



realtimepublishers.com[™]

The Definitive Guide[™] To

Windows 2000 Terminal Services

NEW MOON) SYSTEMS[™]

Greyson Mitchem

Chapter 6: Securing Terminal Services.....	118
Using Encryption.....	118
Logon Security	120
Virus Protection.....	120
Critical Updates and Internet Explorer Maintenance.....	120
Access Through a Firewall.....	120
Implementing Terminal Services in an Extranet Environment.....	121
Application-Layer Security.....	122
File and Registry Security.....	124
Remote Access	125
Advantages of Using Terminal Services for Remote Access	125
Summary	126
Afterword: The Future of Terminal Services.....	127
RDP 5.1	127
Remote Desktop	128
Remote Assistance	129
Windows .NET Server	130
Third-Party Products	131
Summary	131

Chapter 6: Securing Terminal Services

In today's world of hackers, crackers, and viruses, security is a top priority for any technology organization. Terminal Services provides IT departments a new set of tools for providing access to the corporate LAN and to vertical applications, but it also presents a unique set of security challenges. Fortunately, with proper planning and implementation, deploying a secure Terminal Services infrastructure can be accomplished.

In this chapter, we will look at a number of security issues that arise when using Terminal Services, and I will present you with options for addressing them. Keep in mind that as with most IT infrastructure designs, there are many ways to accomplish a given task. Your environment might have its own unique security requirements that can either eliminate some of the options I will offer, or present entirely new ways of securing your Terminal Services design. The topics we will cover in this chapter include encrypting RDP, accessing a terminal server through a firewall, deploying a terminal server in an extranet environment, and using remote access strategies.

Using Encryption

Your first line of security when using Terminal Services is encryption. Unlike the traditional computing model, which transfers entire files from the server to the client, Terminal Services typically sends only video data and metafiles to the user. So, even if the data stream could be decrypted, a hacker would only be able to see fragmented bits of images rather than capture a sensitive file. We are more concerned about protecting the keystrokes that the user is sending back to the terminal server—a hacker could theoretically reconstruct a password or even an entire document from this data stream. As a result of this possibility, the data sent from the client to the server is always encrypted, even in low encryption mode.

When you configure RDP on your server, you can select one of three levels of encryption for the server to use. The default encryption level is medium, as Figure 6.1 shows.

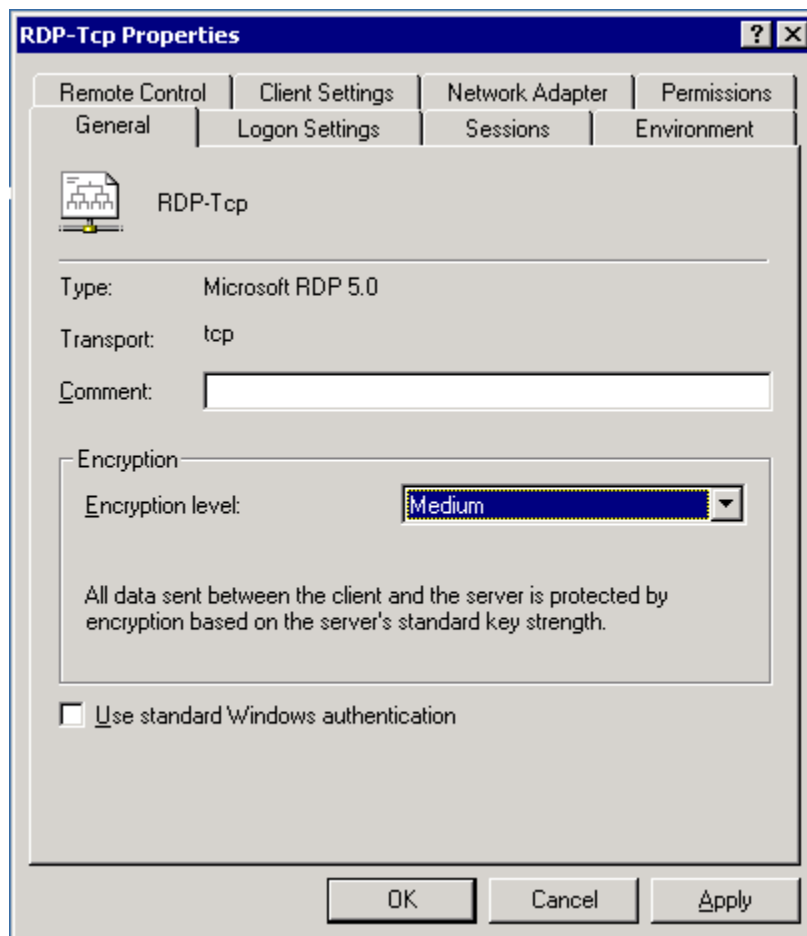


Figure 6.1: Setting the encryption level for RDP.

Microsoft defines the three encryption levels as follows:

- **Low**—With low encryption, traffic from the client to the server is encrypted using the RC4 algorithm and a 56-bit key (40-bit key for RDP 4.0 clients); whereas traffic from the server to the client is unencrypted. Low encryption protects sensitive data such as password entry and application data. The data sent from the server to the client is screen refreshed, which is difficult to intercept even when unencrypted.
- **Medium**—With medium encryption, traffic in both directions is encrypted using the RC4 algorithm and a 56-bit key (40-bit key for RDP 4.0 clients).
- **High**—With high encryption, traffic in both directions is encrypted using the RC4 algorithm and a 128-bit key. In the export version of Terminal Services, high encryption uses the RC4 algorithm and a 56-bit key (40-bit for RDP 4.0 clients).

The bandwidth overhead that is added by using medium encryption is negligible. Thus, unless you have unique networking conditions, I recommend using the default setting even when working within the safety of a corporate network.

Logon Security

If you have implemented some kind of token-based or biometric security in your Windows environment, you must deal with the fact that Terminal Services does not natively support this type of authentication. So, if your security guidelines require it, you will have to place the terminal server behind an authentication server or find a third-party authentication product that supports Terminal Services.

Virus Protection

At one time, an acceptable practice was to not install virus protection software on terminal servers. The software products that were available were not designed for terminal servers and tended to develop memory leaks in a multi-user environment. So administrators did their best to protect the systems using very restrictive access control lists (ACLs) on the file system and registry. Unfortunately, viruses have evolved to a point at which ACLs are no longer a sufficient barrier. Many viruses take advantage of security holes in the OS and applications to function under the system context. Luckily, virus protection software has also evolved, and today there are a number of products available that will function well on a terminal server.

☞ When selecting virus protection software, be sure to choose a product that will allow you to update the virus definition files without rebooting. Otherwise, you will be forced to interrupt your users if you need to apply an emergency update during operating hours. Also, many products use a system-tray icon as a status monitor. Having this monitor program run in each user's session isn't necessary, so you might want to contact the software publisher and see if it can be disabled.

Critical Updates and Internet Explorer Maintenance

If names like Melissa and NIMDA send chills down your spine, you are already aware of the pains we systems administrators go through to keep our systems secure. As new security holes are discovered, Microsoft is quick to release patches and updates for both Win2K and Internet Explorer (IE). Using terminal servers greatly simplifies the deployment of these critical updates. Installing a security patch on a few servers is much easier than deploying the patch to a thousand desktops. To stay up to date on security patches, subscribe to Microsoft's security newsletters at <http://www.microsoft.com/security>.

☞ Most critical updates require the system to be rebooted, so be sure to disable new logons and force any existing users to log off before installing the update. You can disable new logons from a command line using the command

```
CHANGE LOGON /DISABLE
```

Access Through a Firewall

RDP communicates over the TCP port number 3389. If you need to access a terminal server on the other side of a firewall, this port must be open. Also, you must be able to find the server—either by hostname or IP address, so the server must have a routable IP address or utilize port forwarding on your router. (You'd be surprised how many people forget that.) You might want

to only allow inbound port 3389 traffic to the specific IP addresses of your terminal servers or allow outbound traffic on port 3389 only to trusted terminal servers on the outside. Figure 6.2 shows the data flow when accessing a terminal server on either side of a firewall.

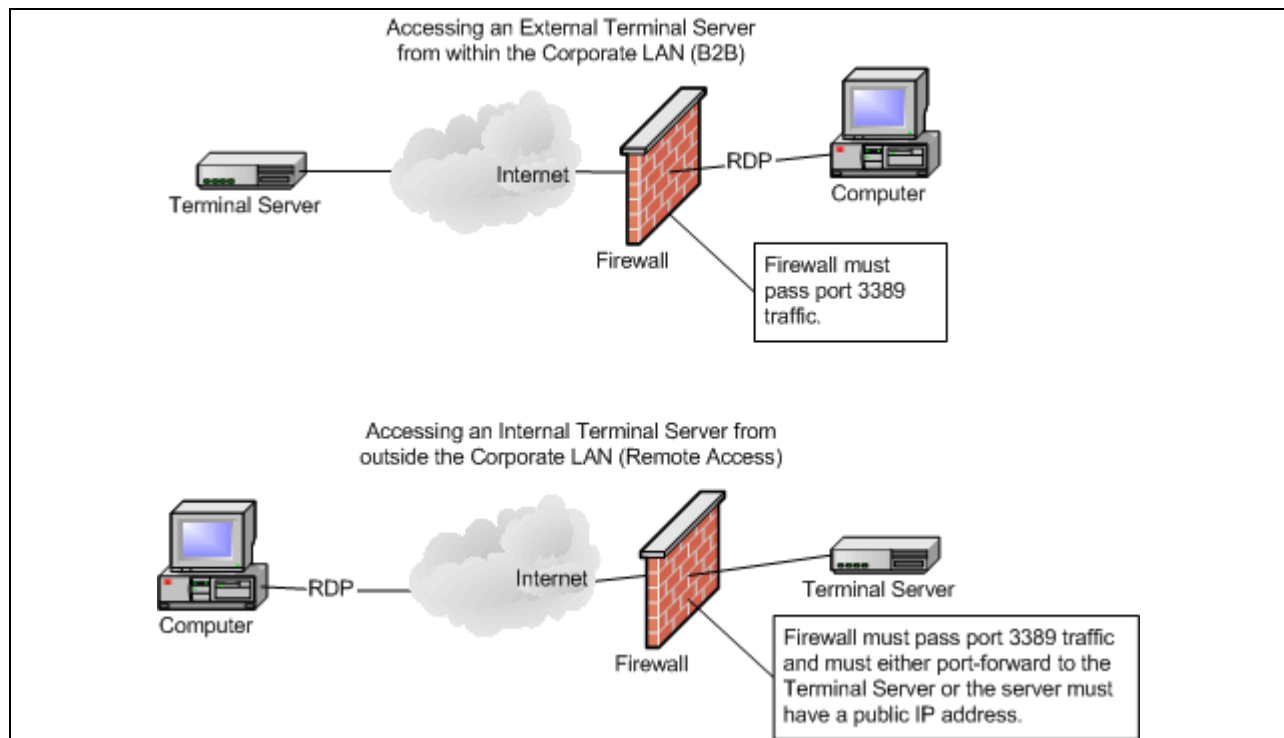


Figure 6.2: Accessing a terminal server through a firewall.

Another, often more tempting, option when your users need to access a terminal server on the outside of a firewall is to use a Windows Sockets (SOCKS) proxy. Unfortunately, using a SOCKS proxy is only possible when you use the Citrix Independent Computing Architecture (ICA) protocol. At this point, Microsoft’s RDP client does not support connections by way of SOCKS.

Implementing Terminal Services in an Extranet Environment

As a result of the many complex data flows required by today’s business-to-business (B2B) marketplace, many enterprises are building extranets at the periphery of their LANs. This setup enables them to place systems in a “buffer zone” in which they have control over access from both the external networks as well as the intranet. If you are deploying a vertical application to which both internal and external users require access, then an extranet may be the perfect solution.

Think of an extranet as a network segment with firewalls at both the trusted and untrusted sides. One major advantage to this model when using Terminal Services is that once an outside user has established a session on the terminal server, the user still does not have full access to the corporate LAN—only to systems, IP addresses, and ports that you have specified on the trusted-side router. Figure 6.3 shows a simplified version of this model.

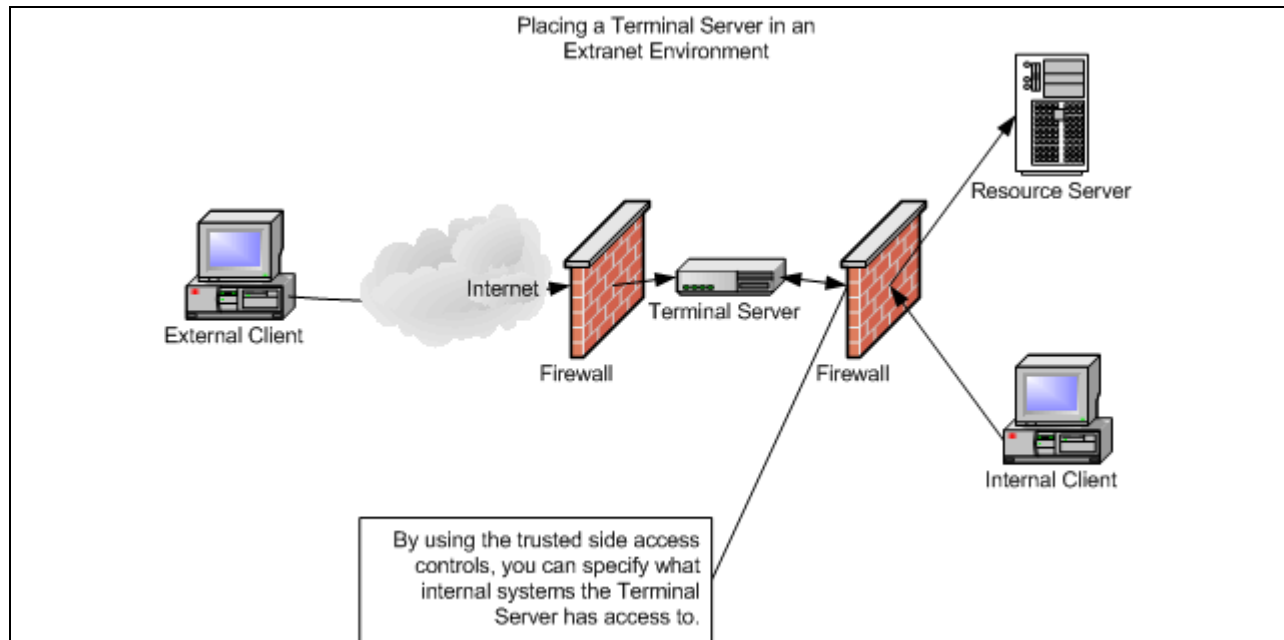


Figure 6.3: Placing a terminal server in an extranet.

👉 If users of a terminal server in the extranet require access to internal domain resources, you will need to define data flows for domain authentication on the internal access controls.

Application-Layer Security

After you have determined how your users will gain access to the terminal server itself, you can implement application-layer security on the terminal server. You do so by using a resource kit utility called the Application Security tool, or AppSec, and implementing a Group Policy—either domain or local—that restricts which executables users of the terminal server can invoke.

🔴 The version of AppSec that is included with the Win2K resource kit is missing required files. To update your kit, download AppSec.zip from <ftp://ftp.microsoft.com/reskit/win2000>.

With AppSec, you define a list of executables that non-administrators can invoke. AppSec monitors the CreateProcess application programming interface (API) thread and only allows specified processes to be created. When you first launch AppSec, you will see a predefined list of applications that are allowed. These executables are required for the system to run, and you should not remove them without serious testing. Figure 6.4 shows the AppSec interface.

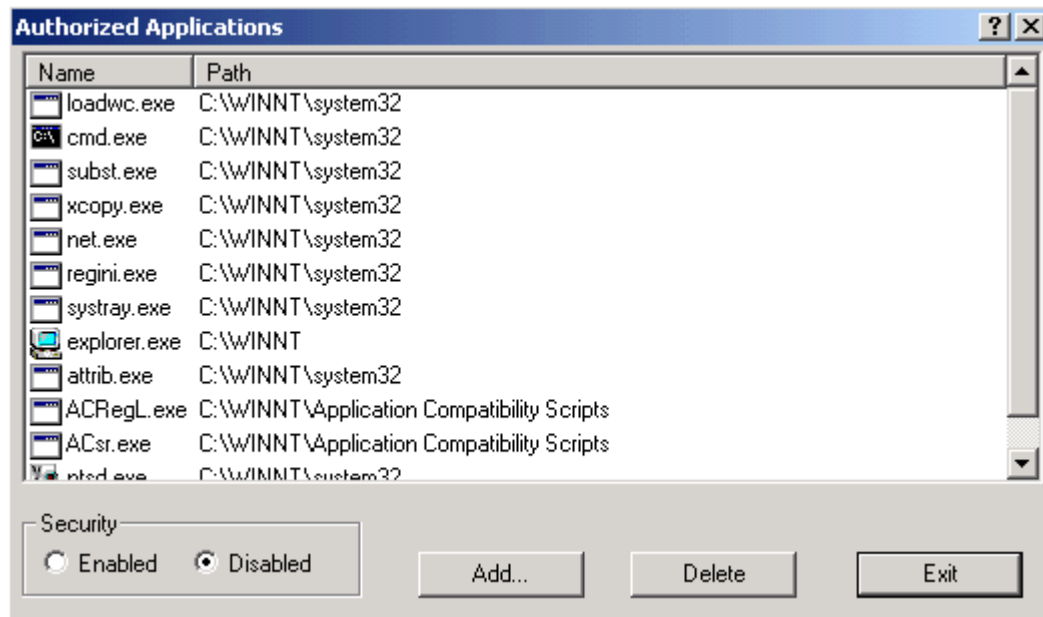


Figure 6.4: The AppSec utility.

When you enable AppSec security, 16-bit applications are disabled by default. If your users need access to any 16-bit programs, you must add NTVDM.EXE to the access list.

In addition to enabling application security, you will also want to apply the *Run only allowed Windows applications* policy. This policy prevents users from seeing disallowed applications in their Start menu, as well as adding a second layer of security by preventing the system from invoking other application from Explorer or a Run command. This setting is found in the Group Policy Editor under User Configuration, Administrative Templates, System. Figure 6.5 shows the editor for this policy.

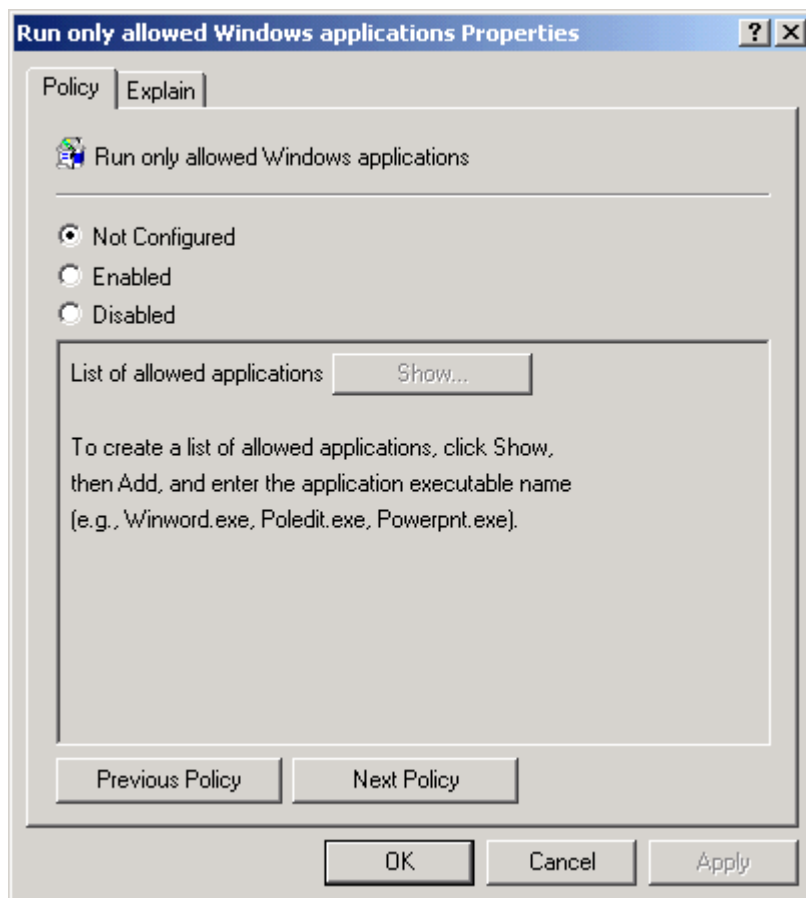


Figure 6.5: Setting the Run only allowed Windows applications Group Policy.

You should be aware that if you do not take precautions by restricting file-level access, a malicious user could bypass both AppSec and the policy by renaming an executable, then invoking it. Both security measures monitor threads by name, so by renaming WINWORD.EXE to SYSTRAY.EXE, a user could start Word because SYSTRAY is an allowed program.


File and Registry Security

Back in Chapter 2, you saw that there are two options for local file and registry permissions—Win2K permissions and NT 4.0 WTS permissions. You can select the permission mode when installing Terminal Services, and change it using the Terminal Services Configuration administrative tool.

Microsoft does not provide any explicit documentation about the exact differences between the two modes other than stating that in NT 4.0 compatibility mode, users have full access to critical registry and file system locations. Thus, if you are required to run a terminal server in NT 4.0 compatibility mode because of a legacy application, you should take extra care to be sure that registry-editing tools and access to the hard drive of the terminal server are disabled in your users' Group Policies.

Better yet, use registry and file-access monitoring tools to pinpoint the exact keys and files to which the legacy application needs access and manually grant permission to those files. That

way, you can run the terminal server in Win2K mode and protect the rest of the HKEY_LOCAL_MACHINE registry key and the file system.

 Winternals Software publishes excellent file and registry monitoring tools that are available at (<http://www.winternals.com>).

For example, if an application errors out under Win2K permissions mode for a user who is not in the Administrators group, and the application runs correctly under NT 4.0 compatibility mode, you would leave the server in NT 4.0 compatibility mode and run the application while using a file-access monitoring tool. The logs generated by the monitoring utility may indicate that the application needs write access to the program's application directory. You would then grant the Authenticated Users group write permission on that specific directory under C:\Program Files, leaving the rest of the Program Files directories protected.

Now change the server back to Win2K permission mode and test the application again using a non-administrative account. If the application now runs, you can add this ACL change to your installation documentation and continue to benefit from the safety of Win2K permission mode. You can diagnose and correct registry permission problems in the same way.

Remote Access

If you are implementing Terminal Services as a remote access option for your users, often, a desirable option is to use security measures that are independent of the terminal server. This way, you can treat the server as just another workstation within the corporate LAN.

There are many options for a secure remote-access model, and most organizations will already have one in place. Terminal Services will function as long as your Remote Access Service (RAS) model supports TCP/IP connectivity and will pass port 3389. You can use a virtual private network (VPN), Point-to-Point Tunneling Protocol (PPTP), IP Security (IPSec), HTTP over Secure Sockets Layer (HTTPS), and any of the token-based security measures that are common today. Once a user has been granted trusted access to the LAN, connecting to the terminal server and logging onto the domain become easy.

Advantages of Using Terminal Services for Remote Access

When designing your remote access infrastructure, you might want to consider using the terminal server as a portal to the corporate LAN. This way, in addition to the security measures that your RAS solution provides, you can further restrict access by only allowing port 3389 and requiring that all remote users work through Terminal Services.

Most security administrators see Terminal Services as a great tool for locking down the access that external users have. The terminal server, or cluster of terminal servers, becomes a single point of entry which can be easily monitored, audited, and disabled if necessary.

Summary

Terminal servers centralize your computing environment, often making it easier to secure. They also provide new options for your remote-access strategy. If proper care is taken when designing and deploying Terminal Services, you can create an environment that is highly stable and secure.

If you take Terminal Services security in layers—starting with RDP encryption to communicate with the terminal server and moving outwards in your design from registry, file, and application security—by the time you reach the secure boundary of your corporate LAN, you can easily implement a routing or remote access solution that meets your needs. Be sure to work closely with your network engineers to come up with a design that pleases everyone.

Afterword: The Future of Terminal Services

There are many changes coming in the landscape of Terminal Services technology. New products are being released to take advantage of centralized computing and enhancements to RDP are being made. Microsoft has even integrated Terminal Services technology into their new desktop OS—Windows XP. I'll show you a few of the new options that are on the horizon so that you can keep them in mind as you design your Terminal Services infrastructure.

RDP 5.1

Perhaps the greatest change to the Terminal Services landscape is RDP 5.1. This new protocol is available today as part of Windows XP, and you can download the new Remote Desktop client from Microsoft's Web site at

<http://www.microsoft.com/windowsxp/pro/downloads/rdclientdl.asp>

This new client supports both the Remote Desktop functionality of Windows XP as well as RDP 4.0 and 5.0 connections to existing terminal servers. The client also includes support for connection files (text files with a file extension of .RDP), which allow you to save, edit, and distribute connection definitions without having to edit the registry. Figure A.1 shows the new interface.

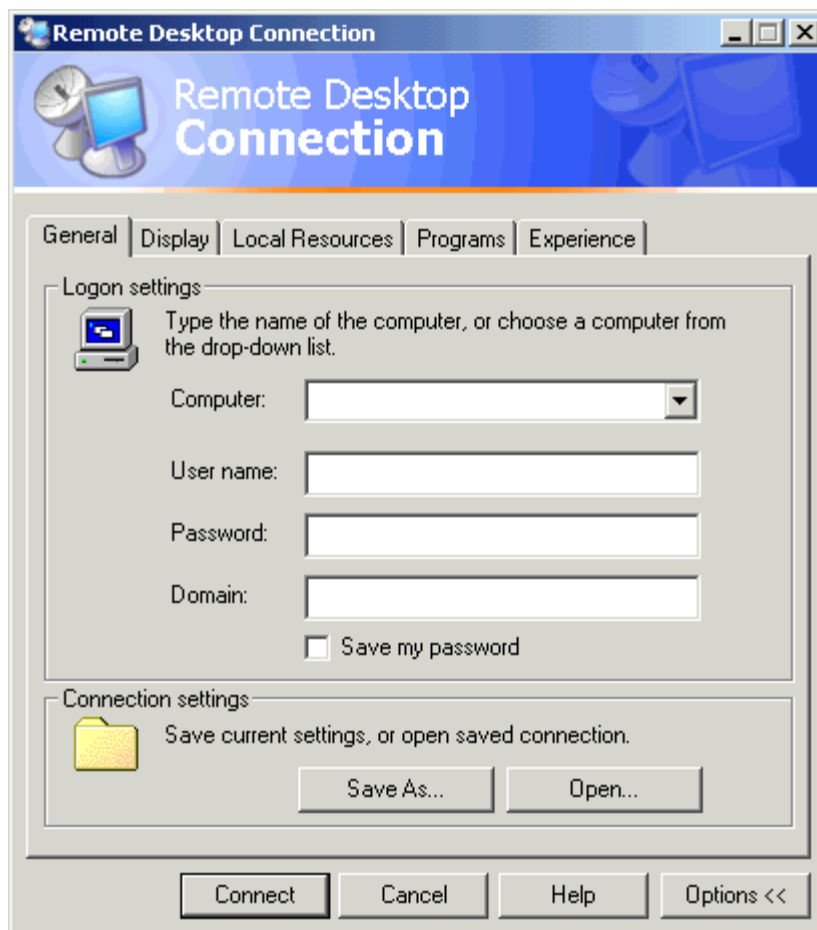


Figure A.1: The new Remote Desktop connection client interface.

RDP 5.1 will also be available on Microsoft's upcoming Windows .NET Server platform—the successor to Win2K Server. The new version of the protocol adds native support for client drive mapping, audio, and a new connection bar that users can “pin” to the top of their screen during full-screen Terminal Services sessions. The connection bar lets you easily determine which server or Remote Desktop you are working on.

Video resolution and color depth are also enhanced in RDP 5.1. The protocol now supports as high as 24-bit color (although the client GUI offers only as high as 16-bit support). Figure A.2 shows the Display configuration tab of the new client.

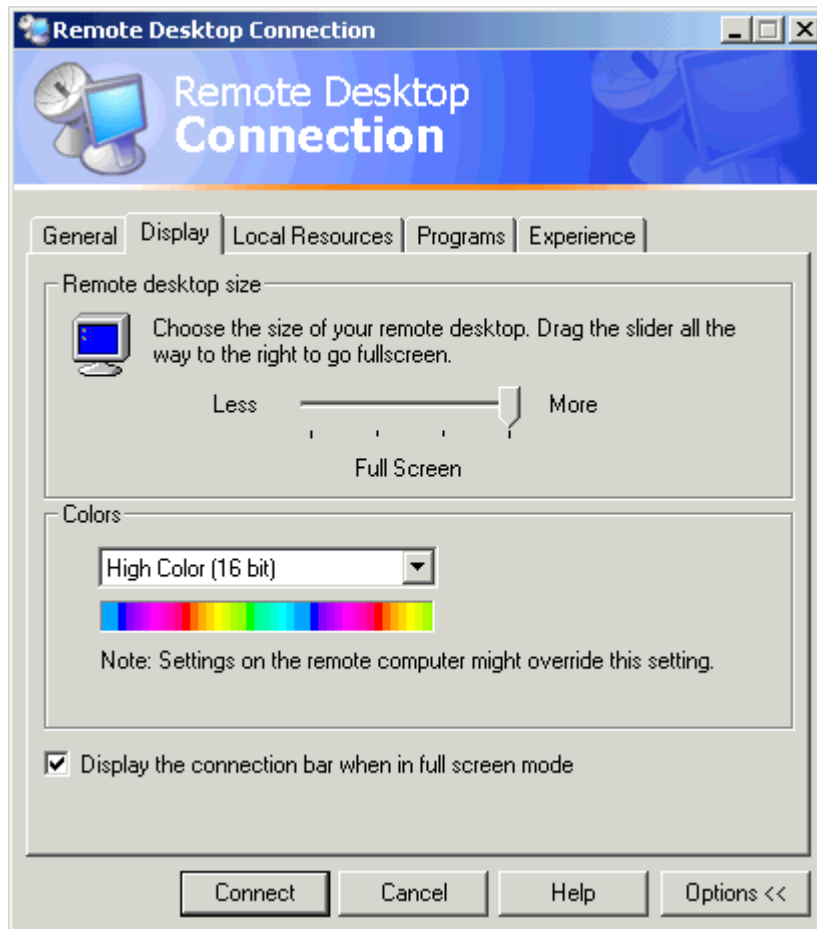


Figure A.2: The Display configuration tab of the RDP 5.1 client.

Remote Desktop

Windows XP Professional includes a new feature called Remote Desktop. This functionality takes advantage of Microsoft's Terminal Services technology and the new RDP 5.1 protocol to allow you to remotely connect to your workstation. With Remote Desktop enabled, you can redirect your video, keyboard, and mouse from the local console to the RDP stream, thus making your computer available from anywhere on the network.

This ability might completely change how we use Terminal Services for remote access and mobile enterprise users. Why connect to a terminal server that offers a generic set of applications

when you can connect directly to your personal computer and have the exact same experience and applications that you have at your office?

Terminal Services will certainly maintain its place as the platform of choice for the application service provider (ASP) model and B2B connectivity. And the advantages of thin client devices will still play a role in larger homogeneous computing environments because these devices virtually eliminate end-node support and increase the hardware lifecycle far beyond that of a traditional PC.

Remote Assistance

If you have supported users in a Terminal Services environment, you know the advantages of using Remote Control. With this ability, you can assist your users in configuring their applications, demonstrate processes to new users, and correct technical problems without visiting the user's desk. Windows XP's Remote Assistance offers these same abilities on the desktop platform. Remote Assistance also takes advantage of Terminal Services technology and the RDP 5.1 protocol to enable support personnel to shadow their users. Remote Assistance requires that the computers at both ends of the connection be using Windows XP.

Both Remote Desktop and Remote Assistance are configured through the System Control Panel applet on Windows XP, as Figure A.3 shows. In an enterprise, you can also configure these features through Group Policy. You can specify which users and groups can request or provide Remote Assistance, and select users and groups that can open Remote Desktop connections.

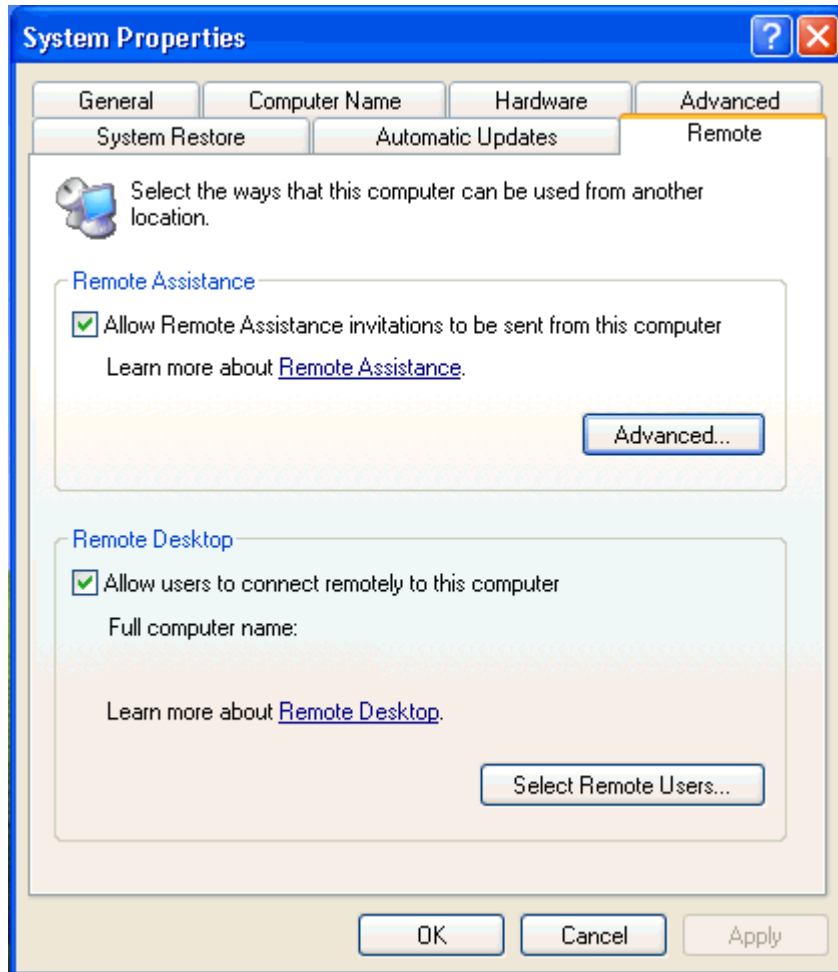


Figure A.3: Configuring Remote Assistance and Remote Desktop in the System Control Panel applet.

Windows .NET Server

The current beta of Microsoft Windows .NET Server offers a number of enhancements to Terminal Services. First, in .NET Server, Microsoft has separated all Terminal Services-related parameters of user accounts into their own attributes, so administrators can now populate, query, and modify these settings through standard Active Directory Service Interfaces (ADSI) calls.

In addition, .NET Enterprise Server and .NET Datacenter Server feature a new technology called Terminal Services Session Directory, which will enhance a user's ability to reconnect to an active session on a terminal server cluster.

All versions of .NET Server also include the new RDP 5.1 protocol and a new advanced client.

 For more information about Windows .NET Server, see <http://www.microsoft.com/windows.netserver/>

Third-Party Products

As Microsoft releases these new technologies, third-party application vendors will be enhancing their products as well. I'm sure in the near future we will see such technologies as integrated file associates for applications provided by a Terminal Services ASP solution. Imagine being able to double click on a .DOC file on a network share and have your system automatically spawn a connection to a terminal server that provides you with Microsoft Word.

Hardware vendors are also keeping in stride. There are now thin client devices integrated into flat-panel monitors and tablet devices that use 802.11 wireless LAN to connect you to a terminal server. New Pocket PC devices can natively communicate with terminal servers, so we may soon see Win32 applications designed specifically for that form factor.

Summary

As we look to these new technologies over the next year, the gap between locally installed applications and Terminal Services/ASP applications will become much smaller. We, as Terminal Services administrators, will have an easier time selling the benefits of Terminal Services when there are fewer differences for the end user.

Also, in a desktop replacement environment, more and more application vendors are complying with the Microsoft Windows Logo specification, so application integration on Terminal Services is becoming easier. I am already seeing more and more terminal servers without a single application compatibility script, and I spend less and less of my time creating wrappers and special installation instructions for legacy programs.

If you work in a mixed Terminal Services and workstation environment, be sure to get involved in the Windows XP deployment. You will need to take XP's new features into account when planning for the future of your terminal servers. And your experience and knowledge with Terminal Services technologies will make the integration of Remote Desktop and Remote Assistance much easier for your enterprise. It is an exciting time for Windows technologies, and Terminal Services will play an important role as computing becomes more mobile and pervasive.

I'd like to thank you all for reading *The Definitive Guide to Windows 2000 Terminal Services*. I have enjoyed writing it. I'd like to thank the people that helped me make this book as accurate and detailed as it is—Scott Hill, my technical editor; Laurie Nocella, my style editor; everyone at New Moon; my partner, Michel, for all the encouragement, and of course, Sean Daily and David Templeton of Realtimerepublishers for making it all happen.

Copyright Statement

© 2001 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com