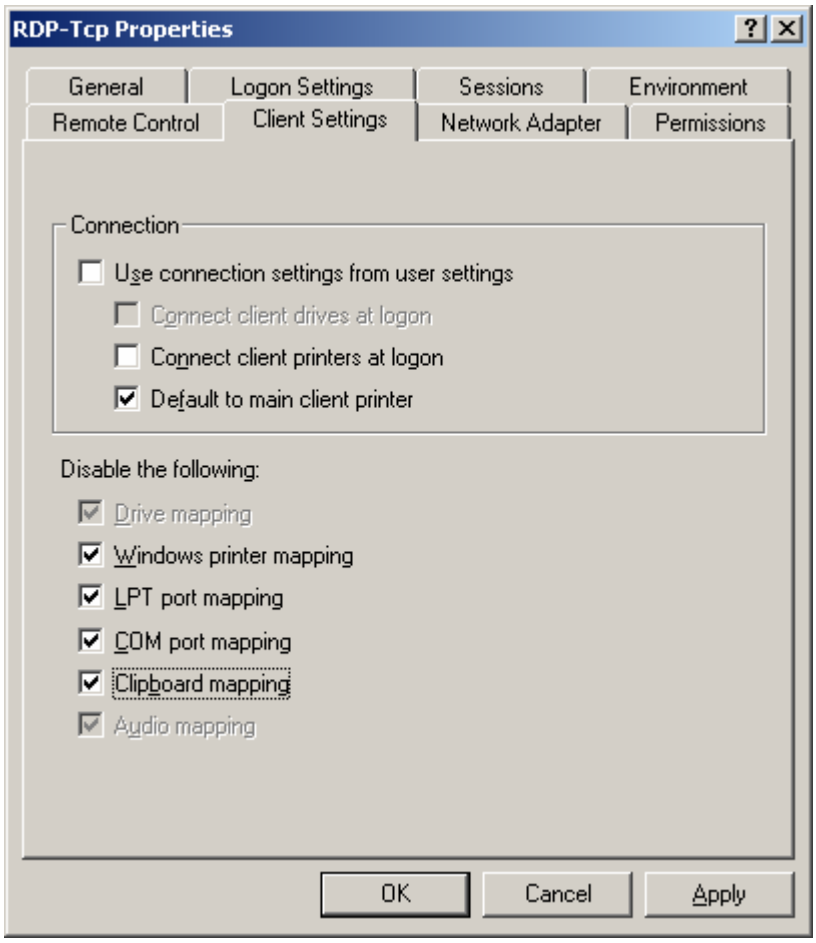

Figure 13 Client Settings Tab for RDP-TCP Properties

Client Settings for RDP-TCP Properties	Recommended Settings
Use connection settings from user settings When selected, allows the user to control the settings vice the server administrator. Default is Selected.	Not Selected
Connect client printers at logon When selected, local printers that the user has setup on the client computer will be available from within the WTS session. Unless there is a requirement for this capability, the recommendation is that it be disabled. If Selected, the "(Disable) Windows printer mapping" option must be Not Selected. Default is Not Selected.	Not Selected
Default to main client printer When selected, the default printer that the user has set up on the client computer will be the default printer from within the WTS session. Default is Not Selected	Selected
Disable Windows printer mapping Prevents the user from creating printer mappings for use during a WTS session. Unless there is a requirement for this capability, the recommendation is that it be disabled. It must be enabled if the user needs to print to a local printer on the user's computer. Default is Not Selected	Selected
Disable LPT port mapping Prevents the user from accessing devices that require a parallel (LPT) port mapping from within the user's WTS session. Unless there is a requirement for this capability, the recommendation is that it be disabled. Default is Not Selected	Selected
Disable COM port mapping Prevents the user from accessing devices that require a serial (COM) port mapping from within the user's WTS session. Unless there is a requirement for this capability, the recommendation is that it be disabled. Default is Selected	Selected
Disable Clipboard mapping Prevents the user from cutting and pasting information using the Windows clipboard between the applications running on the client computer itself and the applications running from within the user's WTS session. Unless there is a requirement for this capability, the recommendation is that it be disabled. If enabled, a user must also have the Virtual Channels permission in order for the clipboard mapping to work. Default is Not Selected.	Selected

Table 6 Client Settings for RDP-TCP Properties

Permissions Settings

Under the Permissions tab for RDP-TCP Properties, use **Add** and **Remove** to ensure that only the appropriate users and administrators are listed. For Intranet Application Sharing, typically the Administrators group, SYSTEM, and a user group are appropriate. For Remote Administration, typically only the Administrators group and SYSTEM are appropriate. Members of the Administrators group for the server should be limited to those with that responsibility. Members of the users group should be limited to those that require the use of application-sharing WTS on the server. **Figure 14** shows the Permissions tab window for Intranet Application Sharing.

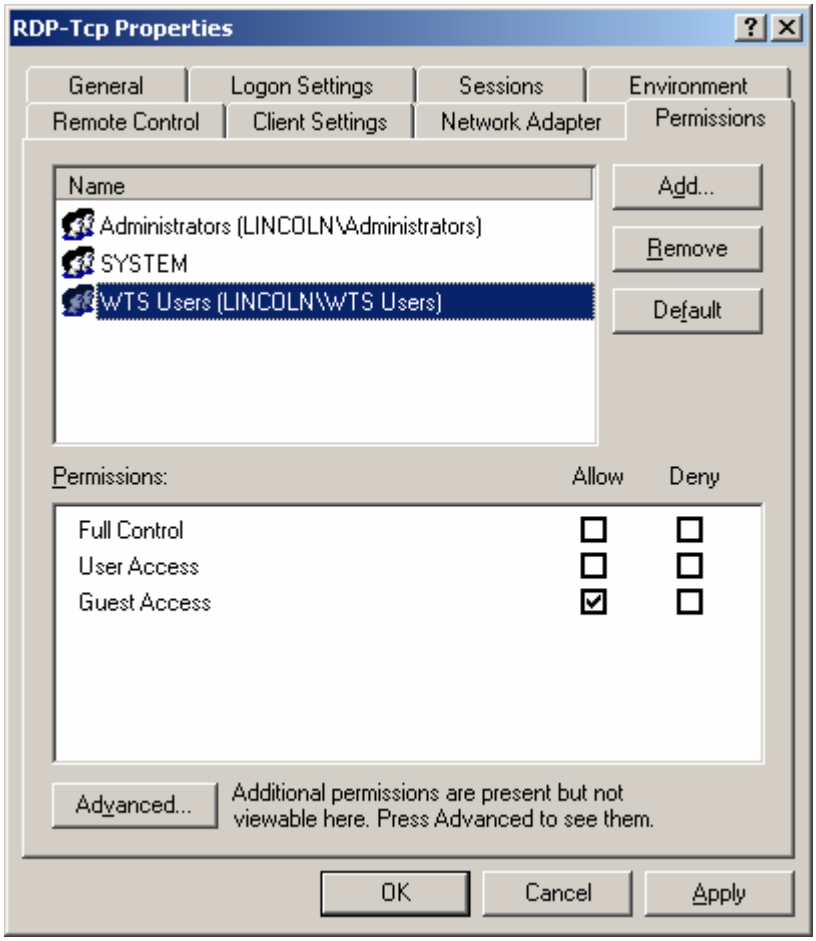

Figure 14 Permissions Tab for Intranet Application Sharing for TDP-TCP Properties

Figure 15 and **Table 7** shows the recommended settings for the terminal service user group for Intranet Application Sharing. To set permissions on the terminal services user group for Intranet Application Sharing:

- Select the user group
- Click **Advanced**
- Select the user group with the type **Allow** and click on **View/Edit**
- Select **Allow** for **Query Information, Logon**, and **Connect**

  NOTE: Logon is the minimum required to establish a session. Query Information is required if the server is limiting the user to one application via the Environment settings. Connect is required if users will be permitted to connect to disconnected sessions. Note that if additional capabilities/privileges are required that this guidance will need to be modified. For example, Virtual Channels is required if Clipboard Mapping is a requirement.

- Select **Deny** for **Set Information**, **Reset**, **Remote Control**, **Logoff**, **Message**, **Disconnect**, and **Virtual Channels**
- Click **OK → OK**

- Click **Yes** if asked "Caution! Deny entries take priority over Allow entries, which can cause unintended effects due to group memberships. Do you wish to continue?"
- The users group should have **Allow** for only **Guest Access**

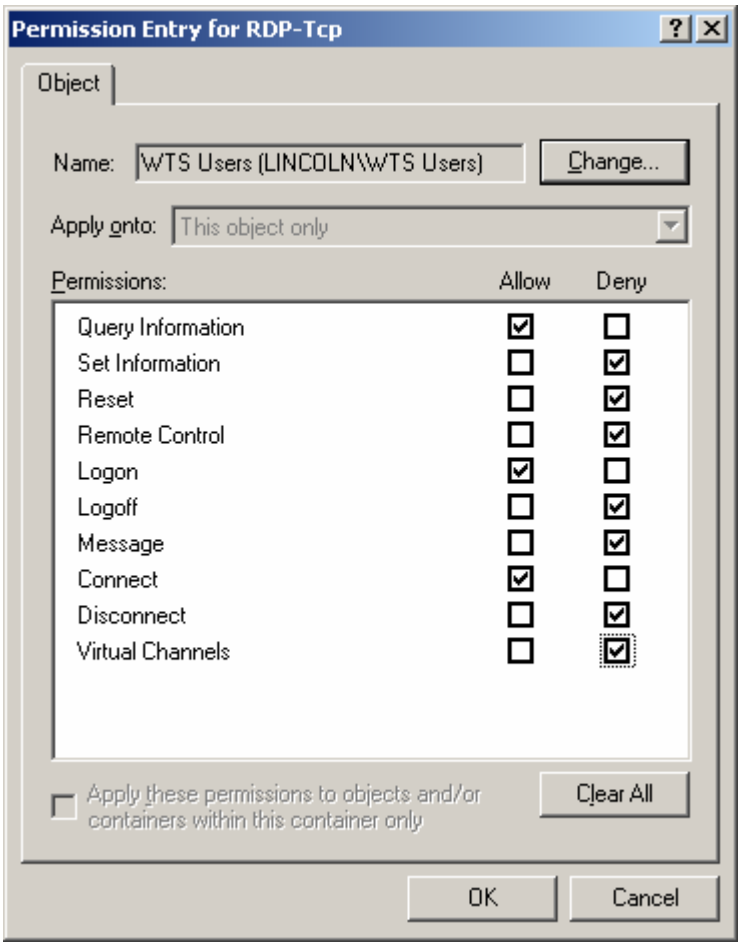

Figure 15 User Permission Entry for Intranet Application Sharing for RDP-TCP Properties

Permissions Settings for WTS Users	Recommended Settings for Intranet Application Sharing
Query Information Allows a user to access information about sessions. This permission is needed to limit a user to the single application specified in the Environment settings. Default is Allow.	Allow
Set Information Allows a user to change the settings for connection properties. Note that an account with administrator privileges may be able to change the connection properties even if this permission is set to Deny. Default is Deny.	Deny
Reset Allows a user to close another user's session without warning. A reset can result in the loss of user data (for example, if the user had entered data into an application provided via WTS but not saved it prior to the reset occurring). Default is Deny.	Deny
Remote Control Allows a user to take control of another user's session, possibly taking actions with the other user's permissions/account. Default is Deny.	Deny
Logon The Logon permission is the minimum permission needed for a user to be able to establish a WTS session. Default is Allow.	Allow
Logoff Allows a user to log off (close) another user's session without warning. Default is Deny.	Deny
Message Allows a user to send messages to other users with a session on the server. The recommendation is to deny this permission unless a user has a requirement for the capability. Default is Allow.	Deny
Connect Allows a user to connect to a disconnected session. Default is Allow.	Allow
Disconnect Allows a user to disconnect another user's session without warning. Default is Deny.	Deny
Virtual Channels Allows a user's session to access additional virtual channels. The recommendation is to deny this permission unless there is a requirement for the capability. This permission must be allowed if Windows clipboard mapping is enabled in the Client Settings. Default is Deny.	Deny

Table 7 Permissions Settings for WTS Users for Intranet Application Sharing

Figure 16 and **Table 8** show the recommended permissions for the Administrators group. To set permissions on the Administrators group for both Intranet Application Sharing and Remote Administration:

- Select the Administrators group
- Click **Advanced**
- Select the administrators group with the type **Allow** and click on **View/Edit**

- Select **Allow** for **Query Information**, **Set Information**, **Reset**, **Logon**, **Logoff**, **Message**, **Connect**, and **Disconnect**
- Select **Deny** for **Remote Control** and **Virtual Channels**
- Click **OK → OK**
- Click **Yes** if asked "Caution! Deny entries take priority over Allow entries, which can cause unintended effects due to group memberships. Do you wish to continue?"
- The Administrators group should have **Allow** for **User Access** and **Guest Access** and SYSTEM should have **Allow** for **Full Control**, **User Access** and **Guest Access**.

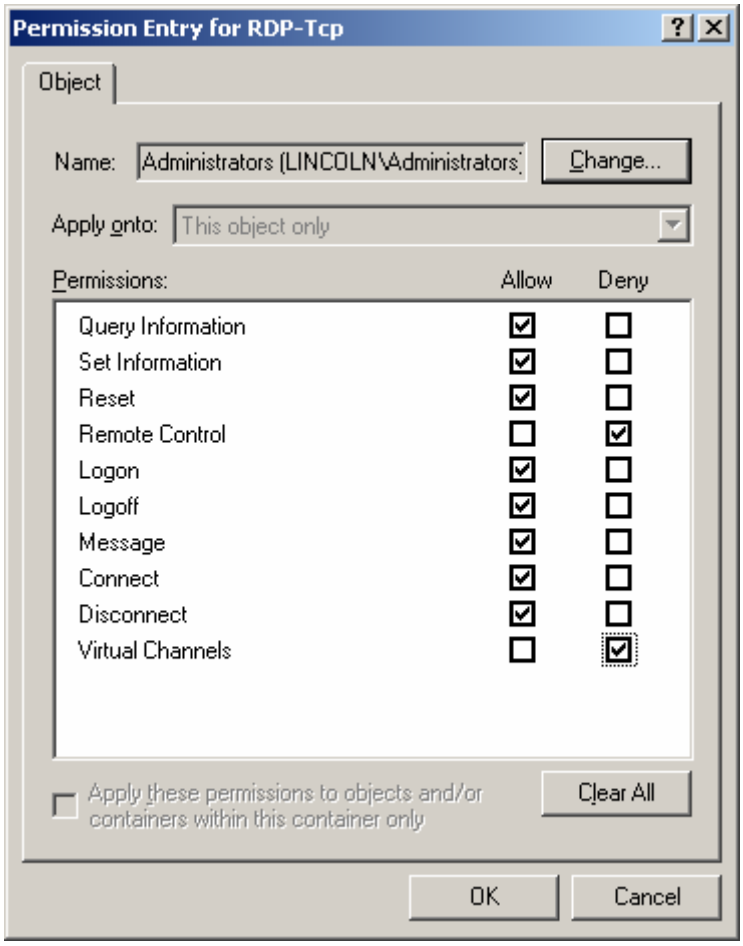

Figure 16 Administrator Permission Entry for RDP-TCP Properties

Permissions Settings for Administrators	Recommended Settings
Query Information Allows an administrator to access information about a user's session. Default is Allow.	Allow
Set Information Allows an administrator to change the settings for connection properties. Note that the account being used must also have administrator privileges on the server in order to change the settings and with these privileges may be able to change the settings for connection properties even if this permission is set to Deny. Default is Allow.	Allow
Reset Allows an administrator to close a user's session without warning. Default is Allow.	Allow
Remote Control Allows an administrator to take control of a user's session, possibly taking actions with the user's permissions/account. The recommendation is to deny this permission, even to administrators, unless there is a requirement for this capability. Default is Allow.	Deny
Logon The Logon permission is the minimum permission needed for an administrator to be able to establish a WTS session. Default is Allow.	Allow
Logoff Allows an administrator to log off (close) a user's session without warning. Default is Allow.	Allow
Message Allows an administrator to send messages to users with a session on the server. Default is Allow.	Allow
Connect Allows an administrator to connect to a disconnected session. The password for the user that initiated the session is required to connect to a session, preventing one user from connecting to the disconnected session of another user. Default is Allow.	Allow
Disconnect Allows an administrator to disconnect another user's session without warning. Default is Allow.	Allow
Virtual Channels Allows an administrator's session to access additional virtual channels. The recommendation is to deny this permission unless there is a requirement for the capability. Default is Allow.	Deny

Table 8 Permission Settings for Administrators

Click OK to close the RDP-TCP Properties window.

Guidance for Server Settings for WTS

Available settings under the **Server Settings** tab for **RDP-TCP Properties** are shown in **Figure 17** and **Figure 18**. **Table 9** gives the recommended settings.

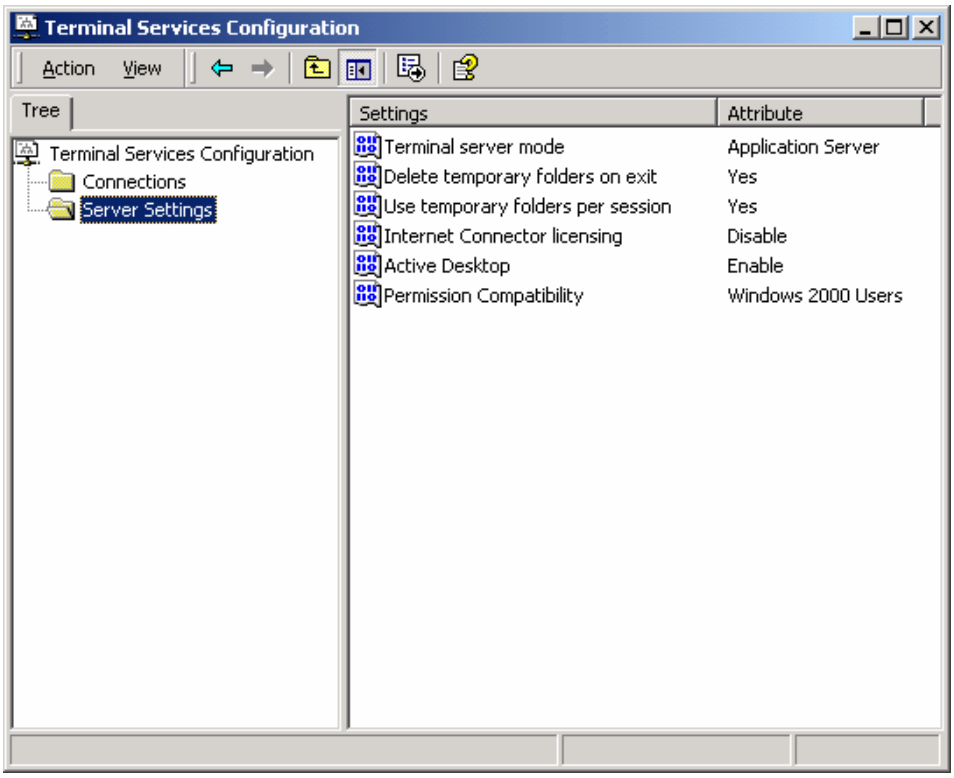

Figure 17 Server Settings for WTS for Intranet Application Sharing

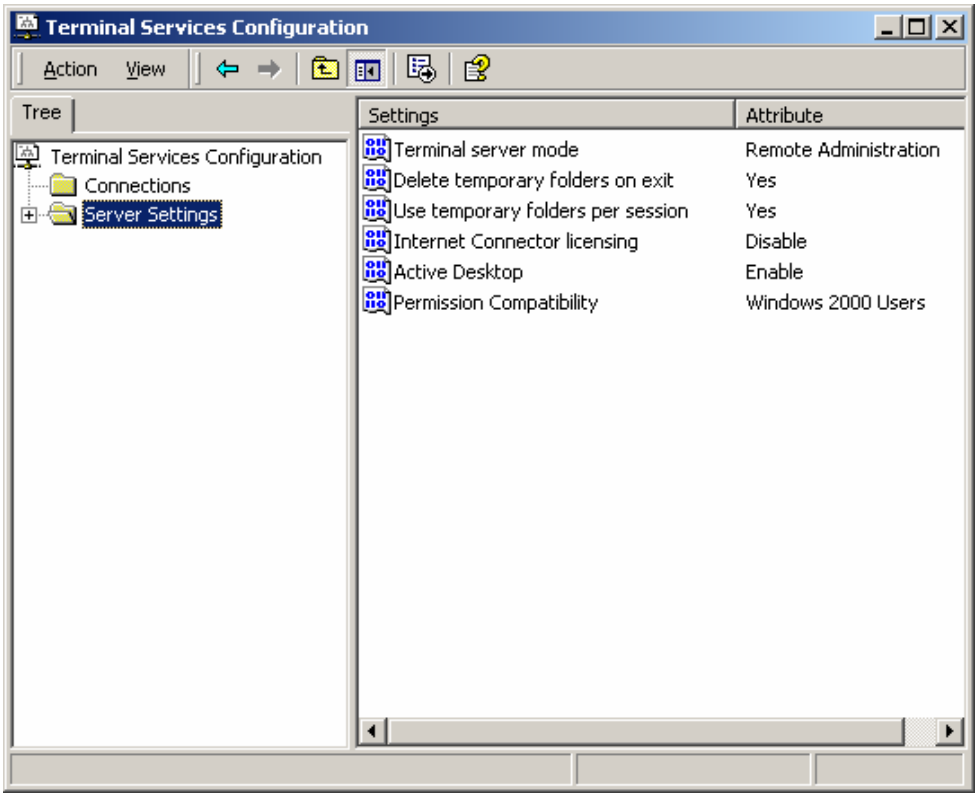

Figure 18 Server Settings for WTS for Remote Administration

Server Settings	Recommended Settings
Terminal server mode This setting cannot be changed from the Terminal Services Configuration tool. "Application Server" will be the setting if Application Server mode was selected when WTS was installed. "Remote Administration" will be the setting if Remote Administration mode was selected when WTS was installed.	Application Server for Intranet Application Sharing Remote Administration for Remote Administration
Delete temporary folders on exit If "Yes", the server will delete the temporary folders created to support a user's WTS session when the session is closed. Note that the folders are not deleted when a session is disconnected, but only when a session is closed by logging off from that session. Deleting the folders reduces the risk of their being accessed inappropriately. Default is Yes.	Yes
Use temporary folders per session If "Yes", the server will create separate temporary folders for each session it is supporting. Creating separate folders reduces the risk of data being accessed inappropriately. Default is Yes.	Yes
Internet Connector licensing "Disable" must be the setting unless a WTS Internet Connector license is being used. The Internect Connector license permits a server to support up to 200 user sessions, however the license requires that the users not be employees. This license is used for the WTS Internet Application Sharing scenario, but not for the WTS Intranet Application Sharing scenario.	Disable
Active Desktop If "Enable", the server will permit sessions to use Active Desktop. Default is Enable.	Enable
Permission Compatibility "Windows 2000 Users" will be the setting if it was chosen when WTS was installed. This setting requires users to run an RDP 5.0 compatible client such as that provided with Windows 2000 and not an RDP 4.0 client such as that provided with Windows NT. Using "Terminal Server 4.0 Users" results in users being granted additional permissions to the registry and system files that increase the security risk.	Windows 2000 Users

Table 9 Server Settings for WTS

Guidance for File Permissions for WTS

The security guidance for file permissions provided in the *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set* is the recommendation for WTS servers as well. Particular attention should be focused on the installation of new applications on the server. When an application is installed on the server, the file permissions associated with any directories created by the application should be checked to ensure that the least amount of privileges necessary are being assigned to the users. In some cases, it may be necessary to modify the file permission recommendations for some files and/or directories on the server in order for the permissions to be compatible with the new application.

Guidance for Auditing for WTS

The security guidance for auditing as defined in the *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set* is the recommendation for WTS servers as well.

Guidance for Router and Firewall Settings for WTS

The following guidance is for the routers and firewalls shown in **Figure 1 Operational Scenarios for Windows 2000 Terminal Services**. Although your environment will be different, the general guidance below should be applied appropriately.

Communications between the WTS server and client are via the Remote Desktop Protocol (RDP), version 5. RDP uses port 3389 for communications. The WTS servers on the Intranet should be protected from the Internet by Router A, the Firewall, and Router B. Specifically, Router A, the Firewall, and Router B should ensure that, from the Internet, access to port 3389 of the servers on the Intranet is blocked. All other ports not required to be available should also be blocked.

This Page Intentionally Left Blank

Appendix

A

Limiting Access to Applications

When Windows 2000 Terminal Services (WTS) is installed on a server in Application Server mode with the default settings, it allows WTS users to run virtually any application they choose on the server. For security purposes it is necessary to limit the applications that a WTS user can run on the server. Limiting users to just one application can be done using the Environment settings as described in Chapter 2. However, in many cases, limiting the users to one application on the server is undesirable.

Windows 2000 provides administrators the ability to control user access to applications in a number of ways. Group Policy can specify which applications are visible to a user. In addition, it can prevent users from launching applications through the Windows Explorer shell. However, users can launch hidden applications either by using the **Run** command or by launching an embedded object. Group Policies can affect a user's computer as well as their WTS sessions if not created properly.

The Microsoft Application Security tool (Appsec) allows an administrator to control access to each application/executable on the server. If configured properly, it can limit a user to accessing only specific applications via a WTS session.

The recommended approach to limiting access to applications is to implement both Appsec and Group Policy. Appsec can restrict the user to only executing the applications the user should have access to, and Group Policy can effectively **hide** the applications the user should not have access to. Note that Appsec does not restrict administrators from accessing any application on the server, only users.

Appsec allows an administrator to restrict the access of users to a predefined set of applications on the server. When application security is enabled, non-administrator users can execute only the programs on the authorized application list. Attempts to execute programs not on the authorized application list are rejected.

The Appsec tool identifies which applications a user is allowed to use based on the full path name. All applications not explicitly allowed are denied. This prevents users from running an application that is not allowed by just naming it the same as an allowed application. For example, if C:\WinNT\Program Files\Accessories\wordpad.exe is allowed, the user cannot run an application such as C:\Temp\wordpad.exe.

Despite the application of these recommendations, a user may be able to run unintended applications. Thorough testing to identify the applications and restrict them is recommended.

Installation of the Application Security Tool

The Appsec tool is in the Microsoft Windows 2000 Server Resource Kit. **Figure 15** shows the Appsec installation window. Install Appsec using the following procedures:

- **Start → Settings → Control Panel → Add/Remove Programs**
- Click **Add New Programs**

- Click **CD or Floppy**
- Click **Next**
- Browse to the location of the Windows 2000 Server Resource Kit and select setup.exe.
- Click **Next** and then click **Next** again
- Select **I Agree** and then click **Next**
- Enter your name and organization and then click **Next**
- Select **Custom** and then click **Next**
- To install Appsec, only the **Computer Management Tools** and **Tool Documentation** need to be selected. **Figure 19** shows the Custom Installation window.
- Click **Next** and then click **Next** again
- Click **Finish** and then click **Next**
- Click **Finish** and then click **Close**
- After the installation is completed, restart the computer

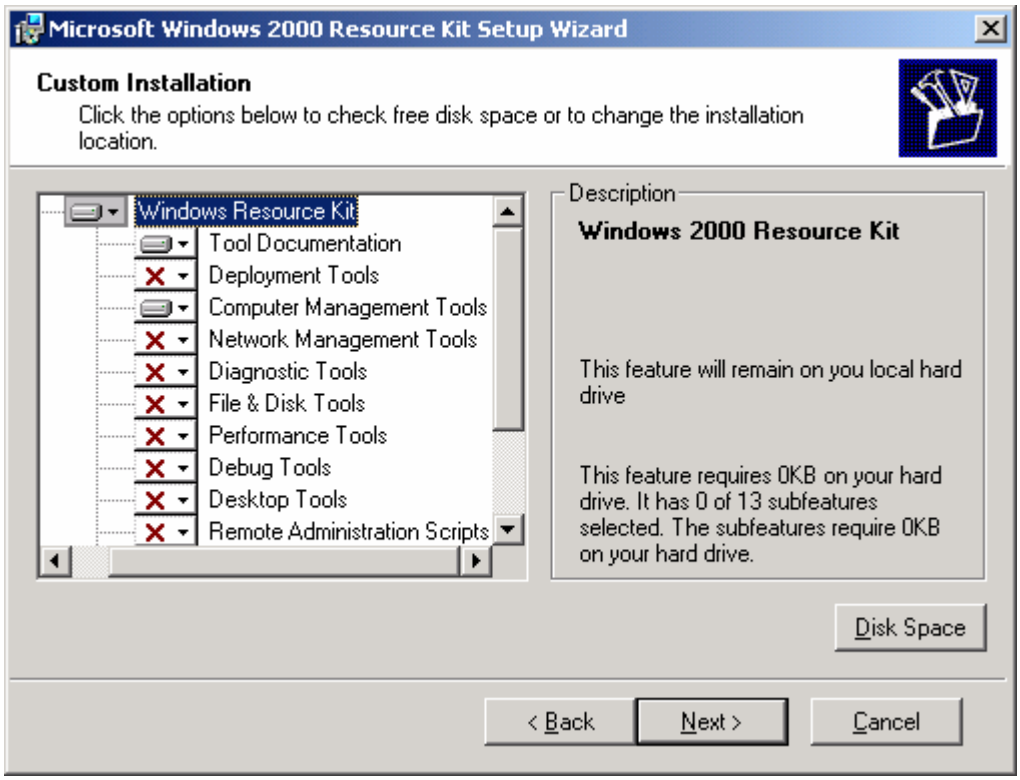

Figure 19 Appsec Installation

There is a Microsoft patch for Appsec that must be applied for it to function correctly. The patch installs several files needed by Appsec that are not in the Microsoft Windows 2000 Resource Kit. Article Q257980, *Appsec Tool in the Windows 2000 Resource Kit Is Missing Critical Files*, contains details concerning the patch, and the patch itself. Q257980 is available at the following URL:

http://support.microsoft.com/directory/article.asp?id=KB;EN-US;q257980

Install the patch in accordance with Q257980.

Using Appsec for Limiting Access to Applications

Applications that users will be permitted to access during a WTS session with the server must be explicitly defined as authorized applications within Appsec. Users are denied access to all other applications. Note that Appsec does not restrict an administrator's access to applications.

Enabling Application Security

To enable Application Security:

- **Start → Programs → Windows 2000 Resource Kit → Tools→Computer Management Tools → Application Security**
- Click **Add** to place applications in the list of authorized applications and **Delete** to remove them. See **Figure 20** for an example.

  NOTE: If 16-bit applications are added to the authorized applications list, it is possible that Appsec will not perform correctly. It is recommended that only 32-bit applications be placed in the list of authorized applications.

- To enable application security, click **Enabled** under **Security**. When application security is enabled, non-administrator users can execute only the listed applications.
- To disable application security, click **Disabled** under **Security**. When application security is disabled, users can run any application for which they have the necessary permissions.

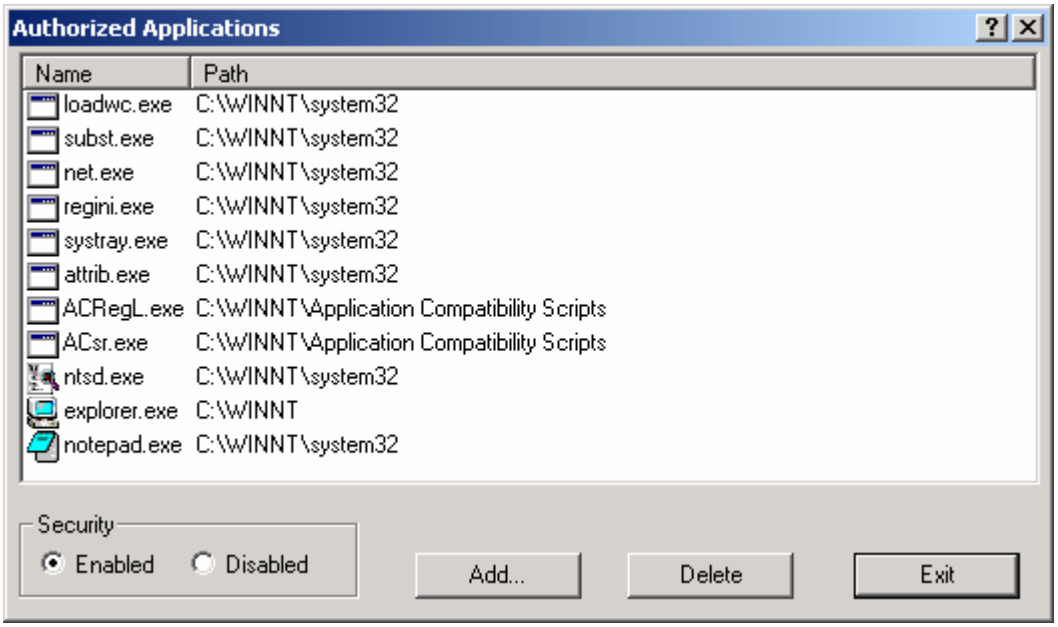

Figure 20 Authorized Applications List in Appsec

Appsec's Tracking Feature

Appsec has a tracking feature that allows administrators to track the processes started by a particular application. The tracking feature is started, the application is started and used (including exercising its features), and then the tracking feature is stopped. This period of time is called the "tracking period." After tracking is over, administrators can view the processes that were started during the tracking period and add some or all of these processes to the list of authorized applications. This feature also enables administrators to find the applications that are started from within other application (for example, Microsoft Outlook starting Microsoft Word as an editor for e-mails). These additional applications can be added to the list of authorized applications.

To start Tracking:

- Click **Start Tracking**
- Start the application and exercise its features.
- To stop Tracking, click **Stop Tracking**

All the processes that were started during the "Tracking period" will be listed in the "Tracking Results" list.

To add these applications to the list of Authorized Applications, delete all entries that should not be added and then click OK.

Additions to the List of Authorized Applications

In addition to the applications previously identified and placed on the list of authorized applications, the following applications/programs should be added to the list if they are not already included:

- `%Systemroot%\explorer.exe`
- `%Systemroot%\system32\systray.exe`

Microsoft recommends that the following applications/programs be added to the list of authorized applications if they are not already included. Careful consideration should be given to what each of these applications/programs will allow a user to do prior to adding them to the list of authorized applications.

- `%Systemroot%\system32\cmd.exe`
- `%Systemroot%\system32\net.exe`
- `%Systemroot%\system32\regini.exe`
- `%Systemroot%\system32\subst.exe`
- `%Systemroot%\system32\xcopy.exe`

Using Group Policy for Limiting Access to Applications

Group Policy is a flexible and powerful tool for controlling a user's desktop and restricting actions a user can take. It can be used to effectively "hide" applications from the user by preventing them from appearing on the desktop. For example, Group Policy can be used to prevent the Run command from appearing in the Start menu on the user's desktop.

However, care must be taken in applying Group Policy correctly. For example, it might be desirable to use Group Policy to prevent the Run command from appearing in the Start menu of a user's WTS session. But, it may not be acceptable for that same rule to apply to the Start menu when the user is logged on to their own computer.

In many cases, an effective approach to Group Policy as it pertains to WTS application-sharing servers would be to place the servers in a dedicated Organizational Unit (OU) and apply the appropriate Group Policy to the OU. Note that this OU should only contain the servers providing application sharing via WTS, not other computers or any users. The sections of the Group Policy pertaining to Computer Configuration, Windows Settings, Security Settings, and Local Policies are the most applicable for limiting a user's access to applications.

This Page Intentionally Left Blank

Appendix

B

Windows 2000 Terminal Services Default User Permissions

The following is a list of the WTS permissions that are granted to each user by default. In many cases, the security guidance within this document recommends that the WTS server be configured to override these user settings.

Default User Settings for WTS	Default Setting
Remote Control	
Enable remote control	Selected
Require user's permission	Selected
View the user's session	Not Selected
Interact with the session	Selected
These default settings allow one user to take control of another user's WTS session and take actions using that user's permissions/account.	
Terminal Services Profile	
Terminal Services profile	Blank
Terminal Services home directory – local path	Selected
Terminal Services home directory – connect	Not Selected
Allow logon to terminal server	Selected
These default settings allow the user to logon to the WTS server and establishes a local directory on the server as the user's home directory during the session.	
Sessions	
End a disconnected session	Never
Active session limit	Never
Idle session limit	Never
When a session limit is reached or a connection is broken	Disconnect from session
Allow reconnection	From any client
These default settings place no restrictions on how long a disconnected session can remain on the server. They can result in a user having multiple disconnected sessions running on the server without knowing it because the disconnected sessions never expire. The default settings permit an idle session to remain connected indefinitely.	
Environment (Client Settings)	
Start the following program at log on	Not Selected
Connect client drives at logon	Selected
Connect client printers at logon	Selected
Default to main client printer	Selected
These default settings do not limit a user to a single application when connecting to the server. The default settings allow the user access to the local disk space of the client computer and to any printers defined on the client computer from within the WTS session.	

Table 10 Default User Settings for WTS

This Page Intentionally Left Blank

Appendix

C

Windows 2000 Terminal Services Security Guidance Troubleshooting

"The local policy of this system does not allow you to logon interactively" error message

The user (typically from being a member of a group) needs to have the "Log on locally" right. The right can be assigned via a Group Policy at the appropriate Domain, Site, OU, or Local level. The Local Security Policy tool can be used to determine if the user/group has the right.

"Terminal Server has ended the connection" error message

Check the Event Log on the server. Under System Log, look for a Termdd error with a description that discusses a data encryption error. The cause of the problem may be that the server has the Encryption level set to "High," requiring the use of 128-bit encryption, as is recommended in this guide. However, the client computer may not have a 128-bit WTS client. To check, start the Terminal Services Client and check the "About" information to determine the version and cipher strength. If the cipher strength is 56 bits, the client must be replaced with a 128-bit client. The client can be created on the WTS server and then installed on the user's computer.

Appsec is not restricting access to applications

There is a Microsoft patch for Appsec that must be applied for it to function correctly. The patch installs several files needed by Appsec that are not in the Microsoft Windows 2000 Resource Kit. Article Q257980, Appsec Tool in the Windows 2000 Resource Kit Is Missing Critical Files, contains details concerning the patch, and the patch itself. Q257980 is available at the following URL:

http://support.microsoft.com/support/kb/articles/Q257/9/80.ASP

Install the patch in accordance with Q257980.

This Page Intentionally Left Blank

Appendix

D

References

Clark, David, Microsoft Windows 2000 Security Technical Reference, Microsoft Press, 2000

Davis, Peter T. and Barry Lewis, Sams Teach Yourself Microsoft Windows 2000 Server in 21 Days, Sams Publishing, 2000

Komar, Brian, Designing Microsoft Windows 2000 Network Security Training Kit, Microsoft Press, 2001

Mathers, Todd W., Windows NT/2000 Thin Client Solutions, MacMillan Technical Publishing, 2000

Microsoft web page, http://www.microsoft.com, http://www.microsoft.com/security

Microsoft Windows 2000 Resource Kit, Microsoft Press, 2000

Minasi, Mark, Windows 2000 Resource Kit, Sybex, 2000

NT Bug Traq, http://www.ntbugtraq.com/

Schultz, Eugene, Windows NT/2000 Security, Macmillan Technical Publishing, 2000

Schmiedt, Jeff, Microsoft Windows 2000 Security Handbook, Que Corporation, 2000

Windows 2000 Magazine website, http://www.win2000mag.com

Windows IT Security website, http://www.windowsitsecurity.com