realtimepublishers.com™

The Definitive Guide™ To

Windows Server 2003 Terminal Services

triCerat Software®

Gresyon Mitchem

Introduction

By Sean Daily, Series Editor

Welcome to *The Definitive Guide to Windows Server 2003 Terminal Services*!

The book you are about to read represents an entirely new modality of book publishing and a major first in the publishing industry. The founding concept behind Realtimepublishers.com is the idea of providing readers with high-quality books about today's most critical IT topics—at no cost to the reader. Although this may sound like a somewhat impossible feat to achieve, it is made possible through the vision and generosity of corporate sponsors such as triCerat, who agree to bear the book's production expenses and host the book on its Web site for the benefit of its Web site visitors.

It should be pointed out that the free nature of these books does not in any way diminish their quality. Without reservation, I can tell you that this book is the equivalent of any similar printed book you might find at your local bookstore (with the notable exception that it won't cost you $30 to $80). In addition to the free nature of the books, this publishing model provides other significant benefits. For example, the electronic nature of this eBook makes events such as chapter updates and additions, or the release of a new edition of the book possible to achieve in a far shorter timeframe than is possible with printed books. Because we publish our titles in "real-time"—that is, as chapters are written or revised by the author—you benefit from receiving the information immediately rather than having to wait months or years to receive a complete product.

Finally, I'd like to note that although it is true that the sponsor's Web site is the exclusive online location of the book, this book is by no means a paid advertisement. Realtimepublishers is an independent publishing company and maintains, by written agreement with the sponsor, 100% editorial control over the content of our titles. However, by hosting this information, triCerat has set itself apart from its competitors by providing real value to its customers and transforming its site into a true technical resource library—not just a place to learn about its company and products. It is my opinion that this system of content delivery is not only of immeasurable value to readers, but represents the future of book publishing.

As series editor, it is my raison d'être to locate and work only with the industry's leading authors and editors, and publish books that help IT personnel, IT managers, and users to do their everyday jobs. To that end, I encourage and welcome your feedback on this or any other book in the Realtimepublishers.com series. If you would like to submit a comment, question, or suggestion, please do so by sending an email to feedback@realtimepublishers.com, leaving feedback on our Web site at www.realtimepublishers.com, or calling us at (707) 539-5280.

Thanks for reading, and enjoy!

Sean Daily

Series Editor

Copyright Statement

© 2003 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.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

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.

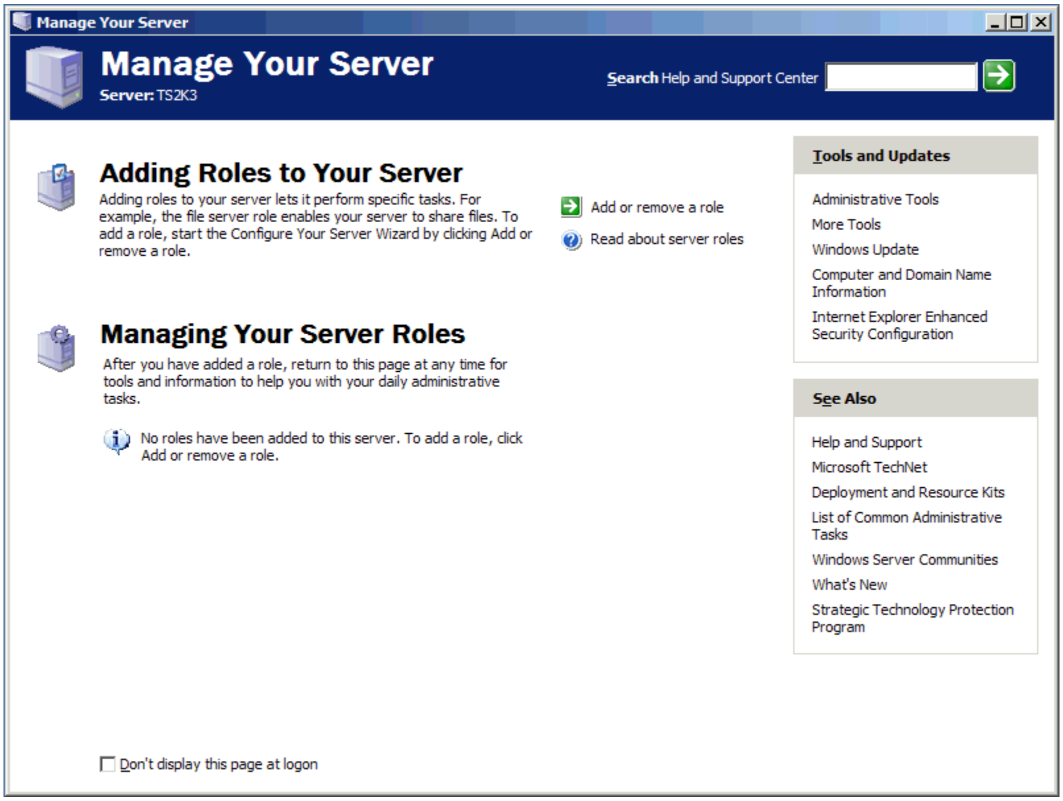
Chapter 1: Introduction to Windows Server 2003 Terminal Services

With the launch of Windows Server 2003 (WS2K3), Microsoft has continued to improve upon Terminal Services. At the launch event, Microsoft focused on the fact that this version of Windows is the most customer driven to date. Terminal Services' new features clearly demonstrate this focus—there are certainly several enhancements that I have been hoping for.

In this book, I will introduce you to the new features and enhancements in WS2K3 Terminal Services. I will also discuss best practices for configuring and managing Terminal Services with an eye to the new techniques available to systems administrators in WS2K3. As we'll explore, with Remote Desktop Protocol (RDP) 5.2, Active Directory Service Interfaces (ADSI) access to Terminal Services attributes of user objects, new Group Policy Object (GPO) controls, and Session Directory, we now have the ability to use native Terminal Services as an enterprise-class solution for providing users with Terminal Services–based desktops.

Server Roles

When you install WS2K3, most non-critical subsystems and services are disabled or not installed. The reason for this default configuration is Microsoft's new focus on security. Because the system is secure by default, systems administrators can focus on designing systems that perform only desired functions and not worry about server hardening as much. To help enable desired functions, Windows now offers Server Roles, as Figure 1.1 shows.


Manage Your Server
Manage Your Server
Server: TS2K3
Search Help and Support Center
Tools and Updates
Administrative Tools
More Tools
Windows Update
Computer and Domain Name Information
Internet Explorer Enhanced Security Configuration
See Also
Help and Support
Microsoft TechNet
Deployment and Resource Kits
List of Common Administrative Tasks
Windows Server Communities
What's New
Strategic Technology Protection Program
Add or remove a role
Read about server roles
□ Don't display this page at logon

Adding Roles to Your Server

Adding roles to your server lets it perform specific tasks. For example, the file server role enables your server to share files. To add a role, start the Configure Your Server Wizard by clicking Add or remove a role.

Managing Your Server Roles

After you have added a role, return to this page at any time for tools and information to help you with your daily administrative tasks.

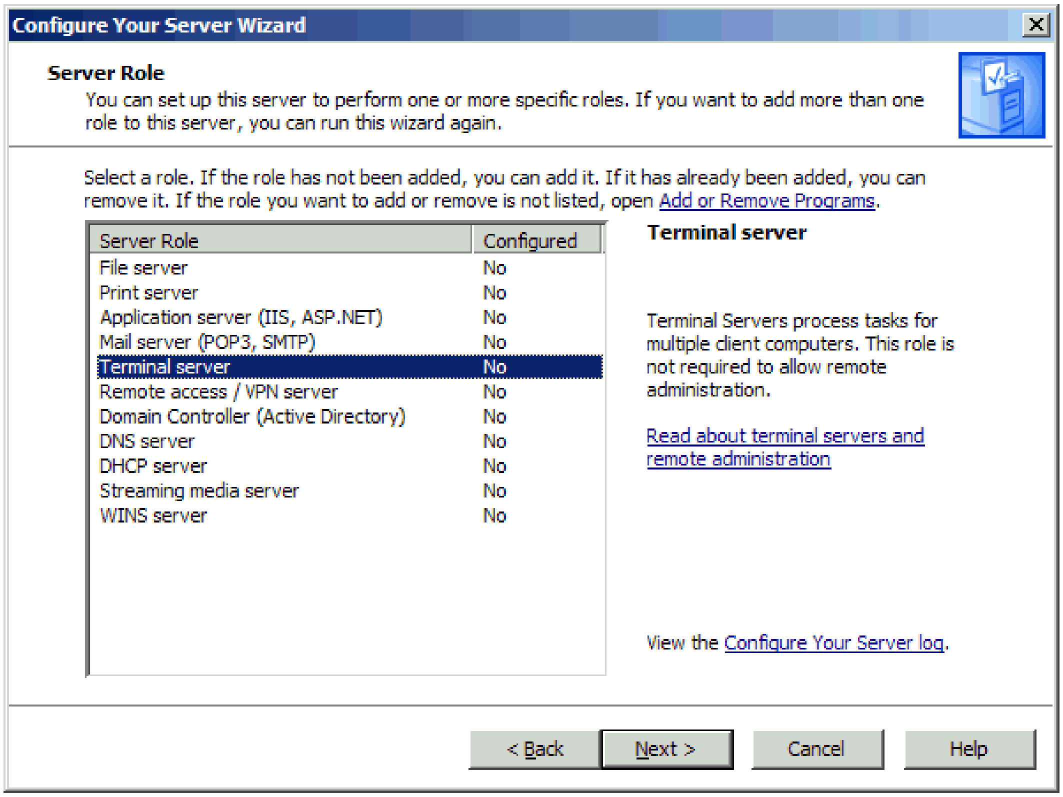
No roles have been added to this server. To add a role, click Add or remove a role.

Figure 1.1: The Manage Your Server wizard.

A *role* is a server function (for example, mail server, domain controller). A single server can perform more than one role if desired, enabling you to do more with less—the slogan for WS2K3. When an administrator logs on to a server, the Manage Your Server wizard offers to assist in adding new roles and managing currently installed roles.

When adding a new role, the Manage Your Server wizard enables services and performs any security changes required by the role. You can still add and remove services the old-fashioned way through the Add/Remove Windows Components and Services Control Panel applet, but I find that the Manage Your Server Wizard is very useful. (The useable wizard in WS2K3 is quite a change from the one in Windows 2000—Win2K; most of us disabled the Win2K Configure Your Server wizard at first boot.)

After you add a role, the Manage Your Server wizard provides easy access links to common tools and settings used for each role. Figure 1.2 shows the default roles available in WS2K3 Standard Edition.



Server Role

You can set up this server to perform one or more specific roles. If you want to add more than one role to this server, you can run this wizard again.

Select a role. If the role has not been added, you can add it. If it has already been added, you can remove it. If the role you want to add or remove is not listed, open Add or Remove Programs.

Server Role	Configured
File server	No
Print server	No
Application server (IIS, ASP.NET)	No
Mail server (POP3, SMTP)	No
Terminal server	No
Remote access / VPN server	No
Domain Controller (Active Directory)	No
DNS server	No
DHCP server	No
Streaming media server	No
WINS server	No

Terminal server

Terminal Servers process tasks for multiple client computers. This role is not required to allow remote administration.

Read about terminal servers and remote administration

View the Configure Your Server log.

Figure 1.2: Default roles available in WS2K3 Standard Edition.

File Server

Adding the file server role optimizes the server for network shares and file storage. After adding the file server role, you will be able to set disk space quotas for users, use the indexing service to search for files, and even search for documents in different formats and languages by using the Start menu's Search tool or a new Web-based search interface. WS2K3 offers many new features to improve file serving:

- Shadow copy—Maintains byte-level backups of previous versions of documents to allow end users to undo changes made to documents stored on the server.
- Enhanced Distributed File System (DFS)—Lets you create a single logical namespace for multiple shares spanning servers across the enterprise. This functionality keeps your end users from having to memorize the server names for shares they frequently use. WS2K3's DFS also provides a robust file replication service with topology choices not available in Win2K. In addition, WS2K3 servers can host more than one DFS root.
- Volume shadow copy service—Creates a point-in-time copy of the original data share. Backup programs can use this copy to make a share appear static while the actual documents are changing. In addition, you can move shadow copies to other servers for backup, testing, and data mining.

Print Server

Print servers are used to provide and manage access to printers. The print server role lets you manage printers through a Web browser, send print jobs to a printer's URL using the Internet Printing Protocol (IPP), and connect to printers using Point and Print. Microsoft has made several enhancements to printing services in WS2K3:

- Print cluster support—Automatically replicates printer drivers to all servers in the cluster
- Active Directory (AD) enhancements—Lets administrators publish printers in AD so that users can search for printers based on location, color, and speed
- Security enhancements—Includes new Group Policies that let administrators prevent managed clients from connecting to untrusted print cues and prevent connections to the print spooler if the server is not providing print services

Application Server

When you configure a server to be an application server, you are installing Internet Information Services (IIS) 6.0 as well as several optional technologies and services such as COM+ and ASP.NET. Microsoft has optimized IIS 6.0 for Web server reliability, server management and consolidation, faster application development, and increased security.

WS2K3's application server role provides support for new Web services and the .NET platform, including enterprise Universal Description, Discovery, and Integration (UDDI) services as well as Simple Object Access Protocol (SOAP) and Web Services Description Language (WSDL). Application servers are often configured to include:

- Resource pooling
- Distributed transaction management
- Integrated security
- Failover and application health detection services

Mail Server

WS2K3 now offers a Post Office Protocol 3 (POP3) and Simple Mail Transfer Protocol (SMTP) server option. This option lets you manage basic email accounts for your users and enables users to send and retrieve mail from the server. Mail servers provide email transfer and retrieval services. User email can be stored on the server until retrieved by a POP3 client. To utilize the mail server role, you must have:

- An active Internet connection
- A registered email domain name
- A registered mail exchanger (MX) record for your email domain with your Internet Service provider (ISP)

Terminal Server

By installing the terminal server role, you enable users to connect to the server to run applications as if the applications were installed on users' workstations. I will discuss the installation, configuration, and new features of the terminal server role throughout the book. Unlike Win2K, which immediately grants access to all users when Terminal Services is installed, WS2K3 restricts access by default to administrators only. You must add users or groups to the Remote Desktop Users group to enable access.

Remote Access/VPN Server

Remote access and virtual private network (VPN) servers provide an entry point into your network for remote users. By using the remote access/VPN server role, you can implement routing protocols for both LAN and WAN environments. This role supports both dial-up connections and VPN connections over the Internet.

Domain Controller

Domain controllers maintain the AD database. Domain controllers provide authentication services for users and computers and control access to network resources. The domain controller role replaces the DCPROMO tool that Win2K provides. This role lets you add a domain controller to an existing domain, create a new domain in an existing forest, and create a new forest.

DNS Server

The Domain Name System (DNS) is the TCP/IP name resolution service that is used on the Internet. DNS lets computers resolve Fully Qualified Domain Names (FQDNs) to IP addresses. The implementation of DNS that WS2K3 includes is a Dynamic DNS (DDNS) service, which means that computers can self register into the DNS database. The WS2K3 implementation of DNS also offers integration with the Windows Internet Naming Service (WINS) server role to allow non-NetBIOS clients to resolve NetBIOS names via DNS.

DHCP Server

A Dynamic Host Configuration Protocol (DHCP) server will enable your TCP/IP-based clients to be automatically assigned an IP address when needed. The DHCP server can also provide additional network configuration information—DNS server IP addresses, WINS server addresses, and so on—to the clients. Having a server with the DHCP role installed greatly reduces the time required to set up and configure clients on your network.

Streaming Media Server

Streaming media servers provide Windows Media Services to network clients. Windows Media Services manages and delivers Windows Media content—streaming audio and video—over an intranet or the Internet.

WINS Server

WINS lets NetBIOS clients resolve computer names to IP addresses. Unlike DNS, which requires that the request include the FQDNs of the target system, WINS is designed to function within an intranet environment, so simple NetBIOS names can be resolved. The WINS database is dynamic, letting clients self-register their names upon receiving an IP address from the DHCP server.

> ✎ Although it is possible to run a Windows network without using NetBIOS or WINS, many utilities still depend on the WINS database. Many record types are available in WINS that are not present in DNS. These types let servers offering specific services (including Terminal Services) be easily identified through browsing. One such utility is the Terminal Server Administration tool. Without a WINS server on the network, you will need to manually specify terminal servers to manage.

Terminal Services Technology

So what is a terminal server? Windows was designed to be a single-user operating system (OS), meaning only one user could be interactively logged onto a system at a time. Terminal Services breaks that model by implementing a Session Manager layer between the system and user layers. The Session Manager responds to new session requests by creating a separate instance of the Win32 subsystem, WIN32K.SYS, for each session. The Session Manager then executes the client server runtime subsystem, CRSS.EXE, and the windows logon service, WINLOGON.EXE, within the session. Figure 1.3 shows the processes that make up Terminal Services divided up between user mode and kernel mode and indicates whether they are per server or per session.

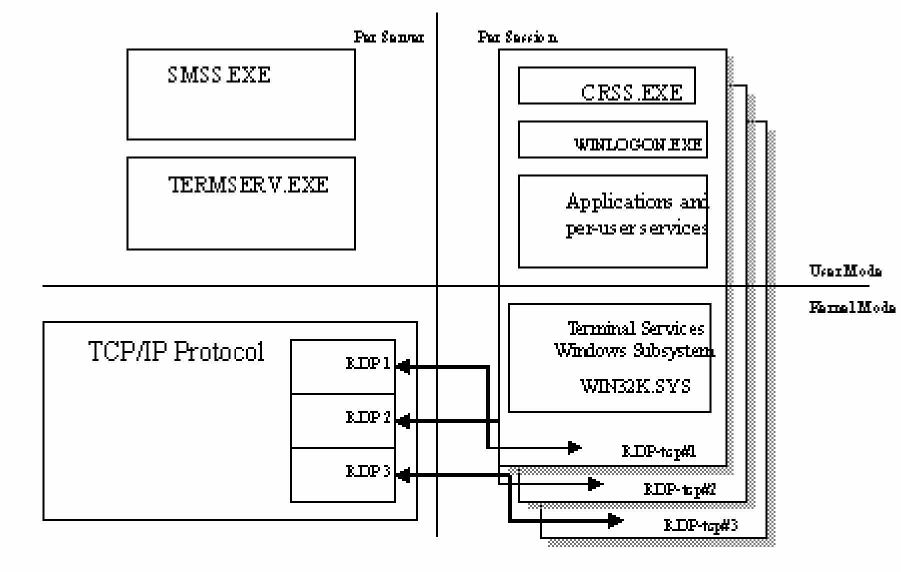


Figure 1.3: Services that create a multi-user environment.

This process allows multiple user sessions to run simultaneously on a Windows system. Session Manager acts like a maitre d' in a restaurant, directing new patrons (clients) to their tables (sessions), then directing the serving staff (applications, services, and resources) to the new table. Session Manager assigns each session a unique ID and address space so that resource and network requests can be directed to the correct user.

Another very important component to Terminal Services is RDP. This presentation layer protocol is what allows users to interact with sessions running on a remote server. Without RDP, each user would need to have a console directly connected to the server.

RDP functions as a virtual display, keyboard, and mouse on the server. Instead of sending video output to the VGA port, terminal servers redirect it to the video channel in the RDP stack. Doing so transmits the display information across the network and draws it on the client's workstation display. RDP also takes keystrokes and mouse movements at the remote client and transmits them back to the terminal server, where they are processed as if they came from a local keyboard and mouse.

By using Terminal Services, you can install applications on a few servers in a datacenter rather than on hundreds of workstations. You can also take advantage of inexpensive and highly robust solid-state thin clients instead of managing the lifecycle of workstation hardware. If you have an environment that requires personal computers for your end users, you can still leverage terminal servers to centralize network traffic for specific high-bandwidth client/server applications.

Many companies also use terminal servers for remote access. Doing so enables the organizations to lock down the majority of the network and allow remote connections to only a few servers. These servers can be easily maintained with the latest security patches, hotfixes, and virus protection.

New Answers for Old Challenges

If you manage terminal servers in your environment today, you already know many of the challenges that they pose—configuring user accounts, managing roaming profiles, load-balancing servers, configuring protocol settings, and managing printing. With WS2K3, many of these tasks become much easier to deal with.

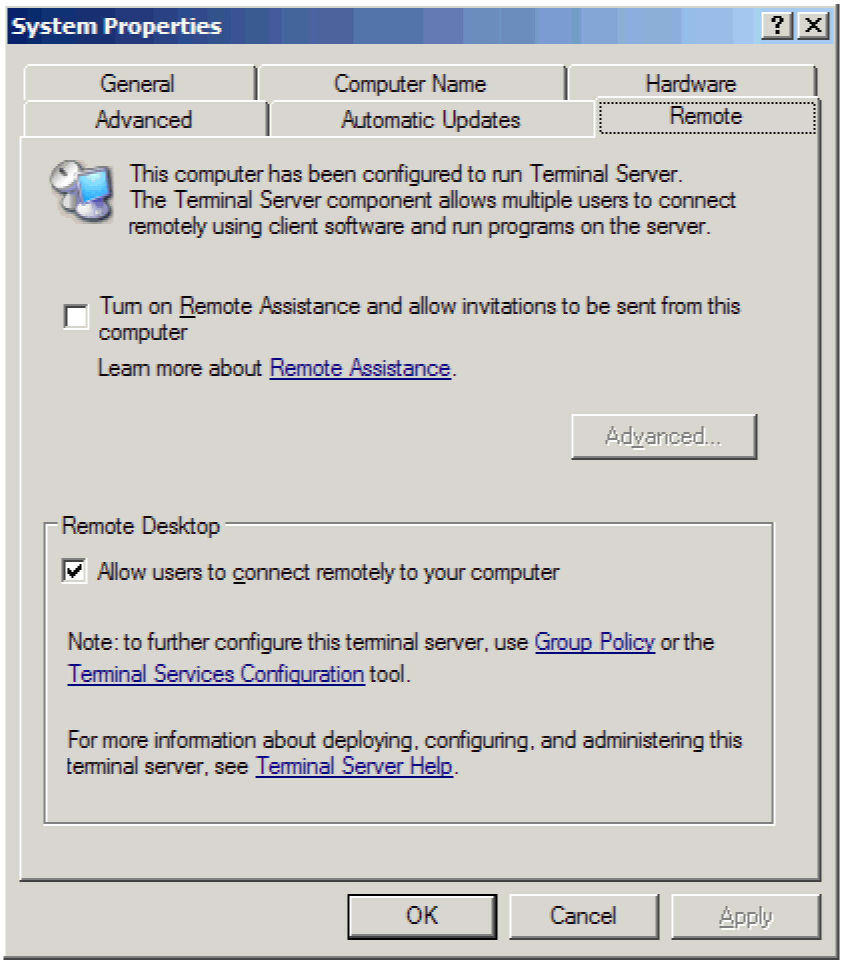
Remote Desktop

The first change you will notice in WS2K3 Terminal Services is the elimination of Remote Administration Mode. Under Win2K, this mode of Terminal Services is used to enable two remote sessions in addition to the console session for systems administration. This terminology causes a great deal of confusion for systems administrators because enabling Terminal Services does not necessarily make a server a “terminal server.” Also, Remote Administration Mode causes a server to register as a terminal server in WINS and thereby shows up in the Terminal Server Administration tool. This behavior makes finding your Win2K application terminal servers more difficult.

Don’t be alarmed, you will still be able to remotely administer your WS2K3 servers. However, instead of installing Terminal Services, you simply enable Remote Desktop. If you have been using Windows XP, you are already familiar with Remote Desktop. Under WS2K3, Remote Desktop allows the creation of two RDP-based virtual sessions as well as a remote connection to the server’s console session—something that administrators have been asking for since the release of Win2K. Also, unlike Remote Administration Mode in Win2K, WS2K3 Remote Desktop does not cause the server to be listed in the Terminal Server Administration tool.

> ☞ To force a server with Remote Desktop enabled to show up in the Terminal Server Administration tool, in the registry, change the TSAdvertise value from 0 to 1 in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server subkey.

To enable Remote Desktop, go to the System Control Panel applet, select the Remote Tab, and select the *Allow users to remotely connect to your computer* check box, as Figure 1.4 shows. By default, only members of the local administrators group will be allowed to connect remotely, but you can add users to the Remote Desktop Users group. Keep in mind, however, that enabling Remote Desktop does not enable any application compatibility subsystems, so applications may not function correctly for users other than the installer.



This computer has been configured to run Terminal Server. The Terminal Server component allows multiple users to connect remotely using client software and run programs on the server.

□ Turn on Remote Assistance and allow invitations to be sent from this computer

Learn more about Remote Assistance.

Remote Desktop

☑ Allow users to connect remotely to your computer

Note: to further configure this terminal server, use Group Policy or the Terminal Services Configuration tool.

For more information about deploying, configuring, and administering this terminal server, see Terminal Server Help.

Figure 1.4: Enabling Remote Desktop.

Microsoft has added the ability to connect to and shadow the console session to WS2K3 Terminal Services. To connect to the console session, you can either use the Remote Desktop administration tool or launch the Remote Desktop Connection client with the /console switch. To shadow the console session, use the Terminal Server Administration tool just as you would to shadow any other RDP session.

To quickly shadow the console session of a server you are already connected to via RDP, open a command prompt and type

```
SHADOW 0
```

(that is a zero).

Compatibility Modes

Like Win2K, WS2K3 offers two compatibility modes for Terminal Services: Full Security and Relaxed Security. Compatibility modes let you run legacy applications that cannot function under WS2K3's more restrictive file and registry permissions.

I'll cover the differences between the modes in Chapter 5.

RDP 5.2 Protocol Enhancements

Some of the biggest changes in WS2K3 Terminal Services from previous versions come in the enhancements made to RDP. The protocol now supports several new resource redirection abilities. You might be familiar with some of them if you have been using Windows XP's Remote Desktop ability. These enhancements bring RDP up to par with Citrix's ICA protocol in many ways.

You are now able to redirect client drives, audio output, clipboard, ports, time zone, and Windows keys (for example, ALT+TAB). RDP 5.2 even supports smart card authentication. All of these features can be enabled or disabled at the server by the administrator. RDP 5.2 adds support for greater color depth—up to 24-bit full color—and screen resolutions up to 1600 × 1200. Table 1.1 shows a comparison between RDP 5.2 and ICA.

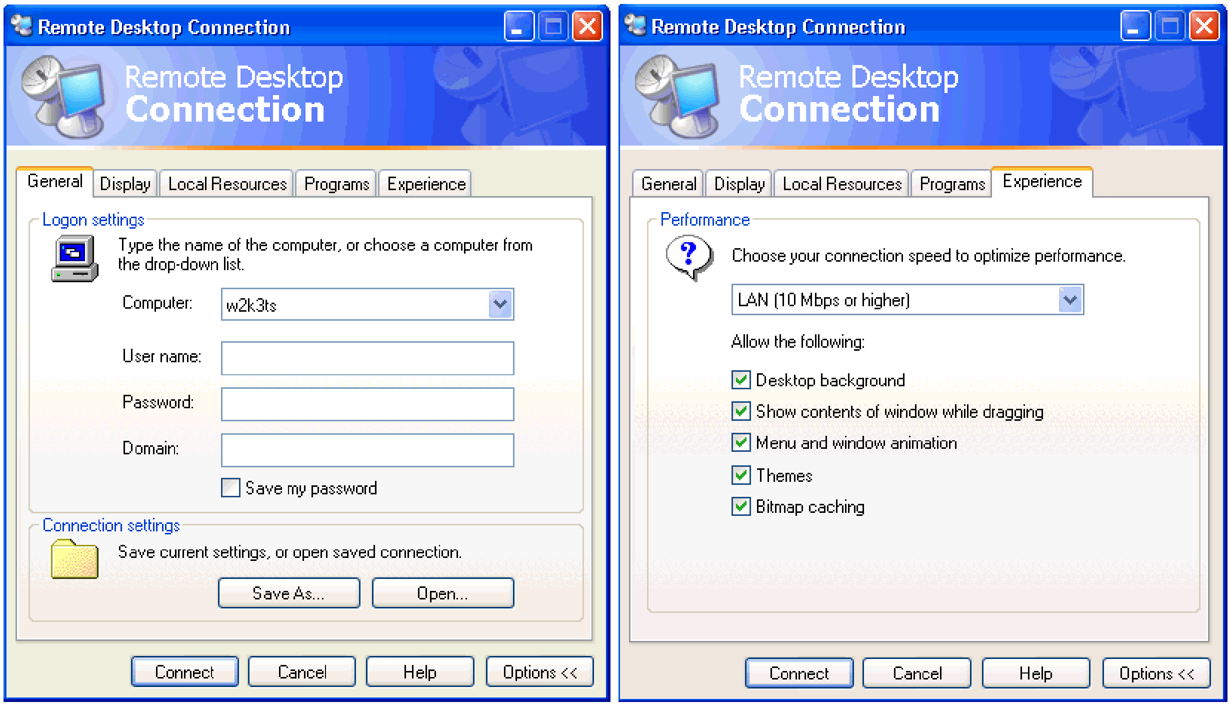
Feature	RDP 5.2	ICA
Client drive mapping	Automatically connects to all client local and network drives	Automatically connects to client local drives
Client clipboard mapping	Automatic	Automatic
Shadowing	Supported	Supported
Mapping of local client printers	Automatic	Automatic
Mapping of client network printers	Automatic	Automatic
Smart card sign on	Supported	Supported
Reconnection of dropped sessions	Automatic	Automatic
Sound	Supported	Supported
Encryption	Up to 128 bit	Up to 128 bit
Compression	Automatic	Automatic
Client time zone mapping	Supported	Supported
Windows keys	Automatic	Requires alternative key combinations
Client serial and parallel port mapping	Automatic	Automatic
Supported client OSs	Win32, Win16, Windows CE, CE.NET, PocketPC, Macintosh	Win32, Win16, Windows CE, PocketPC, MS-DOS, UNIX, Macintosh, Linux, Java
Transport protocol	TCP/IP	TCP/IP, IPX/SPX, NetBEUI
Seamless Windows	Not available natively	Automatic

Table 1.1: Comparison of RDP 5.2 and ICA.

Remote Desktop Connection Client

Remote Desktop Connection is the new client for RDP 5.2. Remote Desktop Connection supports all of the new features of RDP 5.2. It eliminates the Connection Manager interface and no longer stores connection definitions in the registry. Instead, Remote Desktop Connection supports RDP Files—text files containing connection parameters to connect to a terminal server or Windows XP Remote Desktop. With RDP Files, it is easy to distribute or centrally store common connections for your users.

Through the Remote Desktop Connection interface, which Figure 1.5 shows, you can control connection options—resource redirection, initial program, and window size. There is also a new option called Experience through which you can enable or disable features of the new Aqua interface in Windows XP and WS2K3—wallpaper, themes, and menu animation—to improve performance over low-bandwidth connections.



Logon settings

Type the name of the computer, or choose a computer from the drop-down list.

Computer: w2k3ts

User name:

Password:

Domain:

☐ Save my password

Connection settings

Save current settings, or open saved connection.

Performance

Choose your connection speed to optimize performance.

LAN (10 Mbps or higher)

Allow the following:

☑ Desktop background

☑ Show contents of window while dragging

☑ Menu and window animation

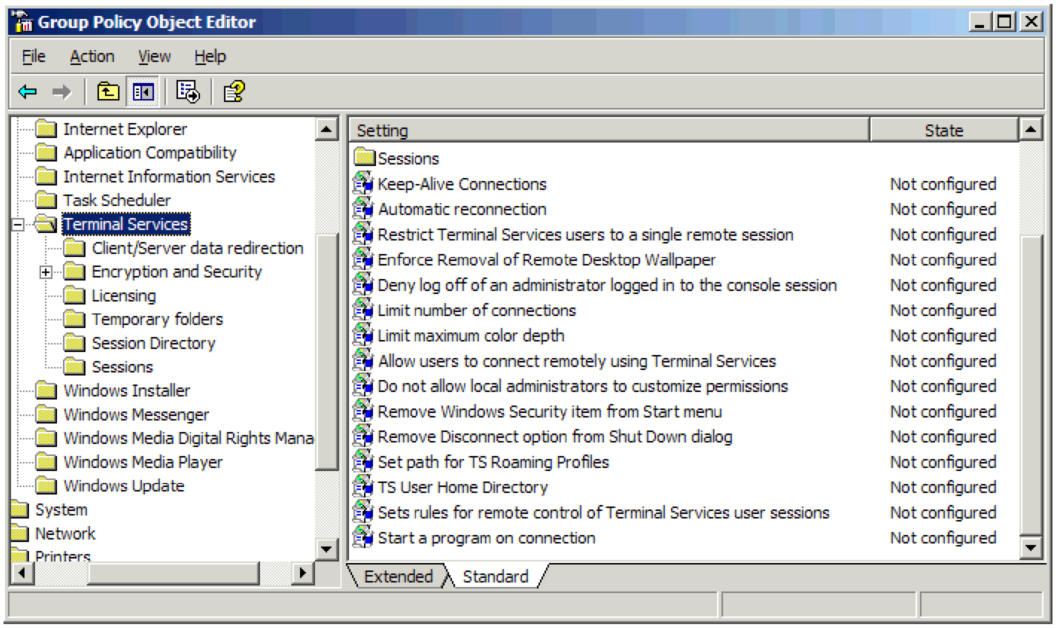
☑ Themes

☑ Bitmap caching

Figure 1.5: The Remote Desktop Connection client.

Group Policy–Based Configuration

Under WS2K3, you can now centrally configure and manage virtually all Terminal Services parameters via Group Policy. Figure 1.6 shows some of the settings available.



Setting	State
Sessions	
Keep-Alive Connections	Not configured
Automatic reconnection	Not configured
Restrict Terminal Services users to a single remote session	Not configured
Enforce Removal of Remote Desktop Wallpaper	Not configured
Deny log off of an administrator logged in to the console session	Not configured
Limit number of connections	Not configured
Limit maximum color depth	Not configured
Allow users to connect remotely using Terminal Services	Not configured
Do not allow local administrators to customize permissions	Not configured
Remove Windows Security item from Start menu	Not configured
Remove Disconnect option from Shut Down dialog	Not configured
Set path for TS Roaming Profiles	Not configured
TS User Home Directory	Not configured
Sets rules for remote control of Terminal Services user sessions	Not configured
Start a program on connection	Not configured

Figure 1.6: Group Policy settings for WS2K3 Terminal Services.

As you can see, Microsoft has provided the centralized control we've always wanted.

> 🕮 I'll go over the available settings and recommended usage in Chapter 2.

ADSI Access to User Parameters

Under Win2K, the only Terminal Services parameter of a user object that was accessible from the command line was the Terminal Services Profile Path attribute; accessing this attribute required the TSPROF tool. WS2K3 exposes all Terminal Services attributes to ADSI. Using the Windows Script Host (WSH) and your preferred scripting language, you can now easily configure users' Terminal Services settings. I'll discuss the ADSI objects and provide some sample scripts in Chapter 4, but for now, here is a list of the available attributes:

```
objUser.ConnectClientDrivesAtLogon
objUser.ConnectClientPrintersAtLogon
objUser.DefaultToMainPrinter
objUser.TerminalServicesInitialProgram
objUser.TerminalServicesWorkDirectory
objUser.TerminalServicesProfilePath
objUser.TerminalServicesHomeDirectory
objUser.TerminalServicesHomeDrive
objUser.AllowLogon
```

```
    objUser.MaxDisconnectionTime
    objUser.MaxConnectionTime
    objUser.MaxIdleTime
    objUser.BrokenConnectionAction
    objUser.ReconnectionAction
```

Session Directory

When using WS2K3 Enterprise Edition for terminal servers in a load-balanced environment, you can use the new Session Directory service to provide a single point of entry into the terminal server farm. Session Directory not only acts as a load balancer—connecting users to the least loaded server, but also maintains a database of active sessions in the farm. This feature enables a disconnected user to resume an active session on the same server from which the user was disconnected.

When a user connects to the farm through the Session Directory server, Session Directory checks the list of active and disconnected sessions; if the username is found in the database, the connection is directed to the server running the session. Session directory can be used with Microsoft's load-balancing service or any third-party load balancer.

📖 I will cover Session Directory in depth in Chapter 3.

Terminal Services Licensing

For a terminal server to continue accepting connections after the 120-day trial period, you must configure a Terminal Services Licensing server. WS2K3 adds new options and new layers of complexity to the Terminal Services licensing landscape. To connect to a WS2K3 terminal server, clients will need to be issued new WS2K3 license tokens. These new tokens can only be issued by a WS2K3 Terminal Services License server—Win2K license servers cannot issue these new tokens. Thus, even if your environment already contains a Win2K license server, you will be forced to either upgrade that server to WS2K3 or activate a separate WS2K3 license server.

Terminal Server Licensing Components

Terminal Services licensing consists of the Microsoft Clearinghouse, one or more WS2K3 Terminal Services Licensing servers, and one or more terminal servers. You access the Microsoft Clearinghouse to activate license servers and obtain license key packs to be installed on the Terminal Services Licensing server. The clearinghouse can be accessed directly over the Internet, through a Web page, or by telephone.

A Terminal Services Licensing server can be any edition of WS2K3 with Terminal Services Licensing installed. The Terminal Services Licensing server stores all Terminal Services CAL tokens and tracks the tokens that have been issued to computers or users. All terminal servers must be able to communicate with the Terminal Services Licensing server to issue permanent tokens. If the licensing server has not been activated, it will issue only temporary licenses.

The terminal server is any WS2K3 edition with the terminal server role installed. When a client connects to the terminal server, the server first determines whether the client needs a license token. If so, the server contacts the licensing server and requests a token on the client's behalf, then delivers the token to the client. The first time a client connects to a terminal server in per-device licensing mode, a temporary token is issued. Temporary licenses are stored on the Terminal Services Licensing server for 90 days. Only at the second connection (within 90 days) is the permanent CAL assigned to the device.

The term "permanent" is not really accurate here, as device tokens are set to expire after a random number of days (between 52 to 89 days). This configuration is designed to recapture CALs that have been issued to devices that are no longer in the environment or have had their OSs re-installed. This behavior was first implemented in Win2K Service Pack 3 (SP3).

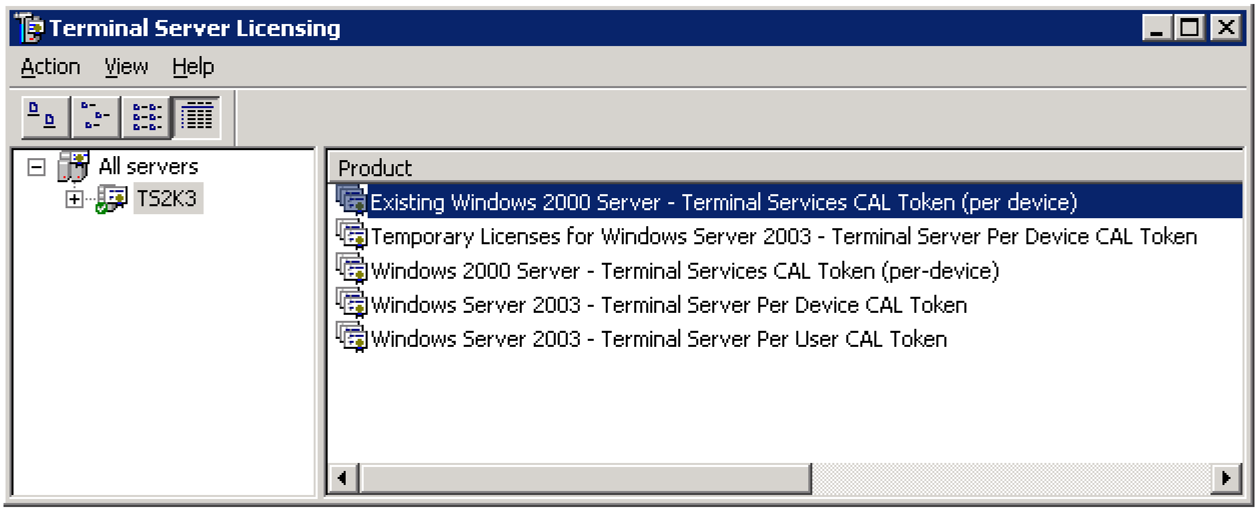
License Types

A WS2K3 Terminal Services Licensing server can manage seven types of license tokens. In addition to supporting the CALs required for connecting to Win2K terminal servers, there are three new types of CALs specific to WS2K3 Terminal Services (the following list shows the three new types as well as the three types that have been supported since Win2K):

> ✎ There are no built-in licenses for WS2K3 Terminal Services. You will need to purchase CALs for all devices or users connecting to these servers regardless of the client OS.

- WS2K3 Terminal Server Device CALs—WS2K3 terminal servers that are in Per Device licensing mode will request these licenses from the Terminal Services Licensing server.
- WS2K3 Terminal Server User CALs—WS2K3 terminal servers that are in Per User licensing mode will request these licenses.
- WS2K3 Terminal Server External Connector licenses—These licenses allow unlimited connections to a terminal server running WS2K3 by external users. These licenses are not yet available.
- Win2K Terminal Services CALs—Terminal servers running Win2K will request these licenses from the licensing server for clients running OSs other than Win2K Professional or Windows XP. You only need these licenses if you have terminal servers running Win2K.
- Win2K Terminal Services Internet Connector licenses—These licenses allow as many as 200 simultaneous anonymous connections to a terminal server running Win2K by non-employees across the Internet.
- Win2K Built-In licenses—Clients that are running Win2K Pro or Windows XP are issued a token from the built-in pool of license tokens when connecting to a terminal server running Win2K.

Figure 1.7 shows the licenses available in the Terminal Server Licensing administration tool. Notice that user CAL tokens are tracked separately from device CAL tokens. User CAL tokens are new in WS2K3. Terminal servers can now be placed into either Per Device or Per User licensing mode. A single Terminal Services Licensing server can serve tokens to terminal servers in any combination of these modes if the proper licenses are installed.



All servers
TS2K3

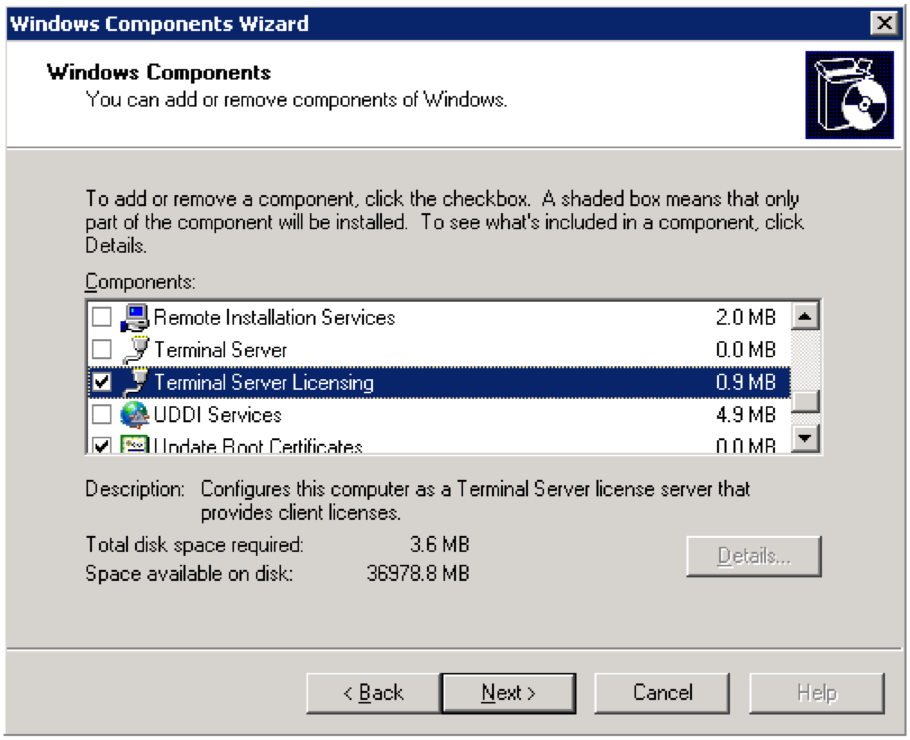
Product
Existing Windows 2000 Server - Terminal Services CAL Token (per device)
Temporary Licenses for Windows Server 2003 - Terminal Server Per Device CAL Token
Windows 2000 Server - Terminal Services CAL Token (per-device)
Windows Server 2003 - Terminal Server Per Device CAL Token
Windows Server 2003 - Terminal Server Per User CAL Token

Figure 1.7: License types available in the Terminal Server Licensing administration tool.

Installing Terminal Server Licensing

Unless you are working in a single server environment, Terminal Server Licensing should be installed on a separate server from Terminal Services. If you are in a domain environment, you will probably want to install the licensing service on a domain controller, as doing so makes the discovery process easier for the terminal servers.

To install Terminal Server Licensing, go to the Add/Remove Programs Control Panel applet, and select Add/Remove Windows Components. In the Windows Components Wizard window, select the Terminal Server Licensing check box, as Figure 1.8 shows.



Windows Components
You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☐	Remote Installation Services	2.0 MB
☐	Terminal Server	0.0 MB
☑	Terminal Server Licensing	0.9 MB
☐	UDDI Services	4.9 MB
☑	Update Root Certificates	0.0 MB

Description: Configures this computer as a Terminal Server license server that provides client licenses.

Total disk space required: 3.6 MB
Space available on disk: 36978.8 MB

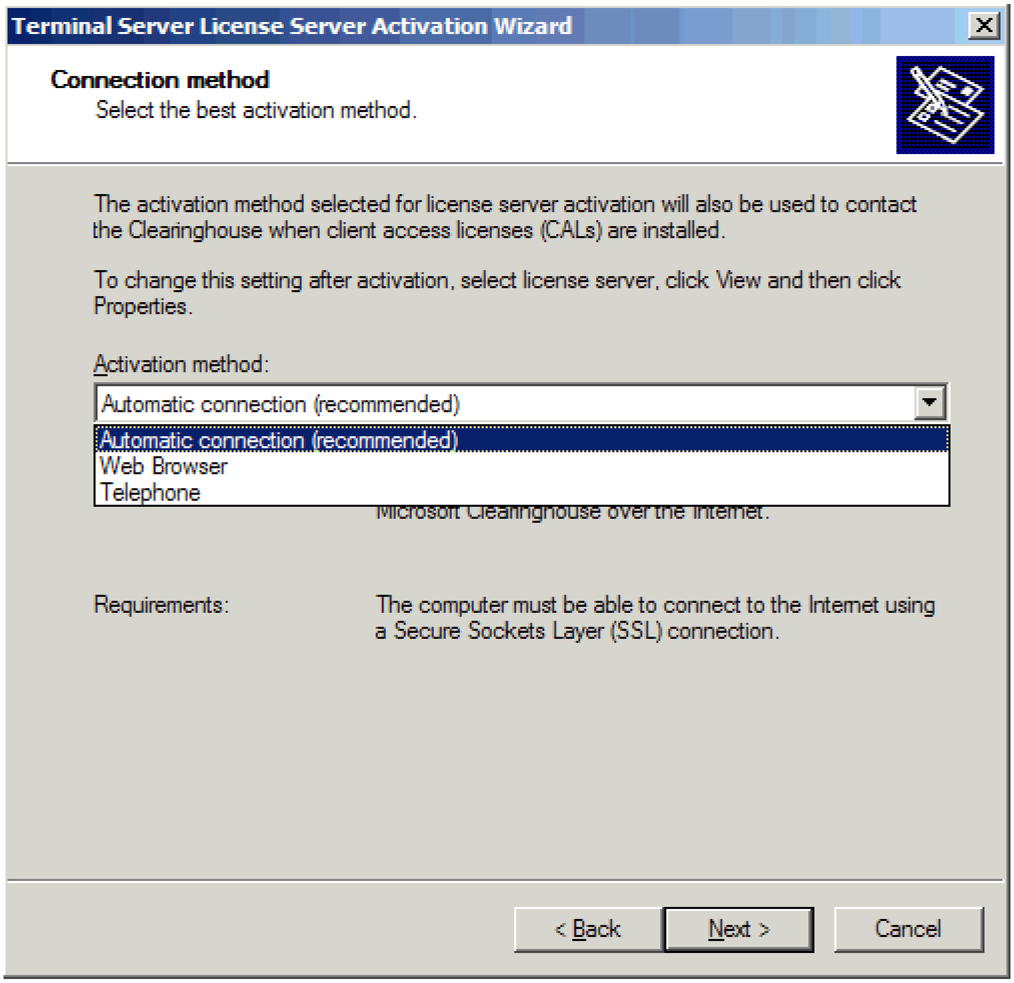
Figure 1.8: Installing Terminal Server Licensing.

If you are installing Terminal Server Licensing on a server in AD, you are presented with two options for the mode of the server: Domain/Workgroup and Enterprise. The mode selected determines how the licensing service advertises itself to the terminal servers. If you are in a workgroup or non-AD domain, the Enterprise option is not available.

I will explain the discovery process in the next section, but for now, you should understand that an Enterprise license server will be discoverable by terminal servers from any trusted domain but *only* within the same AD site as the licensing server. Whereas, a Domain/Workgroup license server will be discoverable only by terminal servers in the same workgroup or domain, but, depending on the type of domain, may be discoverable across site boundaries.

After you install Terminal Server Licensing, the license server must be activated by contacting the Microsoft Clearinghouse. Launch the Terminal Server Licensing administration tool from the Start menu, right-click the server, and click Activate Server. The Terminal Server License Server Activation Wizard will launch, offering you three options for contacting Microsoft. Figure 1.9 shows the options in the wizard:

- Automatic connection—This method is the easiest way to activate the licensing server. This method requires that the server running Terminal Server Licensing has Internet connectivity on port 443 (Secure Sockets Layer—SSL). Simply fill in the company and contact information, and click Activate.
- Web Browser—If the server running Terminal Server Licensing does not have Internet connectivity, you can still activate the server over the Web from another computer. To do so, from a Web browser, go to https://activate.microsoft.com, and fill in the company and contact information as well as the unique Terminal Server Licensing ID number that the activate server wizard provides. The Web site will respond with the activation code that you can then enter into the licensing service.
- Telephone—If you do not have Internet connectivity, you can contact the Microsoft Clearinghouse by telephone. Select your country/region in the activate server wizard, and the correct phone number will be displayed. Provide the customer service person your company name, contact information, and server ID code, and they will provide you with the activation code. Be sure to either activate the server while still on the phone with the customer service representative or be very careful to record the activation code accurately.



Terminal Server License Server Activation Wizard

Connection method

Select the best activation method.

The activation method selected for license server activation will also be used to contact the Clearinghouse when client access licenses (CALs) are installed.

To change this setting after activation, select license server, click View and then click Properties.

Activation method: Automatic connection (recommended)

Microsoft Clearinghouse over the Internet.

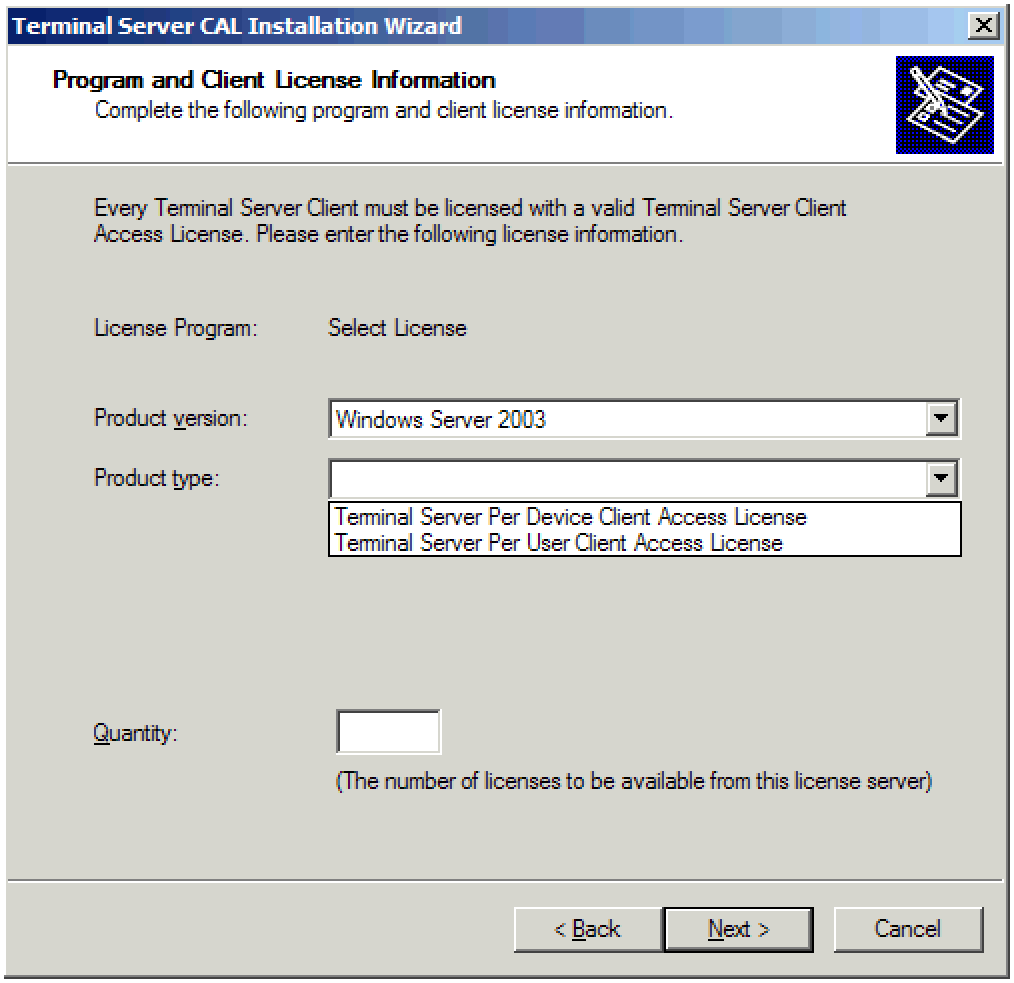
Requirements: The computer must be able to connect to the Internet using a Secure Sockets Layer (SSL) connection.

Figure 1.9: Activating a Terminal Services Licensing server.

After the license server is activated, it will immediately begin to issue temporary Win2K and WS2K3 terminal server tokens, which gives the administrator a 90-day period in which to install the appropriate permanent CALs on the license server so that it can issue permanent tokens.

> ☞ If you are upgrading a Win2K server with Terminal Server Licensing installed to WS2K3, you might need to re-activate the licensing service. To do so, select Re-Activate Server from Advanced in the Actions menu in the Terminal Server Licensing administration tool.

To add a license pack to the license server, right-click the server in the Terminal Server Licensing administration tool, and click Install Licenses. You will have the same connection options as you had to activate the server. If you are installing a retail license pack, the type of license will be automatically selected. If, however, you are installing licenses through a Select, Open, or other Microsoft license agreement, you will have to select which type of licenses you want to add. Figure 1.10 shows the Terminal Server CAL Installation Wizard.



Terminal Server CAL Installation Wizard

Program and Client License Information

Complete the following program and client license information.

Every Terminal Server Client must be licensed with a valid Terminal Server Client Access License. Please enter the following license information.

License Program: Select License

Product version: Windows Server 2003

Product type:

Terminal Server Per Device Client Access License
Terminal Server Per User Client Access License

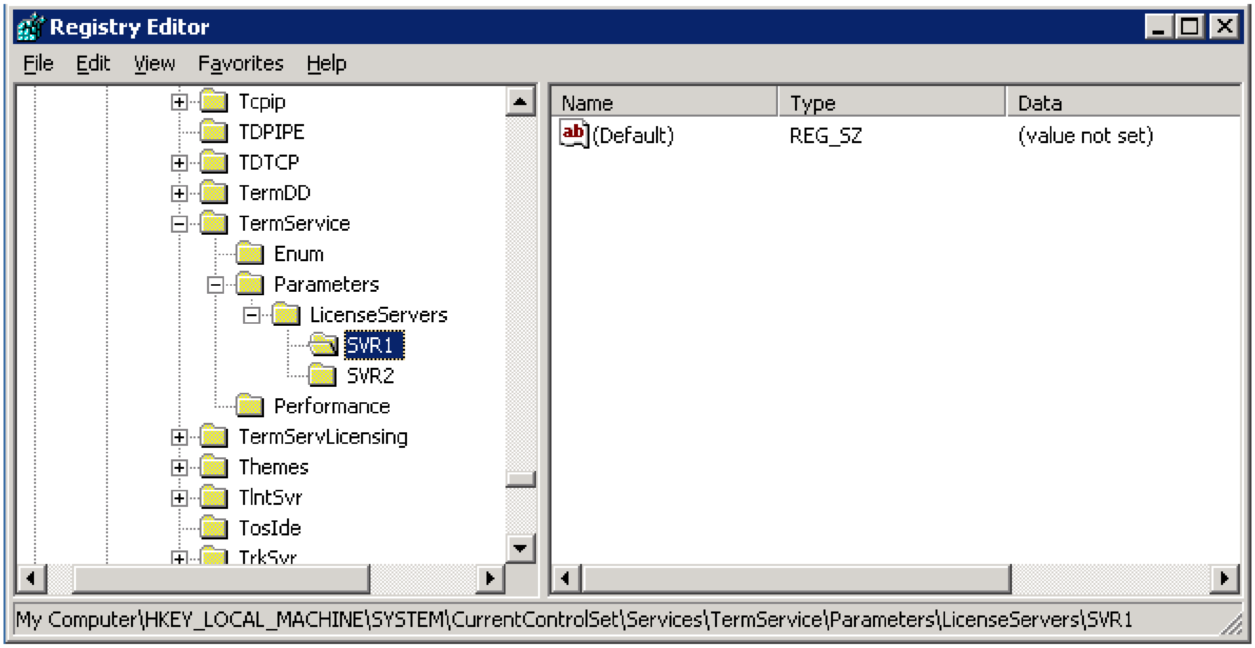
Quantity:

(The number of licenses to be available from this license server)

Figure 1.10: Adding licenses to a Terminal Services Licensing server.

License Server Discovery

When Terminal Services is started, the server attempts to locate terminal server license servers using a predefined discovery process. The method used is dependant on the server environment and the mode in which the licensing server is configured to run. You can override the discovery process by modifying the registry to point to a specific license server or servers. Under Win2K, you can specify only a single license server in the registry, whereas WS2K3 lets you list multiple preferred license servers. To override the discovery process, add subkeys to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService\Parameters\LicenseServers subkey. Each subkey should be named with the hostname of the license server that you want the terminal server to use. Figure 1.11 shows a registry with two license servers defined.



Name	Type	Data
(Default)	REG_SZ	(value not set)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService\Parameters\LicenseServers\SVR1

Figure 1.11: Overriding license server discovery by specifying license servers in the registry.

If you don't predefine license servers in the registry, the discovery process proceeds as follows: workgroup and non-AD domain–based terminal servers send a mailslot broadcast to locate license servers. Thus, only license servers in the same subnet will be discovered.

AD-based terminal servers first look for any license servers in Enterprise licensing mode. They do so by performing a Lightweight Directory Access Protocol (LDAP) query for the CN TS-Enterprise-License-Server, specifying their own site as the scope. The terminal server then contacts each domain controller within its site looking for a Domain license server. Finally, the terminal server will contact all remaining domain controllers within its domain.

Once the discovery process is complete, the terminal server caches all license servers that were discovered in the following registry keys: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSLicensing\Parameters\EnterpriseServerMulti and HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSLicensing\Parameters\DomainLicenseServerMulti.

It is important to note that if both Enterprise and Domain license servers are found, the terminal server will always prefer to use the Domain license server—even if a site boundary must be crossed to do so. Also, if no license servers are found, the terminal server will repeat the discovery process once every hour until a license server is found. Once one or more license servers are found, discovery is not repeated until such a time when none of the servers cached in the registry are available.

License Assignment

Every time a client connects to a terminal server, the license server is contacted to either validate an existing license or issue a new license. The type of licenses that a terminal server will issue is determined by its licensing mode—Per Device or Per User. You can set the mode through either the Terminal Services Configuration administration tool or by Group Policy. The default is Per Device mode, unless you are upgrading Win2K terminal server that is in Internet Connector mode, in which case it will default to Per User mode.

> In order to support both Per User and Per Device tokens, the terminal server must be in Per User mode.

The following steps walk you through the process taken by a terminal server at each client connection:

1. Regardless of the licensing mode, the terminal server will first query the client device to determine whether a device token has been written to the registry. If a token is present, the terminal server will contact the license server indicated in the token to validate the license. If the license is a temporary license, the license server will assign a permanent token at this time, which will be recorded in the client registry.
2. If the client device does not have a token, the next step is dependent on the licensing mode of the terminal server:
    a. Per-User licensing mode—The terminal server requests credentials from the user and performs authentication. The terminal server will then query the license server to either validate that the user has a token assigned or request a license for the user. The token is stored on the license server.

    b. Per-Device licensing mode—The terminal server will request a temporary token from the license server and write it to the client registry. After the user has been authenticated, the terminal server instructs the licensing server to mark the temporary token as validated. If the user does not authenticate, the token is immediately returned to the pool of available licenses.
3. In either case, if the license server does not have any tokens available, another license server is contacted. If the first license server is aware of another license server that has licenses available, it will request the token on behalf of the terminal server. If the license server does not know of other license servers in the environment, the terminal server will query the next license server cached in the registry.

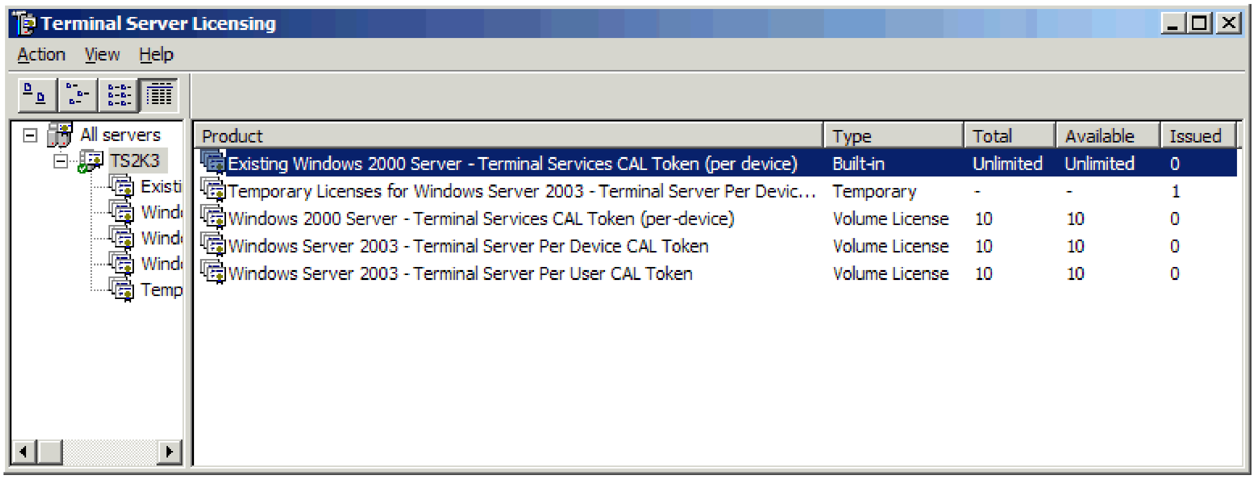
In most cases, license servers will inform each other when licenses are added to or removed from their pools. This communication allows the license servers to proxy requests for licenses to other licensing servers. This process is called License Token Announcement and occurs in the following scenarios:

- Between domain license servers within the same domain
- Between enterprise license servers within the same site and domain
- From enterprise license servers to domain license servers
- From Win2K license servers to WS2K3 license servers

License Server Administration

After your license servers are activated and have licenses installed, there is very little administration to be done. However, there are a few utilities that you should familiarize yourself with in order to troubleshoot any licensing issues that may arise.

The Terminal Sever Licensing tool is the primary administration tool. Figure 1.12 shows the interface. This tool is used to activate a license server, install licenses, and view available and assigned license tokens. Through this interface you can view which users and devices have been assigned CAL tokens, the date that the token was assigned, and when it will expire.



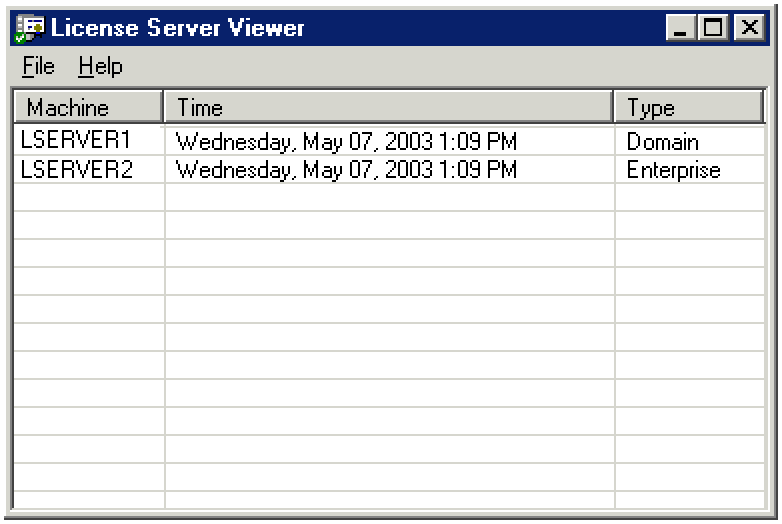
Product	Type	Total	Available	Issued
Existing Windows 2000 Server - Terminal Services CAL Token (per device)	Built-in	Unlimited	Unlimited	0
Temporary Licenses for Windows Server 2003 - Terminal Server Per Devic...	Temporary	-	-	1
Windows 2000 Server - Terminal Services CAL Token (per-device)	Volume License	10	10	0
Windows Server 2003 - Terminal Server Per Device CAL Token	Volume License	10	10	0
Windows Server 2003 - Terminal Server Per User CAL Token	Volume License	10	10	0

Figure 1.12: The Terminal Server Licensing tool interface.

The WS2K3 resource kit contains a command-line interface to the Terminal Server Licensing tool—LSREPORT.EXE. With this tool, you can output a list of tokens assigned by a license server. This tool accepts parameters to limit the date range of licenses to include, include only temporary licenses, include the hardware ID of device tokens, and specify which license server or servers to query.

Another resource kit utility is the Client License Test Tool—TSCTST.EXE. This tool is used to query details about device tokens installed on a given client. The default output includes the name of the license server that issued the token, the scope, the name of the computer, the user that was authenticating when the token was issued, the license ID, and the date range for which the license is valid. When executed with the /A switch, the tool will also include the server certificate version, the licensed product version, the hardware ID, the client platform ID, and the company name in the output.

The License Server Viewer Tool—LSVIEW.EXE, which Figure 1.13 shows—is also included in the resource kit. This GUI-based tool performs a license server discovery process and displays all Terminal Services license servers in the environment. It also identifies the type of license server—Domain or Enterprise—and can create a log with diagnostic information about the discovery process.

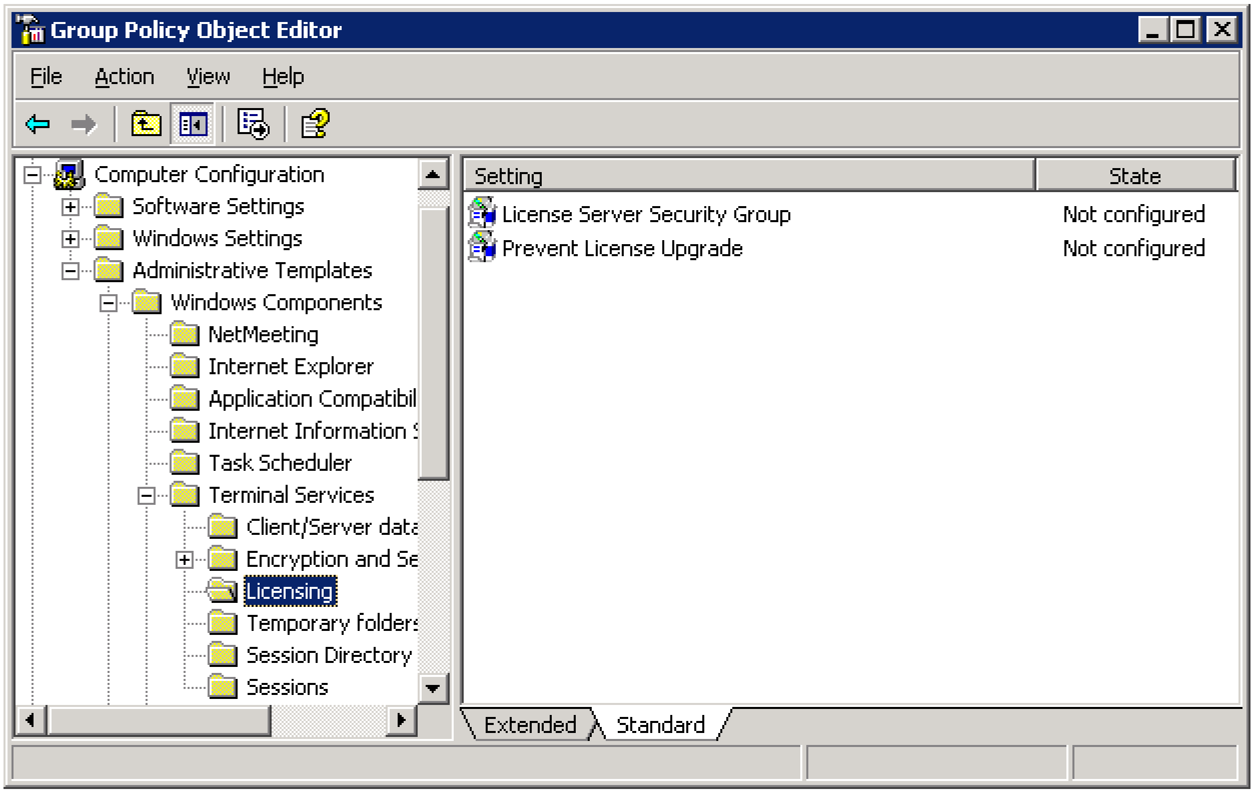


Machine	Time	Type
LSERVER1	Wednesday, May 07, 2003 1:09 PM	Domain
LSERVER2	Wednesday, May 07, 2003 1:09 PM	Enterprise

Figure 1.13: The License Server Viewer interface.

License Server Group Policy Settings

WS2K3 includes several Group Policy settings to control terminal server licensing. With these settings, it is easy to centrally configure license servers and maintain consistency in the environment (Figure 1.14 shows the available settings in the Group Policy Object Editor):



Setting	State
License Server Security Group	Not configured
Prevent License Upgrade	Not configured

Figure 1.14: The License Server Group Policy settings.

- License Server Security Group—By default, a license server will issue tokens to clients connecting to any terminal server. If you enable this setting, the license server will only respond to requests from terminal servers in the Terminal Services Computers local group. If the licensing server is a domain controller, this is a domain local group. Enabling this setting prevents rogue terminal servers from requesting licenses and lets you enforce separate license pools for groups of terminal servers in your environment. If you have more than one license server providing licenses for a single group of terminal servers, be sure to add the license servers to the group, as they can request licenses on behalf of the terminal servers.
- Prevent License Upgrade—As you know, a WS2K3 license server can distribute both Win2K terminal server device CALs and WS2K3 terminal server device CALs. If a Win2K terminal server requests a token, and the license server does not have any Win2K terminal server CALs available, it will automatically issue a WS2K3 Per-Device token (if there are any available). This behavior can be prevented by enabling this policy setting. With it enabled, the license server will only issue temporary tokens to clients connecting to Win2K terminal servers. If the client's temporary token has expired, the connection will be refused.

The Terminal Services Computers group is empty be default; be sure to add servers to the group before enabling the policy setting to prevent refused connections.

Summary

In this chapter, I introduced you to the new role-based model in WS2K3. I also briefly covered the new features of Terminal Services. I will continue to address these enhancements throughout the book. Finally, I went into depth about Terminal Services licensing, as a thorough understanding of licensing is required to maintain a terminal server infrastructure for more than 120 days.

In Chapter 2, I will cover the installation and configuration of Terminal Services. I will take you through all the new Group Policy settings for Terminal Services, and show you a few tricks to use to make administrating groups of servers easier.