Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Secure Remote Access using Windows Terminal Services 2003

Microsoft's Terminal Server has improved considerably since its release in 1998 in functionality, performance and security. With the increasing demand for flexible, simple and fast remote access for the endless variety of users including vendor support staff, home users, mobile workers and remote offices, Terminal Server is now becoming an attractive and inexpensive solution particularly for smaller, less complex environments. The primary focus of this paper will be to present options for securing Windows Terminal Serv...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

Secure Remote Access using

Windows Terminal Services 2003

GSEC Certification Practical
Option 1, Version 1.4b
By Darlene Fletcher
February 2nd, 2004

© SANS Institute 2004, Author retains full rights.

Secure Remote Access using Windows Terminal Services 2003

Abstract

Microsoft's Terminal Server has improved considerably since its release in 1998 in functionality, performance and security. With the increasing demand for flexible, simple and fast remote access for the endless variety of users including vendor support staff, home users, mobile workers and remote offices, Terminal Server is now becoming an attractive and inexpensive solution particularly for smaller, less complex environments. The primary focus of this paper will be to present options for securing Windows Terminal Services 2003 remote access in application mode (now referred to as Terminal Server mode). This will include an overview of the new features of Windows Terminal Services 2003 and how they affect security, as well as implementation considerations, current threats and recommended security configurations. The configuration sections will focus primarily on using the Group Policy tools. Configured correctly, Terminal Services 2003 can provide a secure, feature rich, remote access solution for many corporate environments.

Table of Contents

Abstract 1
Table of Contents 1
Windows Terminal Services 2003 Overview 2
What's New in Terminal Services 2003 2
Client Features 3
Table 1 - Remote Desktop Connection Client Features 4
Table 2 – Remote Desktop Web Connection 6
Server Features 7
Table 3 – Terminal Server 2003 New Features and Improvements 7
Planning a Defense in Depth Strategy 9
Terminal Server Specific Attacks 9
Enumeration 9
Password Guessing Attacks 10
Local Privilege Escalation 10
Network Security Considerations 11
Using VPNs with Terminal Server 11
Using Firewalls with Terminal Server 12
Network separation 13
RDP Port Considerations 13
Authentication and Access control 14
Logging and Auditing 15
Policies, Awareness training, Procedures 15
Best Practices Recommendations 15
Terminal Server Configuration 17
Choosing a Terminal Server Configuration Tool 17
Table 4 Benefit and Restriction Comparison for Configuration Tools 17
Configuring Terminal Services with Group Policy 18
Planning Considerations for Group Policy 18
Enabling Group Policy 19
Configuring Group Policy Settings 19
Summary 23
Appendix A - User Group Policies 24
Appendix B – Permissions Settings 27
Appendix C – Server Group Policy Settings 28

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Appendix D – Terminal Server Connection Configurations 31
Appendix E – Client Connection Settings 34
List of References 37

Windows Terminal Services 2003 Overview

Terminal Services is an optional component of the Windows Server operating system that provides remote administration or application services to a variety of devices such as computers and PDAs, and non-windows devices such as Mac computers. Connectivity can be provided over LAN, WAN or the Internet. Otherwise known as server-based computing, Terminal Services lets you provide Windows-based applications, or the Windows desktop itself to users for remote access or applications, or to administrators for remote administration of servers. In both cases, a unique session is created for each user when they connect to the server and each server can support multiple simultaneous sessions. All processing is performed at the server, and only information from the monitor, keyboard and mouse are generally transmitted between the client and server. The protocol used for communications between the client and server is called Remote Desktop Protocol (RDP) and includes encryption capabilities up to 128-bit. This allows administrators to provide secure access to applications and administration tools over even low-bandwidth connections. Terminal Services is also a required component for other 3rd party server-based computing products such as Citrix MetaFrame and Tarantella.

Terminal Services can be enabled in one of two modes: "Terminal Server" mode (previously application mode in Windows 2000 Server), that allows multiple remote clients to simultaneously access windows applications running on the server, and Remote Desktop for Administration" mode (previously Remote Administration mode in Windows 2000 Server), which is used to remotely manage Windows based servers.

This paper will focus on securing Terminal Services for use in Terminal Server mode for remote access applications and/or the full windows desktop. An additional use of the secured server could also include providing a central access point for connecting to servers in administration mode. The paper will also primarily focus on securing the Remote Desktop Connection client, however, a few comments and references will also be provided for the other clients available.

What's New in Terminal Services 2003

Windows Server 2003 adds a number of important new features to provide improved management of terminal servers. This includes several new client features that provide both additional functionality and new security challenges. Fortunately, improvements have also been made in both managing and configuring security settings, and Microsoft has provided some excellent resources and tools to assist you with your implementation. A description of some of these new features is provided in this section.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Client Features

The Terminal Services clients have gone through several transformations over the last few years, each version providing improvements in functionality, flexibility and security. Microsoft offers four clients for use with Terminal Services 2003, as well as with previous versions of Terminal Server. These are the Remote Desktop Connection (RDC), Remote Desktop Web Connection, Remote Desktop Connection for Mac, and the Windows CE version of RDC. A 3rd party vendor also provides a Linux client. These new clients provide significant improvements in capability through a simplified user interface, and bring them closer in functionality to 3rd party products such as the Citrix ICA client. The most significant change is the resource redirection feature that allows the client to interact with their local resources including local drives and smart cards. Even if you don't switch to the 2003 version of Terminal Server, it is well worth moving to one of these new clients. Microsoft is also reportedly working on RDP version 6, possibly for Windows Server 2003 SP2, which is expected to add features that rival the Citrix ICA client such as seamless application publishing. Tables 1 and 2 outline the features of the RDC and RDWC clients. The table is compiled primarily using the material provided in Microsoft's technical articles "Technical Overview of Terminal Services" and "What's New in Terminal Server".

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Table 1 - Remote Desktop Connection Client Features

New Features/ Improvements	Description	Terminal Server Version Required
Remote Desktop Connection (RDC)	Included in Windows 2003 and Windows XP. Unless otherwise indicated, supports Windows 9x, Windows NT, Windows 2000, Windows ME, Windows XP clients. The client can be used to connect to previous versions of Terminal Services (Windows NT® 4–Terminal Server Edition and Windows 2000). Some of the newer features, such as full color and resource redirection are only supported on Terminal Server 2003. Download the RDC client from http://www.microsoft.com/windowsxp/remotedesktop/.	NT 4 Server TS Edition, Windows 2000 Server, Windows 2003, Windows XP Pro
Simplified Interface	• A new connection bar now appears when connected to the terminal server that sits at the top of a full-screen RDC session. This allows users to easily switch between their terminal server session and their local desktop. The bar at the top also makes it easier for some users to differentiate between their sessions and local desktop as well (which also assists the help desk personnel talking to them on the phone!). • Easier customization of remote connection options. A tabbed property sheet is now available to configure the controls for Display, Local Resources, Programs to run on connection, and other Experience settings. The Experience settings make it easier to optimize performance over lower-bandwidth connections. The client also boasts increased network bandwidth savings over RDP 5.0. • Managing multiple connections is now easier. The old Connection Manager's functionality has been enhanced and integrated directly into the client. Users and administrators can then save and open connection settings files and use them locally or deploy them to other users. Saved passwords are securely encrypted, and can only be decrypted on the computer on which it was saved.[1]	NT 4 Server TS Edition, Windows 2000 Server, Windows 2003, Windows XP Pro
Automatic Reconnects	Dropping of connections has historically been a problem for this type of thin-client computing and is a particular problem for users on poor dialup or unstable wireless connections. To alleviate this annoyance, RDC now automatically attempts to reconnect to a server when a network interruption causes a lost session.[1] In windows 2000, the user had to manually reconnect their session and re-enter their logon credentials if the connection was dropped. This option can be set using the client or group policy. A maximum of 20 connection attempts are made at 5-second intervals. A description of this feature is provided in KB article 323258.	Windows 2003, Windows XP Pro
Full Color	Starting with RDP 5.1, color depth can be selected from 256 colors (8-bit) to True Color (24-bit), and resolution can be set from 640 x 480 up to 1600 x 1200. By default, remote sessions are in full-screen and full color. Running in full color does present some performance issues in terms of resources – high color will use more memory at the server and will also generally use up more bandwidth. The setting can be controlled on the server side by group policy, limiting the color depth a client can connect with.	Windows 2003 or Windows XP Pro required for full color
Client Resource Redirection	A wide variety of data redirection types are supported. Each of these can be disabled by either the client or the server. A security alert is displayed when file system, port, or smart card redirection is requested; the user can cancel the connection or disable the redirection at that time.[1] This addition poses significant benefits, particularly the ability to use smart card redirection for authentication. It also raises new issues of concern due to the ability to redirect local hard drives for use within the terminal server session. The following items provide additional details on this new feature. Unless noted, client resource redirection features are only available to clients connecting to the Windows Server 2003 family or computers running Windows XP Professional.	
File System	"Client drives, including network drives, are mounted inside the server session. This lets users open or save files on their own computers' disk drives, in addition to opening and saving files on the server."[1] As this raises new security issues for both the client and the server, either party can disable it. This can also be controlled by group policy, and should only be enabled when connecting to trusted systems.	Windows 2003 or Windows XP Pro

[1] "Technical Overview of Terminal Services", pg 4-5 URL http://www.microsoft.com/windowserver2003/techinfo/overview/termserv.mspx

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

New Features/ Improvements	Description	Terminal Server Version Required
Ports	Client serial ports can now be mounted to the server. This enables a variety of hardware on the client computer to be accessed by software on the server including COM, LPT and USB ports.[1] Firewire port redirection is not natively supported, however, a registry entry can be added to enable this support. COM and LPT ports can be disabled using group policy.	Windows 2003 or Windows XP Pro
Printers	In Windows 2000 Terminal Services, network printers were not automatically redirected which complicated this part of the service. In 2003, all printers installed on the client are redirected for use, even network printers. The naming convention for the redirected printers has also been improved. For example: "printername on printserver (from clientname) in session 9"; whereas in Windows 2000, they would have seen "_printserver_printername/clientname/Session 9."[2]	Windows 2000 Server, Windows 2003 or XP Pro
Audio	Clients can now receive the sounds that indicate errors and events such "new mail" notification events.[2]	Windows 2003 or Windows XP Pro
Smart Card Sign On	Clients that support smartcards, such as Windows 2000, Windows XP, and Windows CE .NET can now use a smart card that contains Windows logon credentials to logon to the terminal server. This is a critical improvement for those environments that already use this type of 2-factor authentication in their LAN environment or would like to enhance remote access security by providing better access control for remote connections to the terminal server.[2]	Windows 2003 or Windows XP Pro
Windows Keys	"Keys such as **Alt-tab** and **Control-Escape** are sent to the remote session by default. The **Control-Alt-Del** combination is always interpreted at the client computer for security reasons. **Note** These redirections also work when connected to a Windows 2000-based terminal server, but only when using Windows NT-based client operating systems. They do not work with Windows 9x-based operating systems."[2]	Windows 2000 Server, Windows 2003 & XP Pro
Clipboard (+File)	This feature was previously available on Windows 2000 server using the rdpclip hotfix only, and allows you to cut and paste text, graphics, files and folders between the client and server sessions. This feature uses virtual channels for file transfer.	Windows 2003, Windows XP Pro
Time Zone	"A RDC client computer can provide its time zone to the server, or users can manually set their own time zones. This enables an administrator to use one server for multiple users across different time zones. It's also helpful for applications that support features such as calendars." [2]	Windows 2003 or Windows XP Pro
Virtual Channels	Virtual Channels can be used to move data between client and server computers, such as the clipboard + file feature mentioned above. Information about using Virtual Channels is available from MSDN® at http://msdn.microsoft.com/default.asp.[2]	Windows 2000 Server, Windows 2003 & XP Pro

[2] "Technical Overview of Terminal Services", pg 4-6 URL http://www.microsoft.com/windowserver2003/techinfo/overview/termserv.mspx

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Table 2 – Remote Desktop Web Connection

New Features/ Improvements	Description	Terminal Server Version Required
Remote Desktop Web Connection	Remote Desktop Web Connection is an improved safe-for-scripting ActiveX® control/COM object that allows users to connect using their Internet Explorer browser and the ActiveX control that is automatically downloaded from the Terminal Server, rather than the RDC client. It can be used to deploy Web pages built with Web applications that include Win32® components. It also provides the ability to connect to the login screen using SSL prior to initiating a remote session. The latest control can be downloaded from http://www.microsoft.com/windowsxp/pro/downloads/rdwebconn.asp. The latest version, as of this paper, is 5.2 (post XP SP1). Previous versions should be avoided due to a buffer overrun security vulnerability described in MS02-046. Instructions for configuration and embedding the control in a web page are included in the download. Note that pre XP SP1 versions will not work on a system that has been patched with the latest IE security patches.[3]	NT 4 Server TS Edition (IIS v 4+), Windows 2000 Server (all versions), Windows 2003 Server (all versions), Windows XP Pro
Benefits	• The client is a Win32 ActiveX control that runs in Internet Explorer, on any Windows 32-bit operating system. The web pages can either link directly to a hosted application, or run the entire desktop. The client is especially useful for fast access to terminal servers as needed from multiple computers or locations by both users and administrators. In my experience, users on poor dial-up or low speed wireless connections also noted significant performance gains when using the web client vs. the RDC client. • Users do not have to manually download and install the client. Rather than sending an application to remote users, administrators need only supply a URL. If the client is ever updated, users will automatically pick up the new version when they connect to the Web page. Corporations that want to deploy Terminal Services connections to vendors, suppliers, or customers can use Remote Desktop Web Connection to distribute them easily, inexpensively, and efficiently over the Internet. Users who gain access in this manner do not need to reconfigure their computers, and they do not gain access to your internal network.[4] • Ability to be embedded in Web pages or launched in separate pages. Using Internet Explorer, Terminal Services sessions can be embedded in the current Web page, or launched in a separate window. You can create simple scripting code that allows users to launch multiple Terminal Services sessions from the same Web page, or start multiple sessions within a single Web page. As with any ActiveX control or COM object, many applications development systems can insert and set properties on the control. Scripts that communicate between an application running on the desktop and a Terminal Services-hosted application using the control and the RDP virtual channel architecture can be developed.[4]	

Security	• The security of this client, as with any remote access solution, is highly dependent on its implementation, including IIS security as well as firewall/perimeter security. Windows 2003 Server provides improved security and performance for both IIS and SSL that should help with this part of the implementation.
	• RDWC includes the same high-encryption capabilities as the standard client, and is therefore also dependent on the capabilities of the client that is connecting. RDWC uses the well-known RDP TCP port (3389) to communicate. This port was previously hard coded into the control, so you were not able to change this port number. This has been changed in this version using the port property of the "AdvancedSettings2" method embedded in the web page. Other settings such as printer and file redirection are also easily controlled using the AdvancedSettings2 properties within the web page.
	• To allow clients to protect themselves from potentially untrustworthy servers, some properties of the Remote Desktop Web Connection ActiveX component object are restricted to certain Internet Explorer security zones. This means that when a Web user accesses the page from a computer in a less secure zone, these properties are disabled. Some of these restricted properties are[5]:
	  o StartProgram – Specifies a program to start upon connection.
	  o WorkDir – Specifies the working directory for the program specified in StartProgram.
	  o FullScreen – Specifies whether the connection will be displayed as full screen or windowed mode.	

[3] "Technical Overview of Terminal Services", pg 6. URL: http://www.microsoft.com/windowserver2003/techinfo/overview/termserv.mspx

[4] "Microsoft Terminal Services Advanced Client". URL: http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/tsac.asp#heading2

[5] "Providing for RDP Client Security". URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/termserv/termserv/providing_for_rdp_client_security.asp

Server Features

Windows 2003 Terminal Server provides improved Server Management capabilities as well as a different approach for configuration. Windows Server 2003 now separates the remote administration and Terminal Services functionality into separate configurable components, rather than installing terminal server and choosing which mode to use afterwards as in Windows 2000. Remote Desktop for Administration is installed by default in Windows Server 2003. You can choose to enable it through the System control panel's Remote Tab as shown in Figure 1. This makes it much easier to turn on and off remote administration on servers than in previous editions. No licenses are required to use this mode, however, you are limited to 2 remote sessions plus the console. Terminal Services mode (application mode) must be installed through control panel by selecting "Terminal Server" in the Windows Components section of Add/Remove Programs as shown in Figure 2. You much purchase licensing to use this mode.

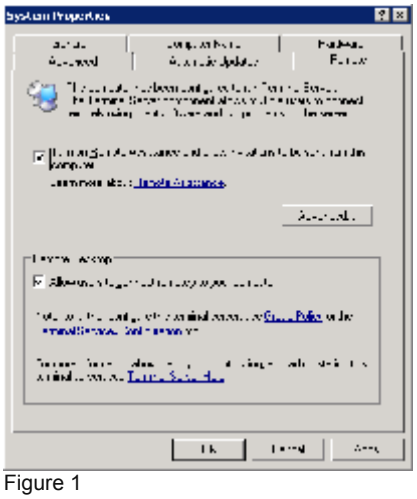


Figure 1

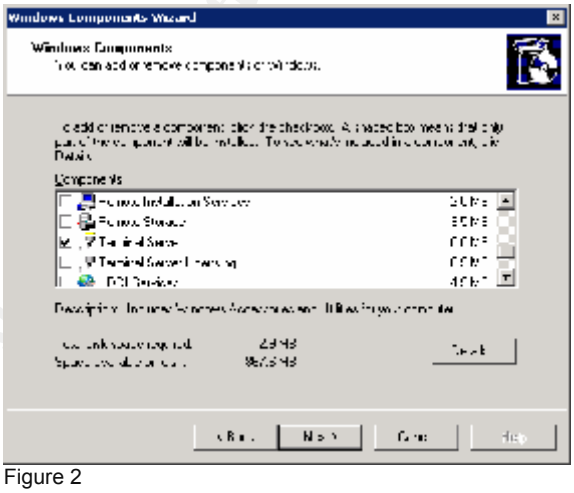


Figure 2

Table 3 outlines some of the new or improved server features in Terminal Server 2003. The content was primarily compiled using the material provided in Microsoft's technical article "Technical Overview of Terminal Services".

Table 3 – Terminal Server 2003 New Features and Improvements

Feature	Description
Server Management	
Configuration Tools	Group Policy can now be used to configure most of the Terminal Services properties. This enables configuration of groups of servers simultaneously.[6] Scripted configuration of Terminal Services is now supported using a full Windows Management Instrumentation (WMI) provider. In addition, several WMI aliases are included to provide a simple front end for frequently used WMI tasks.[6]
Printer driver mapping	"Printer driver mapping has been enhanced to provide better matching in near-miss cases. When a driver match can't be made, the Trusted Driver Path lets you specify other standard printer drivers that you sanction on your terminal servers. The print stream is compressed for better slow-link performance between a server and client."[6]
License Manager	It is now much easier to assign and activate licenses. The license service also no longer has to be installed on a domain controller. A new license type, per user (vs. per device) has also been introduced.

[6] "Technical Overview of Terminal Services", pg 9-10. URL: http://www.microsoft.com/windowserver2003/techinfo/overview/termserv.mspx

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Feature	Description
Diagnose connections	Client Error Messages – More than 40 new client error messages make it easier to diagnose client connection problems.
More users supported	Terminal Server 2003 improves server performance, supporting more users on each server than Windows 2000. Brian Madden suggests a 10-40% increase, Microsoft boasts up to an 80% increase.
Security Enhancements	
Remote Desktop Users Group	The Remote Desktop Users Group is setup by default for controlling access to the terminal server. Adding members to this group allows access. This also allows access to terminal servers to be controlled through Group Policy across groups of servers.[7]
Security Policy Editor	Terminal Services user rights can also be assigned to individual users or groups, using the Security Policy Editor. Using this method allows you to give users the ability to log on to a terminal server without having to be a member of the Remote Desktop Users group described above.[7]
Encryption	By default, connections to terminal servers are secured by 128-bit, bi-directional RC4 encryption, for clients that supports 128-bit. There is also a setting to use the highest encryption the client support, in order to allow older clients that don't support 128-bit to connect. For secure environments, you can also restrict encryption to 128-bit so that only high-encryption clients are allowed to connect.[7] A "FIPS Compliant" encryption level is now also an option. "This level of security encrypts data sent from the client to the server and from the server to the client, with the Federal Information Processing Standard (FIPS) encryption algorithms using Microsoft cryptographic modules. This new level of encryption is designed to provide compliance for organizations that require systems to be compliant with FIPS 140-1 (1994) and FIPS 140-2 (2001) standards for Security Requirements for Cryptographic Modules."[7]
Software Restriction Policies	New software restriction policies enable administrators to use Group Policy to allow only certain programs to be run by specified users. This replaces the AppSec (Application Security) tool used in previous versions of Terminal Services. For example, specific corporate-wide applications can be restricted from running unless they're executed from a particular directory. These policies can also be configured to prevent virus-infected or malicious code from running.[7]
Connection Auditing	Auditing of user connections is still far from perfect, but offers some improvement over Terminal Server 2000. The Terminal services manager still logs the local IP of the connected user rather than the public address used for the connection, as is also the case in Windows 2000. However, the event log now records the public IP address for logons and disconnected sessions, whereas, Windows 2000 only recorded the IP for a session disconnect. This is a marginal improvement, but does improve the ability to trace connections to the actual IP address.
Terminal Server Advertising	In Windows 2000 terminal server, terminal servers in both remote administration mode and application mode advertised themselves on the network. In the 2003 version, by default only the application server, or terminal server mode, is advertised. Servers with remote administration mode enabled will not be advertised. This can easily be changed for either mode using the following registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server REG_DWORD value: TSAdvertise; 0 disables and 1 enables advertising.[7]
Session Directory	Terminal servers can now be organized into farms using Microsoft tools. This allows clusters of load-balanced servers to appear to as one service to their users for fault tolerance and load balancing. The new Session Directory feature in Terminal Services allows users to reconnect to the server where their disconnected session resides, rather than just being directed to the least loaded server when they re-connect. Session Directory can use the Windows Load Balancing Service (must run Enterprise Edition of Windows Server 2003), or a third-party load balancer. As Microsoft's Load Balancing service is based on network load, rather than server based performance parameters such as CPU and memory, an alternate load balancing solution may be a better solution for some environments.[7]

[7] "Support WebCast: Microsoft Windows Server 2003 Terminal Servers: New Features". URL: http://support.microsoft.com/default.aspx?scid=/servicedesks/webcasts/wc121702/wcblurb121702.asp

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Planning a Defense in Depth Strategy

Using a defense in depth strategy for securing your remote access environment, as well as your internal network, will ensure that should a breach occur at the Terminal Server, the attacker or user would have limited success in accessing sensitive information or causing damage or significant outages. It would also ensure that information is available about the attack to assist with investigations. The primary goals for securing any environment are to protect the integrity, confidentiality, and availability of information. These same requirements must also apply to your remote access solution. A risk assessment must be performed to determine what the acceptable level of risk is for the access being provided in your corporate environment. This assessment will help you to determine an appropriate level of defense for your solution. The following sections provide information on specific attack methods for Terminal Servers, network security considerations, and best practices to help with evaluating and planning an appropriate strategy for your environment.

Terminal Server Specific Attacks

Many of the threats for this type of remote access are common to those for any network with public exposure. However, there are also attacks that are specific to Terminal Servers. This section examines some of the tools and methods currently used to attack Terminal Servers and how to protect against them. There are a few inherent weaknesses in the standard implementation of Terminal Server that make it vulnerable to attack.

Enumeration

Identifying active Terminal Server ports is generally the first step in an attack. One method for locating a web based client installation is to use an internet search engine such as google to locate the ActiveX authentication form in the default location TSWeb/default.htm. I also received multiple hits for active web connection logon pages, including some with saved domain name information, by searching for “Remote Desktop Web Connection” which is at the top of the sample web page provided by Microsoft. Changing these default parameters and removing these common text strings from your installation can easily “hide” your connection page from this type of search.

Another common method for finding active Terminal Servers is to do a port scan for TCP port 3389, which is the default port for RDP. Unless other protections are in place, once an open port is located, an attacker need only use their Terminal Server client to connect to the target IP and be prompted for login and password. This port number can now easily be changed to a non-standard port for both the Remote Desktop Connection and Remote Desktop Web Connection. Connecting to the Terminal Server using other methods such as VPN, RAS or SSL will prevent external attacks using this method. This issue is discussed further in the Network Security Considerations section of this paper.

A few tools are available to find active Terminal Servers within your private network as well. TSEnum is one of the pen-testing tools written by Tim Mullen from www.hammerofgod.com and is used to find active Terminal Servers, regardless of

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

the port they are listening on. When a server comes online, it registers itself with the master browser of the network, including the server type which can be retrieved from the NetServerEnum function. TSEnum uses this to return any Terminal Server that the browser has registered. It also allows you to query a remote machine, providing that access to port 139 or 445 is available. No special domain credentials are required, and it works even if Restrict Anonymous has been set to 1 on the target. Restrict Anonymous=2 will defeat this method, however. Providing that you deny access to ports 139 and 445 on your firewall, this method would also have to be performed from inside your network.[8] Terminal Services Manager (tsadmin.exe) is a built in tool that provides a view of sessions, users and processes for each terminal server in trusted domains. The user only requires access to a member of a trusted domain to gain the ability to find all of the systems with remote management enabled.[9]

Password Guessing Attacks

Password guessing is still the primary method for attacking Terminal Servers. Unfortunately, the same tools available on the Internet to help you pen-test your security can also be used by attackers without the skills to develop their own, so it is critical that you take steps to protect against this type of attack. Preventing attackers from gaining even low-level account access is of primary concern, as the interactive rights required for terminal server access increases the ability to launch privilege escalation attacks.[9]

Another tool available from hammerofgod.com is a brute force, dictionary based password-cracking tool called TSGrinder. It takes advantage of the fact that the Administrator account cannot be locked out for local logins, and, therefore, can be brute forced. This is all done through the encrypted channel, which may allow it to be undetected by intrusion detection systems. There are specific technical steps you can take to limit the success of these types of attacks, however, these steps will be useless if the attacker gets the login information through social engineering methods, or is simply a previous user of a shared account that still has the same password. Whatever technical controls you put in place, supplement them with user awareness training on account and password management and policies. Important technical controls include low account lockout thresholds with manual reset, complex passwords changed on a frequent basis, a logon banner, no shared accounts, and renaming the Administrator account (see Best Practices section). Connecting through a VPN or SSH tunnel, limiting access control by IP or other information, or using 2-factor authentication will add further protection against this threat.

Local Privilege Escalation

The default configuration of users in terminal server mode allows a significant range of commands, even with software restriction policies in place. The interactive rights required for terminal server access allows the ability to run privilege escalation attacks that normally couldn't be run by a low-level user account, and gain the attacker Administrator equivalent privileges. These attack tools are freely available for download on the Internet, and other methods use only

[8] "Hammer of God Downloads and stuff". URL: http://www.hammerofgod.com/download.htm

[9] McClure et al, pg 350

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

the tools available in a session. Access control lists and software restriction policies must be carefully designed to protect against this threat. Disabling Active Desktop also prevents a few specific attacks.[10]

Network Security Considerations

There are many scenarios that can be used for deploying a remote access solution using Terminal Server. Which one you choose will depend on your intended client base and the role of the server. A full discovery of these issues at the beginning of the planning stage is critical to developing a secure strategy. A few important questions for the client base include whether the clients are trusted or untrusted, what operating systems and level of encryption they will be using, whether they will use full desktops of just specific applications, will both external and internal users be connecting and what speed and quality of connection they have to connect with. You will also need to evaluate the sensitivity of the data being accessed, what type of work will be done, how many of each user type will be connected (load on server), how much downtime can be tolerated for the service and who is available to support it. You may want to consider providing a load-balanced solution with the new session directory service if there are a significant number of users, and little downtime can be tolerated. Microsoft provides good resources for both capacity planning and load balancing (see reference list).

Using VPNs with Terminal Server

Connecting to your Terminal Server through an encrypted tunnel such as an IPSEC VPN or SSH can provide an additional level of security that some corporations may require. However, network layer VPNs have risks of their own that need to be evaluated. This type of access is generally not limited to only terminal server sessions and the client pc becomes a part of your network with all of the resource access that entails. Connecting an untrusted client to your network may expose it to viruses and Trojans or other undesirable programs. Other considerations are the additional bandwidth required that may decrease performance for users on low bandwidth connections such as dial-up, as well as the additional configuration and installation required to install VPN clients or hardware devices. This option makes it difficult to use your solution to connect from guest or multiple computers, or from computers in remote locations with no local IT support. If your intended clients are already connected via VPN for other purposes, then connecting to the Terminal Server from within the tunnel is the obvious choice.[11]

An alternative to using a network layer VPN is to use the clientless application layer SSL VPN solution which has recently become popular. Many vendors offer this in combination with their IPSEC VPN appliances to allow corporations to choose the appropriate solution for each remote access situation. SSL VPNs greatly reduce the administrative issues related to remote access, as only specific applications are permitted across the SSL VPN, reducing the potential for unauthorized network intrusions. As SSL is integrated in most devices already, it is easy to deploy and tunneling applications through SSL eliminates the need to open additional ports on the firewall. SSL VPNs provide the ability to restrict access

[10] McClure et al, pg 350

[11] Madden, pg 22.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

control on a per-user basis to a strictly specified list of applications, which can include Terminal Services. This allows you to have the extra security of providing Terminal Services within a VPN tunnel, without giving untrusted clients more access to your network than is needed.

It has been reported that Windows Server 2003 SP1, which is expected to be released sometime in 2004, will include added security functionality for both VPNs and Terminal Services. This is expected to include the ability for an RDP client to connect and authenticate to a Terminal Server completely via SSL over port 443, rather than the current method of either using more than one port for SSL and RDP, or using IPSec. The service pack is also expected to provide support for client network isolation so that the server can prevent clients from accessing your corporate network until their security state is verified, as well as a VPN Quarantine feature that will let remote Windows clients safely access network features. These new features may mitigate some of the concerns with using VPNs for untrusted clients as discussed above.

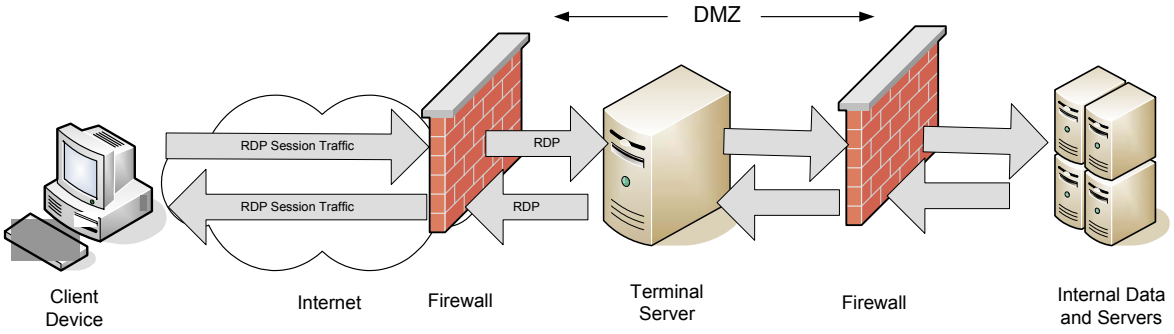
Using Firewalls with Terminal Server

A securely configured firewall is a key component of a defense in depth strategy for remote access. Where you place your Terminal Server in relation to the firewall will depend on the role of your server as discussed above. There are three basic options for placement of your Terminal Server: outside the firewall, inside the firewall and inside the firewall in a DMZ (de-militarized zone).

Placing your server outside the firewall poses significant risks, and should only be used in very limited, specific situations. Because your server is directly exposed to attacks on the internet, this solution must be limited to stand-alone applications for anonymous users that do not require internal access to or from your internal network and do not require high availability. This configuration would not require you to open undesirable ports on your firewall. One benefit of this configuration is that if the server is breached, the attacker would have no access to your internal network and could do limited damage.

Placing the server inside your firewall is a more secure configuration, as only a port for RDP traffic needs to be opened on the firewall. However, if the server is breached, there is still some risk that your internal network could be open to attack. The recommended option for most configurations is to place your Terminal Server in a DMZ to provide maximum protection of your internal network. In this configuration, traffic from the outside is passed through the firewall to the Terminal Server, and the Terminal Server accesses the resources on the internal network. Some firewalls allow this configuration, or it can be created with two firewalls. See the following diagram for an example of a DMZ configuration using two firewalls. DMZs are also commonly used for segregating services that connect to the outside network such as E-Mail gateways and Web Servers.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.



Most firewalls also allow you to do NAT, which allows you to assign a non-public address to your server. In this configuration, the firewall maintains two IP addresses for a server – a public, routable address on the external interface, and an internal, non-routable address on the internal interface. Microsoft's ISA Server uses the term "publishing" to describe its method for providing NAT for internal servers such as Terminal Server and Exchange Server. Using NAT forces all communication to travel through the firewall, allowing servers on the inside to be protected and hidden from the public network. The advantage to using NAT is that as the internal IP addresses of the servers are not valid on the public network, it is technically impossible for an attacker to find a "back door" into the network and also protects against certain TCP/IP based Denial-of-Service attacks. You should also implement filter rules to ensure this traffic can reach only the terminal servers.[12]

Network separation

Network separation is the separation of RDP traffic from other network traffic protocols. Microsoft recommends splitting network traffic between two network adapters; one used for Terminal Server, and the other for access to other network resources, applications and infrastructure; placed on different subnets. By allowing RDP traffic only over the Terminal Services adapter, you can reduce network adapter bottlenecks; have more consistent traffic analysis and better security and auditing. IP packet filtering can be used to restrict traffic. You can specify the network adapter on which you want to place the RDP traffic on the Network Adapter tab of the TSCC. You should also configure your home directories and other user data storage in such a way that your users can easily access their data regardless of which server they connect to. Also consider placing your terminal server farm and your clients on the same network backbone with your user profile servers and at least one domain controller for best client performance.[13]

RDP Port Considerations

Unless you are using a VPN or other tunnel to connect, in order to allow RDP traffic to reach your terminal server inside your firewall, you have to open a port to allow it through. The standard port for RDP traffic is 3389. This can now be easily changed, but must be done for both the client and the server. There are differing

---

[12] Madden, pg 39.

[13] "Load Balancing Terminal Servers". URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_nfow.asp

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

opinions on whether this port should be changed. Microsoft suggests that it should be left at the default, as "changing the RDP port, for example to a well known and already open port such as 80, makes separation, identification, and audit of RDP traffic much more difficult".[14] Hacking Exposed, however, suggests that it is too easy to enumerate a terminal server service if you use the default port. "Changing the port number has the potential to eliminate 80-90% of attacks."[15] To avoid enumeration on port 3389 and separate the traffic from known ports, you can set the port to a custom port that may not be included in routine port-scans. For more information about changing the RDP port, see article 187623, "How to Change Terminal Server's Listening Port" and for the RDWC as discussed in the new client features section above.

Another option is to use the WTS gateway product developed by Terminal Soft (www.terminalsoft.net). This product allows you to provide a single gateway for connecting to your terminal server farm using a port of your choosing, for example, a common port that is already open such as 443 (similar to Citrix Secure Gateway). You can create a Terminal Server farm by identifying your internal Terminal Servers by IP address and RDP port number used on each server. The gateway accepts the connection based on your criteria and redirects the request to an appropriate server in the farm. A load balancing option is also included that will choose the server for the connection based on CPU and memory usage, and will also direct reconnecting clients to the server that contains their disconnected session. This tool would be used in place of the Windows load balancing and session directory option. Some connection logging is also built in to the tool, however, the IP logging is of limited use since it logs the internal IP of the client rather than the public IP when NAT is used by the client.

Authentication and Access control

Improving the standard password only authentication method is a critical factor in securing your remote access solution. Your firewall may be able to provide additional access control using user-based authentication or IP restrictions. You may also want to consider using IPSEC at the server to provide additional security. IPSEC is built into windows and can be configured to reject any unauthorized attempts to connect to terminal services. The following paper discusses this option in greater detail: "Terminal Services, Part 4", http://www.winnetmag.com/articles/Print.cfm?ArticleID=20288. Providing 2-factor authentication using smart cards is a new feature of Terminal Server 2003 and can improve access control for remote access significantly. To use smart cards with Windows Server 2003 Terminal Server, you must have Active Directory deployed and your clients must be running a Microsoft operating system with built-in smart card support, such as Windows XP or Windows 2000, or most devices running Microsoft Windows CE .NET. You must also install smart card readers on the client computers.

You can also control which versions of the client can access your terminal server using the tool TSVer that is available from Microsoft. This allows you to ensure secure patched clients are used to connect, as well as limiting who can connect.

---

[14] "Planning Network Security Components". Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_deco.asp

[15] McClure et al, pg 343.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Creating your own custom client build is also possible and allows you to limit access to only those with your client installed. TSVer also logs failed logon attempts and you can send a customized message to rejected clients. Unfortunately, this tool logs the internal client IP address rather than the public address for remote users using NAT. TSVer functionality is integrated into a third party utility designed to filter based on a combination of rules such as client name, IP address, MAC address (same subnet only), allowing you to use a single tool for managing these access control settings. See SecureRDP from TerminalSoft at http://www.terminalsoft.net/ for further details.

Logging and Auditing

In event of a security breach, it is important that you be able to track logons. Some logging and auditing is available with terminal server, however it is limited and sometimes not reliable. The client IP address recorded in the Terminal Server Manager tool is not the public IP address that the connection is made from, but the IP address of the client machine, which is generally a non-public IP address due to the high use of NAT software and devices. The event log in Windows 2003 does log more events than the 2000 version, and now logs both logon and disconnect events with the correct public IP address. You may want to use a 3rd party utility for logging if it is critical for your implementation. You may also be able to do additional logging at your firewall. Either way, these logs must be reviewed on a regular basis for them to be of any value, and preferably moved to another server so that they cannot be tampered with. One 3rd party utility recommended by Brian Madden is ONEAPP at www.oneapp.co.uk; another is using the windump utility.

Policies, Awareness training, Procedures

Remote access privileges come with additional responsibilities for protecting your corporation's information assets. Remote Access Users must be made aware of their security responsibilities and be given guidance on how this should be accomplished. This is particularly important for remote field offices and home offices that may not have the same level of IT support available as the corporate head office. Written policies, procedures and guidelines on security topics such as acceptable use of systems, Internet and email, accompanied with awareness training, must be part of your strategy for securing remote access. Remote access agreements with system requirements, secure practices when working in a non-corporate environment such as home or when traveling, and personal firewall and virus software requirements should be part of the approval process and include a user sign off that is reviewed and re-approved on a scheduled basis. You may also want to consider a more frequent audit schedule for checking complexity of passwords for your remote access users. The use of shared accounts for remote access should be allowed only if absolutely necessary, due to the difficulty of ensuring the security of the account as well as user accountability issues.

Best Practices Recommendations

- **Secure Installation** – Install terminal server mode on a hardened and fully patched operating system, and check for patches again when the installation is complete. Because of the multi-user nature of Terminal Services, it is strongly recommended that you use the Windows Server 2003 version of NTFS to secure the OS. Microsoft has a good Security Guide to use as reference for hardening your operating system. The National Security Agency is generally also a good resource for publishing security guides, but in this case, they simply refer you to the "High" security settings in

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Microsoft's Windows Server 2003 Security Guide. This guide can be downloaded from the following URL. http://go.microsoft.com/fwlink/?LinkId=14846. Hacking Exposed Windows Server 2003 is also an excellent resource for securing the OS.

- **Patch management** – Apply security patches as soon as practicable. It is important to test patches on a test server first, however, as previous patches have caused losses of connection and problems with applications. One example is the Internet explorer client update that caused the RDP web client to stop functioning until upgraded with the new version. This was not well known when the patch was released, so took some time for a lot of administrators to determine the cause.
- **Limit what users can do, access and run using system, group and software restriction policies** - Restrict user sessions on the Terminal Server to only the applications and desktop functionality deemed necessary. If users only need one application, have it start automatically rather than providing the entire desktop. If you have an active directory domain structure, use group policy as much as possible for ease of configuration.
- **Disable unneeded services** – Best practice for any server includes disabling any services that are either not needed, or inappropriate for the server role. The "Runas" service (allows users to run programs with different user rights), in particular, should be disabled. According to Brian Madden the concern is that "with this service, a user could connect to an anonymous application and then launch additional processes with his native user account, bypassing the anonymous user security that you configured on the server."[15]
- **Rename the original Administrator account** – The administrative account does not lock out when interactive users enter incorrect login information, making this account vulnerable to password cracking attacks. Rename the original account and remove the description for it. Create a dummy Administrator account with the original description, disable the account and set a difficult random password, don't allow password changes, place the account in the Guests group, and remove from all other groups.
- **Create a Logon banner** that states the typical Authorized Use Only text that is displayed before a user logs on. This not only gives you the legal ability to charge attackers if they enter your network without authorization, but can make password guessing more difficult by requiring the button to be clicked to continue. Do not display the last logged on user, and set the number of cached logons to 0.
- **Don't install terminal services on a domain controller** – Users must be granted rights to log on locally to the terminal server. Because domain controllers cannot be managed separately from one another, these users would then have this right on all domain controllers, which should only be allowed by administrators. Domain controllers must also be located in the domain controllers OU, making it difficult for you to use group policy configuration.
- **Virus control -** If users will be using email and browsing the Internet, implement policies to limit the risk of user's downloading or running viruses or Trojans. Block unsafe attachments, chat rooms, instant messaging software and set safe security zones for Internet explorer. Ensure your virus software is updated at least daily.
- **Microsoft Office Security** - If users will be using Microsoft Office software on the Terminal Server, implement restrictive policies for macros, visual basic and activeX security.
- **Other Policies -** Set a policy based screen saver to protect unattended sessions at the client to 15 minutes or less. Ensure you have a good remote access policy that users have to sign to gain access, and that it includes standards for virus software and firewalls. Awareness training is also important including topics on creating secure passwords, virus management, and safe computing practices. It is critical to set a low account lockout policy, complex passwords, and forced password changes to protect from password guessing attacks.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Terminal Server Configuration

Once terminal server mode has been installed, there are several areas of configuration that will have to be planned, completed and tested prior to rollout, including which configuration tool(s) to use. These areas include:

- User Group Policy Settings
- User Rights and Logon
- Server Settings
- Terminal Server Connection Settings
- Software Restriction Policies
- Other utilities such as TSVer to limit RDP client version

Choosing a Terminal Server Configuration Tool

Your choice of configuration tool(s) will depend on your connection requirements, your server environment, your administration rights and level at which you want to apply settings. If you run only Windows Server 2003 in your environment, Terminal Server Group policy can be used to configure all settings that apply across an OU, or you can use local Group Policies to configure individual servers. If your environment includes other versions of windows, you may need to use a combination of tools for configuration. Table 4, summarized from Microsoft's on-line guide "Choosing a Terminal Server Configuration Tool", provides a comparison of the tools available.[16]

Table 4 Benefit and Restriction Comparison for Configuration Tools

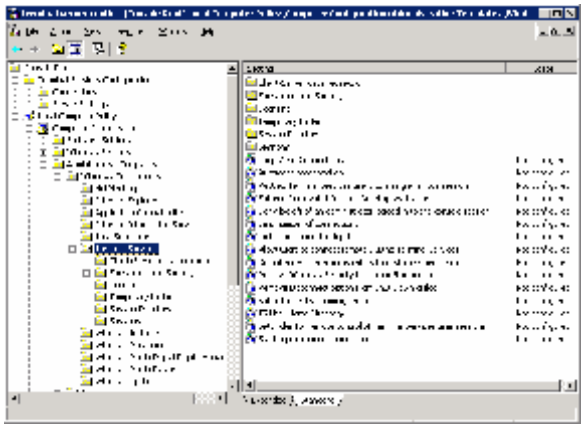
Tool	Benefits	Restrictions
Group Policy	• Can centrally configure terminal servers and Terminal Server users by applying policies to OUs. Includes connections, user policies, clusters, and sessions. • Apply GP settings for users of a computer through Remote Desktop Users group, for individual computers through local Group Policy, or groups of computers through an OU. • Always overrides configurations set by using other tools.	• Administrator must be a domain administrator to apply Group Policy settings to OUs and must have Active Directory in place. • To set local policies for users of a particular server, must be local administrator of the server. • Cannot use if you need different connection configurations on the same server. • Can only be used to configure settings for Windows 2003 terminal servers.
WMI Terminal Server provider	Can configure many terminal servers or Terminal Server users using scripts.	Administrator must know how to write scripts and must be local administrator on each server.
Terminal Server Connection Configuration snap-in	• Can configure unique per-server and per-connection settings. • Some configurations only available in TSCC snap-in.	• Can be overwritten by Group Policy settings. • Can be applied only to a single terminal server and its users. • Cannot be used to configure a remote server.

[16] "Choosing a Terminal Server Configuration Tool". URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_soru.asp

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Configuring Terminal Services with Group Policy

The following section outlines some considerations for planning for use of Group Policies to configure your Terminal Services environment. It also reviews the settings available and some recommendations for settings related to security. Although specific information is supplied for configuring using group policy, the Terminal Server specific settings can also be set using the Terminal Services Configuration Console as discussed above.



Planning Considerations for Group Policy

The most important consideration when planning for group policy configuration is to test all new policies in a test environment. The policies available can restrict functionality of all accounts, including the administration account in certain configurations, so testing is critical prior to implementing in production. You also want to ensure that your policies will not affect other servers in your domain and be able to apply user-based restrictions that are specific to terminal server logon or to all users. Microsoft suggests two methods for accomplishing these goals. In both cases, you will need to create both a new organizational unit (OU) and a GPO for locking down the OU based on your security requirements.

- **Terminal Server specific OU with loopback processing** – Place your Terminal Server object(s) in the new OU. The OU should not contain users or other servers. To apply user-based policies to users only when they logon to the server objects in the locked down OU, enable loopback processing. Without loopback enabled, the user's Group Policy objects would determine which user policies apply, rather than the Terminal Server specific policies set in the locked down OU. This allows you to apply stricter policies to users when logging in remotely without having to setup multiple accounts. This will apply the policies to administrators as well, preventing many local changes from being applied to the Terminal Server while it is in production. If full administrative access is required, the server will have to be removed from the locked down OU temporarily while the maintenance is performed, then returned to the locked down OU.[17]
- **User accounts are placed into the locked down OU** – Create user accounts for use specifically when logging on to the Terminal Server and place them in the Terminal Server OU. Allow user logons to the Terminal Server for only these users. Disable loopback processing and place the Terminal Server object into the OU. With the exception of computer-based policies, users can have different levels of restrictions on the same Terminal Server. This allows Administrators to perform some operations while users are active on the server.[17]

[17] "Locking Down Windows Server 2003 Terminal Server Sessions". URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/lockdown.mspx

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Enabling Group Policy

Group Policy can be enabled for users of a server, individual servers, or groups of servers in a specific OU of a domain. If you are using Group Policy to configure an individual server, you can configure policy settings for the server or users of the server using the Group Policy Object Editor snap-in to edit the local Group Policy. See the explain text for each policy to review the Enabled, Disabled, and Not Configured behavior in the Group Policy Object Editor snap-in. Group Policy settings that are set to Not Configured will be obtained from the Terminal Services Configuration tool settings and/or the individual user connection settings. To configure Terminal Services policies for an OU in a domain, you use the Active Directory Users and Computers console on a domain controller. Select Group Policy on the Extensions tab in the Add/Remove Snap-in dialog box. Then select the Administrative Templates (Users) extension for Group Policy.[18]

Configuring Group Policy Settings

Deciding what policies are appropriate to use in your environment can be a daunting task. As previously stated, a thorough risk assessment will help you determine which policies will help you meet your security goals. There are many good resources to help you understand the implications of each policy setting as well as providing guidance on recommended settings for a secure environment. One excellent resources to help you organize and document your Terminal Server Group Policy configuration decisions is an excel worksheet which is available for download from Microsoft, ("Group Policy Configuration Worksheet" (SDCTS_2.xls)), from http://www.microsoft.com/downloads/details.aspx?FamilyID=edabb894-4290-406c-87d1-607a58fc81f0&DisplayLang=en. Group Policy settings for consideration will fall into 5 areas: User Group Policy, User Rights and Logon, Server Settings, Client Connection Settings, and Software Restriction policies.

User Group Policy Settings

These settings are not specific to Terminal Server, and may already be in use in your domain environment. If your Terminal Server will be part of your domain structure, confirm what domain policies are already in place before planning for these settings in the locked-down Terminal Server OU, as these policies may be required by corporate policy and will already have been tested in your environment. Review the levels set for these policies and determine whether they need to be restricted further. Following are a few specific settings that are particularly important to consider for Terminal Server security.

- **Screen Savers -** In a remote access environment, it is particularly difficult to ensure that users are following security policies related to their network logon. Enabling the screen saver policy with a short timeout period is an easy way to ensure that unattended sessions are protected from unauthorized users and require authentication to continue. A 5 minute setting is recommended for a high security environment. You should also use a low-resource screen saver such as the blank screen or starfield to minimize performance impact on the server.
- **Restricting Terminal Server Drive Access** - Use of this policy is highly recommended, not only as a security measure, but also to reduce confusion for users that use full desktop mode. You can hide and restrict access to local drives on the terminal server. By enabling these settings, you can minimize the confusion that some users have with the difference between their local desktop and their terminal server session desktop, ensuring that they do not accidentally store files in the wrong

[18] "Configuring Terminal Services with Group Policy". URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/ts_gp_topnode.asp

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

location, inadvertently access data stored on other drives, or delete or damage program or other critical system files on the C drive.

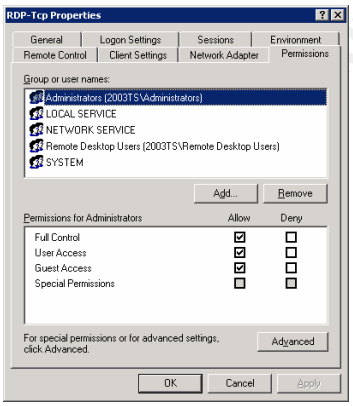
- **Browsing the Network or Server** – There are several policies and settings that help to prevent users from browsing the network or server for configuration information, shares and mapping network drives. These are important settings for a server used for remote access in order to restrict what users (or attackers) can view and access. These policies include removing the "My Network Places" icons, removing the ability to map drives from windows explorer, and restricting access to Control Panel.

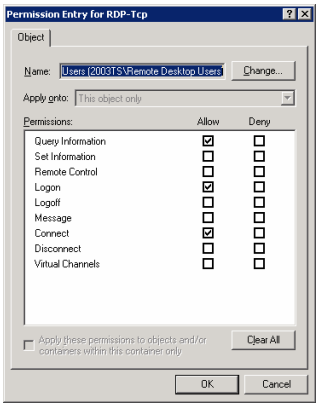
Additional detail on these and other policies is provided in table format in Appendix A. This table is a compilation of selected policies that should be considered for most environments where security is of primary concern.

Terminal Server User Rights and Logon

Introduced in Windows Terminal Server 2003, the Remote Desktop Users group can be used to manage user rights and permissions. Special Internet Explorer security configurations are also available for use on the Terminal Server.

- **The Remote Desktop Users Group** - Administrators, by default, are allowed to remotely connect to the Terminal Server; however, users must be assigned specific permissions to connect. One way to easily manage this right is to add users to the built-in local group "Remote Desktop Users", which is empty by default and has remote logon permissions assigned. This group gives administrators control over the resources that Terminal Server users can access. The default permissions can be adjusted for extra security using the permissions tab of the TSSC tool. The default permissions for the Remote Desktop Users group are shown in the two figures below. (The Permissions Entry window is found by selecting the advanced button from the main permissions window, the selecting the user you want to view or edit, and clicking on the edit button.) Administrators have "Allow" access for all permissions by default. These settings can be adjusted to suit your needs, however, some settings will affect the ability to use certain features such as client resource redirection (virtual channels required). If you want to control specifically who has rights to add members to the Remote Desktop Users group, you may want to consider adding it to Restricted Groups and assign this administrative role to specific user accounts. Appendix B contains a table from NSA's "Guide to Security Microsoft Windows 2000 Terminal Services" that describes each available permission as well as their recommendations for settings.[19]





- **Internet Explorer Enhanced Security Configuration** - The Internet Explorer Enhanced Security Configuration is enabled by default when you install Windows Server 2003. This configuration is intended to protect your server from browser based attacks. This configuration restricts certain scripts and code from running, therefore, some Web sites might not display or perform as designed. As users normally have lower privileges on the server, they present a lower level of risk to your server if exposed to this type of attack. If Internet browsing is one of the applications your are providing on your Terminal Server, you can remove the enhanced security configuration from

[19] "Planning Terminal Server User Rights and Logon". URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_ubgc.asp

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

members of the Users group, to provide a better experience for them while using the Internet. Administrators and Power User accounts should continue to use the restricted configuration.[20]

Server Setting Configurations

There are several server settings available for configuration. Use the "Group Policy Configuration Worksheet" mentioned above to document these settings. These include Terminal Specific settings such as whether to delete temporary folders on exit, licensing options, limiting users to a single session, permission compatibility and locations of home directory and roaming profiles. Of particular importance in this area is the TSCC setting for Permission Compatibility. This setting is set to **Full Security** by default, which is the recommended configuration. This setting restricts users from accessing critical system resources such as the registry. Some legacy applications may require this access, however, which is why the **Relaxed Security** setting is available. It is critical that this setting only be used if your testing proves that it is absolutely required for the application you are providing.

There are also additional computer policies that are non-specific to Terminal Servers that can improve your overall server security, some of which were discussed in the Best Practices section. This includes renaming the administrator account, logon banners, and local account caching settings. As for the User Group Policies, I have compiled a table of policies that should be considered in a secure environment with descriptions and recommendations for each setting in Appendix C.

Terminal Server Connection Configurations

This area includes settings to control the requirements for connections such as the data encryption level, logon requirements, session limits, setting an application to start on connection, and restricting the use of the remote control feature. Again, the Group Policy Configuration Worksheet is a valuable tool for recording your policy decisions. Several of these policies decisions are critical to the security of your remote access, so must be considered carefully. A brief discussion on a few of the important settings follows. As for the User Group Policies, I have compiled a table of policies that should be considered in a secure environment with descriptions and recommendations for each setting in Appendix D.

- **Data Encryption** – The encryption level used for remote RPC connections is a critical component in protecting your sessions. For secure communications using RDP only (not within VPN or other encrypted tunnel), use the highest encryption settings available which is FIPS or 128-bit. This may prevent older legacy clients from using your service, however, reducing the encryption level should only be considered if your risk assessment indicates this is an acceptable risk. FIPS encryption is recommended if smart cards are used for authentication.
- **Logon Settings** - This setting ensures that clients cannot save their password in their connection and logon to the server without entering the password. This prevents unauthorized users who gain physical access to a client's computer from accessing the server without knowing the password.

[20] "Internet Explorer Enhanced Security Configuration". URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/iesechelp.asp

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- **Remote Control** – Remote control gives users the ability to view or interact with another user's session. In highly secure environments, this feature should be disabled. For most environments, however, this can be an excellent tool for remote user support and training. If you do allow remote control, set it require the user's permission, and train the user to only allow this access if they have verified through other means who is requesting the permission and for what purpose.

Client Settings

You can use the settings discussed in this section to control the use of the resource redirection features of the client as well as color depth. Again, the Group Policy Configuration Worksheet is a valuable tool for recording your policy decisions. The role of your server and type of clients connecting will drive the policy decisions in this area. One of the more important considerations is whether to allow clients access to their own drives from within their session, allowing them to easily copy information from the server or network and access files or programs from their local drives within their session. Unless this is an important aspect of your user experience, it is not recommended to allow this redirection. The setting for using smart cards is also covered in this section. As for the User Group Policies, I have compiled a table of policies that should be considered in a secure environment with descriptions and recommendations for each setting in Appendix E. The sources for the information are as listed above in User Group Policies.

Software Restriction Policies

Software restriction policies replace the AppSec tool used to restrict applications in previous versions of Terminal Server. These policies are not specific to Terminal Servers, and can be applied to a server, OU, site or domain, but are particularly useful for locking down servers running in Terminal Server mode. These policies enable you to define what software can run on the server and by whom, allowing you to regulate the use of unknown or untrusted software as well as administrative tools and other restricted programs. This can help protect your organization against viruses, Trojans and hacker tools.

Software restriction policies are located in the Group Policy Object Editor under Windows Settings/Security Settings. Windows Installer operates with applications permitted by these Software Restriction Policies.

Microsoft recommends the following Best Practices for Using Software Restriction Policies.[21]

- Create a separate Group Policy object for software restriction policies – This allows you to easily disable software restriction policies in an emergency without disabling the rest of your policy.
- "Use caution when defining a default setting of Disallowed. When you define a default setting of Disallowed, all software is disallowed except for software that has been explicitly allowed. Any file that you want to open has to have a software restriction policies rule that allows it to open. To protect administrators from locking themselves out of the system, when the default security level is set to Disallowed, four registry path rules are automatically created. You can delete or modify these registry path rules; however, this is not recommended."[21]
- "For best security, use access control lists in conjunction with software restriction policies. Users might try to circumvent software restriction policies by renaming or moving disallowed files or by overwriting unrestricted files. As a result, it is recommended that you use access control lists (ACLs)."[21] This can be done using NTFS, but this doesn't restrict them from running applications

[21] "Best Practices for Using Software Restriction Policies". URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/safer_topnode.asp

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

from elsewhere on the system if they have access, and has to be set on each server manually, however, the main benefit of this method according to Brian Madden is that "NTFS permissions that prevent users from accessing certain files or applications are absolute—there is no way for a user to get around them. Very granular control of who can and cannot access applications".[22]

Summary

Windows Server 2003 Terminal Server has improved security and functionality of its clients and server management tools, making it a feature rich, inexpensive alternative for providing remote access to applications or the full windows desktop. This paper reviewed the primary security issues to consider when planning a secure remote access environment using the principles of Defense in Depth. One important step in the planning process is to perform a thorough risk assessment of your proposed service so that you can plan an appropriate level of defense. To aid in this assessment, review the Terminal Server specific attack summary provided such as password guessing. Other considerations include planning a secure network perimeter with the appropriate use of Firewall, VPNs and encryption. A review of the configuration tools available for configuring your servers was provided, with Group Policy being the method of choice for most environments. The Group Policy recommendations and best practices provided should be a good start for planning a secure remote access solution using Terminal Services 2003.

[22] Madden, pg 6, 11.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Appendix A - User Group Policies

This table is a compilation of selected policies that should be considered for most environments where security is of primary concern. The comments and recommendations are based primarily on information from Microsoft Corporation's articles "Configuring User Group Policy Settings" at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_lgvk.asp and "Locking Down Windows Server 2003 Terminal Server Sessions" at http://www.microsoft.com/windowsserver2003/techinfo/overview/lockdown.mspx and cross-referenced for comparison against NSA's "Guide to Securing Windows 2000 Terminal Server" and Hacking Exposed Windows Server 2003. The settings description information has been quoted directly from these Microsoft sources, occasionally supplemented with information directly from "Windows Server 2003 Help".

User Group Policies	Comments	Settings
User Display	A graphic-intensive display can affect performance for users of Terminal Server.	User Configuration/Administrative Templates/Control Panel/Display
Desktop Items	User Configuration/Administrative Templates/Control Panel/Display Screen savers can be used as an important security tool to protect unattended sessions. If you do not already have a domain level policy for locking desktops using password protected screen savers, setting this policy using a low-CPU screen saver and a time-out of 10-15 minutes is highly recommended.	**Recommended settings:** Enable screen savers using a low-cpu screen saver and a 5 timeout. • **Screen savers** - Disable screen savers by disabling the **Screen Saver** policy. Specify a screen saver by enabling and specifying the screen saver executable name in the **Screen Saver executable name** policy. • **Wallpaper** - Enable the **Prevent changing wallpaper** setting to disable all the options in the Desktop tab of Display in Control Panel. This includes changing the wallpaper and changing the appearance of the desktop icons.
Desktop Theme	User Configuration/Administrative Templates/Control Panel/Display/Desktop Themes Desktop themes, which provide a unified look for your desktop such as windows, icons, fonts, colors, background, sounds and screen savers, can be a useful tool if you are hosting the full desktop with Terminal Server. You can choose a common environment using settings with the least performance impact for all of your users. By default the desktop environment resembles a Windows Classic desktop.	Themes are not enabled by default. To use themes, start the Themes service and configure it to start automatically. Enforce a specific desktop theme as follows: • Open the "Load a specific visual style file" or "force Windows Classic setting". To force Windows Classic, enable this setting. • To load the Windows XP theme, enable the setting and type %windir%\resources\Themes\Luna\Luna.msstyles in the Path to Visual Style dialog box. To load another theme or a custom theme, type the path to that theme in the dialog box.
Desktop	User Configuration/Administrative Templates/Desktop Although this policy is somewhat cosmetic, enabling it is recommended to remove easy desktop access to network browsing tools.	**Recommended settings:** Enabled • **Hide My Network Places icon on desktop** - This setting only affects the desktop icon. It does not prevent users from connecting to the network or browsing for shared computers on the network with other methods.
Restricting Terminal Server Drive Access	User Configuration/Administrative Templates/Windows Components/Windows Explorer You can hide and restrict access to local drives on the terminal server. This ensures users do not accidentally store files in the wrong location, inadvertently access data stored on other drives, or delete or damage program or other critical system files on the C drive.	**Recommended settings:** Enabled • **Hide these specified drives in My Computer.** You can remove the icons for specified drives from a user's My Computer folder by enabling this setting and using the drop-down list to select the drives you would like to hide. However, this setting does not restrict access to these drives. • **Prevent access to drives from My Computer.** Enable this setting to prevent users from accessing the chosen combination of drives. Use this setting to lock down the terminal server for users accessing it for their primary desktop.
Windows Explorer Settings	User Configuration/Administrative Templates/Windows Components/Windows Explorer These settings limit users from easily browsing the domain, viewing security settings and running applications using windows explorer tools.	**Recommended settings:** Enabled • **Remove Map Network Drive and Disconnect Network Drive** - Prevents users from connecting and disconnect to shares with Windows Explorer. It does not prevent mapping and disconnecting drives from other applications or the run command. If mapped drives are necessary, they can be mapped from a logon script.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

User Group Policies	Comments	Settings
		• **Remove Security Tab** - Removes the Security tab from Windows Explorer object properties. Enable this policy to prevent users from changing the security settings or viewing a list of all users who have access to the object. • **No "Computers Near Me" in My Network Places** - Removes computers in the user's domain from lists of network resources in Windows Explorer and My Network Places. It does not prevent users from connecting to other computers by other methods, such as the command prompt or the Map Network Drive dialog box. It is recommended that you enable this policy to remove easy access to browsing the domain. • **No "Entire Network" in My Network Places** - Removes all computers outside of the user's local domain from lists of network resources in Windows Explorer and My Network Places. It does not prevent users from connecting to other computers by other methods, such as command prompt or the Map Network Drive dialog box. • **Turn off Windows+X hotkeys** - Keyboards with a Windows logo key provide users with shortcuts to common shell features. For example, pressing the keyboard sequence Windows+R opens the **Run** dialog box; pressing the Windows+E starts Windows Explorer.
Start Menu & Taskbar Items	User Configuration/Administrative Templates/Start Menu and Taskbar These allow you to remove and restrict access to items from the Start menu for Terminal Server users. Removing Run from the start menu is critical to your server security, as it can prevent users from running undesirable applications. Although there are other ways to run unauthorized, enabling this setting makes it more difficult for the average user. User Configuration/Windows Settings/Folder Redirection If you want to provide a custom start menu for all users, you can use the folder redirection policy to share a Start Menu for all users. Create a Programs\Startup folder under a shared startup folder such as c:\userdata\start\programs\startup. Change the share permissions for the "everyone" group to "read" and place links to applications in the folder.	**Recommended settings:** Enabled • **Remove Run menu from Start Menu** - Removes this menu from the Start menu. It also removes the New Task command from Task Manager and blocks the user from accessing Universal Naming Convention (UNC) (i.e. *\\servername\sharename\directory\filename*) paths, local drives, and local folders from the Internet Explorer address bar. • **Remove and Prevent access to the Shut Down command** - Prevents administrators from accidentally shutting down the terminal server. • **Remove links and access to Windows Update** - Prevents users from attempting to download updates to Windows on to the server. • **Remove Network Connections from Start Menu** - Prevents the Network Connections folder from opening. The policy also removes Network Connections from Settings on Start Menu. Network Connections still appears in Control Panel and in Windows Explorer, but if users try to start it, a message appears explaining that a setting prevents the action. It is recommended that you enable this policy to prevent users from creating new connections such as VPN or Dial-up. • **Remove My Network Place icon from Start Menu** - Removes the My Network Places icon from the **Start** menu. It is recommended that you enable this policy to prevent easy access to browsing the network.
Control Panel	User Configuration\Administrative Templates\Control Panel User Configuration\Administrative Templates\Control Panel\Add or Remove Programs User Configuration\Administrative Templates\Control Panel\Printers Enabling these settings helps prevent users from viewing configuration information about the Terminal Server, browsing the network or searching active directory for printers.	**Recommended settings:** Enabled • **Prohibit access to the Control Panel** - Removes access to Control Panel and disables all Control Panel programs. It also prevents Control.exe, the program file for Control Panel, from starting. • **Remove Add or Remove Programs** - Removes Add or Remove Programs from Control Panel and removes the Add or Remove Programs item from menus. If access to Control Panel is prohibited, this policy can be used to remove the links to Add or Remove Programs from places like My Computer. The link then displays an access denied message if clicked. This setting does not prevent users from using other tools and methods to install or uninstall programs. • **Prevent addition of printers** - Prevents users from using

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

User Group Policies	Comments	Settings
		familiar methods to add local and network printers. This policy does not prevent the auto-creation of Terminal Server redirected printers, nor does it prevent users from running other programs to add printers.
Command Prompt & Registry Editor	User Configuration\Administrative Templates\System Enabling these policies can prevent users from trying to use the command prompt to search for files or run applications instead of Windows Explorer as the shell or accessing the registry.	**Recommended settings:** Enabled • **Prevent access to the command prompt** - Set "Disable the command prompt script processing also" to **No** to prevent users from running the interactive command prompt Cmd.exe. From the command prompt users can start applications. This setting also determines whether batch files (.cmd and .bat) can run on the computer. Do not prevent the computer from running batch files on a Terminal Server. This policy does not prevent access to Command.com (16-bit command interpreter). To disable the Command.com, you can restrict access with NTFS permission, or disable all 16-bit applications with the "Prevent access to 16-bit application" policy. • **Prevent access to registry editing tools** - Restricts users from changing registry settings by disabling Regedit.exe. It is recommended that you enable this policy to prevent users from changing their shell to the command prompt or bypassing several other policies. This policy does not prevent other applications for editing the registry.
16-bit applications	User Configuration\Administrative Templates\Windows Components\Application Compatibility The MS-DOS subsystem by default runs for all users. MS-DOS applications generally do not perform well on Terminal Servers and can cause high CPU utilization, therefore, this policy should be enabled. Enabling this policy also prevents the 16-bit command interpreter, Command.com, from executing. This policy can be configured in both Computer Configuration (system-wide) and User Configuration (user specific).	**Recommended Settings**: Enabled • **Prevent access to 16-bit applications** – Prevents the MS-DOS subsystem (ntvdm.exe) from running for the user. This setting affects the starting of all 16-bit applications in the operating system.
Windows Update	User Configuration\Administrative Templates\Windows Components\Application Compatibility Use this policy to prevent system updates to the Terminal Server while it is in production. This will help to ensure that updates are planned and tested properly before updating the server.	**Recommended Settings**: Enabled • **Remove access to use all Windows Update features** – Removes access to windows update and removes all features. Includes blocking access to the windows update web site from the Windows Update hyperlink on the **Start** menu, and also on the **Tools** menu in Internet Explorer. Windows automatic updating is also disabled; you are neither notified about critical updates nor do you receive critical updates from Windows Update. This setting also prevents Device Manager from automatically installing driver updates from the Windows Update Web site.
Task Scheduler	[User Configuration\Administrative Templates\Windows Components\Task Scheduler] These settings can be used to limit what users can do with the task scheduler, including administrators.	**Recommended Settings**: Enabled • **Hide Property Pages** - Prevent users from viewing and changing the properties of an existing task. • **Prohibit New Task Creation -** Prevents users from creating new scheduled tasks and browsing for applications. This does not prevent administrators from creating new tasks with the AT command, or from a remote computer.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Appendix B – Permissions Settings

The following table is an excerpt from the National Security Agency "Guide to Securing Microsoft Windows 2000 Terminal Services" (pg 28), http://nsa2.www.conxion.com/win2k/download.htm.

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

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Appendix C – Server Group Policy Settings

This table is a compilation of selected policies that should be considered for most environments where security is of primary concern. The comments and recommendations are based primarily on information from Microsoft Corporation's articles "Locking Down Windows Server 2003 Terminal Server Sessions", http://www.microsoft.com/windowsserver2003/techinfo/overview/lockdown.mspx, "Chapter 9 - Windows XP, Office XP, and Windows Server 2003 Administrative Templates" http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/hardsys/TCG/TCGCH00.asp and "Designing Server Setting Configurations" at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_hbkw.asp and cross-referenced for comparison against NSA's "Guide to Securing Windows 2000 Terminal Server" and Hacking Exposed Windows Server 2003. The settings description information has been quoted directly from these Microsoft sources, occasionally supplemented with information directly from "Windows Server 2003 Help".

Server Group Policies	Comments	Settings
Keep-Alive Connections	Computer Configuration/Administrative Templates/Windows Components/Terminal Services After a terminal server session looses the connection to a terminal server, the session might remain active instead of changing to a disconnected state. A user would then likely create a new session when reconnecting instead of connecting to their previous session. Use this setting if you are having problems with users who cannot reconnect to their sessions.	**Recommended settings**: Enabled • **Keep-Alive Connections** – Specifies whether persistent connections are allowed. Enabling keep-alive connections ensures that the session state is consistent with the client state. A keep-alive interval must also be set and determines how often, in minutes, the server checks the session state.
Temporary Folders	Computer Configuration/Administrative Templates/Windows Components/Terminal Services These settings can be set in the Server Settings folder of TSCC or in Group Policy. When these settings are enabled, temporary folders are used per session and deleted upon logging off. This limits the risk of any information stored in these folders from being accessed inappropriately.	**Recommended settings**: Enabled • **Delete or retain temporary folders when exiting** It is recommended that you configure your servers so that the data stored in the temporary folder for user sessions is deleted when users log off. This provides added security by eliminating a point of access for user data. It also provides a way to manage the load on the server, because temporary folders tend to grow quickly in size in a multi-user environment. If you are using Group Policy to set this setting (set to Disable to delete temporary folders), you must also configure the server to use per-session temporary folders. • **Use separate temporary folders for each session** This setting keeps each session's temporary folders in a separate folder, which enables you to configure the server to delete temporary folders when a single user logs off without affecting other users' sessions.
Active Desktop	User Configuration/Administrative Templates/Desktop/Active Desktop You can restrict users from using Active Desktop by using TSCC or Group Policy. Enabled by default, Active Desktop can negatively affect performance because of the amount of data that needs to transfer from the server to the desktop. It is recommended that you disable Active Desktop for this reason and to limit potential exposure to privilege escalation attacks.	**Recommended settings**: Disabled • **Disable Active Desktop** – Prevents users from choosing JPEG and HTML wallpaper.
Licensing	Computer Configuration/Administrative Templates/Terminal Services/Licensing Use the following settings to configure the license server for Terminal Server. Most of these settings can be configured only through Group Policy. Exceptions are noted.	• **Licensing Mode** You can set the licensing mode to Per Device or Per User through the TSCC Server Settings folder • **License Server Security Group** Enabling this Group Policy setting and applying it to your license server creates a local group called Terminal Services Computers. The license server issues licenses only to the terminal servers in this group. You must add both the terminal servers for which you need to provide licenses and any license servers that might need to acquire licenses to this group for each license server. For ease of management in a large Terminal Server deployment, create an Active Directory global group named Terminal Server Licensing and add all of your terminal servers and all of your license servers to this group. Then add this group to the Terminal Services Computers group of each license server.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Server Group Policies	Comments	Settings
		Whenever you deploy a new terminal server or license server, if you add it to the Terminal Server Licensing group, it automatically appears in the Terminal Services Computers group for each license server. • **Prevent License Upgrade** In an environment with both Windows Server 2003 and Windows 2000 Terminal Server, enable this Group Policy setting to prevent the license server from handing out Windows Server 2003 CALs to terminal servers that are running Windows 2000.
Limit users to one remote session	Computer Configuration\Administrative Templates\Windows Components\Terminal Services This policy ensures that a user who disconnects can reconnect to the same session rather than creating a new session. This conserves server resources by limiting the number of sessions on your server. The default setting is enabled.	**Recommended settings**: Enabled • **Restrict Terminal Services users to a single remote session** – Specifies whether to restrict users to a single remote Terminal Services session. If the status is set to enabled, users are restricted to a single session on that server. If the user leaves the session in a disconnected state, they will automatically reconnect to that session. If the status is set to disabled, users are allowed to make unlimited remote simultaneous remote connections.
Permission Compatibility	During installation you are asked to select one of these settings, however, it can be changed later using the TSCC tool. The Full Security setting restricts access to system resources, such as the registry, to members of the Users group on a terminal server. Although some older applications may require this access, do not use the Relaxed Security setting unless your testing indicates compatibility issues in Full Security mode. The Relaxed Security setting provides users with nearly Power User level access to some system folders and registry keys. If you must use the Relaxed Security setting, consider enabling policies to restrict access to registry editors and file browsers.	**Recommended settings**: Full Security • **TSCC setting**: Select Full Security to provide the most secure environment or Relaxed Security to provide an environment that is compatible with most legacy applications.
Home Directory and Roaming Profiles	Computer Configuration\Administrative Templates\Windows Components\Terminal Services Use the Home Directory Group Policy to set the path for storing your user home directories. Unless this is a standalone server outside your domain, set the home directories to a network share rather than storing locally to provide network separation, ability to use load balanced servers and better file security in the case the security of the Terminal Server is breached. Use the roaming profile policy to set the path for storing your roaming user profiles. Again, to facilitate load balancing, it is better to store these on another server.	**Recommended settings**: Use network share rather than storing locally. • **TS User Home Directory** – Specifies whether Terminal Services uses the specified network share or local directory path as the root of the user's home directory for a Terminal Services session. • **Set path for TS Roaming Profiles** – Specifies a path for storing Terminal Services roaming profiles. Specify in the form \\Computername\Sharename.
Windows Installer	Computer Configuration\Administrative Templates\Windows Components\Windows Installer Use of this setting can prevent users from installing software or permit users to install only those applications offered by a system administrator. If this is set for non-managed applications only, the windows installer still functions for applications that are published or assigned by means of group policies. If set to Always, Windows Installer is completely disabled. Disabling Windows Installer doesn't prevent installation of applications with other setup programs. All applications must be installed and configured prior to enabling this policy.	**Recommended setting**: Enabled – Always • **Disable Microsoft Windows Installer** – "Never" option indicates WI is fully enabled and users can install and upgrade software unless restricted by other means. "for non-managed applications only" option permits users to install assigned or published applications. "Always" disables Windows Installer completely.
Other Security	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options	**Recommended settings**: All Enabled except for cached logons • **Devices: Restrict CD-ROM access to locally logged-on**

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Server Group Policies	Comments	Settings
Options	The device policies restrict terminal server users from accessing the CD-ROM drive and floppy disk drive. Unless you have some reason for providing data this way, enable these restrictions. The interactive logon policies restrict storage of logon information for use in future logons including their logon name when connecting to the console of the server, and cached logon information for use when the domain is not available. The use of a logon banner is also a good practice for terminal servers, as it may thwart some password guessing attacks, as well as for legal reasons such as notifying users that their actions will be audited and that logon is restricted to authorized users only. Renaming the administrator account is a best practice for terminal servers. Since this account cannot be locked out, it is a primary target for password guessing attacks. Renaming the account makes this attack slightly more difficult. If your existing domain policies do not already restrict LAN hash storage, or this is a standalone server outside your domain, it is recommend that you restrict the storage of the weak LAN Manager (LM) hash value. Since the LM hash is stored on the local computer in the security database, the passwords can be compromised if the security database is attacked. This setting can cause issues if Windows 95 or 98 clients must be supported on your network.	**user only** - Allows only users who log on to the console of the Terminal Server access to the CD-ROM drive. • **Devices: Restrict floppy access to locally logged-on user only** - Allows only users who log on to the console of the Terminal Server access to the floppy disk drive. • **Interactive logon: Do not display last user name -** Does not display the last logged on user account at the Windows logon prompt on the console of the Terminal Server. This does not affect Terminal Server clients that locally cache the logon user name. • **Interactive logon: Number of previous logons to cache –** Determines the number of times a user can log on to a windows domain using cached account information. A setting of 0 disables logon caching. • **Interactive logon: Message text for users attempting to logon –** Specifies a text message that is displayed to users when they log on. • **Accounts: Rename administrator account** – Determines whether a different account name is associated with the security identifier (SID) for the account Administrator. • **Network security: Do not store LAN Manager hash value on next password change –** Determines if, at the next password change, the LAN Manager (LM) hash value for the new password is stored.
Administrator Privileges	Computer Configuration\Administrative Templates\Windows Components\Terminal Services Configuring the Deny log off setting to Enabled prevents anyone from logging off an administrator connected to the system. Use this policy to ensure a connected administrator cannot be logged off by another administrator. Logging off the connected administrator will lose any unsaved data. An attacker who has managed to establish a Terminal Server session with administrative privileges could make regaining control of the server difficult by forcibly logging off an administrator trying to log onto the server at the Session 0 console. User access is best managed by adding users to the Remote Desktop Users Group. Not allowing local administrators to customize permissions prevents an attacker who has gained administrative permissions from modifying the permissions and preventing other users from connecting.	**Recommended setting**: Enables • **Deny log off of an administrator logged in to the console session** – Specifies whether to allow an administrator attempting to connect to the console of a server to log off an administrator currently logged on to the console. Selecting Not Configured for this setting allows one administrator to log another off, but this permission can be revoked at the local computer policy level. • **Do not allow local administrators to customize permissions** – Specifies whether to disable the administrator rights to customize security permissions in the TSCC tool. Enabling this setting prevents the TSCC Permissions tab from being used to customize per – connection security descriptors or to change the default security descriptors for an existing group. All of the security descriptors become Read Only. Disabling or not configuring this setting gives server administrators full Read/Write privileges to the user security descriptors in the TSCC Permissions tab.
Loopback processing mode	Computer Configuration\Administrative Templates\System\Group Policy This setting is used to determine how user configuration policies will be applied. Enabling loopback processing applies the restrictive user configuration policies to all users on the Terminal Server, including administrators, regardless of where their user account is located. When the policy is disabled, only the computer configuration policies for the locked down OU are applied to the Terminal Server, unless user accounts are placed into the OU.	**Recommended setting**: Dependent on Configuration • **User Group Policy loopback processing mode** - Two modes are available. Merge mode first applies to the user's own GPO, then to the locked down policy. The lockdown policy takes precedence over the user's GPO. Replace mode just uses the locked down policy and not the user's own GPO. This policy is intended for restrictions based on computers instead of the user account.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Appendix D – Terminal Server Connection Configurations

This table is a compilation of selected policies that should be considered for most environments where security is of primary concern. The comments and recommendations are based primarily on information from Microsoft Corporation's articles "Locking Down Windows Server 2003 Terminal Server Sessions", http://www.microsoft.com/windowsserver2003/techinfo/overview/lockdown.mspx, "Chapter 9 - Windows XP, Office XP, and Windows Server 2003 Administrative Templates" http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/hardsys/TCG/TCGCH00.asp and "Designing Terminal Server Connection Configurations" at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_hbkw.asp and cross-referenced for comparison against NSA's "Guide to Securing Windows 2000 Terminal Server" and Hacking Exposed Windows Server 2003. The settings description information has been quoted directly from these Microsoft sources, occasionally supplemented with information directly from "Windows Server 2003 Help".

Group Policy	Comments	Settings
Data Encryption	Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security Data encryption levels for communication between the Remote Desktop client and Terminal Server can be set by using either Group Policy or TSCC. This setting must be enabled in order to specify the level of encryption for all connections to the server using Group Policy. The encryption is set to High Level by default. It is recommended that High (128-bit) or FIPS Compliant encryption be used for all connections. Computer Configuration\Windows Settings\Security Settings\Security Options Note: If FIPS compliance has already been enabled by the "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" Group Policy as above, you cannot change the encryption level by using this Group Policy or by using the TSCC tool. Also note that setting the encryption level to High may prevent some legacy clients from connecting.	**Recommended setting**: High or FIPS Compliant • **FIPS Compliant.** Encrypts traffic between client and server to meet the Federal Information Processing Standard 140-1 (FIPS 140-1). Use this level when Terminal Services connections require the highest degree of encryption, such as those required by the U.S. federal government. This level is set in the security options group policy. • **Client Compatible.** With Client Compatible encryption, traffic between the client and the server is encrypted using the RC4 algorithm and the strongest key the client supports (40-bit, 56-bit, or 128 bit). The server negotiates with the client to determine the key strength on connection, however the server does not accept non-encrypted client connections. • **High.** Traffic in both directions is encrypted using the RC4 algorithm and a 128-bit key only. If a client does not support 128-bit encryption, it is not permitted to connect. • **Low.** Traffic from the client to the server only is encrypted, at the strongest key that the client supports. This can improve performance on the client because the client does not have to decrypt the screen update data coming from the server. The client still encrypts the keystroke and mouse data that it sends to the server. This also allows you to use products to improve performance over a WAN, for example to use between a branch and a home office. Use this setting only if you are planning to use these products. A malicious user can monitor documents and data coming from the server over the link if this setting is used. • On the **General tab** of TSCC or on the Data Encryption property page of the Terminal Services Connection Wizard, the **Use standard Windows authentication** check box is cleared by default. If you select this check box, lower security authentication mechanisms are permitted.
Logon Settings	Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security Terminal Services allows users to automatically log on by saving a password in the Remote Desktop Connection client by default. For more secure access control, require users to provide logon credentials whenever they connect to the terminal server. If the server running Terminal Services allows users to store their username and password in a Remote Desktop connection shortcut in order to log onto the server without having to enter the password, then it is possible that an attacker who has gained physical access to the user's computer could connect to a Terminal Server using the Remote Desktop connection shortcut, even though they may not know the user's password.	**Recommended setting**: Enabled • **Always prompt client for password upon connection** – Specifies whether specifies whether Terminal Services always prompts the client for a password upon connection. You can use this setting to enforce a password prompt for users logging on to Terminal Services, even if they already provided the password in the Remote Desktop Connection client. Enabling this setting prevents users from automatically logging on to Terminal Services by supplying their passwords in the Remote Desktop Connection client.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Group Policy	Comments	Settings
Remote Procedure Call (RPC)	Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security\RPC Security Enable this Group Policy setting to allow Terminal Server to accept only authenticated and encrypted requests. Allowing unsecured RPC communication may expose the server to man-in-the-middle attacks and data disclosure attacks. This attack occurs when an intruder captures packets between a client and server and modifies them before allowing the packets to be exchanged, usually to obtain sensitive information.	**Recommended setting**: Enabled • **Secure Server (Require Security)** – Specifies whether a Terminal Server requires secure remote procedure call (RPC) communication with all clients or allows unsecured communication. You can use this setting to strengthen the security of RPC communication with clients by allowing only authenticated and encrypted requests. Enabling this setting causes the Terminal Server to only accept requests from RPC clients that support secure requests, and does not allow unsecured communication with clients that are not trusted. Disabling this setting causes the Terminal Server to always accept requests at any level of security for all RPC traffic. However, unsecured communication is allowed for RPC clients that do not respond to the request. Not configuring this setting allows unsecured communication to take place.
Sessions	Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Sessions Set Terminal Server time-out and reconnection settings on the server to limit the number of simultaneous sessions running on the terminal server, manage unreliable connections for remote users. Users often have disconnected sessions running on the server without knowing, particularly those on poor connections, so it is important to set a limit on how long disconnected sessions continue to run on the server. You can also set a limit on how long a user can maintain an active session on the server. Selecting Never allows an active session to continue indefinitely. Idle sessions occur when there has been no mouse or keyboard activity for a certain period of time, and can indicate that the user left his session unattended, creating a potential security risk. When a session has been idle for more than the time limit set, the user is notified and given two minutes to place the session back into an active state. If the two minutes elapse, the server disconnects or ends the session, depending on the settings you choose. It is important to understand users' work patterns and needs when choosing a limit for idle and active sessions. You can also set these settings per user through Group Policy User Configuration and through Active Directory Users and Computers user properties. However, the Group Policy computer settings take precedence over user settings.	**Recommended setting**: Enabled, 1 day • **Set time limit for disconnected sessions** – Specifies a time limit for disconnected Terminal Server sessions. You can use this setting to specify the maximum amount of time that a disconnected session remains active on the server. Enabling this setting deletes disconnected sessions from the server after a specified amount of time. **Recommended setting**: Enabled, dependent on work patterns • **Sets a time limit for active Terminal Services sessions** – Specifies a time limit for active sessions. You can use this setting to specify the maximum amount of time that an active session remains active on the server. Enabling this setting deletes or disconnects active sessions from the server after a specified amount of time, depending on whether you enable the **Terminate session when time limits are reached** policy. If this policy is disabled, the session will be disconnected only. **Recommended setting**: Enabled, dependent on work patterns • **Sets a time limit for active but idle Terminal Services sessions** – Specifies a time limit for idle sessions. You can use this setting to specify the maximum amount of time that an idle session remains active on the server. Enabling this setting deletes or disconnects active sessions from the server after a specified amount of time, depending on whether you enable the **Terminate session when time limits are reached** policy. If this policy is disabled, the session will be disconnected only. **Recommended setting**: Enabled, dependent on work patterns • **Sets a time limit for active but idle Terminal Services sessions** – Specifies a time limit for idle sessions. You can use this setting to specify the maximum amount of time that an idle session remains active on the server. Enabling this setting deletes or disconnects active sessions from the server after a specified amount of time, depending on whether you enable the **Terminate session when time limits are reached** policy. If this policy is disabled, the session will be disconnected only.
Launch application on connection	Computer Configuration\Administrative Templates\Windows Components\Terminal Services If you are providing a single application with Terminal Server or for a particular user or group of users, you can have that application start automatically when the user logs on. This eliminates the possibility of the user running unauthorized applications on the server or accessing other parts of the server or the network through the server. You	**Recommended setting**: Enable if client only requires access to one application. • **Start a program on connection –** Specifies a program to start automatically upon connection. By default, Terminal Services Sessions provide access to the full Windows desktop. Enabling this setting overrides the "Start Program" settings set by the server administrator or user. The Start menu and Windows desktop are not displayed, and the session is automatically logged off when the user exits the program.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Group Policy	Comments	Settings
	can configure this setting by using Group Policy (which you can apply to both computers and users), TSCC, and for users through the Remote Desktop Connection tool.	

Remote Control	Computer Configuration\Administrative Templates\Windows Components\Terminal Services
	
	Remote Control is a useful tool for controlling or troubleshooting a user's session from a remote location. You can apply this setting to both computers and users or using TSCC.
	
	For high security configurations, it is recommended that you disable remote control, however, for many environments, the tool can be an important part of user support, training, or other purposes. To prevent abuse of this tool configure the setting so that the user's permission is required to allow another person to access their computer through Remote Control.
		Recommended setting: For highest security, disable by selecting No Remote control allowed. If needed for support or other purposes, Enable with user's permission.
		• **Sets rules for remote control of Terminal Services user sessions -** Specifies the level of remote control permitted in a Terminal Server session. Remote control can be established with or without the session user's permission. You can use this setting to select one of two levels of remote control: View Session permits the remote control user to watch a session; Full Control permits the remote control user to interact with the session. Following are the enabled settings. Disabling or not configuring this setting allows the server administrator to determine the remote control rules using the TSCC tool.
		  ○ No remote control allowed
		  ○ Full Control with user's permission
		  ○ Full Control without user's permission
		  ○ View Session with user's permission
		  ○ View Session without user's permission
		• This setting exists under both Computer Configuration and User Configuration. When it is configured in both places, the setting under Computer Configuration overrides the same setting under User Configuration.

© SANS Institute 2004, Author retains full rights.

Appendix E – Client Connection Settings

This table is a compilation of selected policies that should be considered for most environments where security is of primary concern. The comments and recommendations are based primarily on information from Microsoft Corporation's articles "Locking Down Windows Server 2003 Terminal Server Sessions", http://www.microsoft.com/windowsserver2003/techinfo/overview/lockdown.mspx, "Chapter 9 - Windows XP, Office XP, and Windows Server 2003 Administrative Templates" http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/hardsys/TCG/TCGCH00.asp and "Designing Terminal Server Connection Configurations" at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_hbkw.asp and cross-referenced for comparison against NSA's "Guide to Securing Windows 2000 Terminal Server" and Hacking Exposed Windows Server 2003. The settings description information has been quoted directly from these Microsoft sources, occasionally supplemented with information directly from "Windows Server 2003 Help".

Group Policy	Comments	Settings
Client/Server data redirection	Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client\Server data redirection Data redirection settings enable users to access and use resources on their desktop computers within their Terminal Server session. The most common example is redirected printing, however, you can now also redirect drive, audio, smart card, and the clipboard to the client computer. Use the principle of least privilege for restricting user's options and allow redirection only if required in order to reduce the risk of introducing a vulnerability to the system. These settings can be applied through Group Policy (computers only) or TSCC unless noted otherwise. Most of these settings are also available for configuration by using the Remote Desktop Connection tool on the client.	
Time zone	Must be configured using Group Policy. The session time zone is the same as the time zone of the terminal server by default. If your applications have time dependencies, and you have users in different time zones accessing them, you may need to enable this setting. Otherwise, it is not recommended. Remote Desktop Connection and Windows CE 5.1 currently support time zone redirection. Session 0, the console session, always has the server time zone and settings. To change the system time and time zone, connect to Session 0.	**Recommended settings:** Disabled • **Allow Time Zone Redirection** - Specifies whether to allow the client computer to redirect its time zone settings to the Terminal Server session. By default, the session time zone is the same as the server time zone, and the client computer cannot redirect its time zone information. Enabling this setting allows clients that are capable of time zone redirection to send their time zone information to the server. The server base time is then used to calculate the current session time. Disabling this setting prevents time zone redirection from occurring. Not configuring this setting does not specify time zone redirection at the Group Policy level, and the default behavior is for time zone redirection to be turned off. When an administrator changes this setting, only new connections display the behavior specified by the new setting. Sessions that were initiated before the change must log off and reconnect to be affected by the new setting. Microsoft recommends that all users log off the server after this setting is changed.
Clipboard	By default, you can copy and paste between the terminal server and the Remote Desktop client. Disable this ability if you have sensitive data on the terminal server or network that should not be copied. For high security implementations, the recommended setting is to not allow redirection.	**Recommended settings:** Enabled • **Do not allow clipboard redirection** - Specifies whether to prevent the sharing of clipboard contents (clipboard redirection) between a remote computer and a client computer during a Terminal Server session. Enabling this setting prevents users from redirecting clipboard data. Disabling the setting causes Terminal Services to always allow clipboard redirection. Not configuring this setting does not specify clipboard redirection at the Group Policy level. However, an administrator can still disable clipboard redirection using the Terminal Services Configuration tool.
Smart card	This new feature of Windows Server 2003 Terminal	**Recommended settings:** Enable if not using smart cards for

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Group Policy	Comments	Settings
	Services allows you to use smart cards for session logon.	Terminal Services authentication. • **Do not allow smart card device redirection** - Specifies whether to prevent the mapping of smart card devices in a Terminal Services session. By default, Terminal Services automatically maps smart card devices on connection. Enabling this policy prevents users from using a smart card for logging on to a Terminal Services session. If the status is set to Disabled, smart card device redirection is always allowed. If it is not configured, an administrator can disable this using the TSCC.
Audio	By default, users cannot play audio on the Remote Desktop client. The sound plays on the server rather than the client computer. If you enable this setting, users can specify on the Remote Desktop Connection tool whether to play audio at their computer or the server, or to not have the sound play at all. For high security implementations, the recommended setting is disabled as data could be forwarded from the user's session to the user's local computer without any direct user interaction. Allowing audio redirection may also have a negative performance impact on your server.	**Recommended settings:** Disabled • **Allow audio redirection** - Specifies whether users can choose where to play the remote computer's audio output during a Terminal Server session. Users can select the Remote computer sound option button on the Local Resources tab of Remote Desktop Connection to choose whether to play audio on the remote computer or 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. Enabling this setting allows users to apply audio redirection. Disabling this setting prevents users from applying audio redirection. Not configuring this setting does not specify audio redirection at the Group Policy level. However, an administrator can still enable or disable audio redirection by using the TSCC tool.
Serial port	This policy is enabled by default, allowing users to redirect data to devices attached to the serial (COM) port. This feature should be disabled unless there is a specific requirement for it.	**Recommended settings:** Enabled • **Do not allow COM port redirection** - Specifies whether to prevent the redirection of data to client Component Object Model (COM) ports from the remote computer in a Terminal Server 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 Server session. By default, Terminal Services allows COM port redirection. Enabling this setting prevents users from redirecting server data to the local COM port. Disabling this setting always allows Terminal Services COM port redirection. Not configuring this setting does not specify COM port redirection at the Group Policy level. However, an administrator can still disable COM port redirection using the TSCC tool.
Client printer	This policy is enabled by default and allows users to redirect print jobs to their local or network printer. Disable this capability unless specifically required to limit users ability to print or copy sensitive data stored on the terminal server and to reduce exposure to vulnerabilities.	**Recommended settings:** Enabled • **Do not allow client printer redirection** - Specifies whether to prevent the mapping of client printers in Terminal Server sessions. You can use this 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 client printer mapping. Enabling this setting prevents users from redirecting print jobs from the remote computer to a local client printer during Terminal Server sessions. Disabling this setting allows users to redirect print jobs with client printer mapping. Not configuring this setting does not specify client printer mapping at the Group Policy level. However, an administrator can still disable client printer mapping using the TSCC tool.
Parallel port	This policy is enabled by default, allowing users to redirect data to parallel (LPT) port devices. Disable this capability unless specifically required.	**Recommended settings:** Enabled • **Do not allow LPT port redirection** - Specifies whether to prevent the redirection of data to client parallel ports (LPT) during a Terminal Server session. You can use this setting to prevent users from mapping local LPT ports and redirecting

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Group Policy	Comments	Settings
		data from the remote computer to local LPT port peripherals. By default, Terminal Services allows LPT port redirection. Enabling this setting prevents users in a Terminal Server session from redirecting server data to the local LPT port. Disabling this setting always allows LPT port redirection. Not configuring this setting does not specify LPT port redirection at the Group Policy level. However, an administrator can still disable local LPT port redirection using the TSCC tool.
Drive	This policy is enabled by default, allowing users to redirect data to the local drives on the client computer. Disable this capability unless absolutely required to prevent users from copying sensitive data stored on the terminal server or network onto their local computer. This is particularly important if the client is untrusted.	**Recommended settings:** Enabled • **Do not allow drive redirection** – Specifies whether clients can redirect data to local drives on their computer. Enabling this setting prevents client drive redirection during Terminal Server sessions. Disabling this setting always allows client drive redirection. Not configuring this setting does not specify client drive redirection at the Group Policy level. However, an administrator can still disable client drive redirection by using the TSCC tool.
Default Printer	The Terminal Server designates the client default printer as the default printer in a session by default. Disable this capability unless specifically required.	**Recommended settings:** Enabled • **Do not set default client printer to be default printer in a session** - Directs Terminal Services not to specify the default client printer as the default printer for Terminal Server sessions. By default, Terminal Services automatically designates the default client printer as the default printer during Terminal Server sessions. Enabling this setting prevents the terminal server from setting the default client printer as the default printer for the session. Instead, the server specifies the default at the server. Disabling this setting ensures the default printer is always the default client printer. Not configuring this setting does not enforce the default printer designation at the Group Policy level. However, an administrator can configure the default printer for client sessions by using the TSCC tool.
Color depth	You can reduce or increase the maximum color depth depending on your bandwidth and fidelity requirements (greater color depth requires more bandwidth and resources on the terminal server).	

© SANS Institute 2004, Author retains full rights.

List of References

1. "Designing Terminal Server Connection Configurations". URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_hbkw.asp

2. Klemenc, J. October 2001. URL: http://archives.neohapsis.com/archives/sf/ms/2001-q4/0192.html

3. Madden, Brian S. "Citrix MetaFrame XP Security Design". Excerpted from Citrix MetaFrame XP: Advanced Technical Design Guide, Including Feature Release 2. November 2002, URL: http://www.brianmadden.com/papers/MetaFrame_Security_Design.htm

4. "Load Balancing Terminal Servers". Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_nfow.asp

5. "Planning Network Security Components". Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_deco.asp

6. "Configuring User Group Policy Settings". Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_lgvk.asp

7. "Designing Terminal Server Installation and Configuration". Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_lxbm.asp

8. "Chapter 9 - Windows XP, Office XP, and Windows Server 2003 Administrative Templates". Threats and Countermeasures Guide. Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/hardsys/TCG/TCGCH00.asp

9. "How to Apply Group Policy Objects to Terminal Services Servers". Microsoft Corporation. URL: http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q260/3/70.asp&NoWebContent=1

10. "Locking Down Windows Server 2003 Terminal Server Sessions". Microsoft Corporation. July 2003. URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/lockdown.mspx

11. McClure, Stuart and Scambray, Joel. Hacking Exposed Windows Server 2003. California: McGraw-Hill/Osborne, 2003. 337-358.

12. "Windows Server 2003 Terminal Server Capacity and Scaling". Microsoft Corporation. June 2003.

URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/tsscaling.mspx

13. "Session Directory and Load Balancing Using Terminal Server". Microsoft Corporation. March 2003. URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/sessiondirectory.mspx

14. "Hammer of God Downloads and stuff". URL: http://www.hammerofgod.com/download.htm

15. "HOW TO: Use the Terminal Services Version Limiter Tool in Windows 2000 Terminal Services". Microsoft Corporation. URL: http://support.microsoft.com/?kbid=320189

16. U.S. National Security Agency. Guide to Securing Microsoft Windows 2000 Terminal Services, [by Vincent J. DiMaria, et al] Ft. Meade, MD, July 2, 2001 Version 1.0. URL: http://nsa2.www.conxion.com/win2k/download.htm

17. U.S. National Security Agency. "Windows 2003 Security Guide". URL: http://nsa2.www.conxion.com/support/winserver03.htm

18. "Remote Administration of Windows Servers Using Remote Desktop for Administration". Microsoft Corporation. March 2003. URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/tsremoteadmin.mspx

19. "Technical Overview of Terminal Services". Microsoft Corporation. July 2002. URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/termserv.mspx

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

20. "What's New in Terminal Server". Microsoft Corporation. URL: http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/terminalserver.mspx

21. "Support WebCast: Microsoft Windows Server 2003 Terminal Services: New Features".URL: http://support.microsoft.com/default.aspx?scid=/servicedesks/webcasts/wc121702/wcblurb121702.asp

23. "Choosing a Terminal Server Configuration Tool". Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_soru.asp

24. "Configuring Terminal Services with Group Policy". Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/ts_gp_topnode.asp

25. "Software Restriction Policies Best Practices". Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/safer_topnode.asp

26. "Microsoft Windows Server 2003 - What's New in Security". Microsoft Corporation. URL: http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/security.mspx#summary

27. Thurrott, Paul. "Windows 2003 SP1 and Windows XP SP2: Not Your Average Service Packs". Windows & .NET Perspectives. Nov 2003. URL: http://www.winnetmag.com/Article/ArticleID/40766/Windows_40766.html

28. Smith, Randy Franklin. "Terminal Services, Part 4", Windows and .Net Magazine Network, March 15, 2001. URL: http://www.winnetmagcom/articles/Print.cfm?ArticleID=20288.

29. Madden, Brian S. "Windows Server 2003 SP1 will Add End-to-End SSL Terminal Server Encryption". September, 2003. URL: http://www.brianmadden.com/reviews/Terminal_Services_2003.htm

30. "Providing for RDP Client Security". Microsoft Corporation. URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/termserv/termserv/providing_for_rdp_client_security.asp

31. "Microsoft Terminal Services Advanced Client". Microsoft Corporation. URL : http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/tsac.asp#heading2

32. "Planning Terminal Server User Rights and Logon". Microsoft Corporation. URL : http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_ubgc.asp

33. "Internet Explorer Enhanced Security Configuration". Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/iesechelp.asp

34. "Designing Server Setting Configurations". Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/sdcce_term_hbkw.asp

35. Conover, J. "SSL VPN: IPSec Killers or Overkill?". Analyst Corner, CIO Magazine. October, 2003 http://www2.cio.com/analyst/report1816.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced