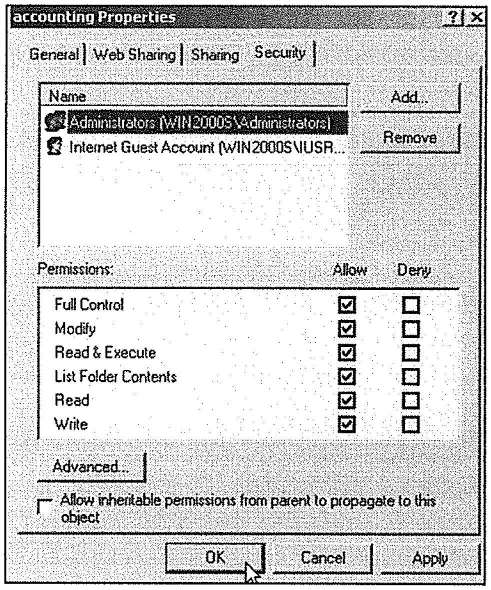


Name

- Administrators (WIN2000S\Administrators)
- Internet Guest Account (WIN2000S\IUSR...

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

□ Allow inheritable permissions from parent to propagate to this object

FIGURE 2.36
NTFS permissions are usually used to restrict access to a Web-shared folder.

continued

7. From the Security tab (see Figure 2.36), add local permissions for all the users you want to allow to access this folder over the Web by clicking the Add button and adding them from the directory of your choice. You can add users and groups as you normally would. However, to allow anonymous users to access the data, either you must explicitly add the IIS anonymous users, or you must implicitly add these users by adding the local group Guests. You will need to set as much NTFS permissions for any user as you have given out access in step 4. If you gave out Read and Write access, you must also give out Read and Write NTFS permission, otherwise the lesser of the access levels will prevail for your Web users. Click OK when you are done.

To modify or to stop Web sharing, you can return to the properties for the folder and add a new alias, remove an existing alias, or stop sharing altogether. If you stop sharing, all the aliases for the folder will be removed, and you will have to re-create them if you change your mind.

Web Sharing in Its Context

Web sharing does not happen in a vacuum. You have to realize that the shared permissions you assign are going to interact with both the local NTFS security that you have applied to the shared data as well as the security you have set up for the Web site the folder is shared under.

Like shared folder permissions, Web sharing interacts with local security. If Web sharing is configured for a folder that is on an NTFS partition, the more restrictive of the two permissions will be effective for a Web browser client connecting to the folder. For example, if the anonymous Web user account (IUSR_*servername*) has been given Read access through NTFS permissions and the folder has been given Web Sharing permissions of Read and Write, a Web Browser client connecting to the share will get only Read access (the more restrictive of the two permissions). Conversely, if the

Guests group is given Full Control through NTFS permissions (thus giving the anonymous Web account Full Control) but you have given out only Read access to the Web share, browser clients will get only Read access to the data.

In addition to NTFS security, you also need to know what the security is on the whole Web site that you are sharing under. Any browser client trying to get to a Web share must pass through the Web site security before it gets to that share. If the site is secured so that only Read access is allowed, even if Write access is given to the Web share, that access will not be effective for the browser client trying to access the data.

Troubleshooting Web Sharing

A number of things can go wrong with Web sharing. The first major problem is a lack of an IIS server. Without a local IIS server, you will not be able to find the Web Sharing tab on the Properties dialog box for your folder. To solve this, install IIS on your Windows 2000 server.

After an IIS server has been configured, the next problem may be your permissions to share a folder. You must have Power User or Administrator access to be able to Web share a folder. If your user account is not a member of one of those two groups, you need to gain membership or have one of the members create Web shares for you.

If the folders have been shared, the next problems might be those of access. The major problems are going to be with server access (is the server up and is the Web service running?) and permissions.

Lack of server access can result from a number of things. The server itself may not be running. If it is, the Web service may not be running. If it is, the Web site in which the folder is being shared may not be enabled. If it is, the TCP port it is running on might not be the default (port 80). Any or all of these things can prevent users from accessing the Web folder you have configured.

Problems related to the server being down (that is, the operating system is not running) are beyond the scope of this particular discussion. The bottom line is that the server must be running in order to provide access to your Web folders.

If the Web service itself is not running, you can start it by following Step by Step 2.23.

STEP BY STEP

2.23 Starting the World Wide Web Publishing Service

1. From the Start menu, choose Programs, Administrative Tools, Services.
2. Scroll down the Services list until you find World Wide Web Publishing Services. Right-click it and choose Start from the menu that appears.
3. Exit the Services console.

If the Web service is running, the problem might be that the Web site is not running. To start it, you need to open the IIS Services Manager console. Step by Step 2.24 leads you through the process of starting a Web site.

STEP BY STEP

2.24 Starting a Web Site

1. From the Start menu, choose Programs, Administrative Tools, Internet Services Manager.
2. In the IIS Console window, you can locate your Web sites by expanding the Console Root, Internet Information Services, and Your Server. When you see your Web site in the tree under the name of your server, right-click it and choose Start from the menu presented.
3. Exit the IIS console.

Finally, even if the Web site is up, if the administrator of the site has configured access on a TCP port other than the default (80), Web users will not be able to get to the Web site without specifying the new port in the URL. For the purposes of this discussion, a TCP port can be thought of like a TV channel. You may have your TV on, but if it is not tuned to the right station you will not be able to get to the program you want. All browsers are configured to access Web sites on port 80. If the Web server is not "listening" on port 80, either the server needs to be changed or the Browser has to be told which port to connect on. If the port is not 80 and you want Web users to connect, you can give them the port number. Then they will be able to connect using the following syntax:

```
http://servername:portnumber/foldername
```

For example, to connect to the folder Accounting on a server called Win2000S using the port 8080, you would use the following syntax:

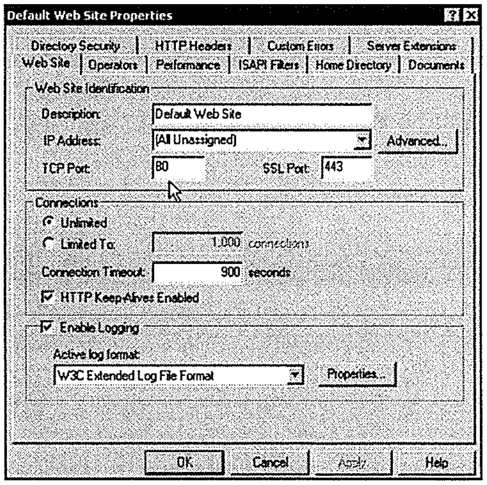
```
http://Win2000S:8080/Accounting
```

To find out what the port is or change it, follow Step by Step 2.25.

STEP BY STEP

2.25 Discovering and Changing a Web Server's TCP Port

1. From the Start menu, choose Programs, Administrative Tools, Internet Services Manager.
2. In the IIS Console window, you can locate your Web site by expanding the Console Root, Internet Information Services, and your server. When you see your Web site in the tree under the name of your server, right-click it and choose Properties.
3. In the Web Site Properties dialog box, the Web Site tab contains a field called TCP Port (see Figure 2.37). That number is your TCP port number. If you change that, all browsers (and HTML links coded into pages) will have to explicitly use that TCP port number. Therefore, it is not a good idea to change it without first consulting your Web master to discuss the implications.
4. Click OK to update the Web site's properties.



Web Site Identification

Description: Default Web Site

IP Address: (All Unassigned)

TCP Port: 80 SSL Port: 443

Connections

● Unlimited

○ Limited To: 1,000 connections

Connection Timeout: 900 seconds

☑ HTTP Keep-Alives Enabled

☑ Enable Logging

Active log format: W3C Extended Log File Format

FIGURE 2.37
The TCP port number can be used to effectively hide a Web site from those who do not know the number.

When a user is able to connect to your Web site, the issue of permissions might come up. Remember from the discussion in the last section that all the levels of permissions interact to form an effective permission. As a result, you must check permission levels at the NTFS level, the Web folder level, and at the Web site level. Thus far, the only one of these three that has not been discussed is the Web site level. That's covered in the next section.

Controlling Access to Web Sites

Web sites are made available through the Web service component of Internet Information Services. Because these Web sites contain data, they need to be secured at one level or another (even if that security is to leave everything unsecured).

To publish any material to either an intranet or the Internet, you must first install IIS. You can look back to Step by Step 2.21 for instructions on how to do that. From that point, any security you want to place on your Web site(s) can be done through the Internet Services Manager (which you bring up by choosing Start, Programs, Administrative Tools, Internet Services Manager).

The following list outlines ways in which you can control access to your Web site:

- Changing the TCP port
- Changing access permissions
- Changing execute permissions for scripts and programs
- Changing authentication methods (including enabling and disabling anonymous access)
- Adding IP address and domain name restrictions
- Adding server certificates for Secure Socket Layer (SSL) transmissions
- Authenticating users with client certificates

These topics will be discussed in the following sections.

scripts / se puede usar en
alta de usuarios se da click a
un usuario en especial y
se da al script que quiere)
que accese.

Controlling Web Site Access Through TCP Port Number

Most common TCP/IP utilities have specific TCP ports associated with them, and the software that allows you to use these expect the ports to conform to the standard defaults. However, like a TV channel, these ports can be changed. If a certain set of data is being broadcast on a certain port, and that port is not the default port for that utility (like port 80 for HTTP traffic), the port must be determined in order to access the data. This may sound trivial, but because there are more than 65,000 TCP ports to choose from, you can hide your site from most casual users by choosing any TCP port other than 80.

Of course, this is not very robust security because if someone knows what port you are running on, that person will be able to return to your site. In addition, if you have a port sniffer or a security scanner, you would be able to easily determine the port that a particular Web server is running on. However, it is a good way to hide information from people who do not know what they are looking for.

If you change the TCP port for your Web site (to 8080, for example), any browser client who wants to access your site will have to manually type in the TCP port number along with the address of your site. For example, if your site was `www.mydata.com` and you were using TCP port 8080, a browser client would access your site with the URL `http://www.mydata.com:8080`.

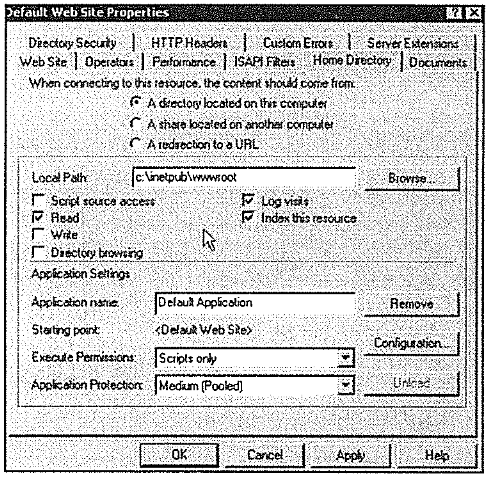
Step by Step 2.25 showed you how to determine and change a Web site's TCP port.

WARNING

Change the Port Right Away If you want to change the TCP port number, you should do it before any Web developers begin developing content for it because any links to your site need to be hard-coded with the TCP port number. If you change the TCP port number after the page development has been done, extensive re-coding will have to be done (something your Web developers will not appreciate).

Controlling Web Site Access Through Access Permissions

One of the most common ways to secure a Web site is to change the global settings for what all users can do. By making a Web site Read-Only, for example, you ensure that no one will be able to accidentally or purposefully make changes to the content of your site.



Default Web Site Properties

When connecting to this resource, the content should come from:

● A directory located on this computer
○ A share located on another computer
○ A redirection to a URL

Local Path: c:\inetpub\wwwroot

□ Script source access
☑ Read
□ Write
□ Directory browsing
☑ Log visits
☑ Index this resource

Application Settings

Application name: Default Application
Starting point: <Default Web Site>
Execute Permissions: Scripts only
Application Protection: Medium (Pooled)

FIGURE 2.38
Web access rights can be used to restrict the file-level permissions of the files on a site.

As you can see in Figure 2.38, there are four access rights that you can control for the entire site: Script Source Access, Read access, Write access, and Directory Browsing access.

Enabling Script Source Access allows users to see the source code behind the HTML page they are currently viewing. This would allow users to access not only HTML but also JavaScript, VBScript, and ASP source code.

Read access allows users to look at the content of the Web page and download files. If Read access is not enabled, no users will be able to access the content on the site.

Write access enables users to upload content to the site. This includes being able to modify the HTML or script content as well as placing new files into the site folder on your server.

Directory Browsing allows users to see a file listing in your Web site's main folder. This would allow a user to know what the names of your files are and to navigate through your file path to subfolders in your Web site. If this is not enabled, users must connect through the HTML pages you have set up on your Web site. If no default HTML page has been configured, browser clients will not be able to navigate your Web site at all.

You will need to make choices about which of these rights you want to enable for your user community. Remember that these rights are global across all users of your Web site; they will not discriminate. If you want to allow some users to upload files while denying other users, you will have to give Web site rights to Write and then control access using NTFS permissions on the local files or folders themselves.

You will also notice in Figure 2.38 that there is a logging setting. This setting, which is usually enabled, allows you to log all user interaction with this site. This log will allow you to monitor who is connecting to your site and what he or she is doing. The logging options (including the location of the log file) can be configured on the Web Site tab of the Web site's Properties dialog box.

Step by Step 2.26 shows you how to adjust the site access permissions.

STEP BY STEP

2.26 Changing Site Access Permissions

1. From the Start menu, choose Programs, Administrative Tools, Internet Services Manager.
2. In the IIS Console window, you can locate your Web site by expanding the Console Root, Internet Information Services, and Your Server. When you see your Web site in the tree under the name of your server, right-click it and choose Properties from the menu that appears.
3. In the Web Site Properties window, click the Home Directory tab. There you see check boxes under the Local Path field that you can use to set site access permissions. Select or deselect the appropriate rights.
4. Click OK to update the Web site's properties.

Controlling Web Site Access Through Execute Permissions

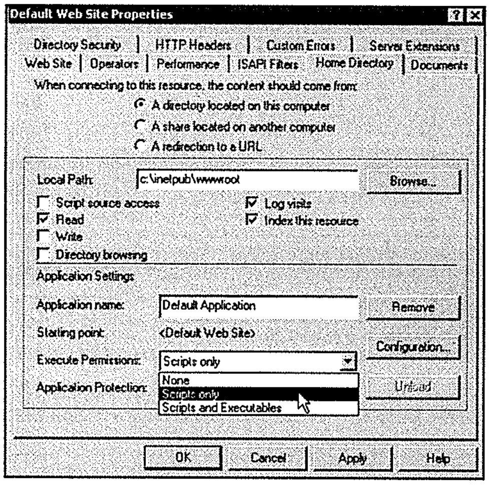
Another way to control site access is through execute permissions. Execute permissions (shown at the bottom of Figure 2.38) define what kind of scripts or executables a browser client can invoke on your site. The Execute Permissions include None, Scripts Only, and Scripts and Executables.

If you select None, no scripts will run on this Web site. This is obviously problematic because it means that Active Server Page scripts, JavaScript, and VBScript will not function. However, this is the most secure route to take because scripts can damage data and the underlying file system.

If you select Scripts Only, scripts (such as ASP, JavaScript, and VBScript) will run on this Web site. However, executables cannot be invoked.

WARNING

Write + Run Access = Trouble A user that has Write access to a Web site and the ability to run scripts and/or executables could pose a serious security risk to your site. The danger is so great that if this combination is allowed, IIS will display a message informing you of the inherent risks involved. By doing this, you could allow a user to create a damaging script or program, upload it to your site, and then run it.



When connecting to this resource, the content should come from:

● A directory located on this computer
○ A share located on another computer
○ A redirection to a URL

Local Path: c:\inetpub\wwwroot

□ Script source access
☑ Read
□ Write
□ Directory browsing
☑ Log visits
☑ Index this resource

Application Settings

Application name: Default Application

Starting point: <Default Web Site>

Execute Permissions: Scripts only

Application Protection:

None
Scripts only
Scripts and Executables

FIGURE 2.39
Execute permissions control the execution of programs and scripts on your Web server.

If you select Scripts and Executables, a user will be able to invoke any script or executable the user can get at. Although this provides a lot of functionality to the user, it is the most dangerous option in terms of security.

Step by Step 2.27 demonstrates how to change a site's execute permissions.

STEP BY STEP

2.27 Changing Site Execute Permissions

1. From the Start menu, choose Programs, Administrative Tools, Internet Services Manager.
2. In the IIS Console window, you can locate your Web site by expanding the Console Root, Internet Information Services, and Your Server. When you see your Web site in the tree under the name of your server, right-click it and choose Properties from the menu that appears.
3. In the Web Site Properties window, click the Home Directory tab. Click the Execute Permissions drop-down arrow to see the list of permissions (see Figure 2.39). Choose the level of script execute privileges you want to give out for your site.
4. Click OK to update the Web site's properties.

Controlling Web Site Access Through Authentication Methods

One of the strengths of using IIS as a Web server on a Windows 2000 server is the ability to integrate Windows 2000 computer or domain security into Web access. Essentially, you have the ability to force users to provide names and passwords from the local machine accounts or from the Active Directory to access Web sites. This eliminates the need to create your own security model.

Web authentication happens at two levels: anonymous and authenticated. Anonymous access is the first method attempted when a user tries to connect to any Web site. If anonymous access is disabled, or if a Web user tries to access a function that cannot be performed by an anonymous user, authenticated access is attempted. Anonymous access does not require a password. However, authenticated access always requires confirmation of identity, which might be in the form of a password challenge. But security information may be passed transparently (such as Integrated Windows access or with Client certificates, both of which will be covered later).

Under IIS, anonymous access is mapped to a user account. Therefore, any attempt to access a Web site anonymously will treat the user as though he or she were logged in as the anonymous IIS account. By default, the name of this account is IUSR_*servername.* That means that if your server were called "Green," the anonymous user account would be called "IUSR_Green" unless you change it to something else.

One way of securing your Web site is to disable anonymous access to the whole site. Then for any attempted access, the browser client will be prompted for a name and password to access the site. Another way to secure your site is to put NTFS security locally on some or all of your Web site. If you do this, for any attempted access of files or folders that do not allow anonymous access, a name and password will be required (whether the user is prompted for it depends on the type of authentication you require).

If you do require that a user log on to your site (or some portion thereof), you can set the type of authenticated access you want to require. There are three levels: basic authentication, digest authentication for Windows domain servers, and Integrated Windows authentication.

Basic authentication is the least secure but most accessible across a variety of browsers. This kind of authentication sends all login information in clear text. Unfortunately, if someone is "watching" your logon using a "packet sniffer" or other network analysis tool (Windows 2000 or NT Network Monitor, for example), he or she might be able to capture your user name and password as you log on. Basic authentication needs to be used for all browsers that do not support Integrated Windows authentication (non-Microsoft).

Although sending passwords in clear text is a security risk, this can be overcome by using server certificates and SSL (covered later).

When a user logs in using basic authentication, the user's combined name and password are checked against the directory that IIS has been told to use (either local or an Active Directory for the domain). If the name and password pass authentication, local security is checked on the files the user is trying to access, and if the user name has appropriate access in the ACL, access continues. If the name and password do not pass authentication, the user is prompted repeatedly until the user cancels the login operation. If the user name is not authorized to access the resource it is trying to access, it will pass authentication but be given an "Access denied" message.

NOTE

Configuration for Digest Authentication Two things are required in order for this kind of authentication to work. First, the IIS server must be a member of a domain. Second, each user that needs to authenticate through a browser must have his or her account to store the password using "reversible encryption." To do this, that setting must be enabled in the properties for the user (Account tab), and then the password for the user must be reset.

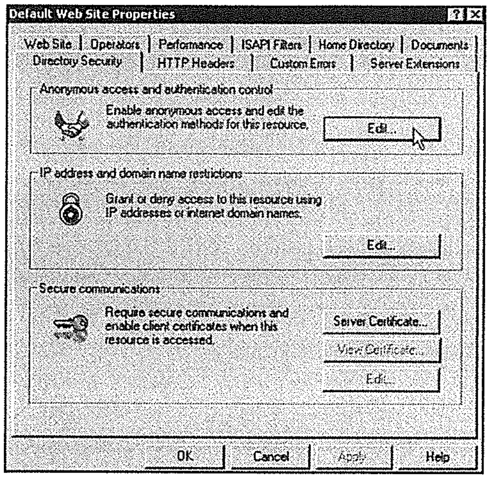
A second—and more secure—type of authentication is digest authentication. It is similar to basic authentication. However, it uses a hashing algorithm to encrypt data sent between the browser and the server. This hashing algorithm is classed as one-way in that it can be used to encrypt but not decrypt the data. This type of authentication works only on browsers that support the HTTP 1.1 standard and can respond to the requests the IIS server is making. At this point, only IE4.x and IE5.x support this authentication method. Although this method has some advantages over basic authentication, it has a major security flaw in that the password must be stored in clear text on the domain controller in order for the reverse encryption to be processed and compared. As a result, it is rarely used.

If digest authentication is configured and either the user's browser is not capable of using this type of authentication or the user's account has not been configured properly (as described in the Note titled "Configuration for Digest Authentication"), the authentication will fail.

The final authentication method is Integrated Windows authentication (formerly called NTLM or Windows NT Challenge/Response authentication). This method uses special encryption protocols to secure the authentication process. Unlike the other two authentication methods, IWA does not initially prompt for a user name and password. Instead, it checks the Windows logon currently in force on the client's machine. If this can be determined and authenticated, the user might never know that any restrictions are in place on the site. If the user does not authenticate or a Windows logon name cannot be determined, the browser will display a logon dialog box.

The benefit of this authentication method is its security. The disadvantages are that it does not work through a proxy server and that it works only on Internet Explorer 2.x or later (no Netscape support). This type of authentication is best used in an intranet environment where the browser type is known.

Step by Step 2.28 demonstrates changing the kind of user authentication required by your Web server.



Anonymous access and authentication control

Enable anonymous access and edit the authentication methods for this resource.

IP address and domain name restrictions

Grant or deny access to this resource using IP addresses or internet domain names.

Secure communications

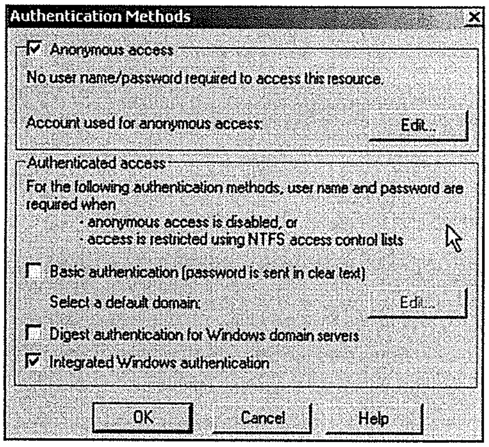
Require secure communications and enable client certificates when this resource is accessed.

FIGURE 2.40
You can configure access authentication from the Directory Security tab of the Properties dialog box.

STEP BY STEP

2.28 Changing Site Authentication Methods

1. From the Start menu, choose Programs, Administrative Tools, Internet Services Manager.
2. In the IIS Console window, you can locate your Web site by expanding the Console Root, Internet Information Services, and Your Server. When you see your Web site in the tree under the name of your server, right-click it and choose Properties from the menu that appears.
3. In the Web Site Properties window, on the Directory Security tab, click the Edit button in the section labeled Anonymous Access and Authentication Control (see Figure 2.40).
4. From the Authentication Methods dialog box, choose whether or not you want anonymous access to be configured (see Figure 2.41). If you do, you can choose to modify the account used for anonymous access or its password. To do that, click the Edit button and type in a new account name and password.
5. If you want to enable basic authentication, select the appropriate check box. When the Internet Service Manager warning comes up about the nature of basic authentication, click Yes to continue. Click Edit to define the location of the accounts used to authenticate Web users. If you leave it at default, the local accounts for the server will be used. You can also enter a domain name to access an Active Directory to use for authentication; however, both cannot be used.



☑ Anonymous access

No user name/password required to access this resource.

Account used for anonymous access:

Authenticated access

For the following authentication methods, user name and password are required when
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☐ Basic authentication (password is sent in clear text)

Select a default domain:

☐ Digest authentication for Windows domain servers

☑ Integrated Windows authentication

FIGURE 2.41
You can configure anonymous access and/or any of three authentication methods.

continues

NOTE **Multiple Authentication Methods** If you choose more than one authentication method, after attempting anonymous access, IIS will attempt to authenticate using the most secure method (Integrated Windows) first. Then it will try less secure methods until all avenues of authentication have been exhausted.

continued

6. If you want to enable digest authentication or Integrated Windows authentication, select the appropriate check boxes.
7. Click OK to update the Web site's properties.

Controlling Web Site Access Through IP Address and Domain Name Restrictions

You can control the access that people have to your Web site to include only people with certain IP addresses (from within your company, for example) or to exclude people with certain addresses. By using IP address and domain name restrictions, you can ensure that even if someone obtains a user name and password that is valid, that person could still be prevented from accessing data. This could allow company employees to access the intranet when they are at their desks (with known TCP/IP addresses) but prevent them from accessing the intranet from home (where they have unknown or unauthorized TCP/IP addresses). In that scenario, you, as administrator, could configure your home IP address to be accessible but exclude all others.

When you restrict based on IP addresses or domain names, you can configure single IP addresses, multiple addresses based on a network ID and a subnet mask, or addresses falling into a certain domain. If you choose to restrict based on domain (for example, to exclude all users whose IP addresses are registered to BADGUYS.com), your IIS server will have to do a reverse lookup on each IP address that traffic comes from. This is always very time and resource intensive and might not yield accurate results. Caution should be exercised when choosing this method.

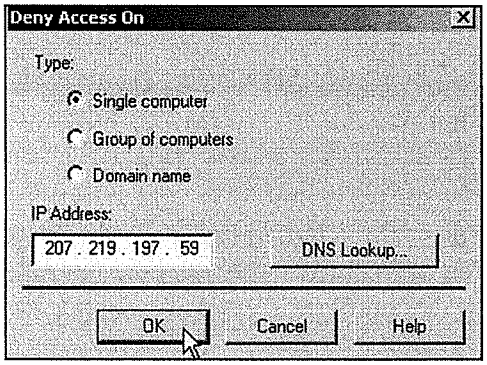
Disallowing accesses using this method has precedence over all other access a user might have been given to the Web site.

This method for changing site address and name restrictions is covered in Step by Step 2.29.

STEP BY STEP

2.29 Changing Site IP Address and Domain Name Restrictions

1. From the Start menu, choose Programs, Administrative Tools, Internet Services Manager.
2. In the IIS Console window, you can locate your Web site by expanding the Console Root, Internet Information Services, and Your Server. When you see your Web site in the tree under the name of your server, right-click it and choose Properties from the menu that appears.
3. In the Web Site Properties window, on the Directory Security tab, click the Edit button in the section labeled IP Address and Domain Name Restrictions (see Figure 2.42).
4. In the IP Address and Domain Name Restrictions dialog box, choose whether you want to implicitly grant access except to listed addresses or to implicitly deny access except to listed addresses (see Figure 2.43). Then click the Add button.
5. From the Deny Access On or Allow Access On dialog box (see Figure 2.44), choose Single Computer and enter the IP address, or choose Group of Computers and enter the network address and subnet mask, or choose Domain Name and enter the domain name. Then click OK to exit.
6. Click OK until you exit back to the IIS console.


Deny Access On

Type:

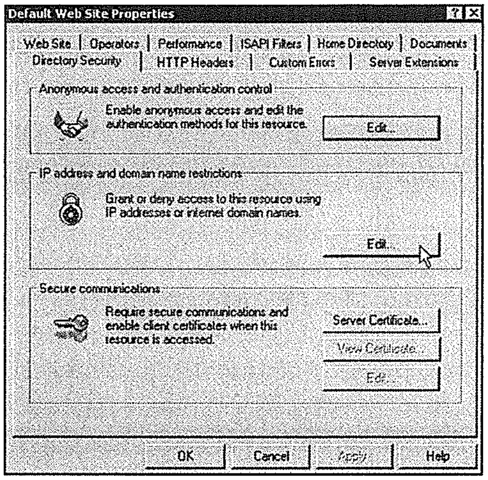
● Single computer

○ Group of computers

○ Domain name

IP Address: 207 . 219 . 197 . 59

FIGURE 2.44
You can deny access by specific IP address.


Default Web Site Properties

Anonymous access and authentication control

Enable anonymous access and edit the authentication methods for this resource.

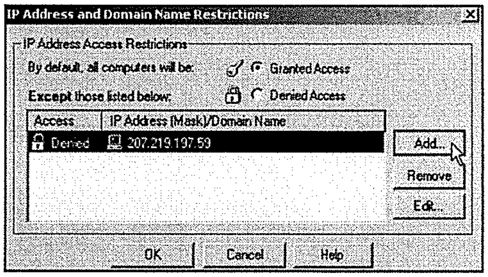
IP address and domain name restrictions

Grant or deny access to this resource using IP addresses or internet domain names.

Secure communications

Require secure communications and enable client certificates when this resource is accessed.

FIGURE 2.42
You can configure IP address and domain name restrictions from the Directory Services tab of the web site's Properties dialog box page.


IP Address and Domain Name Restrictions

IP Address Access Restrictions

By default, all computers will be: ● Granted Access

Except those listed below: ○ Denied Access

Access	IP Address (Mask)/Domain Name
Denied	207.219.197.59

FIGURE 2.43
You can explicitly grant or explicitly deny access by IP address or domain name.

Securing Web Access Using Certificates

Certificates are a final way of securing Web access and authenticating users. In Windows 2000, the use of certificates is pervasive, as much of the security uses certificates in one way or another. As a result, the discussion of certificates here will be restricted to their use in Web transactions.

The idea of the certificate as it applies to Web transactions is that an entity (server or client) proves its identity to another using a piece of identification—the certificate. The passport will provide an excellent example of how certificates work. As a Canadian citizen, I have been issued a Canadian passport that verifies that I am a certain person and that I am a citizen of Canada. When I cross the border into the United States, I can show my passport to the Customs official as proof of my identification and citizenship. This passport is deemed to be valid only if two conditions are met: The passport must be authenticated by the Canadian government (which is done through special security coding on the passport documents), and the Customs official must recognize the Canadian government as being trusted to make assertions about me. If the passport is deemed to lack authenticity or if the Customs official does not recognize the Canadian government as a trusted authority in passport issues, my passport is not acceptable for the purposes of identification.

Computer certificates work in much the same way a passport does. A server certificate issued to a Web server identifies that server as being a particular entity. This certificate must be authenticated by a third party (not me and not the server itself). This authenticating party is referred to as the Certificate Authority (CA). An example of a CA that is commonly used is Verisign. The authentication is only half of the requirement in order to create a trusted environment; my Web browser must trust Verisign to make assertions about servers. Fortunately, all current browsers are configured to trust certain CAs, of which Verisign is one. Once my browser and the Web server have verified that the server is who it says it is, a security negotiation can take place, thus enabling encrypted transmissions to take place.

Client certificates, on the other hand, are used to verify the identity of a person using a Web browser. Just as a server certificate allows a server to be identified, a client certificate allows a browser client to be identified. As with a server certificate, a client certificate must be authenticated by a third party, and that third party must be trusted by the server. If that is the case, the identity of a browser client can be established without sending a password over the Internet; all that is sent is the certificate information that identifies the particular user. This identification is made possible by incorporating the client certificate into the Web browser and then exporting the certificate to the IIS server. The certificate is then mapped to an account recognized by the IIS server and, when the certificate is seen in the future, it is recognized as being verification of a specific user. From that point, all permissions that apply to the user are applied to the holder of the certificate. Certificates can be mapped on a one-to-one basis with each being mapped to a unique user account, or a group of certificates can be mapped to a single account that has access to a Web site or set of data.

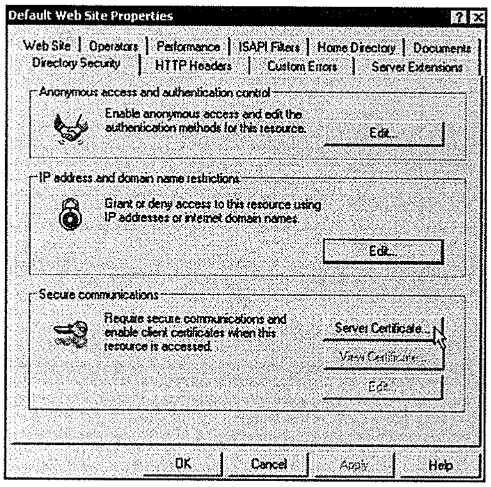
The use of Server certificates enables encryption of Web transmissions by way of secure sockets layer (SSL). The use of Client certificates enables password-free authentication of browser clients. These two certificate uses can be used independently or together.

Certificates can be obtained by purchase from a third party or they can be created by the Windows 2000 Certificate Services (a product that used to be part of IIS but which, because of its use throughout Windows 2000 security, has now been unbundled from IIS and can be installed as a separate operating system component). For Internet applications, third-party certificates are most often used because all browsers trust the third-party certificate vendors and, therefore, no browser configuration is required (except for installing the 128-bit security upgrade if you require it). For Intranet applications, you can use the Windows 2000 CA, but all your browsers must be configured to trust your root certifier.

Securing Web Access Using Server Certificates and SSL

SSL is an encryption methodology that relies on a server certificate to establish server identity and form the basis for encryption. As was mentioned in the introduction above, a certificate held by a server that comes from a CA trusted by a browser client can be used to guarantee a server's identity. In addition, with SSL enabled, it can be used to negotiate an encryption scheme between the browser and the server that ensures secure transmission of data. Under this system, clear text authentication is no longer a security hazard because the clear text password is being encrypted by the SSL connection and, therefore, is not clear text at all. This allows for not only the secure transmission of passwords but also for secure transmission of other confidential information (like credit card numbers on an e-commerce site). In addition, SSL transmissions can pass through firewalls, providing that TCP port 443 is open.

Step by Step 2.30 demonstrates the process of adding a server certificate to a Web site.



Anonymous access and authentication control

Enable anonymous access and edit the authentication methods for this resource.

IP address and domain name restrictions

Grant or deny access to this resource using IP addresses or internet domain names.

Secure communications

Require secure communications and enable client certificates when this resource is accessed.

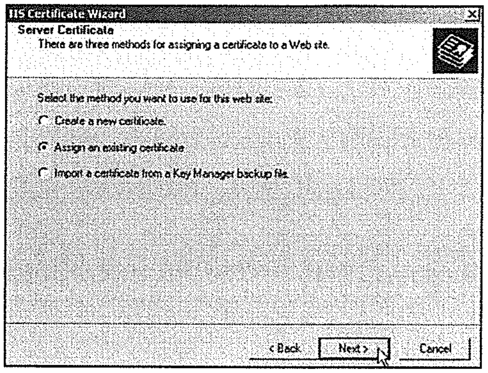
FIGURE 2.45
Server certificates can be added from the Directory Security tab of the Web site's Properties dialog box sheet.

STEP BY STEP

2.30 Adding a Server Certificate to a Web Site

1. Obtain a digital certificate from a trusted source.
2. From the Start menu, choose Programs, Administrative Tools, Internet Services Manager.
3. In the IIS Console window, you can locate your Web site by expanding the Console Root, Internet Information Services, and Your Server. When you see your Web site in the tree under the name of your server, right-click it and choose Properties from the menu that appears.
4. In the Web Site Properties window, on the Directory Security tab, click the Server Certificate button in the section labeled Secure Communications (see Figure 2.45).
5. When the Certificate Wizard appears, click Next to continue.

6. On the Server Certificate page, select the method you are going to use to obtain a server certificate (see Figure 2.46). If you already have a certificate, choose Assign an Existing Certificate. Click Next to continue.
7. On the Available Certificates page, select the certificate you want to assign to this server (see Figure 2.47). Then click Next.
8. Click Next at the summary page, and click Finish at the completion page.


IIS Certificate Wizard

Server Certificate

There are three methods for assigning a certificate to a Web site.

Select the method you want to use for this web site:

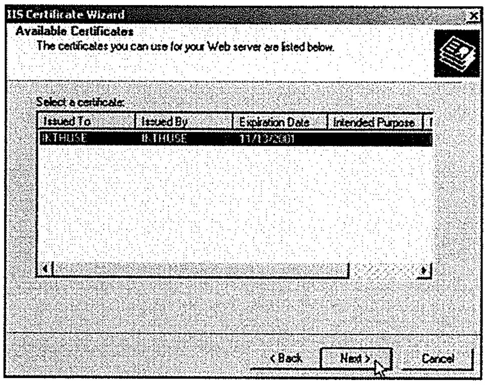
○ Create a new certificate.

● Assign an existing certificate

○ Import a certificate from a Key Manager backup file.

FIGURE 2.46
If you already have a certificate, you can add it to the server.

After the server certificate has been added to your site, you must configure your server for certificate authentication. The following Step by Step shows how to do that.


IIS Certificate Wizard

Available Certificates

The certificates you can use for your Web server are listed below.

Select a certificate:

Issued To	Issued By	Expiration Date	Intended Purpose
IKTHUSE	IKTHUSE	11/13/2001	

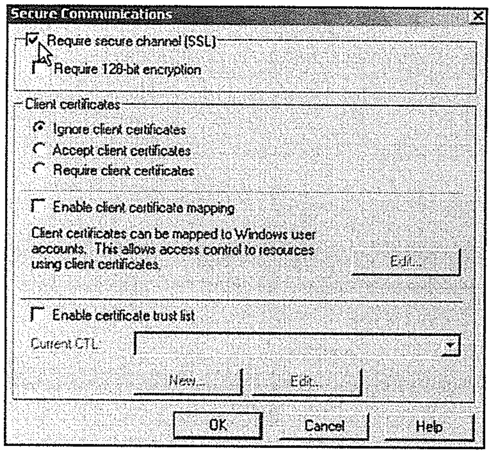
FIGURE 2.47
Select a certificate from the available certificates list.

STEP BY STEP

2.31 Configuring Secure Communications on a Web Site

1. Open the properties for your Web site.
2. From the Start menu, choose Programs, Administrative Tools, Internet Services Manager.
3. In the IIS Console window, you can locate your Web site by expanding the Console Root, Internet Information Services, and Your Server. When you see your Web site in the tree under the name of your server, right-click it and choose Properties from the menu that appears.
4. From the Secure Communications dialog box, select Require Secure Channel (SSL) (see Figure 2.48).

continues



Secure Communications

☑ Require secure channel (SSL)

□ Require 128-bit encryption

Client certificates

● Ignore client certificates

○ Accept client certificates

○ Require client certificates

□ Enable client certificate mapping

Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.

□ Enable certificate trust list

Current CTL:

FIGURE 2.48
After a certificate has been added, you can secure your site using SSL.

continued

5. If you want to enable extra security, you can select Require 128-Bit Encryption. This kind of encryption can be imported to and enabled by people in all countries except for those that have state-supported terrorism. As of the time of this writing, this list includes Cuba, Iran, Iraq, Libya, North Korea, Syria, Sudan, Serbia, and Taliban-controlled areas of Afghanistan. If your Web site supports e-commerce or banking, you should enable this security.

Enabling Client Authentication Using Client Certificates

Client certificates are an alternate form of authentication to the ones described in the previous sections. What sets this form of authentication apart from the others is that no passwords are required by the client when a browser connects to a site requiring authenticated access. Instead, the browser sends certificate information that the Web server has mapped to a certain user account. Using this method, any browser can be used to connect to a site requiring authentication, without having to allow clear-text passwords and without requiring the user to actually log on using a user name and password.

The steps for configuring authentication using client certificates are straightforward. First, the server must have a certificate installed issued by the same CA that the clients' certificates are coming from. This will enable you to set the configuration to allow for client certificates for authentication.

Next, your clients must have a certificate installed on their browser. Like server certificates, these certificates need to be authenticated by a trusted source. If the browsers are connecting to an intranet, you could use the Certificate services to generate a root certifier and client certificates. If the connection is to an Internet site, the clients will most likely use a third-party certificate vendor like Verisign.

Finally, after clients have certificates installed, these need to be exported to the Web server and mapped to user accounts. Once the mapping has occurred, the server will be able to authenticate the client as being a particular user simply by being shown the client certificate. When the user is authenticated, access to resources is the same as that of any other authenticated user.

The next Step by Step shows how to enable client certificates for authentication.

STEP BY STEP

2.32 Configuring a Web Server to Accept Client Certificates for Authentication

1. Install a server certificate on your Web server (see Step by Step 2.31).
2. From the properties of the Web site for which you want to enable client certificate authentication, click the Directory Security tab.
3. On the Directory Security tab, click Edit in the Secure Communications section.
4. In the Secure Communications dialog box, you can select Accept Client Certificates or (if SSL has been enabled) Require Client Certificates. Accept allows, but does not require, a browser to attempt to authenticate with this Web server using a client certificate. Require Client Certificates forces a browser to attempt to authenticate with this Web server using a client certificate; failure or lack of certificate causes authentication to fail.
5. In the Secure Communications dialog box, select the check box labeled Enable Client Certificate Mapping, and then click the Edit button next to it. You can then add mappings between exported client certificates (provided by the clients) and user accounts (one-to-one mapping), or you can add a mapping between a root certifier and a user account (many-to-one mapping). A mapping between a root certifier and a user account ensures that anyone authenticating with a certificate from a specific root certifier will be given the same access on the Web site.

continues

continued

6. In the Secure Communications dialog box, you can also enable a Certificate Trust List (CTL). A CTL is a list of certifiers you trust. If a client tries to authenticate with a certifier not in the CTL, that certificate will be rejected.
7. When configuration is complete, click OK to exit.

Troubleshooting Web Site Access

Web site access is about two things: access to a running server and security.

Troubleshooting lack of access because of a server not running was covered in the earlier section "Troubleshooting Sharing."

Lack of access because of security issues revolves around all the topics that have been covered in this section. Look for TCP port incompatibilities and fix them if uncovered.

If a user is getting "Access denied" messages, check for authentication methods and underlying NTFS permissions. In addition, check for client certificates and see whether they are required. IP address restrictions may also cause these kinds of messages so check for these, too.

If a user can get to your site but cannot do what is desired (like upload files or execute scripts), check for those permissions and adjust them if necessary.

CONFIGURING AND MAINTAINING PRINTERS

Monitor, configure, troubleshoot, and control access to printers.

Next to accessing data, access to printers is probably the most important need for users. Most often, having a print device physically attached to every person's workstation is impractical, so a shared solution is desired. Windows 2000 Server provides you with the ability to host one or more print devices and to make them accessible to users.

Before you get into the mechanics of setting up printers and administering them, first look into the processes and terminology.

The Printing Process

You will rarely print from an application running directly on your Windows 2000 server. Instead, from a client computer, you will print to a printer that is shared on a Windows 2000 server. The act of sharing a printer on a Windows 2000 server denotes that server as a print server (a title which is descriptive, not prescriptive).

The process of printing can be broken down into discrete steps:

1. The client application requests to print to a printer defined on the network (which has been configured on the local client).
2. If the client operating system is Microsoft 32-bit, the following things happen locally on the client:
   - A local printer driver formats the request and sends it to a local spooler. If the client operating system is Windows 2000 or Windows NT 4.0, the client also contacts the print server to ensure that it has the most recent version of the printer driver; if it does not, that server's version of the printer driver is downloaded to the client.
   - A remote procedure call is used to contact the print server and to transfer the print job to the server. If the print server cannot be contacted, the print job is held in the local spooler until the print server can be contacted.
3. If the client operating system is not Microsoft 32-bit (or if it is configured to send only RAW), a local printer driver formats it into a RAW (printable) format and sends it to the print server.
4. When the print server receives the job, it is in RAW format. The job is written directly to disk in the spooler file in preparation to be sent to the print device. If it is not in RAW format, the print job may be modified to include separator pages and to print in duplex modes. This happens in the spooler file.

EXAM TIP

Printer Terminology Terminology is very important, especially for the exam. Keep in mind that when the exam makes reference to a printer, it is talking about a software interface, not a physical device. The device is called a "print device"; all the software that you install and the icon you see in the Printers window is referred to as a printer. In order to make this clearer, I will often refer to this as the "virtual printer." The term "virtual printer" has been known to show up in Microsoft documentation, but I don't envision it making its way to the exam.

5. When the job arises next in the print queue, the job is sent to the print device, and it is converted into a bitmap format and is printed.

A *printer driver* is a piece of software responsible for communicating specific commands to a print device. Each driver is a little different because each print device is different.

A *spooler* is a file on a hard drive, which is the location that a client or a server uses to store print jobs that are pending printing. The print queue is the list of jobs stored on the spooler; this queue can be observed through the print manager.

As you can see from the previous points, Microsoft 32-bit operating systems maintain their own spoolers and keep their own copies of the printer drivers. In this way, the client can ensure that most of the work is done in the printing processes before the job gets sent to the print server. In addition, it also ensures that jobs can "print" even if the printer cannot be contacted at the time the job is submitted. In that case, the job simply sits on the local spooler until the print server can be contacted.

There is a difference between Windows NT and Windows 2000 clients and Windows 9x clients. The difference is that NT and 2000 clients have a mechanism to automatically update their versions of the print driver. When a job is to be submitted, the print server is contacted, and the print drivers are compared. If the server's driver is newer than the one on the client, the client's driver is updated automatically. Not so with Windows 9x clients. When a Windows 9x client establishes a connection to a network printer, the driver is installed (either from the print server or from the Windows 9x CD) and is not automatically updated.

On non-32-bit clients (like Windows 3.11, DOS, or UNIX clients), the print job is completely formatted at the client and sent to the server. There is no spooler on the client, and if the print server cannot be contacted, the print process fails at the client side.

Configuring the Print Server

The print server is the collection of software routines that provides print capabilities either locally or over a network. It is configured from the Printers folder, which is accessible either from the Control

Panel (double-click the Printers icon) or via Start, Settings, Printers. Once the Printers folder has been opened, you can get to the properties of the print server by choosing File, Server Properties.

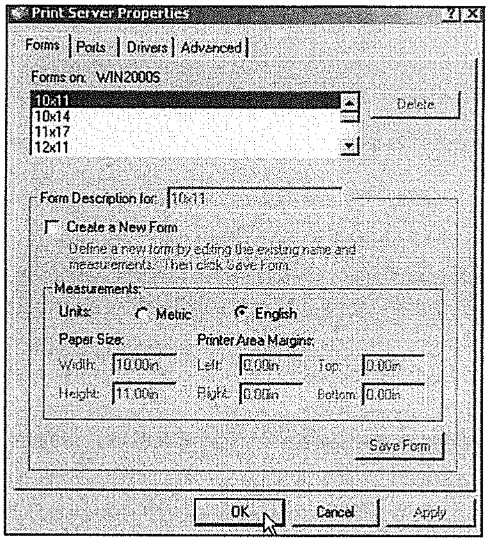
The properties of the print server configuration dialog box are divided into four tabs: Forms, Ports, Drivers, and Advanced.

The Forms Tab

The Forms tab is used to create new form (paper size and format) configurations (see Figure 2.49). These forms are applied globally to the print server and can be made available to any virtual printer defined in it.

A number of forms are predefined, and you cannot modify or delete them. In addition, if you have a need to define a form that is not present, you can do so by selecting Create a New Form check box and then filling in a new name, dimensions, and margins for it. When you click on the Save Form button, the form will be available to any virtual printer that is configured on your server.

The advantage of forms is that they can be assigned to different paper trays on your printer (if you have more than one) and can be used to ensure that a user printing from an application will always print on the right size paper.



Forms on: WIN2000S

10x11
10x14
11x17
12x11

Form Description for: 10x11

□ Create a New Form

Define a new form by editing the existing name and measurements. Then click Save Form.

Measurements:

Units: ○ Metric ● English

Paper Size: Width: 10.00in Height: 11.00in

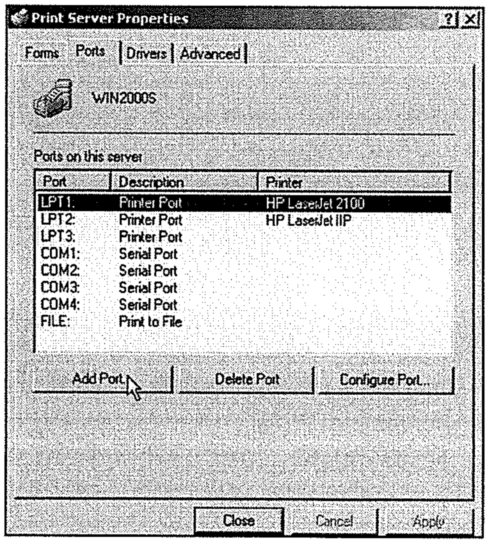
Printer Area Margins: Left: 0.00in Right: 0.00in Top: 0.00in Bottom: 0.00in

FIGURE 2.49
The Forms tab of the Properties dialog box is used to create, modify, and delete printer forms.

The Ports Tab

From the Ports tab, you define output locations for print jobs (see Figure 2.50). When you define a printer on your server, it must print to a location, like a data pipe. When information goes into the pipe, it is assumed that there is a print device at the other end. Ports enable you to define the openings into which print data is poured.

A number of ports come predefined in Windows 2000 Server. Not all of these ports actually define physical connections; these are defined by default, and it is up to you to configure the ones that will actually be used. Most frequently, print devices are physically connected to an LPT (parallel) port.



WIN2000S

Ports on this server

Port	Description	Printer
LPT1:	Printer Port	HP LaserJet 2100
LPT2:	Printer Port	HP LaserJet IIP
LPT3:	Printer Port	
COM1:	Serial Port	
COM2:	Serial Port	
COM3:	Serial Port	
COM4:	Serial Port	
FILE:	Print to File	

FIGURE 2.50
On the Ports tab of the Properties dialog box, you can define connections to output devices (real or virtual).

The default ports cannot really be configured. However, if you require more IRQ's, you could delete them using the Hardware Manager. A parallel port has only one configurable parameter: the retransmission retry in seconds when the print device is unavailable (like when it is out of paper).

This is the place where you can create your own ports and configure them. You might create new ports when you want to create a connection pipe that is not physical or at least not physically connected to a print device attached to your computer. This is done when you want to output print jobs to files, output to printers with network cards, or forward to other print servers (whether or not they are Windows-based).

With no additional services installed on your Windows 2000 server, you have two port types available: Local and Standard TCP/IP (other port types may show up if you have specific print services installed).

A local port defines a connection to a printer that's physically connected to your server (like on a parallel port), a test connection, an infrared connection (accessible through a UNC name), or a local file.

When you define a new local port, you are prompted for the name of the port. The answer you give determines where the print output will be directed. The following list outlines the possible answers and what they indicate:

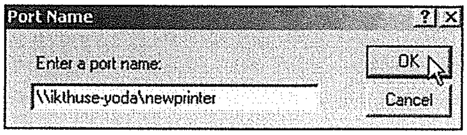
- *A filename (like c:\printout\job.txt).* This defines a file to redirect the jobs to. Each subsequent print job will overwrite the previous.
- *The share name of a printer defined on another computer (like \\server1\hpprinter).* This will redirect the output to a shared printer or another print server. This is often used when a print device goes down and you want to allow clients to continue to print without having to reconfigure all the clients to print to a different print device. When requests come in, they are redirected to the other printer.
- *The word "NUL."* Jobs sent to the null port will be immediately deleted. This port type is used to test whether a client can print without having to waste paper or to queue up in front of other print jobs.
- *The word "IR."* This defines a connection to an infrared port to allow you to print to infrared capable printers.

Step by Step 2.33 demonstrates how to add a new local port to a Windows 2000 computer.

STEP BY STEP

2.33 Adding a New Local Port

1. From the Print Server properties dialog box, select the Ports tab and click the Add Port button.
2. In the Printer Ports dialog box, select Local Port and click New Port.
3. In the Port Name dialog box (see Figure 2.51), enter a local port name and click OK.
4. Exit the local port configuration dialog box.



Enter a port name: \\ikthuse-yoda\newprinter

FIGURE 2.51
A new local port can connect to a shared printer on another server.

A Standard TCP/IP port is used to connect directly to a network printer that supports TCP/IP communication. This kind of printer has a network card in it and acts much like a regular computer on the network. When you configure a Standard TCP/IP port, you define the connection via the TCP/IP address of the printer, and requests to print on this printer will be redirected to its TCP/IP address. The configuration of such a port will generally vary depending on the printer type. Some print devices have special software that you can install on your print server that gives you a console from which to do administration. If you use the standard Windows 2000 TCP/IP port configuration, you will need to know the TCP/IP address of the print device (however that is determined).

NOTE

Printing Directly to a Print Device Many TCP/IP capable printers will allow you to print to them directly without having to have the jobs mediated through a Windows 2000 server. The disadvantage of this is that you do not get the benefits of Windows 2000 printer security, scheduling, or administration.

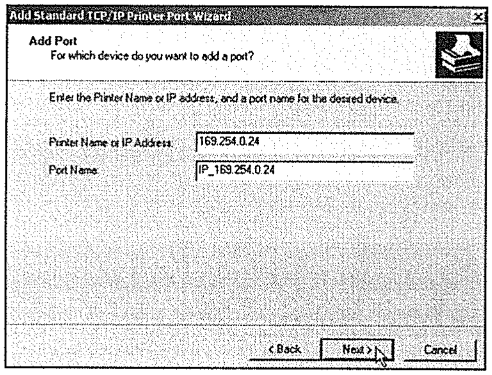
The next Step by Step walks you through the configuration of a Standard TCP/IP port.

STEP BY STEP

2.34 Configuring a Standard TCP/IP Port

1. From the Print Server properties dialog box, select the Ports tab and click the Add Port button.

continues



Add Standard TCP/IP Printer Port Wizard

Add Port

For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 169.254.0.24

Port Name: IP_169.254.0.24

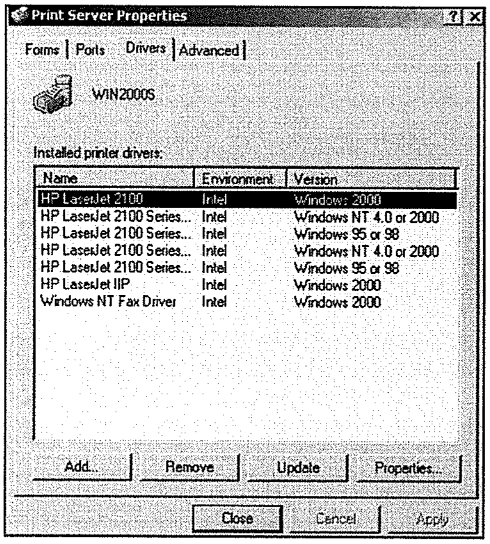
FIGURE 2.52
A TCP/IP printer (or network connected print server) has its own network card and TCP/IP address.

continued

2. In the Printer Ports dialog box, select Standard TCP/IP Port and click New Port.
3. When the Add Standard TCP/IP Printer Port Wizard appears, click Next.
4. In the Add Port dialog box, enter the TCP/IP address and a Port Name for the new port (see Figure 2.52). The port name will automatically default to IP_*ipaddress*. Click Next to continue.
5. When the Completing the Add Standard TCP/IP Printer Port Wizard dialog box appears, click Finish to complete the port configuration.

After ports have been configured, you can then install printers to print to them.

The Drivers Tab



Print Server Properties

WIN2000S

Installed printer drivers:

Name	Environment	Version
HP LaserJet 2100	Intel	Windows 2000
HP LaserJet 2100 Series...	Intel	Windows NT 4.0 or 2000
HP LaserJet 2100 Series...	Intel	Windows 95 or 98
HP LaserJet 2100 Series...	Intel	Windows NT 4.0 or 2000
HP LaserJet 2100 Series...	Intel	Windows 95 or 98
HP LaserJet IIP	Intel	Windows 2000
Windows NT Fax Driver	Intel	Windows 2000

FIGURE 2.53
You should have drivers available for all the clients who will access this printer.

Drivers are the software components responsible for converting high-level requests for printing into commands the processor can execute (see Figure 2.53). These commands are specific to the print device, the operating system that is requesting a print service, and the processor that is in the computer requesting the print service. As a result, a very large number of print drivers are available.

When you install a printer on your Windows 2000 server, the driver for your print device that is specific to an Intel-based Windows 2000 server is installed on your print server. The driver for this installation is obtained from the drivers.bin file local on your Windows 2000 computer (you should never have to produce the Windows 2000 CD-ROM to do a printer installation). However, there are reasons for installing more drivers. As was indicated already, when a client configures connectivity to a network printer, the first check made is to see if the driver is available from the print server. If it is not, the client is prompted to produce the driver (usually from a CD-ROM). You can avoid the user's questions and problems by ensuring that the most up-to-date drivers are available to your clients; this can be done by installing the platform-specific (hardware and software) drivers on your server.

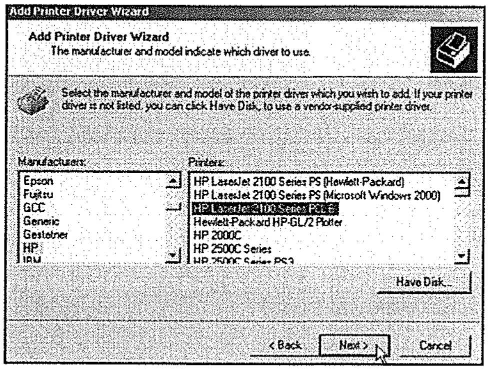
Although Windows 2000 does not support the Compaq Alpha hardware platform, Windows NT 4.0 did. Therefore, you may need to install drivers for Windows 3.5x, Windows NT Alpha, and Windows 9x on your print server.

Step by Step 2.35 outlines the procedure for installing a printer driver on a Windows 2000 server.

STEP BY STEP

2.35 Installing a Printer Driver

1. From the Print Server properties dialog box, select the Drivers tab and click the Add button.
2. When the Welcome to the Add Printer Driver Wizard screen appears, click Next to continue.
3. At the Add Printer Driver Wizard dialog box, choose the printer manufacturer and model of your printer (see Figure 2.54). If the model is not available, you must provide a driver yourself. To do this, click the Have Disk button and browse to the location of your driver (on a disk, hard drive, network drive, CD-ROM, or Internet location). When you have provided the model, click the Next button to continue.
4. In the Environment and Operating Systems dialog box, select the correct environment (hardware platform) and operating system (software platform) combination (see Figure 2.55). Then click Next to continue.
5. At the Completing the Add Printer Driver Wizard dialog box, click Finish to continue.
6. You may be prompted to insert one or more CD-ROMs depending on the platform(s) you are installing.



Add Printer Driver Wizard

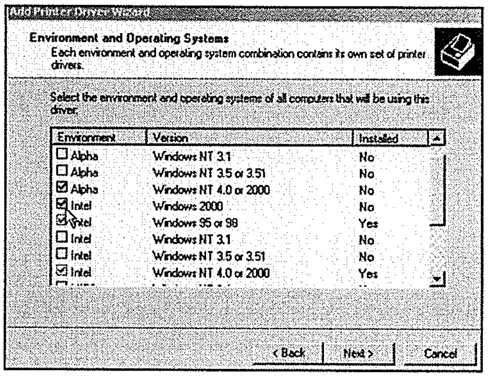
Add Printer Driver Wizard
The manufacturer and model indicate which driver to use.

Select the manufacturer and model of the printer driver which you wish to add. If your printer driver is not listed, you can click Have Disk, to use a vendor-supplied printer driver.

Manufacturers:
Epson
Fujitsu
GCC
Generic
Gestetner
HP
IBM

Printers:
HP LaserJet 2100 Series PS (Hewlett-Packard)
HP LaserJet 2100 Series PS (Microsoft Windows 2000)
HP LaserJet 2100 Series PCL 6
Hewlett-Packard HP-GL/2 Plotter
HP 2000C
HP 2500C Series
HP 2500C Series PS3

FIGURE 2.54
Identify the printer manufacturer and model.



Add Printer Driver Wizard

Environment and Operating Systems
Each environment and operating system combination contains its own set of printer drivers.

Select the environment and operating systems of all computers that will be using this driver.

Environment	Version	Installed
☐ Alpha	Windows NT 3.1	No
☐ Alpha	Windows NT 3.5 or 3.51	No
☑ Alpha	Windows NT 4.0 or 2000	No
☑ Intel	Windows 2000	No
☑ Intel	Windows 95 or 98	Yes
☐ Intel	Windows NT 3.1	No
☐ Intel	Windows NT 3.5 or 3.51	No
☑ Intel	Windows NT 4.0 or 2000	Yes

FIGURE 2.55
Identify the operating systems that will host clients for this printer.

In addition to adding a new driver, you might need to update a driver. When new versions of the drivers are created, it is a good practice to update your drivers with the new versions. For Windows 9.x clients, updating a driver requires actually installing the new driver manually on the computers. For Windows 2000 and NT clients, the new drivers will be automatically downloaded during the printing process.

A walk-through of the procedure for updating printer drivers is shown in Step by Step 2.36

STEP BY STEP

2.36 Updating a Printer Driver

1. From the Print Server Properties dialog box, select the Drivers tab, select the driver you want to update, and click the Update button.
2. When prompted, confirm that you really want to update the driver you selected.
3. When prompted, insert the CD-ROM or browse to the location of the new drivers, and then click OK to update the drivers.

If you find that a driver is no longer required, it is prudent to remove it from your print server. This is especially helpful when you upgrade your printing hardware and the drivers installed are for printers no longer accessible from the print server. Removing a driver is covered in the following Step by Step.

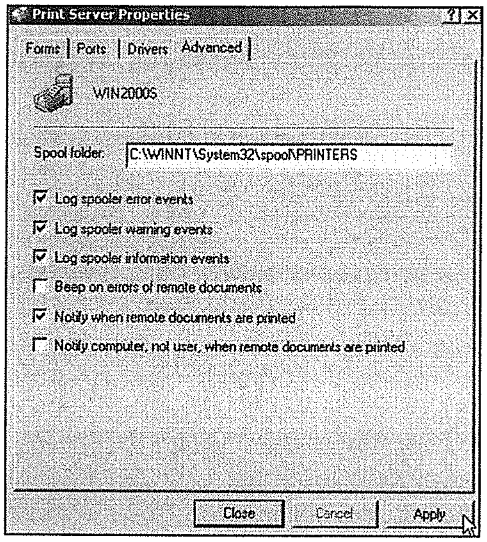
STEP BY STEP

2.37 Removing Printer Drivers

1. From the Print Server Properties dialog box, select the Drivers tab, select the driver you want to remove, and click the Remove button.
2. When prompted, confirm that you want to remove the driver by clicking the Yes button.

The Advanced Tab

The Advanced tab allows you to set such global defaults as the location of the spooler file, whether events having to do with the spooler are logged to the event log, and whether users are informed when documents have finished printing (see Figure 2.56).



WIN2000S

Spool folder: C:\WINNT\System32\spool\PRINTERS

☑ Log spooler error events
☑ Log spooler warning events
☑ Log spooler information events
☐ Beep on errors of remote documents
☑ Notify when remote documents are printed
☐ Notify computer, not user, when remote documents are printed

FIGURE 2.56
Advanced settings are modified on the Advanced tab of the Properties dialog box.

The location of the spooler file is important, especially when the default drive is running out of space. By moving the spooler folder to a drive with more free space, you can save yourself a lot of troubleshooting problems. It is important to mention at this point that a change to the path of the spooler folder will result in immediate change. This change will prevent any documents that are pending printing from printing. To avoid this, it is best to change the spooler folder location when no one is printing to the printer.

The other options available on the Advanced tab of the Properties dialog box can be divided into logging, error notification, and print notification areas.

The first three check boxes define the level of event logging that is done for the printer. You can log errors, warnings, and information. If you do not want your event log to include information about when the printer is working correctly, you might remove logging of informational events.

The fourth check box, Beep on Errors of Remote Documents, instructs the server to beep when printing errors occur.

The last two check boxes have to do with notification of print job completion. If you select Notify When Remote Documents Are Printed, the user (if logged on) who sent the print job will be informed via a popup message when the print job has completed. If you also select Notify Computer, Not User, When Remote Documents Are Printed instead of a specific user being notified, the computer from which the print job was sent will be notified, regardless of who is logged on to it at the time.

When the print server has been configured, you can begin to consider installing printers on your server.

NOTE

Remove Availability by Removing Sharing You can make a printer unavailable on the network by removing the sharing. After you change the spooler folder's location, you can again share the printer, and the documents held in local spool files will be transmitted to the print server.

Installing a Local Printer on a Windows 2000 Server

The underlying assumption of the printer server is that one or more local print devices will be accessible from virtual printers installed on a Windows 2000 server. From those virtual printers, you can configure availability and access to the print devices. This section will examine the installation of virtual printers (icons giving access to print to physical print devices) and their configuration.

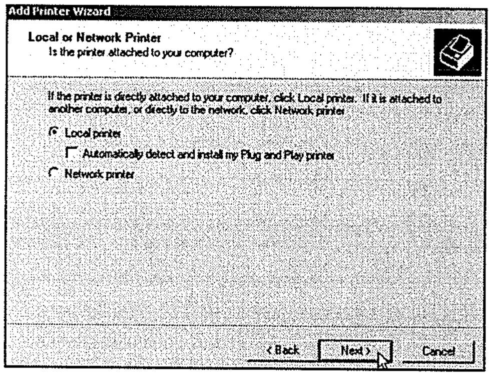
You add and configure virtual printers through the Printers folder. This folder can be accessed from the Control Panel; by choosing Start, Settings, Printers (refer to Figure 2.49); or from the Printers share on the server (this share allows you to access the Printers folder even when you do not have local access to the server).

You already have been exposed to this folder because it is from here that you were able to configure the print server itself. From this folder, you can also add new printers (local and network), share printers for client access, and remove printers. Step by Step 2.38 walks you through installing a local printer.

STEP BY STEP

2.38 Installing a Local Printer

1. From the Start menu, choose Settings, Printers.
2. In the Printers window, double-click the Add Printer icon.
3. At the Welcome to the Add Printer Wizard screen, click Next to continue.
4. At the Local or Network Printer dialog box, select Local Printer (see Figure 2.57). If your printer is Plug and Play compliant, you can (optionally) select the Automatically Detect and Install My Plug and Play Printer check box. If your server detects the printer, it will install the appropriate driver for it (and skip to the end of this procedure). Click Next to continue.



Add Printer Wizard

Local or Network Printer

Is the printer attached to your computer?

If the printer is directly attached to your computer, click Local printer. If it is attached to another computer, or directly to the network, click Network printer

● Local printer

□ Automatically detect and install my Plug and Play printer

○ Network printer

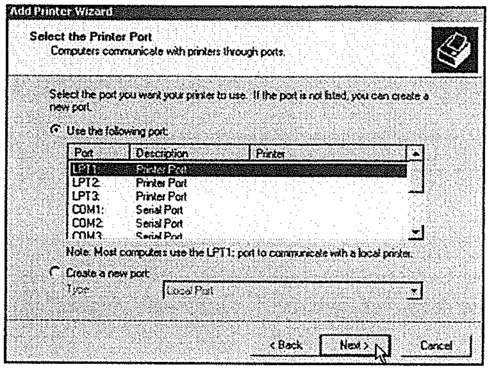
FIGURE 2.57
Identify the printer as connecting through a local port.

5. At the Select the Printer Port dialog box, shown in Figure 2.58, choose the port the printer is attached to (frequently it is LPT1). If you want to, you can create a new port (the procedure is outlined in Step by Steps 2.33 and 2.34). After choosing the port, click Next to continue.

6. At the Add Printer Wizard dialog box, enter the manufacturer and model of the printer you are connecting to (see Figure 2.59). If the model you have is not listed, or if you think that you have a more recent driver than Windows 2000 has, you can browse to the location of the driver by clicking the Have Disk button. Alternatively, you can also go to the Windows Update Web site to search for an updated driver by clicking the Windows Update button (you must have Internet access for this to work). After selecting the appropriate printer, click Next to continue.

7. At the Name Your Printer dialog box (see Figure 2.60), you can enter an intuitive printer name (something that describes its location, function, and/or ownership) and specify whether this is the default printer for this server (whether this device should be printed to if no specific printer is chosen by the user). Click Next to continue.

continues



Add Printer Wizard

Select the Printer Port

Computers communicate with printers through ports.

Select the port you want your printer to use. If the port is not listed, you can create a new port.

● Use the following port:

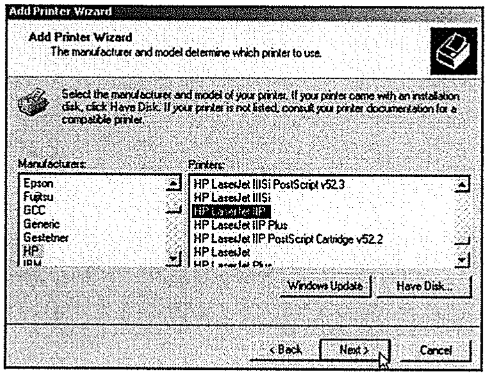
Port	Description	Printer
LPT1:	Printer Port	
LPT2:	Printer Port	
LPT3:	Printer Port	
COM1:	Serial Port	
COM2:	Serial Port	
COM3:	Serial Port	

Note: Most computers use the LPT1: port to communicate with a local printer.

○ Create a new port:

Type: Local Port

FIGURE 2.58
Specify the local port to connect through.



Add Printer Wizard

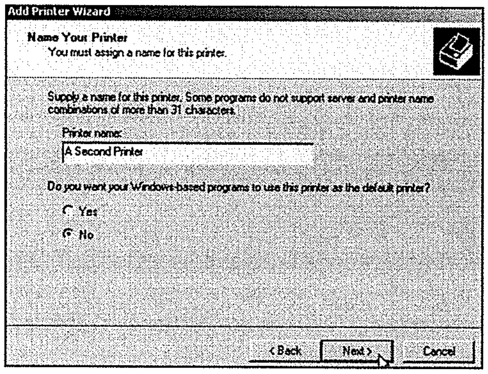
Add Printer Wizard

The manufacturer and model determine which printer to use.

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturers:	Printers:
Epson	HP LaserJet IIISi PostScript v52.3
Fujitsu	HP LaserJet IIISi
GCC	HP LaserJet IIP
Generic	HP LaserJet IIP Plus
Gestetner	HP LaserJet IIP PostScript Cartridge v52.2
HP	HP LaserJet
IBM	HP LaserJet Plus

FIGURE 2.59
Identify the manufacturer and the model of the print device.



Add Printer Wizard

Name Your Printer

You must assign a name for this printer.

Supply a name for this printer. Some programs do not support server and printer name combinations of more than 31 characters.

Printer name: A Second Printer

Do you want your Windows-based programs to use this printer as the default printer?

○ Yes

● No

FIGURE 2.60
A printer should have an intuitive name describing its location, function, or ownership.