Global Information Assurance Certification Paper

Securing Windows 2000 Terminal Service for Remote Administration
Name: Jeff Shively
Version: GIAC Security Essentials Certification Version 1.4 option 1
Date: July 1, 2002

Abstract

For most network administrators, administering the servers can be a nightmare. The major problem is getting access to the servers. For example, the server they may need to access may be in another room, an entirely different building, or in some cases even a different state or country. So how could an administrator easily administer a server that is not convenient? If the server was on a Windows 2000 platform, it can be very easily be administered through the use of Terminal Service.

This paper will illustrate how to install Terminal Service for Windows 2000 and also how to configure it to run securely. As with all software installations, use a non-production server for the initial installation and testing. Once the server has been tested, the server can then be deployed into the production environment.

What is Terminal Service?

Terminal Service is a component that is packaged freely within Windows 2000 Server, Windows 2000 Advanced Server, and Windows 2000 Datacenter Server. After installation, it allows a user using a terminal emulation program the ability to connect to the Windows 2000 Server remotely.

Terminal Service works via a TCP/IP connection and using Microsoft Remote Desktop Protocol (RDP) version 5.0. By using the Remote Desktop Protocol it opens up a wide array of features to the user such as reconnection of disconnected sessions, clipboard mapping, and print redirection to the user's local printer.

Terminal Service can be configured for either remote administration or application server mode. The focus on this paper will be specifically on remote administration.

What is remote administration mode?

Remote administration is designed to simplify server administration. Once the user has connected and been authenticated, any task that can be completed on the console can be done via a Terminal Service connection.

Remote administration mode allows up to two concurrent users to be connected to the server remotely. Those connections have full access to the server and

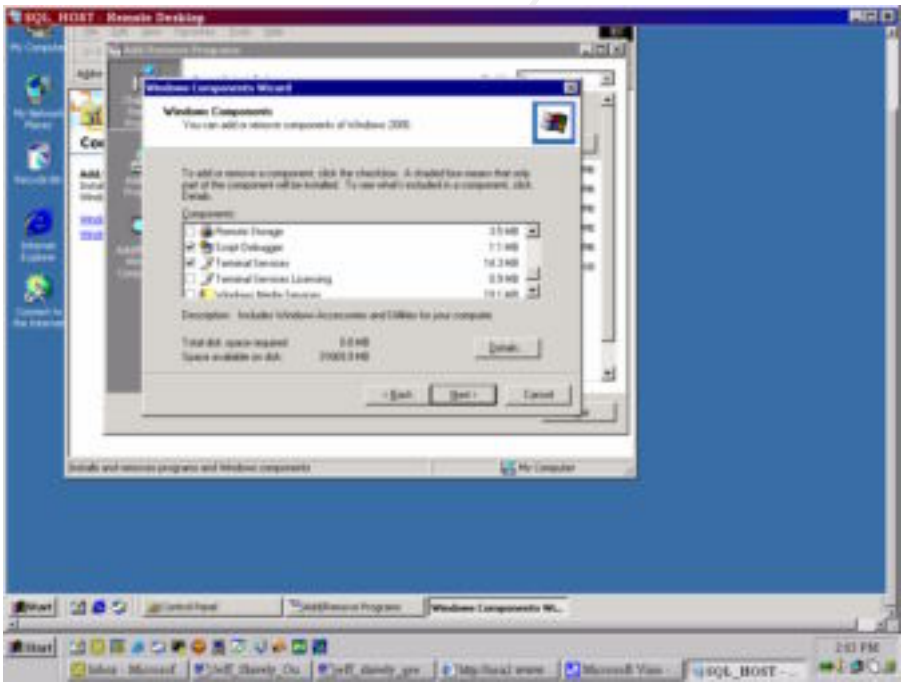
could make registry changes, apply patches, reboot the server, or even modify the Active Directory schema.

Why secure Terminal Service?

The entire system is designed to perform all the processing tasks on the server. After the processing takes place on the server, the server converts all output into network packets and then passes all this data back to the user. Those packets contain all mouse movements and keystrokes. There is a risk that those packets could be intercepted by a malicious user. The user could use the packet to learn passwords or acquire knowledge about the network structure. Therefore, it should be critical that Terminal Service is installed and setup securely (Securing Windows 2000 Terminal Service).

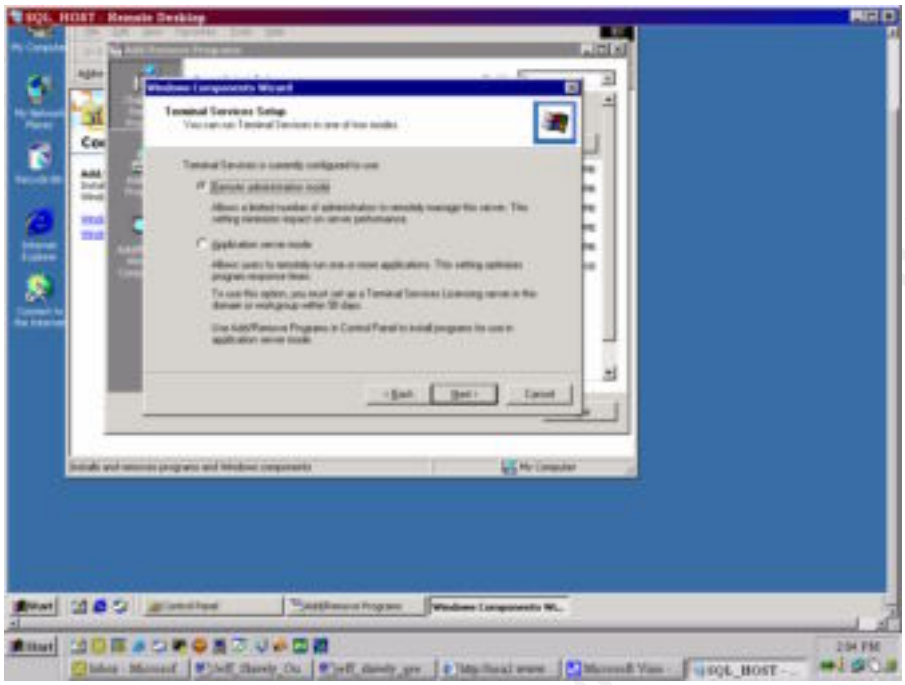
Installation of Terminal Service

Installation of Terminal Service is done through the *Add/Remove Program* in control panel and then selecting *Add/Remove Windows Components* button. At this point, the user is prompted with a list of Windows components that can be installed. In order to use Terminal Service for remote administration, the administrator will need to check Terminal Services checkbox. Licensing of Terminal Services is only applicable if using Terminal Service in application server mode.



After selecting Terminal Service and clicking on *next* button, the administrator is prompted for the method of how to install Terminal Service. Since the application is being configured for remote administration, verify that the “Remote

Administration mode" button is selected. After verifying the appropriate button is selected, click on *next* button.



The application will be installed and the next screen will notify the administrator of the status of the installation. If the installation was successful, the administrator will be instructed to click on the *Finish* button. After clicking on the *Finish* button, the administrator will be prompted to reboot the server. Terminal Service will not work until the server has rebooted. If the installation was not successful, additional work will be needed to correct the problems encountered during the installation.

Default available levels of encryption

Within Terminal Service there are three different available options for encrypting data. The three levels are low, medium, and high.

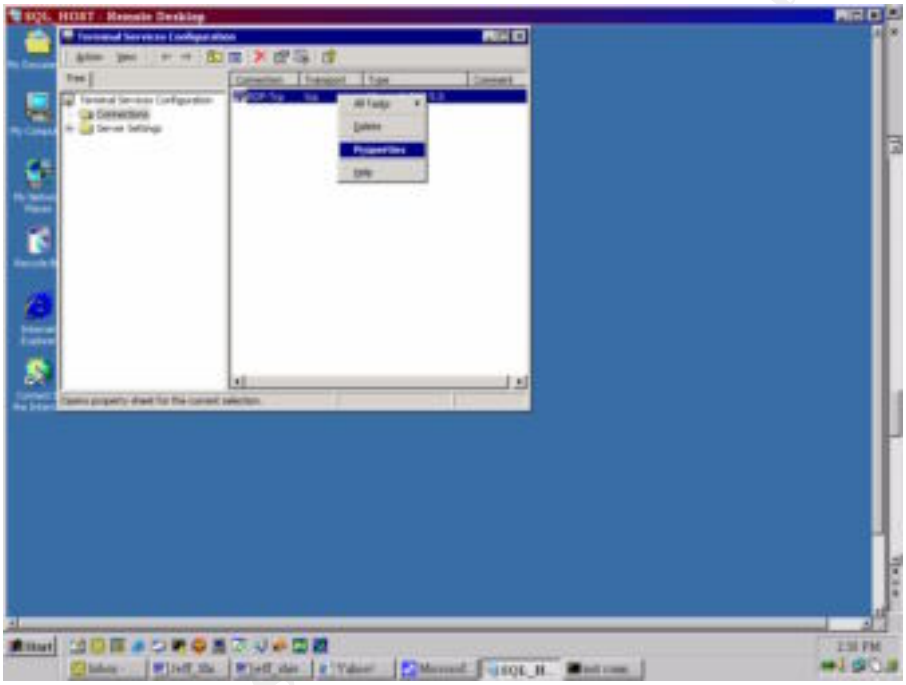
Low encryption only encrypts the traffic from the client to the server. Communications back from the server to the client is not encrypted. This type of encryption has commonly been referred to as "input only encryption" and is used in order to protect the sending of sensitive information such as passwords (Terminal Server Walkthrough: Startup, Connection, and Application (Q186572)). Low encryption employs an RC4 algorithm and a 56-bit key (Chapter 16 – Deploying Terminal Services).

Medium encryption is the default level of encryption and it encrypts the data in both directions using the RC4 algorithm and a 56-bit key (Chapter 16 – Deploying Terminal Services).

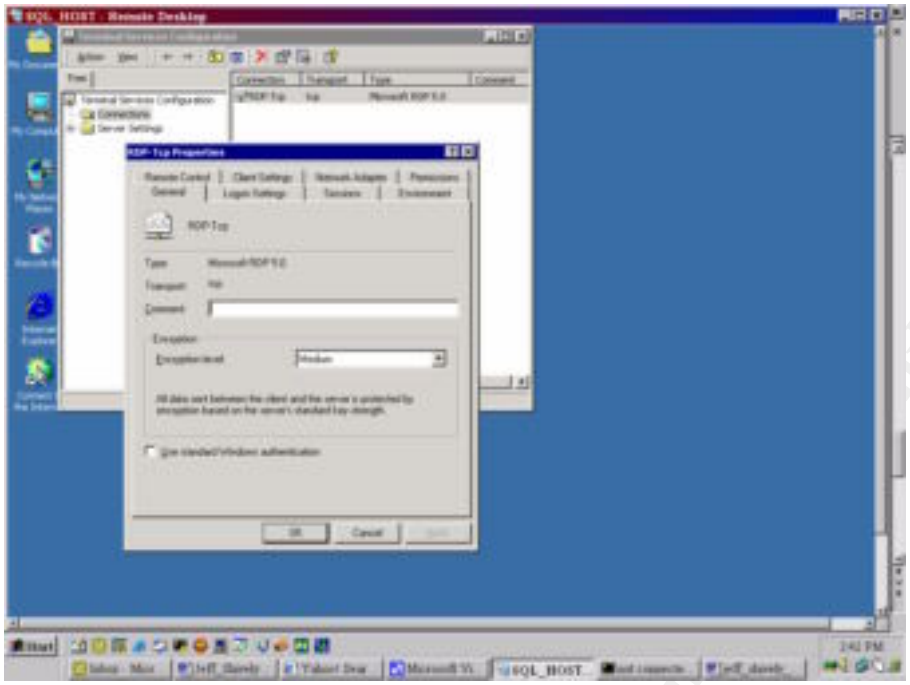
High encryption is available in the North American version of Terminal Service and after applying the high encryption patch. An RC4 algorithm and a 128 bit key are used to encrypt the data in both directions key (Chapter 16 – Deploying Terminal Services).

Changing the Encryption Level that Terminal Service Uses

After the installation of Terminal Service, the administrator will notice under *Programs/Administrative Tools* there are three new options available. In order to change the encryption level being used, the administrator needs to use the "Terminal Service Configuration" utility. From the Terminal Service Configuration utility, right click on the Microsoft RDP 5.0 under the connections folders and select properties.

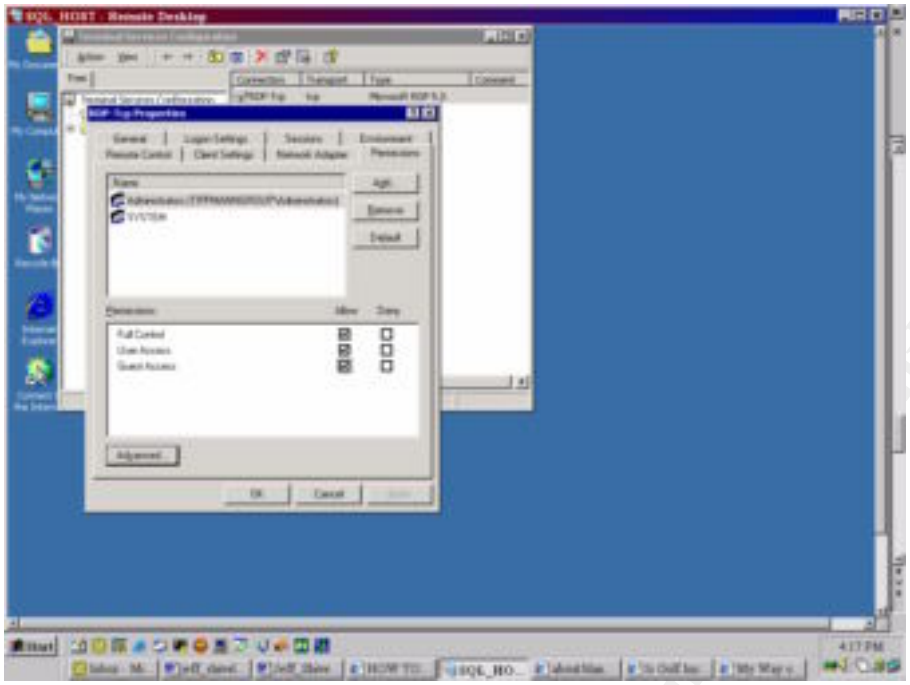


After selecting properties and under the general tab, there is an option that allows the administrator to change the encryption level that is being used.



Changing User Access to Terminal Service

Based upon the needs of the user, the administrator will need to evaluate and assign the appropriate access rights to the user. By default, users are assigned to the administrator's group and have the highest level of access rights. Therefore, it is critical for the administrator to monitor and control this.
In order to change which users can access Terminal Service or change the user access level, the administrator needs to use to the Terminal Service Configuration utility. Under the utility there is a tab that is labeled permissions.



There are two methods which the administrator can add new users or groups.

Method one allows the administrator to assign the user to one of the three predefined groups. Those three groups are full control, user access, and guest access. The full control group is granted all Terminal Service permissions while connected. The user access group is given permission to logon, query information, message, and connect permissions. The guest access is just given access to logon (Explanation of RDP-TCP Permissions in Windows 2000 (Q243554)).

To use the predefined groups the administrator would click on the add button, select the user or group, and assign the user to the appropriate group.

Method two allows more flexibility in assigning permissions to a specific user or group. This is accomplished by clicking on the advanced button and then clicking on the add button. From the box, select the user or group that the administrator wishes to give permission. After selecting the user or group the administrator is presented with another box that allows the administrator to modify the permissions.

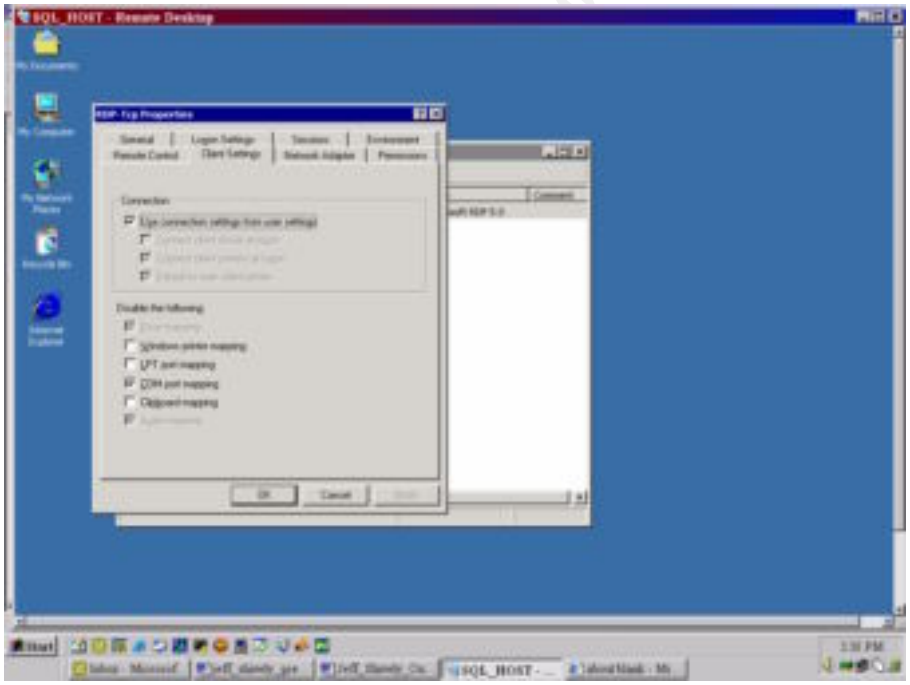
The acceptable permissions and their descriptions are listed in the chart on the next page.

Permission	Description
Query Information	Query sessions and servers for information
Set Information	Configure connection properties
Reset	End a session
Remote Control	View or actively control another user's session
Logon	Log into a session on the server
Logoff	Log off a user from a session
Message	Send a message to another user
Connect	Connect to another session
Disconnect	Disconnect a session
Virtual Channels	Use virtual channels

(Explanation of RDP-TCP Permissions in Windows 2000 (Q243554))

Client Settings

Under the “Client Settings” tab within the “Terminal Service Configuration” utility, the administrator is given options to control the client settings for sessions.



Under the “Disable the following” selection if the specific option is checked the feature will not be available to the user when they logon. The administrator should disable the option unless they are required.

The following explains the functionality of each check box.

The “Drive mapping” feature is only available for Citrix ICA-based clients. Therefore, it does not apply to remote administration (“To configure settings for mapping client devices”).

The “Windows printer mapping” will allow the user’s printers to be automatically mapped when the user connects to Terminal Service. The printers are available within the session. This is enabled by default (“To configure settings for mapping client devices”).

The “LPT port mapping” allows the user to configure a printer within Terminal Service that will print to their local printer. From the Terminal Service session, the user accesses the *Add Printer Wizard* to configure a printer and select their port from the list. Unlike the “Windows printer mapping” this does not automatically map the user’s printer. The user will manually setup their printer. This is enabled by default (“To configure settings for mapping client devices”).

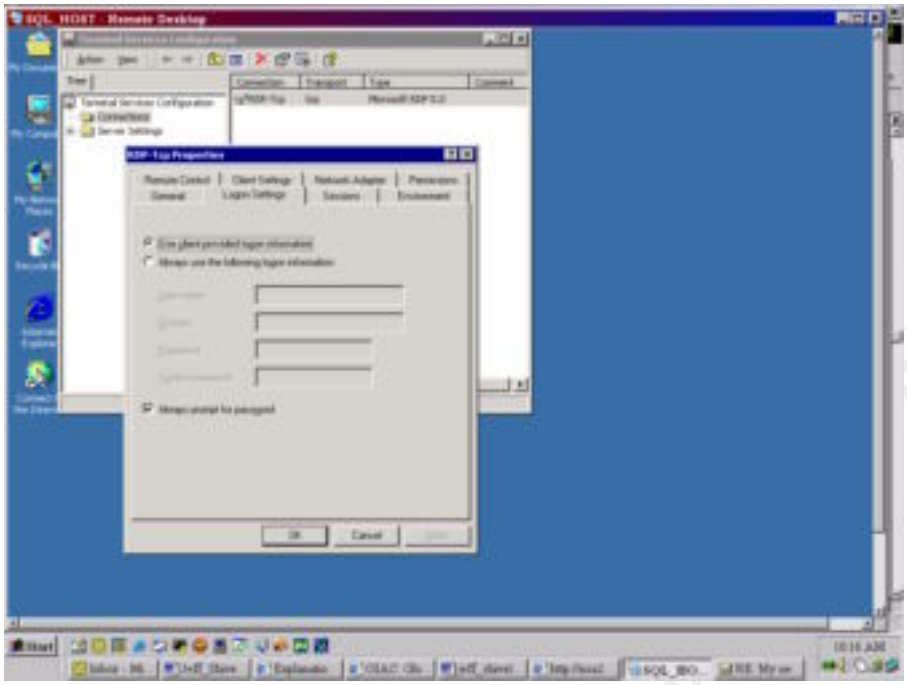
The “COM port mapping” is identical to the “LPT port mapping” selection, however; instead of using the LPT ports it utilizes the user’s COM ports. This selection is disabled by default (“To configure settings for mapping client devices”).

The “Clipboard mapping” allows the user to cut and paste text or graphics from the client’s computer to the Terminal Service session. However, it does not allow files to be cut and pasted. In order for files to be cut and pasted, a utility that is provided within the Microsoft Windows 2000 Resource Kit called rdpclip needs to be installed on the client’s computer and the server. In order for clipboard mapping to work, the user must also have the virtual channel permission (Guide to Securing Microsoft Windows 2000® Terminal Service). This is enabled by default (“To configure settings for mapping client devices”).

The “Audio mapping” is only available for Citrix ICA-based clients. Therefore, it does not apply to remote administration (“To configure settings for mapping client devices”).

Logon Settings

Within the “Terminal Service Configuration” utility, there are specific options that control the logon settings of the users. These settings are accessed using the “Logon Settings” tab.



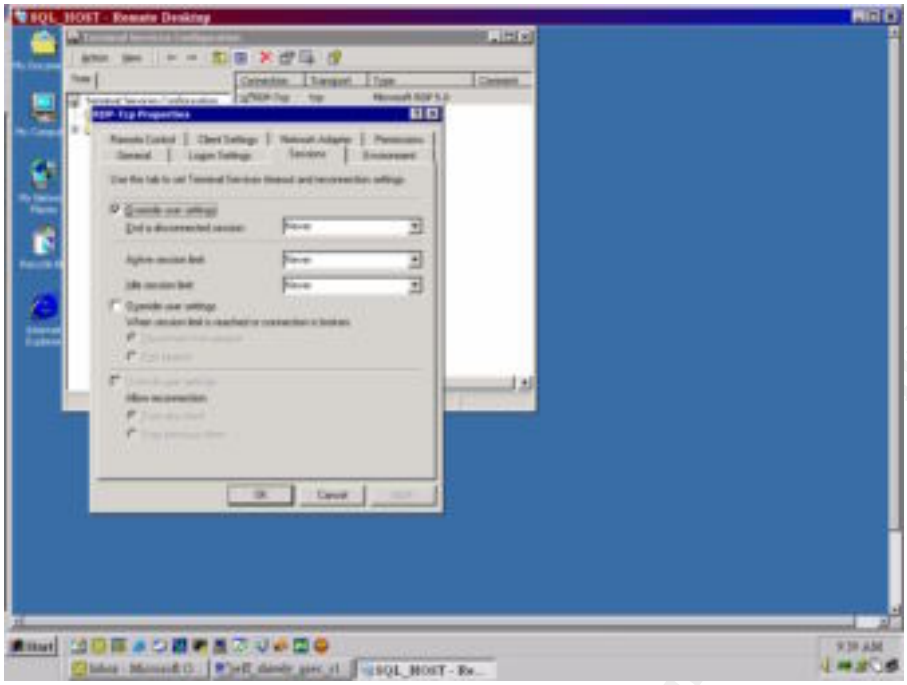
The “use client-provided logon information” checkbox instructs Terminal Service to prompt the user for a username and password at logon. The default for this option is to prompt user, and it is recommended to use the default value (“Securing Windows 2000 Terminal Services”).

The “Always use the following logon information” instructs Terminal Service that when a connection is established to automatically logon. The username and password information is listed under the “use the following logon information” selection. This is not recommended because a user who has knowledge of the Terminal Server address or name can access the server automatically without any authentication (“Securing Windows 2000 Terminal Services”).

The “always prompt for password” checkbox instructs the Terminal Service to always prompt the user for a password. This prevents the user from saving their account information on their computer and executing an auto login. If this option is not enabled an unauthorized user could access the Terminal Server by using another user’s auto login information (“Securing Windows 2000 Terminal Services”).

Session Settings

Within the “Sessions” tab under the “Terminal Service Configuration” utility, there are specific settings that controls the user’s session.



The “Override users settings” checkbox instructs Terminal Service to only use the Terminal Service settings configured on the server and ignore any Terminal Service settings that the client sends to the server (“Guide to Securing Microsoft Windows 2000® Terminal Service”.).

The “End a Disconnected Session” drop box instructs Terminal Service the amount of time to wait before automatically closing a session that is in a disconnected state. A disconnected session can happen when a user does not log off of Terminal Service, their computer crashes, or they lose network connectivity. When a session is disconnected, the processes the user was running are still active on the server (“Guide to Securing Microsoft Windows 2000® Terminal Service”.).

There are advantages and disadvantages to this feature. An advantage is if a user is running database reorganization and they lose network connectivity the reorganization will continue to run thus preventing data corruption in the database. A disadvantage is if the user just closed Terminal Service and did not log off one of the two available licenses is tied up until the disconnected session is closed.

The “Active Session Limit” drop box instructs Terminal Service the length of time a user can maintain an active session. When the active session limit period has been reached, the user is disconnected. By default this feature is disabled. It is recommended not to enable this feature (“Guide to Securing Microsoft Windows 2000® Terminal Service”.).

The “Idle session timeout” drop box instructs Terminal Service how long to wait before putting an idle active session in a disconnected state. After the idle timeout has been reached the server sends the user a message informing the user that the idle session timeout has been reached. The session will be closed within unless the user presses any key (“Guide to Securing Microsoft Windows 2000® Terminal Service”.).

For the “When session limit is reached or connection is broken:” options, there are two methods available. This option is executed when a session is closed abnormally, the idle session timeout is reached, or the active session timeout is reached.

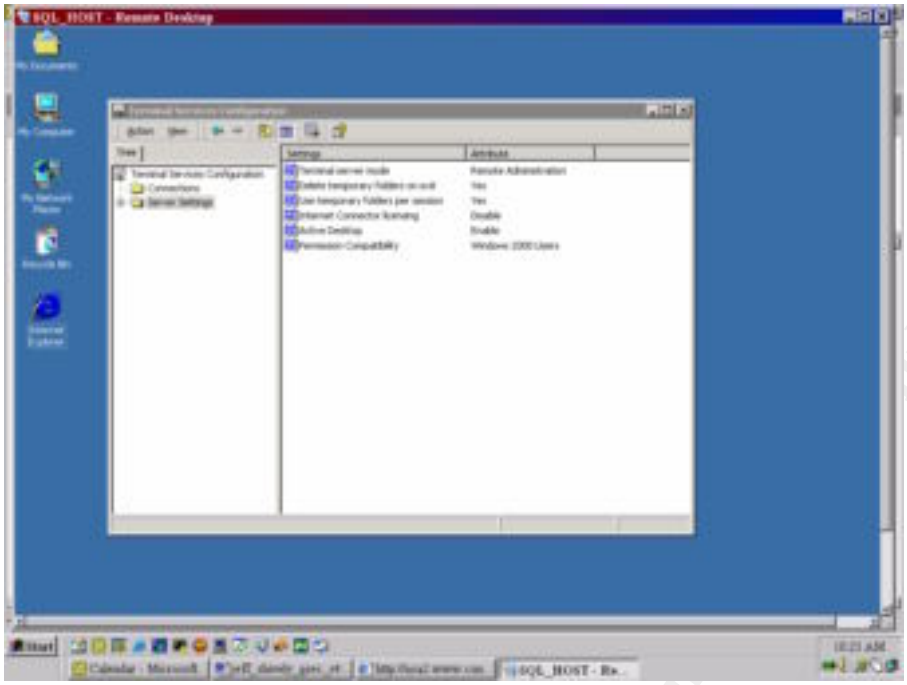
The first method, disconnect the session, instructs Terminal Service to place the session in a disconnected state. Upon re-logon, the user will have the ability to resume the disconnected session (“Guide to Securing Microsoft Windows 2000® Terminal Service”.).

The second method, end the session, instructs Terminal Service to terminate the session and discard any unsaved work (“Guide to Securing Microsoft Windows 2000® Terminal Service”.).

Server Settings

In addition to being able to make changes that only apply to the sessions, there are also changes that can be applied to the Terminal Server.

Under the “Terminal Service Configuration” utility, on the left pane is a folder called Server Settings.



The “Terminal Service mode” selection shows the administrator what mode of Terminal Service is installed. This can not be changed from this window due to the fact the administrator must use the *Add/remove Windows Components* utility to change the mode.

The “Delete temporary folders on exit” instructs Terminal Service after the session is closed to delete all temporary files that the session was using. This setting should be set to yes to prevent access to the environment information that is stored in the temporary folders (“Securing Windows 2000 Terminal Services”).

The “Use temporary folders per session” instructs Terminal Service to create temporary folders for each individual session. This prevents another user from determining the environment information of another user (“Securing Windows 2000 Terminal Services”).

The “Internet Connector License” is an additional license cost. This additional license will allow anonymous users to be able to connect to the Terminal Service. After being activated, it will allow Terminal Service to share applications with people via the Internet. However, the people who use this additional license can not be employees (“Securing Windows 2000 Terminal Services”).

The “Active Desktop” allows the client the ability to utilize the Windows Active Desktop features. The active desktop feature enables the user to access the Terminal Service desktop as a personalized web page. This feature allows items to be displayed such as scrolling stock tickers or the current temperature. However, the drawback is Active Desktop can also expose the session to

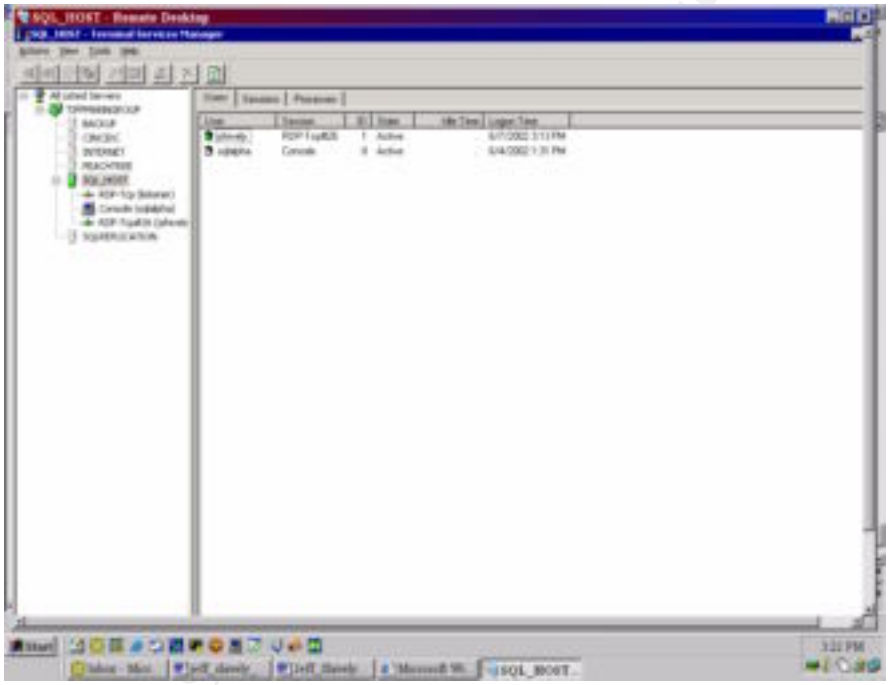
malicious code. It is recommended that this feature be set to disable ("Securing Windows 2000 Terminal Services").

The "Permission Capability" is only applicable for when Terminal Service is running in application server mode ("Securing Windows 2000 Terminal Services").

Logging (Current Users and Past Users)

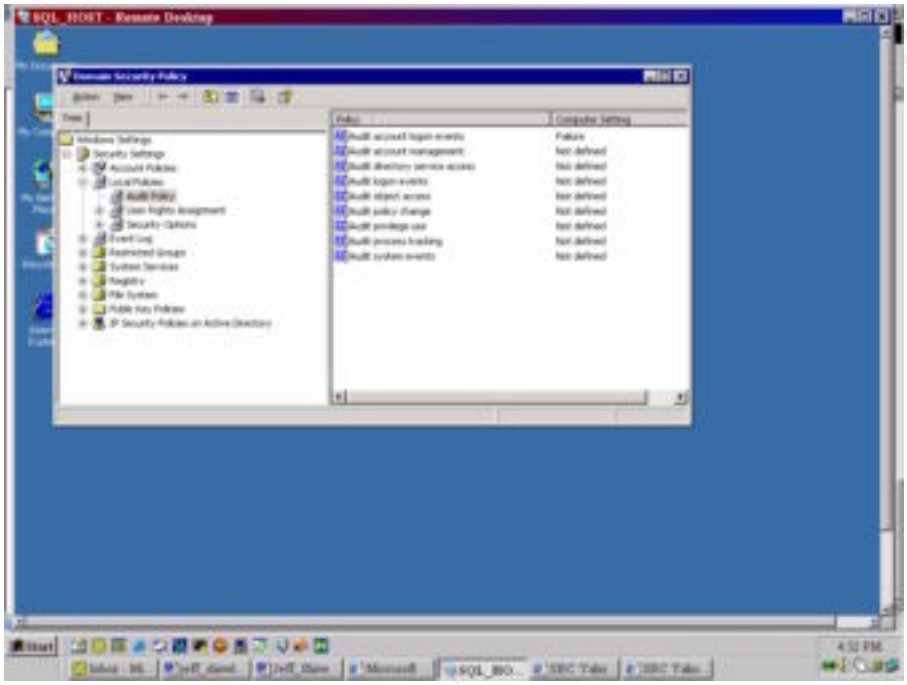
A good security template helps prevent your Terminal Server from being hacked, however; there is no guarantee that it will not be hacked. To determine who is currently logged on or who has logged on a separate set of utilities needs to be utilized.

In order to determine who is currently logged on to Terminal Service requires the "Terminal Service Manager" utility. This utility is located under Programs/Administrative Tools.

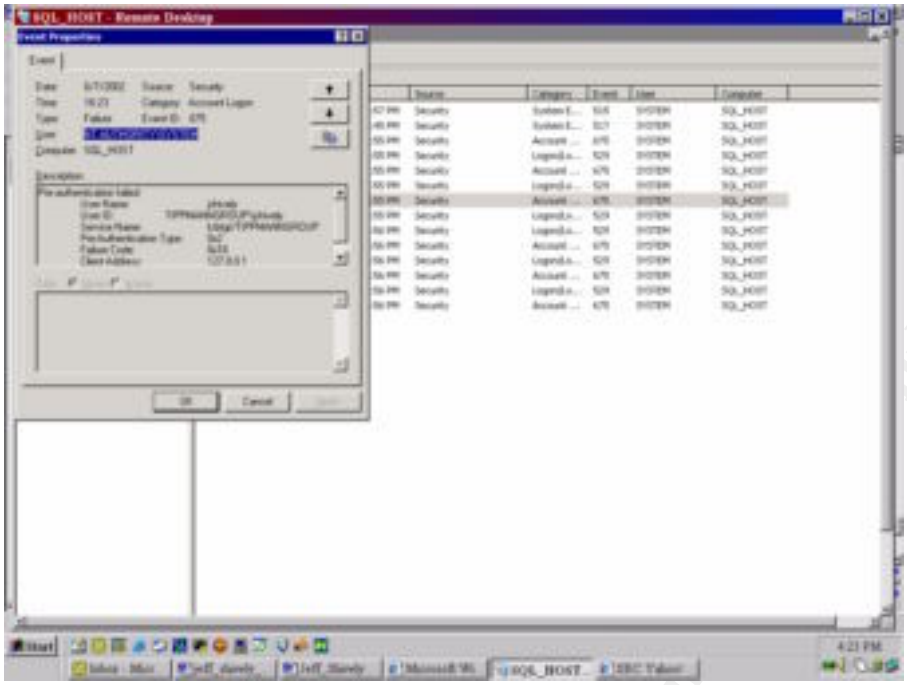


This utility will show the administrator the current users who are connected to the Terminal Service and their status. As shown in the above screenshot, user jshively is logged into Terminal Service via RDP-Tcp#26 and has been connected since 3:13 p.m. Notice the column labeled "state" displays active. This indicates that this is an active session that is currently being used. If the session was disconnected the column labeled "state" would display disconnected.

The Terminal Service Manager will only show the administrator when a user is logged on. To determine if an unauthorized user is attempting to gain access to the Terminal Service, the administrator has the ability to configure Terminal Service to report invalid logon attempts. The administrator will configure this feature through either the “Domain Controller Security Policy” or the “Local Security Policy” under Programs/Administrative Tools. By enabling the “Audit account logon events” selection the administrator enables Terminal Service to send a message to Event Viewer when a login failure occurs.



When an invalid username or password is used to logon to Terminal Service, an event is written to the Event Viewer. As shown in the below example, the password for jshively failed.



Accessing Terminal Service via the Internet

Terminal Service is easily configured to work across an Internet connection. However, since Terminal Service is now exposing the data to more prying eyes the consideration to use Terminal Service with another layer of security needs to be considered.

If a firewall is deployed, the TCP port 3389 needs to be open to allow the Terminal Service traffic to go through ("Terminal Server Walkthrough: Startup, Connection, and Application (Q186572)"). However, as with any firewall configuration, if the port is left wide open any unauthorized user who determines the IP address or DNS name of the server could connect to the server. Consideration must be made in order to limit access to the server. This can be achieved by deploying an extended access list on the firewall.

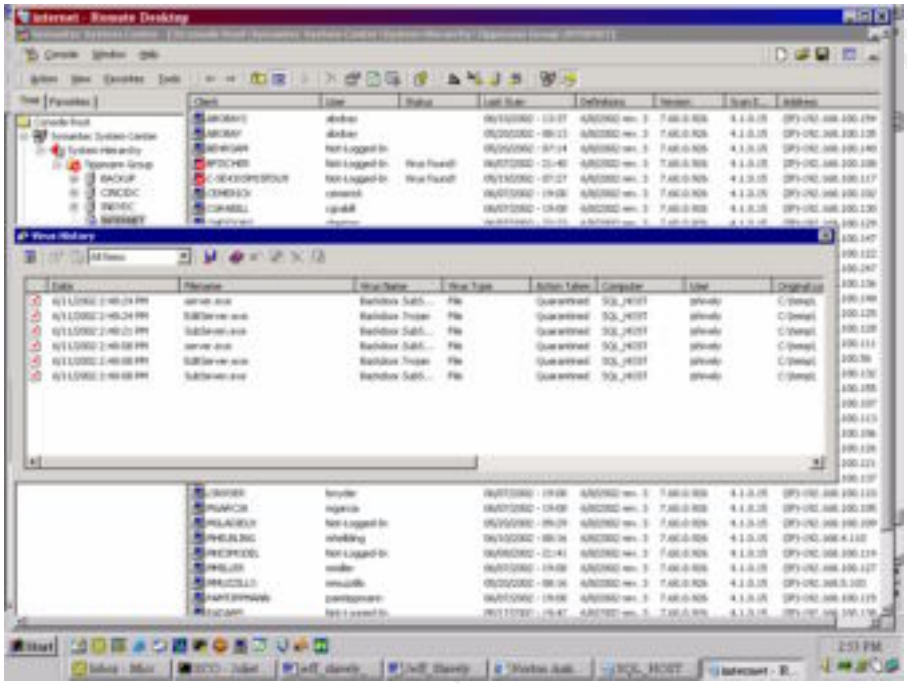
Another option to be considered would be to deploy a Virtual Private Network (VPN). The benefit of employing a VPN is the ability to add another layer of encryption ("Securing Windows 2000 Terminal Service). Along with the encryption offered by Terminal Services, VPN has the ability to be encrypted.

Support of Virus Scanning

Support for Terminal Service is available in Norton Anti-virus Corporate Edition version 7.6. (Norton AntiVirus Corporate Edition 7.6 and Terminal Server

support). Features of Norton Anti-virus would help in preventing a user from logging onto Terminal Service and uploading a virus or a Trojan horse.

Norton Antivirus Corporate Edition also provides the ability to log viruses to a central location. If a user happened to upload a virus or a Trojan horse to the Terminal Server, Norton AntiVirus would delete or quarantine the suspected file and log the event. The example on the next page shows the logging capability of Norton AntiVirus.



Conclusion

Windows Terminal Service can be a valuable tool for the network administrator, especially when the server is physically located in a different site. Since anyone with the required software can access the server remotely, careful consideration must be used when installing and using Terminal Service. By using the recommendations outlined in this report, the administrator can establish a secure environment to run Terminal Service.

References

1) Mackey, David. "Securing Windows 2000 Terminal Service" URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/win2kts/maintain/optimize/secw2kts.asp (10 Jun. 2002).
2) "Terminal Server Walkthrough: Startup, Connection, and Application (Q186572)" 17 Dec. 1998. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q186572 (10 Jun 2002).
3) "Chapter 16 – Deploying Terminal Services" URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/reskit/deploy/part4/chapt-16.asp (10 Jun. 2002).
4) Microsoft Corporation. "Using Terminal Services for Graphical Remote Administration of the Windows 2000 Server Family" 1999. URL: http://www.microsoft.com/windows2000/docs/TSRemote.doc (11 June. 2002).
5) Microsoft Corporation "Explanation of RDP-TCP Permissions in Windows 2000 (Q243554)" 1 Dec. 1999. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q243554 (10 Jun 2002).
6) Microsoft Corporation "Rdpclip.exe: File Copy". URL: http://www.microsoft.com/windows2000/techinfo/reskit/tools/hotfixes/rdpclip-o.asp (12 Jun 2002).
7) DiMaria, Vincent J., James F. Barnes, CDR Jerry L. Birdsong, Kathryn A. Merenyi. "Guide to Securing Microsoft Windows 2000® Terminal Service". 1.0. 2 Jul 2001. URL: http://nsa2.www.conxion.com/win2k/guides/w2k-19.pdf (12-Jun-2002).
8) Microsoft Corporation. "To configure settings for mapping client devices". 28 Feb. 2000. URL: http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/ts_con_h_120.htm (13 Jun 2002).
9) Symantec Corporation. "Norton AntiVirus Corporate Edition 7.6 and Terminal Server support". 7 Jun 2002. URL: http://service4.symantec.com/SUPPORT/ent-security.nsf/docid/2001092012091148 (13 Jun 2002).
10) Bragg, Robert. "Securing Terminal Service". URL: http://www.101com.com/solutions/security/article.asp?ArticleID=531 (13 Jun 2002).
11) Symantec Corporation. "Norton AntiVirus™ Corporate Edition 7.6". URL: http://enterprisesecurity.symantec.com/products/products.cfm?productID=23 (15 Jun 2002).