Help does not exist for this dialog.

Web Site Properties - Web Site Property Sheet

On this property sheet, you set the identification parameters for your Web site. For a site IP address to be available on this tab, the TCP/IP setting for the site must first be configured by using the **Protocols** property sheet in the Windows NT Control Panel Network application. The host header name, and the IP address are optional.

Web Site Identification

Description

You can type any name you want for the server name. This name appears in the tree view of Internet Service Manager. Click the **Advanced** button to configure host header names.

IP Address

For an address to appear in this box, it must have already been defined for use on this computer in Control Panel. See your Windows NT documentation for more information. If you do not assign a specific IP address, this site responds to all IP addresses assigned to this computer and not assigned to other sites, which makes this the default Web site.

TCP Port

Determines the port on which the service is running. The default is port 80. You can change the port to any unique TCP port number; however, clients must know in advance to request that port number, or their requests fail to connect to your server. A port number is required and cannot be left blank.

Connections

Unlimited

Select this option to allow an unlimited number of connections to occur simultaneously.

Limited to

Select this option to limit the maximum number of simultaneous connections to the site. In the dialog box, type the maximum number of connections permitted.

Connection Timeout

Sets the length of time in seconds before the server disconnects an inactive user. This ensures that all connections are closed if the HTTP protocol fails to close a connection.

Enable Logging

Select this option to enable your Web site’s logging features, which can record details about user activity and create logs in your choice of format. The logs can tell you which users accessed your Web sites and what information they accessed. After enabling logging, select a format in the **Active log format** list. The formats are as follows:

Microsoft IIS Log Format

A fixed ASCII format.

NCSA Common Log File Format

The National Center for Supercomputing Applications (NCSA) common format; a fixed ASCII format.

W3C Extended Log File Format

A customizable ASCII format, selected by default.

ODBC Logging (Only Available with IIS)

A fixed format logged to a database.

The default format is W3C Extended Log File Format, with Time, Client IP Address, Method, URI Stem, and HTTP Status selected. For more information about W3C Extended Log File Format, in the property sheet, click **Properties** and then click **Help**.

To configure the criterion by which log files are created (for example, weekly, or by file size), or to configure properties for W3C Extended logging or ODBC logging, click **Properties**.

Add/Edit Application Extension Mapping

Use the **Add/Edit Application Extension Mappings** dialog box to add or modify the mapping between a file name extension and the program or interpreter that processes those files.

In the **Executable** box, type the name of the executable file (.exe or .dll) or use the **Browse** button to search for the file. The executable file must be located on your Web server's local hard disk.

In the **Method Exclusions** box, type the names of any HTTP methods that should not be passed to an application. For example, you might want to prohibit the HTTP PUT or DELETE methods. Separate method names with a comma (,).

Select the **Script Engine** check box when you want the application to run in a directory without Execute permissions. This setting is intended primarily for script-based applications such as ASP and IDC that are mapped to an interpreter. For a script-mapped application to run, either the **Script** or **Execute** access check box must be selected for the directory in which the application is located. To allow only script-mapped applications to run, use the **Script** access. To allow both script-mapped applications and executable files (.exe and .dll) to run, use the **Execute** access.

Select the **Check that File Exists** option to instruct the Web server to verify the existence of the requested script file and to ensure that the requesting user has access permission for that script file. If the script does not exist or the user does not have permission, the appropriate warning message is returned to the browser and the script engine is not invoked. This option can be useful for scripts mapped to non-CGI executables like the Perl interpreter that do not send a CGI response if the script is not accessible. Because the script will be opened twice, once by the server and once by the script engine, there is some performance cost to enabling this option.

Filter Properties

Use the **Filter Properties** dialog box to add ISAPI filters to the master properties for a Web service or to an individual Web site. Use the **Browse** button to search for the filter on your local hard disk or network. You can give a filter a meaningful name that helps you remember what it does. Filter names cannot include commas.

Web Site Properties - Home Directory Property Sheet

Use the **Home Directory** property sheet to change the home directory for your Web site or to modify the properties of your home directory. The home directory is the central location for the files published in your Web site. A default home directory, called Wwwroot, was created when you installed the WWW service. You can change the location of the home directory to one of the following:

- A directory located on this computer.
- A directory located on another computer (a network share). When prompted, type the user name and password needed to access that computer. Click **Connect As** to change the user name and password.
- A redirection to a URL. Browsers requesting a resource at the original URL are automatically given the destination URL provided in the **Redirect To** text box so that they can request the resource again.

In the text box, type the path to the directory or the destination URL. The syntax must match the selected path type:

For a local directory, use the full path; for example, C:\Catalog\Shoes. You can also click the **Browse** button to select a local directory rather than typing the path.

For a network share, use a Universal Naming Convention (UNC) server and share name; for example, \\webserver\htmlfiles.

For a redirected URL, use a valid URL for the destination. To map requests to another Web site, use a fully qualified URL; for example, http://tempserver. To map requests to a virtual directory, use a virtual path; for example, /newcatalog. You can use redirect variables and wild cards in the destination URL to control which portions of the original URL are mapped into the destination URL.

Access Permissions

The **Access Permissions** properties appear when you are working with a local directory or a network share. Use these check boxes to determine the type of access allowed to a directory. If the directory is on a Windows NT File System (NTFS) drive, the NTFS settings for the directory must match these settings. If the settings do not match, the most restrictive settings take effect. For example, if you give a directory Write permission in this property sheet but give a particular user group only Read access permissions in NTFS, those users cannot write files to the directory because the Read permission is more restrictive.

Read Enables Web clients to read or download files stored in a home directory or a virtual directory. If a client sends a request for a file that is in a directory without Read permission, the Web server returns an error. Generally, you should give Read permission only to directories containing information to publish (HTML files, for example). You should disable Read permission for directories containing Common Gateway Interface (CGI) applications and Internet Server Application Program Interface (ISAPI) DLLs to prevent clients from downloading the application files.

Write Enables Web clients to upload files to the enabled directory on your server, or to change content in a Write-enabled file. Write can only be done with a browser that supports the Put feature of the HTTP 1.1 protocol standard.

Content Control

The **Content Control** properties appear when you are working with a local directory or a network share.

Log Access Select this check box to record visits to this directory in a log file. Visits are recorded only if logging is enabled for this Web site. Logging is enabled by default. To turn off logging, select the Web site, click the Properties button on the Toolbar, select the **Web Site** property sheet, and then clear the **Enable Logging** check box.

Directory Browsing Allowed Select this check box to show the user a hypertext listing of the files and subdirectories in this virtual directory so that the user can navigate through the directory structure. A hypertext directory listing is generated automatically and sent to the user when a browser request does not include a specific file name and when no default document is in the specified directory. Because directory browsing reveals your Web site's structure to a user, you should generally leave this option disabled.

Note that virtual directories will not appear in directory listings; users must know a virtual directory's alias and type in its URL address, or click a link in another page, to access virtual directories.

Index This Directory Select this check box to instruct Microsoft Index Server to include this directory in a full-text index of your Web site. A full-text index enables users to quickly search for words or phrases in documents on your Web site. This feature is only available on Windows NT Server.

FrontPage Web Select this check box to create a FrontPage web for this Web site. Clear this check box to delete the FrontPage web from this Web site.

Application Settings

An *application* is defined as all the directories and files contained within a directory marked as an application starting point until another application starting point is reached. If you make your site's home directory an application starting point, then every virtual directory and physical directory within your site can participate in the application. To make this directory an application starting point (and thus create an application), click the **Create** button. To dissociate this home directory from an application, click the **Remove** button.

Type the name of the application in the **Name** text box; the name will appear in the property sheets for any directory contained within the application boundary. To set properties for the application, click the **Configuration** button.

Run in Separate Memory Space (Isolated Process)

Select this check box to run the application in a separate process from the Web server process. Running an isolated application protects other applications, including the Web server itself, from being affected if this application fails.

Permissions

The application permissions properties control whether applications can be run in this directory.

None Do not allow any programs or scripts to run in this directory.

Script Enables applications mapped to a script engine to run in this directory without having Execute permission set. Use Script permission for directories that contain ASP scripts, Internet Database Connector (IDC) scripts, or other scripts. Script permission is safer than Execute permission because you can limit the applications that can be run in the directory. For information on making an application a script engine, see the **App Mappings** property sheet.

Execute Allows any application to run in this directory, including applications mapped to script engines and Windows NT binaries (.dll and .exe files).

The Client Will Be Sent To

These properties appear when you select **A Redirection to a URL**.

The Exact URL Entered Above redirects a virtual directory to the destination URL without adding any other portions of the original URL. You can use this option to redirect an entire virtual directory to one file. For example, to redirect all requests for the /scripts virtual directory to the file Default.htm in the home directory, type **/Default.htm** in the **Redirect To** text box and select this option.

A Directory Below This One redirects a parent directory to a child directory. For example, to redirect your home directory (designated by /) to a subdirectory named /newhome, type /newhome in the **Redirect To** text box and select this option. Without this option, the Web server will continually map the parent to itself.

A **Permanent Redirection for This Resource** sends the following message to the client: "301 Permanent Redirect." Redirects are considered temporary, and the client browser receives the following message: "302 Temporary Redirect." Some browsers can use the "301 Permanent Redirect" message as the signal to permanently change a URL, such as a bookmark.

Redirect Variables

Use redirect variables to pass portions of the original URL with the destination URL. Insert the variable into the **Redirect To** text box along with the destination URL.

$S Passes the matched suffix of the requested URL. The matched suffix is the portion of the original URL that remains after the redirected URL is substituted. For example, if /scripts is redirected to /newscripts and the original request is for /scripts/program.exe, then /program.exe is the suffix. The server automatically performs this suffix substitution; you use the $S variable only in combination with other variables.

$P Passes the parameters in the original URL. For example, if the original URL is /scripts/myscript.asp?number=1, then the string "number=1" is mapped into the destination URL.

$Q Passes both the question mark and the parameters from the original URL. For example, if the original URL is /scripts/myscript.asp?number=1, then the string "?number=1" is mapped into the destination URL.

$V Passes the requested URL, without the server name. For example, if the original URL is //myserver/scripts/myscript.asp, then the string "/scripts/myscript.asp" is mapped into the destination URL.

$0 through **$9** Passes the portion of the requested URL that matches the indicated wildcard.

! Do not redirect. Use this variable to prevent redirecting a subdirectory or an individual file in a virtual directory that has been redirected.

Redirect Wildcards

Use redirect wildcards to match any number of characters in the original URL. Insert the wildcard character (*) directly into the **Redirect To** text box. Begin the destination URL with an asterisk and a semicolon. Separate pairs of wildcards and destination URLs with a semicolon. For example, to redirect all requests for /scripts/*filename*.stm to a single file called Default.stm, and to redirect all requests for /scripts/*filename*.htm to a single file called Default.htm, type the following in the **Redirect To** text box for the /scripts virtual directory:

;.stm;/default.stm;*.htm;/default.htm

When you use wildcards, be sure to select **The Exact URL Entered Above**. For a redirected path, use a URL.

IP Access Restrictions

Use these properties to provide or prevent specific users from accessing this Web site, directory, or file.

By default, all computers will be:

Granted Access Select this button to allow all computers access to this virtual directory, except those computers specifically listed as exceptions. For example, you can exclude a particular individual or group by denying access to your server from a particular IP address, or prevent entire networks from accessing your server, while allowing all others to have access.

Denied Access Select this button to deny access to all remote users except those whose IP addresses have been specifically granted access. IP address security is probably most useful on the Internet, to exclude everyone except known users.

Except those listed below:

To grant or deny access to a specific computer or group of computers:

1 Click **Add**. If the **Granted Access** button is selected, the **Deny Access On** dialog box appears; if the **Denied Access** button is selected, the **Grant Access On** dialog box appears.

2 In the **IP Address** field, type the unique numeric TCP/IP network address of the specific computer to be granted or denied access to your site.

3 In the **Subnet Mask** field, type number that identifies the TCP/IP network subdivision of the group of computers to be granted or denied access to your site.

4 In the **Domain** field, type the domain name of the network to be granted or denied access to your site belongs.

Web Site Properties - Virtual Directory Property Sheet

Use this property sheet to change the properties of a virtual directory in your Web site. A virtual directory is a directory that is not physically contained within the home directory, but which appears as though it were to users who visit your Web site. To add a new virtual directory, right-click the Web site, select **New**, and then click **Virtual Directory**. A virtual directory can be mapped to any of the following:

- A directory located on this computer.
- A directory located on another computer (a network share). When prompted, type the user name and password needed to access that computer. Click **Connect As** to change the user name and password.
- A redirection to a URL. Browsers requesting a resource at the original URL are automatically given the destination URL provided in the **Redirect To** text box so that they can request the resource again.

In the text box, type the path to the directory or the destination URL. The syntax must match the selected path type:

For a local directory, use the full path; for example, C:\Catalog\Shoes. You can also click the **Browse** button to select a local directory rather than typing the path.

For a network share, use a Universal Naming Convention (UNC) server and share name; for example, \\Webserver\Htmlfiles.

For a redirected URL, use a valid URL for the destination. To map requests to another Web site, use a fully qualified URL, for example, http://tempserver. To map requests to a virtual directory, use a virtual path; for example, /newcatalog. You can use redirect variables and wild cards in the destination URL to control which portions of the original URL are mapped into the destination URL.

Access Permissions

The **Access Permissions** properties appear when you are working with a local directory or a network share. Use these check boxes to determine the type of access allowed to a directory. If the directory is on a Windows NT File System (NTFS) drive, the NTFS settings for the directory must match these settings. If the settings do not match, the most restrictive settings take effect. For example, if you give a directory Write permission in this property sheet but give a particular user group only Read access permissions in NTFS, those users cannot write files to the directory because the Read permission is more restrictive.

Read Enables Web clients to read or download files stored in a home directory or a virtual directory. If a client sends a request for a file that is in a directory without Read permission, the Web server returns an error. Generally, you should give Read permission only to directories containing information to publish (HTML files, for example). You should disable Read permission for directories containing Common Gateway Interface (CGI) applications and Internet Server Application Program Interface (ISAPI) DLLs to prevent clients from downloading the application files.

Write Enables Web clients to upload files to the enabled directory on your server, or to change content in a Write-enabled file. Write can only be done with a browser that supports the Put feature of the HTTP 1.1 protocol standard.

Content Control

The **Content Control** properties appear when you are working with a local directory or a network share.

Log Access Select this check box to record visits to this directory in a log file. Visits are recorded only if logging is enabled for this Web site. Logging is enabled by default. To turn off logging, select the Web site, open its property sheets, click the **Web Site** tab, and then clear the **Enable Logging** check box.

Directory Browsing Allowed Select this check box to show the user a hypertext listing of the files and subdirectories in this virtual directory so that the user can navigate through the directory structure. A hypertext directory listing is generated automatically and sent to the user when a browser request does not include a specific file name and when no default document is in the specified directory. Because directory browsing reveals your Web site's structure to a user, you should generally leave this option disabled.

Note that virtual directories will not appear in directory listings; users must know a virtual directory's alias and type in its URL address, or click a link in another page, to access virtual directories.

Index This Directory Select this check box to instruct Microsoft Index Server to include this directory in a

full-text index of your Web site. A full-text index enables users to quickly search for words or phrases in documents on your Web site. This feature is only available on Windows NT Server.

Application Settings

An *application* is defined as all the directories and files contained within a directory marked as an application starting point until another application starting point is reached. If you make this virtual directory an application starting point, every virtual directory and physical directory within this virtual directory can participate in the application. To make this directory an application starting point (and thus create an application), click the **Create** button. To dissociate this directory from an application, click the **Remove** button.

Type the name of the application in the **Name** text box; the name will appear in the property sheets for any directory contained within the application boundary. To set properties for the application, click the **Configuration** button.

Run in Separate Memory Space (Isolated Process)

Select this check box to run the application in a separate process from the Web server process. Running an isolated application protects other applications, including the Web server itself, from being affected if this application crashes or hangs.

Permissions

The application permissions properties control whether applications can be run in this directory.

None Do not allow any programs or scripts to run in this directory.

Script Enables applications mapped to a script engine to run in this directory without having Execute permission set. Use Script permission for directories that contain ASP scripts, Internet Database Connector (IDC) scripts, or other scripts. Script permission is safer than Execute permission because you can limit the applications that can be run in the directory. For information on making an application a script engine, see the **App Mappings** property sheet.

Execute Allows any application to run in this directory, including applications mapped to script engines and Windows NT binaries (.dll and .exe files).

The Client Will Be Sent To

These properties appear when you select **A Redirection to a URL**.

The Exact URL Entered Above redirects a virtual directory to the destination URL without adding any other portions of the original URL. You can use this option to redirect an entire virtual directory to one file. For example, to redirect all requests for the /scripts virtual directory to the file Default.htm in the home directory, type **/Default.htm** in the **Redirect To** text box and select this option.

A Directory Below This One redirects a parent directory to a child directory. For example, to redirect your home directory (designated by /) to a subdirectory named /newhome, type /newhome in the **Redirect To** text box and select this option. Without this option, the Web server will continually map the parent to itself.

A **Permanent Redirection for This Resource** sends the following message to the client: "301 Permanent Redirect." Redirects are considered temporary, and the client browser receives the following message: "302 Temporary Redirect." Some browsers can use the "301 Permanent Redirect" message as the signal to permanently change a URL, such as a bookmark.

Redirect Variables

Use redirect variables to pass portions of the original URL with the destination URL. Insert the variable into the **Redirect To** text box along with the destination URL.

$S Passes the matched suffix of the requested URL. The matched suffix is the portion of the original URL that remains after the redirected URL is substituted. for example, if /scripts is redirected to /newscripts and the original request is for /scripts/program.exe, then /program.exe is the suffix. the server automatically performs this suffix substitution; you use the $S variable only in combination with other variables.

$P Passes the parameters in the original URL. For example, if the original URL is /scripts/myscript.asp?number=1, then the string "number=1" is mapped into the destination URL.

$Q Passes both the question mark and the parameters from the original URL. For example, if the original URL

is /scripts/myscript.asp?number=1, then the string "?number=1" is mapped into the destination URL.

$V Passes the requested URL, without the server name. For example, if the original URL is //myserver/scripts/myscript.asp, then the string "/scripts/myscript.asp" is mapped into the destination URL.

$0 through **$9** Passes the portion of the requested URL that matches the indicated wildcard.

! Do not redirect. Use this variable to prevent redirecting a subdirectory or an individual file in a virtual directory that has been redirected.

Redirect Wildcards

Use redirect wildcards to match any number of characters in the original URL. Insert the wildcard character (*) directly into the **Redirect To** text box. Begin the destination URL with an asterisk and a semicolon. Separate pairs of wildcards and destination URLs with a semicolon. For example, to redirect all requests for /scripts/*filename*.stm to a single file called Default.stm, and to redirect all requests for /scripts/*filename*.htm to a single file called Default.htm, type the following in the **Redirect To** text box for the /scripts virtual directory:

;.stm;/default.stm;*.htm;/default.htm

When you use wildcards, be sure to select the option **The Exact URL Entered Above**. For a redirected path, use a URL.

Authentication Methods

To prevent unauthorized users from establishing a Web (HTTP) connection to restricted content, you can configure your Web server to identify, or *authenticate*, users. The authentication process involves determining whether a user has a valid Windows NT user account that has appropriate Windows NT File System (NTFS) permissions for accessing a particular Web site, directory, or file.

Allow Anonymous Access

Typically, all users attempting to establish a Web (HTTP) connection with your Web server should log on as anonymous users. When a user establishes an anonymous connection, your server will log on the user with an anonymous or guest account, which is a valid Windows NT user account. This account has security restrictions that limit the type of Web content that anonymous users can access.

Set the Windows NT user account to use for all anonymous connections. This account has security restrictions, determined by your Windows NT Files System (NTFS) permissions, that limit the type of Web content anonymous users can access.

By default, your Web server creates and uses the account IUSR_*computername*. When you installed your Web server, Setup created the account IUSR_*computername* in Windows NT User Manager for Domains and in Internet Service Manager.

The IUSR_*computername* is granted Log on Locally user rights by default. This right is necessary if you want to grant anonymous logon access to your site. For more information, consult your Web server security documentation.

Basic Authentication Select this check box to enable your Web server ‘s Basic authentication method, which is a widely used, industry standard method for identifying users.

Your Web server will only use Basic Authentication under the following conditions:

- Anonymous access disabled.
- Anonymous access denied because Windows NT permission have been set, requiring the users to provide a Windows NT user name and password before establishing a connection with restricted content.

During the Basic authentication process, the user’s Web browser will prompt the user to enter a valid Windows NT account user name and password.

Warning

Basic authentication results in the transmission of passwords across the network in an unencrypted form. A determined computer vandal equipped with a network monitoring tool could intercept user names and passwords.

Edit

Users attempting to establish a connection through Basic authentication must provide their logon domain in addition to their user name. By clicking this button you configure your Web server to assume a default logon domain, other than the local domain, for users who do not explicitly provide their domain name.

Windows NT Challenge/Response When this check box is selected, you enable your Web server’s Windows NT Challenge/Response authentication methods. Microsoft Internet Explorer, version 2.0 or later, is the only Web browser that currently supports this authentication method.

Once enabled, your Web server will only use Windows NT Challenge/Response authentication under the following conditions:

- Anonymous access disabled.
- Anonymous access denied because Windows NT permission have been set, requiring the users to provide a Windows NT user name and password before establishing a connection with restricted content.

During the Windows NT Challenge/Response authentication process, your Web server engages in a cryptographic information exchange with the user’s Internet Explorer Web browser. The user’s Web browser does not send actual Windows NT account password information across the network.

Secure Communications

Use this dialog box to establish a Secure Sockets Layer (SSL) encrypted communication link with Web site visitors using a Web browser that supports secure communications (URLs starting with https://). This means that all of the information in both the HTTP request and response is fully encrypted, including the any information exchanged between the user and your Web server.

Use the secure communications feature to protect sensitive information, such as credit card numbers or medical records.

Key Manager

Before you can use your Web server's SSL security features, you must obtain a valid server certificate from a trusted, third-party organization, called *certificate authority*. Click Key Manager to request a server certificate from a certificate authority and to create an SSL authentication key-pair.

After you receive your server certificate, you can use Key manager to install the certificate and attach it to your authentication key-pair. You also use Key Manager to manage multiple certificates and to install certificates on remote Web servers.

For more information, consult your Web server security documentation.

Require Secure Channel when accessing this resource

Select this check box to require an encrypted communication link for a Web browser to connect with this Web site, directory, or file.

Note

The default encryption strength (Require Secure Channel selected, Require 128-bit Encryption cleared) is 40-bit.

Client Certificate Authentication

When you select this check box, you can configure your Web server to either accept, require, or reject client certificates as a means of establishing a connection with a particular file or directory. A client certificate is a digital identification issued by a trusted, third-party organization, called a *certificate authority*.

Do Not Accept Client Certificates

Users logging on with a client certificate, who attempt to connect to a file or directory resource for which this setting is enabled, will be denied access.

Accept Certificates

Users can access a file or directory with a client certificate, but the certificate is not required.

Require Client Certificates

Only users logging on with a valid client certificate can connect to a file or directory resource for which this setting is enabled. Users without a valid client certificate will be denied access.

Enable Client Certificate Mapping

Select this check box to configure to authenticate users who log on with a valid client certificate. M*appings* match information contained in a client's certificate against Windows NT account information. If the certificate information matches account information, the user 's client certificate will be automatically mapped to a particular Windows NT user account, thus authenticating and granting that user access to a restricted resource.

You can use the client certificate mapping feature to do the following:

- Map a single client certificate to a Windows NT account.
- Map multiple client certificates to Windows NT account, based on specific certificate information, such as the user' organization name.

To select and configure a mapping, click the **Edit** button.

Grant Access On or Deny Access On

Use these dialog boxes to list the computers you want to grant or deny access to this resource.

Single Computer Select this button to add access rights for a single computer. Specify the Internet Protocol (IP) address of the computer in the **IP Address** text box, or click **DNS Lookup** if your network supports this naming service. In the **Enter the DNS Name** text box, type the computer's domain name.

Group Of Computers Select this button to add access rights for a group of computers based on Network ID and/or Subnet Mask. Type the network identification and subnet mask in the **Network ID** and **Subnet Mask** text boxes.

Domain Name Select this button to add access rights for a Windows NT domain. Type the Windows NT domain name in the **Domain Name** text box.

Note

You are specifying, by IP address or domain name, which computer or group of computers will be granted or denied access. If you choose, by default, to *grant* access to all users, you are specifying computers that are to be denied access. Conversely, if you choose, by default, to *deny* access to all users, you are then specifying computers that are to be allowed access. You should fully understand TCP/IP networking, IP addressing, and the use of subnet masks before you use this option.

Web Site Properties - HTTP Headers Property Sheet

Use the HTTP Headers properties to set values returned to the browser in the header of the HTML page.

Enable Content Expiration

Select this check box to include expiration information. Include a date in time-sensitive material, such as special offers or event announcements. The browser compares the current date to the expiration date to determine whether to display a cached page, or request an updated page from the server.

Custom Headers

Use this property to send a custom HTTP header from the Web server to the client browser. For example, you could use a custom HTTP header to allow the client browser to cache the page but prevent proxy servers from caching the page. Custom headers are described in the metabase. To have your Web server send a header, click **Add**, and then type the name and value of the header in the **Add Custom HTTP Header** dialog box. To stop sending a header, click **Remove**.

Content Rating

You can configure your Web server's content rating features to embed descriptive labels in your Web page's HTTP headers. Some Web browsers, such as Microsoft Internet Explorer, version 3.0 or later, can detect these content labels in order to help users identify potentially objectionable Web content. Click **Edit Ratings** to set content ratings for this Web site, directory, or file.

MIME Map

Select the **File Types** button to configure Multipurpose Internet Mail Extensions (MIME) mappings. These mappings set the various file types that the Web service returns to browsers. The registered file types that are installed by default on Windows NT are listed in the **File Types** dialog box. File type extensions and MIME mappings are listed for selected file types in the **File type details** box.

To configure additional MIME mappings, click the **New Type** button in the **File Types** dialog box. In the **File Type** dialog box type the extension that is associated with the file in the **Associated Extension** box. In the **Content Type (MIME)** box enter the MIME type followed by the filename extension in the form *mime type /filename extension*.

To remove MIME mappings, select the file type in the **Registered file types** box and click the **Remove** button.

To edit existing MIME mappings, select the file type in the **Registered file types** box, click the **Edit** button and modify the contents of the **Associated Extension** and **Content Type (MIME)** boxes as needed.

If you set MIME mappings in the master property sheets for your computer, the Web sites and directories on your computer use the same mappings. You can modify the MIME mappings for a Web site or directory. However, if you then reapply the master properties, the master properties completely replace the modified properties for the Web site or directory. That is, the properties are not merged.

Content Ratings - Rating Service Property Sheet

Your Web server's default Platform for Internet Content Selection (PICS) based rating system uses a system developed by the Recreational Software Advisory Council (RSAC), which rates content according to levels of violence, nudity, sex, and offensive language. Click **More Information** to obtain more information about the RSAC rating service.

Under **RSAC Registration**, click **Rating Questionnaire** to fill out a RSAC questionnaire and to obtain the recommended content ratings for your particular Web content.

Note

RSAC is a widely recognized rating service, which has earned the trust of a broad range of Web users. Before setting your content ratings (using your Web server’s default RSAC rating system), you should obtain recommended ratings from RSAC.

Encryption Settings

Select this check box to require that a browser be capable of 128-bit encryption to connect with this Web site, directory, or file.

Important

Due to export restrictions, the 128-bit key strength encryption feature is available only in the United States and Canada. For information about upgrading to128-bit encryption capability, available with the Windows NT Server North American Service Pack 2.0, visit the Windows NT Server support Web site at http://www.microsoft.com/NTServerSupport.

Add Custom HTTP Header

Type the name and value of your custom HTTP header.

Web Site Properties - Custom Errors Property Sheet

The **Custom Errors** property sheet lists what is returned to the browser in the event of an HTTP error. Administrators have the option of using the default HTTP 1.1 errors or customizing these error messages with their own content. The HTTP error code is listed, as well as the output type, which can be either the default HTTP 1.1 error, a file, or a URL.. If the default HTTP 1.1 error is used, the contents of the error message will appear under the **Contents** column of the table. If a file or URL is used, then the path to that file or URL will appear under the **Contents** column of the table.

By default, friendly custom error messages (see below) are listed in the **Custom Errors** property sheet. To edit custom error messages, click the **Edit Properties** button. This will launch the **Error Mapping Properties** dialog box, which allows you to set the error message to the HTTP 1.1 default, map the error to a file, or map the error to a URL. If you edit a custom error to map to a file or URL, then later want to revert to the default HTTP 1.1 error, select the custom error and click the **Set to Default** button.

Note

If the output type is a URL, this URL must exist on a local server.

If you are using static custom error files (HTML files), you should always use the File option. If you plan on developing an application (via ISAPI or ASP) to handle errors, then use URL, but be aware that the error status is handed to the application in the URL parameters and it is the application's responsibility to set the HTTP header status, otherwise the HTTP response status will be HTTP 1.1 200 OK.

Friendly Custom Error Messages

IIS and PWS feature their own set of custom errors that provide more informative or "friendly" feedback than the default HTTP 1.1 errors that are returned to client browsers. For example, the HTTP 1.1 404 error message, which by default simply reads "Object Not Found" is expanded to read "The web server cannot find the file/script you asked for. Please check the URL to ensure that the path is correct. Please contact the server's administrator if this problem persists." These friendly custom error messages are set by default in Internet Service Manager.

To configure friendly error messages:

Select the default HTTP error that you would like to change, click the **Edit Properties** button, select URL from the **Message Type** box and type /iisHelp/common/<*file name*>

where <*file name*> is the HTML file name of the friendly error message. Friendly error messages are installed by default to the following location: <*drive letter*>:\WINNT\Help\common. The file names are numbers which correspond to the specific HTTP errors; for example, 400.htm, 401-1.htm, and so on.

Note

Custom errors appear as a list in the **Custom Errors** property sheet and this list is treated as a single property. For example, when a set of custom errors are configured at the Web site level, all directories under that server inherit the entire list of custom errors. That is, the two custom error lists (for server and directory) are not merged. You can configure customized error messages at the Web site, virtual directory, directory, and file level.

Error Mapping Properties

To edit custom error messages, choose either **Default, File,** or **URL** in the **Message Type** drop-down list box.

To return the default HTTP 1.1 error to the client browser, select **Default**. and click **OK**.

To map the custom error to a file, select **File**, enter the path to a file, and click **OK**. To search on a local drive for a file, click the **Browse** button.

To map the custom error to a URL, select **URL** and enter the path to the URL beginning with the virtual directory name, as in */virdir1/errors/404.htm*, for example, and click **OK**.

Note

If the output type is a URL, this URL must exist on a local server.

Directory Properties - Directory Property Sheet

Use this property sheet to change properties for a physical directory in your Web site. A physical directory in a Web site is simply a directory that has not been assigned a specific URL. Physical directories are contained within your home directory or within a virtual directory. While you use the Windows NT Explorer to add a new directory or change the name of a directory, you use this property sheet to set properties that determine how the Web server responds to requests for files in this directory. A physical directory can return content from:

- This directory.
- A redirection to a URL. Browsers requesting a resource at the original URL are automatically given the destination URL provided in the **Redirect To** text box so that they can request the resource again.

Path

Shows the location of the directory.

Redirect To

Type a valid destination URL. To map requests to another Web site, use a fully qualified URL; for example, http://tempserver. To map requests to a virtual directory, use a virtual path; for example, /newcatalog. You can use redirect variables and wildcards in the destination URL to control which portions of the original URL are mapped into the destination URL.

Access Permissions

The **Access Permissions** properties appear when you are working with a local directory instead of a redirected URL. Use these check boxes to determine the type of access allowed to a directory. If the directory is on a Windows NT File System (NTFS) drive, the NTFS settings for the directory should match these settings. If the settings do not match, the most restrictive settings take effect. For example, if you give a directory Write permission in this property sheet but give a particular user group only Read access permissions in NTFS, those users cannot write files to the directory because the Read permission is more restrictive.

Read Enables Web clients to read or download files stored in the directory. If a client sends a request for a file that is in a directory without Read permission, the Web server returns an error. Generally, you should give Read permission only to directories containing information to publish (HTML files, for example). You should disable Read permission for directories containing Common Gateway Interface (CGI) applications and Internet Server Application Program Interface (ISAPI) DLLs to prevent clients from downloading the application files.

Write Enables Web clients to upload files to the enabled directory on your server, or to change content in a Write-enabled file. Write can only be done with a browser that supports the Put feature of the HTTP 1.1 protocol standard.

Content Control

The **Content Control** properties appear when you are working with a local directory instead of a redirected URL.

Log Access Select this check box to record visits to this directory in a log file. Visits are recorded only if logging is enabled for this Web site. Logging is enabled by default. To turn off logging, select the Web site, open its property sheets, click the **Web Site** tab, and then clear the **Enable Logging** check box.

Directory Browsing Select this check box to show the user a hypertext listing of the files and subdirectories in this directory so that the user can navigate through the directory structure. A hypertext directory listing is generated automatically and sent to the user when a browser request does not include a specific file name and when no default document is in the specified directory. Because directory browsing reveals your Web site's structure to a user, you should generally leave this option disabled.

Note that virtual directories will not appear in directory listings; users must know a virtual directory's alias and type in its URL address, or click a link in another page, to access virtual directories.

Important

Your Web server will display an “access forbidden” error message in the user’s Web browser if a user attempts to access file or directory, for which you have disabled *both* of the following:

- Directory browsing.

- The default document that the user’s Web browser renders when a browser request does not include a specific HTML name.

Index This Directory Select this check box to instruct Microsoft Index Server to include this directory in a full-text index of your Web site. A full-text index enables users to quickly search for words or phrases in documents on your Web site. This feature is only available on Windows NT Server.

The Client Will Be Sent To

These properties appear when you select **A Redirection to a URL**.

The Exact URL Entered Above redirects requests for a URL to the destination URL without adding any other portions of the original URL. You can use this option to redirect an entire directory to one file. For example, to redirect all requests for the Scripts directory to the file Default.htm in the home directory, type **/Default.htm** in the **Redirect To** text box and select this option.

A Directory Below This One redirects a parent directory to a child directory. For example, to redirect your home directory (designated by /) to a subdirectory named /newhome, type /NewHome in the **Redirect To** text box and select this option. Without this option, the Web server will continually map the parent to itself.

A **Permanent Redirection for This Resource** sends the following message to the client: "301 Permanent Redirect." Redirects are considered temporary, and the client browser receives the following message: "302 Temporary Redirect." Some browsers can use the "301 Permanent Redirect" message as the signal to permanently change a URL, such as a bookmark.

Redirect Variables

Use redirect variables to pass portions of the original URL with the destination URL. Insert the variable into the **Redirect To** text box along with the destination URL.

$S Passes the matched suffix of the requested URL. The matched suffix is the portion of the original URL that remains after the redirected URL is substituted. For example, if /scripts is redirected to /newscripts and the original request is for /scripts/program.exe, then /program.exe is the suffix. The server automatically performs this suffix substitution; you use the $S variable only in combination with other variables.

$P Passes the parameters in the original URL. For example, if the original URL is /scripts/myscript.asp?number=1, then the string "number=1" is mapped into the destination URL.

$Q Passes both the question mark and the parameters from the original URL. For example, if the original URL is /scripts/myscript.asp?number=1, then the string "?number=1" is mapped into the destination url.

$V Passes the requested URL, without the server name. For example, if the original URL is //myserver/scripts/myscript.asp, then the string "/scripts/myscript.asp" is mapped into the destination URL.

$0 through **$9** Passes the portion of the requested URL that matches the indicated wildcard.

! Do not redirect. Use this variable to prevent redirecting a subdirectory or an individual file in a virtual directory that has been redirected.

Redirect Wildcards

Use redirect wildcards to match any number of characters in the original URL. Insert the wildcard character (*) directly into the **Redirect To** text box. Begin the destination URL with an asterisk and a semicolon. Separate pairs of wildcards and destination URLs with a semicolon. For example, to redirect all requests for /scripts/*filename*.stm to a single file called Default.stm, and to redirect all requests for /scripts/*filename*.htm to a single file called Default.htm, type the following in the **Redirect To** text box for the Scripts directory:

;.stm;/default.stm;*.htm;/default.htm

When you use wildcards, be sure to select the option **The Exact URL Entered Above**. For a redirected path, use a URL.

Application Settings

An *application* is defined as all the directories and files contained within a directory marked as an application starting point until another application starting point is reached. If you make this directory an application starting point, every virtual directory and physical directory under this directory in the Web site can participate in the application. To make this directory an application starting point (and thus create an application), click the **Create**

button. To dissociate this directory from an application, click the **Remove** button.

Type the name of the application in the **Name** text box; the name will appear in the property sheets for any directory contained within the application boundary. To set properties for the application, click the **Configuration** button.

Run in Separate Memory Space (Isolated Process)

Select this check box to run the application in a separate process from the Web server process. Running an isolated application protects other applications, including the Web server itself, from being affected if this application fails.

Permissions

The application permissions properties control whether applications can be run in this directory.

None Do not allow any programs or scripts to run in this directory.

Script Enables applications mapped to a script engine to run in this directory without having Execute permission set. Use Script permission for directories that contain ASP scripts, Internet Database Connector (IDC) scripts, or other scripts. Script permission is safer than Execute permission because you can limit the applications that can be run in the directory. For information on making an application a script engine, see the **App Mappings** property sheet.

Execute Allows any application to run in this directory, including applications mapped to script engines and Windows NT binaries (.dll and .exe files).

File Properties - File Property Sheet

Use this property sheet to set properties for a file in your Web site. When a browser requests this file, the Web server can return either of the following:

- The designated file.
- A redirection to a URL. Browsers requesting a resource at the original URL are automatically given the destination URL provided in the **Redirect To** text box so that they can request the resource again.

Path

Shows the location of the file.

Redirect To

Type a valid destination URL. To map requests to another Web site, use a fully qualified URL, for example, http://tempserver. To map requests to a virtual directory, use a virtual path; for example, /newcatalog. You can use redirect variables and wild cards in the destination URL to control which portions of the original URL are mapped into the destination URL.

Access Permissions

The **Access Permissions** properties appear when you are working with a file instead of a redirected URL. Use these check boxes to determine the type of access allowed to a file. If the file is on a Windows NT File System (NTFS) drive, the NTFS settings for the file must match these settings. If the settings do not match, the most restrictive settings take effect. For example, if you give a file Write permission in this property sheet but give a particular user group only Read access permissions in NTFS, those users cannot write over this file because the Read permission is more restrictive.

Read Enables Web clients to read or download this file. If a client sends a request for a file that does not have Read permission, the Web server returns an error. Generally, you should give Read permission only to files containing information to publish (HTML files, for example). You should disable Read permission for an application file to prevent clients from downloading the file.

Write Enables Web clients to upload files to the enabled directory on your server, or to change content in a Write-enabled file. Write can only be done with a browser that supports the Put feature of the HTTP 1.1 protocol standard.

Content Control

The **Content Control** properties appear when you are working with a file instead of a redirected URL.

Log Access Select this check box to record requests for this file in a log file. Requests are recorded only if logging is enabled for this Web site. Logging is enabled by default. To turn off logging, select the Web site, open its property sheets, click the **Web Site** tab, and then clear the **Enable Logging** check box.

Select Windows NT User Account

Use this dialog box to grant administration privileges for this Web site to Windows NT users and groups.

List Names From

Select the Windows NT domain that contains the user or group you want to add from this list box, which includes the name of the computer you are administering.

Names

Select the user or group you want to add, then click **Add** to add that user or group. If you select a group, you can click **Members** to view a list of the group's members. Click **Search** to search for users and groups by domain.

Add Names

The users and groups you added using the **Names** dialog box appear in this dialog box. Click **OK** to verify these are the users and groups you want to add.

Network Directory Security Credentials

This dialog box appears only if you specify a network directory. Enter a user name and password that has permission to use the network directory.

Important

If you specify a user name and password to connect to a network drive, all Web server access to that directory will use that user name and password. Choose the user carefully to prevent possible security breaches.

Internet Service Manager - Basic Authentication Warning

When your Web server authenticates a user with the Basic authentication method, the user’s Web browser transmits Windows NT account user names and passwords across the network in an unencrypted form.

You can enable your Web server’s Secure Socket’s Layer (SSL) encryption features to protect account information submitted through Basic authentication. To enable SSL, however, you must first install a server certificate. For more information, consult your Web server’s security documentation.

Global Group Membership

Lists the user accounts that are members of the selected global group.

Members of Global Group

Lists the members of the selected global group.

Add

Adds the user accounts or global groups selected in **Members Of** in the **Local Group Membership** dialog box to **Add Names** in the **Add Users And Groups** dialog **box.**

Local Group Membership

Lists the user accounts and global groups that are members of the selected local group.

Members Of Local Group

Lists the members of the selected local group.

Add

Adds the user accounts or global groups selected in **Members Of** in the **Local Group Membership** dialog box to **Add Names** in the **Add Users And Groups** dialog box.

Members

Displays the members of the selected global group (that is itself a member of this local group).

General

Use the wildcard matching rule editor to create custom rules for mapping client certificates to Windows NT user accounts. You can use wildcard rules to match client certificate issuers to your list of trusted certificate authorities. You can match specific information contained in client certificates, such as the issuer’s company name or locality, by creating rules defined with custom matching criteria. When creating matching criteria, you can use the wildcard character to partially specify the text of your criteria.

Enable this wildcard rule

Select this check box to enable a wildcard rule.

Match on all certificate issuers that I trust

Select this option to match a certificate issuing authority against a list of the trustworthy certificate authorities.

Match on selected certificate issuers

Select this option to match the a client certificate’s issuing authority against specific authorities selected from a list of trustworthy certificate issuers.

Select Button

Click this button to select specific issuers from your Web server’s list of trustworthy certificate issuers.

Account Mappings - Basic

You can authenticate users who log on with client certificates by creating a *one-to-one* mapping that relates the contents of a client certificate to a Windows NT user account. To map multiple certificates to a single account you must define a one-to-one mapping for each client certificate.

One-to-one mappings require you to have access to a text (ASCII) copy of the user's client certificate. Since this may not always be possible, nor feasible, you may want to use Active Sever Pages to create a script for extracting client certificate information from the user's HTTP request header. For more information, consult the Active Server Pages documentation.

Edit Rule Element

Client certificates can contain identification information, such as company names, localities, or e-mail addresses, formatted into arrangements of *fields* and *subfields.* Your Web server can inspect this identification information in order to create a Windows NT account mapping.

Using the rule element editor you can define rules that create a mapping if an individual subfield, rather than an entire certificate, meets your acceptance criteria. This means that you do not have to explicitly map each user's client certificate, and thus do not require a user's certificate file to define a mapping, as is the case with the *one-to-one* mapping. For example, you can use the rule editor to quickly map all client certificates issued to the financing department of a particular company - regardless of user identity - to a Windows NT user account.

Match Capitalization

Select this check box to make your rule element case sensitive.

Certificate Field

Use this box to select or enter the certificate field name. Fields are comprised of subfields that contain specific identification information. Field names represent general categories of information; typical field names are Client (Subject), Issuer, and Serial Number.

Subfield

Use this drop down box to select or enter the certificate subfield name. Subfields contain the certificate's specific identification information, such as the client's name or the issuer's Internet address. Valid subfield content can vary depending on how much information the client provided to the certificate authority when the certificate was issued.

The following list describes basic subfields contained in a certificate:

(O) Organization Preferably International Organization for Standardization (ISO)-registered top-level organization or company name.

(OU) Organizational Unit A department within a company, such as Marketing.

(CN) Common Name The domain name of the server, for example, www.microsoft.com.

(C) Country Two letter ISO country designation, for example, US, FR, AU, UK, and so on.

(S) State/Province Type in the full name of the state or province, do not abbreviate. For example, Washington, Alberta, California, and so on.

(L) Locality Type in the full name of the city where your company is located, such as Redmond or Toronto.

The rule editor also supports several, non-standard subfield categories. These include the following:

(I) Initials.

(GN) Given Name.

(T) Title.

Consult a certificate authority to obtain updated subfield information.

Criteria

Use this text box to specify the criteria for matching field and subfield information. You can use the wildcard character to partially specify the text of your criteria.

Mapping

In the **Windows NT Account** text box, specify the Windows NT account where you want to map the certificate. In the **Password** text box, enter an account password. Click **OK** to confirm the account mapping.

Find Account

Use this feature to search domains for a specific user or group.

Find User or Group

Type the user or group that you want to search for in the text box.

Search All

Select this option to search every domain for the user or group you specified in the **Find User or Group** text box.

Search Only In

To limit your user or group search to specific domains, select this option button. Select a domain to search from the list box. To select multiple domains, press the CTRL key while selecting.

Search Results

This box displays the user accounts and groups found by a search. This list is continuously filled as a search progresses.

The list presents the matching users in the form *domainname**username* (full name) description, or *computername**username* (full name) description.

The list presents the matching groups in the form *domainname**groupname* description, or *computername**groupname* description.

Add

Closes the **Find Account** dialog box and adds the accounts selected in **Search Results** to **Add Names** text box in the previous dialog box.

Advanced Multiple Web Site Configuration

This dialog box is used to add additional identities to your Web site. Click the **Add**, **Remove**, or **Edit** buttons to change the identities listed. Each Web site must have a unique combination of identification characteristics. Therefore, while multiple Web sites can share two of their three identification characteristics, (domain or host header name, IP address, and port), they must have one characteristic that is different. Also, because SSL certificates contain the domain name in them, Web sites using certificates cannot share an IP address with other Web sites.

SSL Port

Determines the port used for establishing a Secure Sockets Layer (SSL) connection. For your Web server’s default Web site, this port is set to 443, by default. (If you create a new Web site, you must explicitly set this port.) You can change the SSL port to any unique TCP port number; however, users must know in advance to request that port number, or their requests will fail to connect to your server. This option is not available unless you already have a server certificate installed.

Advanced Web Site Identification

IP Address

For an address to appear in this box, it must have already been defined for use on this computer in Control Panel. See your Windows NT documentation for more information. If you do not assign a specific IP address, this Web site responds to all IP addresses assigned to this computer and not assigned to other Web sites.

TCP Port

Determines the port on which the service is running. The default is port 80. You can change the port to any unique TCP port number; however, clients must know in advance to request that port number, or their requests fail to connect to your server.

SSL Port

Determines the port on which the service is running. The default is port 443. You can change the port to any unique SSL port number; however, clients must know in advance to request that port number, or their requests fail to connect to your server. . This option is not available unless you already have a server certificate installed.

Host Header Name

For your server to have a domain name, you must register it in the Domain Name System (DNS). A domain name server then maps your registered domain name to your IP address, enabling requests addressed to your domain name to reach you. You can assign multiple domain names, or host header names, to a single IP address. If the client browser supports the use of host header names, the name the user types is passed in the HTTP header as host. The server then routes the client to the correct Web site. If the browser does not support the use of host header names, the server responds with the default Web site if a default Web site is enabled. Otherwise, the client receives an error message. If the Web site requested in the host header is stopped, the client receives the default Web site. Therefore, it is recommended that an ISP use the default Web site as the ISP home page, rather than for a customer site.

Web Site Properties - Operators Property Sheet

This property sheet defines which Windows NT user accounts have operator privileges to this site.

Web Site Operators

Use this property sheet to designate the Windows NT User Accounts you want to be able to administer this Web site. To add a Windows NT User Account to the current list of accounts which have administrative privileges, click the **Add** button, select a Windows NT user account to which you wish to grant Operator privileges from the **Names** list, then click **Add** again and **OK**. To remove a Windows NT User account from this list, select the account in the **Operators** list box, then click the **Remove** button. To search for a user to add, click the **Add** button and then the **Search** button.

Note

Web site administrator accounts need *not* necessarily be members of a Windows NT Administrators group.

An operator can carry out a limited set of Web site Administrative functions, including:

- Setting Web server access permissions and logging.
- Changing default Web documents and footers.
- Enabling Web content expiration, HTTP header, and content ratings features.

However, users with Operator privileges cannot carry out strictly Administrative functions, such as:

- Changing the identification of Web sites.
- Reconfiguring the anonymous user name and password.
- Throttling bandwidth.
- Creating virtual directories or changing virtual directory paths.
- Selecting or deselecting application isolations.

Web Site Properties - Performance Property Sheet

Use this property sheet to set properties that affect memory and bandwidth use.

Performance Tuning

Adjust this setting to the number of daily connections you anticipate for your site. If the number is set slightly higher than the actual number of connections, the connections are made faster and server performance is improved. If the number is much greater than the actual connection attempts, server memory is wasted, reducing overall server performance.

Enable Bandwidth Throttling

Check this option to limit the bandwidth used by this Web site. For this Web site only, the value for bandwidth typed here overrides the value set at the computer level, even if this value is greater than the value set at the computer level.

Connection Configuration

HTTP Keep-Alives Enabled allows a client to maintain on open connection with your server, rather than re-opening the client connection with each new request. Keep-Alives are enabled by default.

Web Site Properties - ISAPI Filters Property Sheet

Use this property sheet to set options for ISAPI filters. An *ISAPI filter* is a program that responds to events during the processing of an HTTP request. An ISAPI filter is always loaded in the Web site's memory.

The table lists the status of each filter (loaded, unloaded, or disabled), the name of the filter, and the priority rating of the filter (high, medium, or low) set inside the DLL. Click the **Add**, **Remove**, and **Edit** buttons to modify filter mappings. Click the **Enable** or **Disable** button to modify the status of filters. Select a filter and click the arrows to change the order in which filters are loaded.

The **Details** box lists the status of the selected filter, the filter name, the executable file that contains the filter, and the priority rating of the filter.

All Web sites on a server inherit the filters configured in the master properties for the Web service. If you add filters to an individual site, the filter lists are merged. The filters set by the master properties do not appear on this tab when you view it for a site. Only the filter list for the site appears.

When several filters have registered for the same event, they are called sequentially. Filters with a higher priority are run before filters with a lower priority. If several filters have the same priority, global filters set in the master properties are run before filters set at the site level. Filters with the same priority at the same inheritance level are run according to the order in which they were loaded.

Application Configuration - App Options Property Sheet

Use this property sheet to control how ASP scripts run within the selected application.

Enable Session State

Use this check box to enable or disable session state. When session state is enabled, Active Server Pages creates a session for each user who accesses an ASP application so that so that you can identify the user across pages in the application. When session state is disabled, ASP does not track users and does not allow an ASP script to store information in the **Session** object or use the **Session_OnStart** or **Session_OnEnd** events. A session automatically ends if the user has not requested or refreshed a page in an application by the end of the timeout period. To change the timeout period, type a new number in the **Session Timeout** text box. A script can explicitly end a session by using the **Session.Abandon** method. Even when session state is enabled for an application, you can disable session state for an individual ASP page by using the < %@ ENABLESESSIONSTATE = False %> directive.

Enable Buffering

Select this check box to buffer output to the browser. When this option is selected, all output generated by an ASP page is collected before it is sent to the browser. When this checkbox is cleared, output is returned to the browser as the page is processed. Buffering output enables you to set HTTP headers from anywhere in an ASP script. You can override this option in a script by using the **Response.Buffer** method.

Enable Parent Paths

Select this check box to allow ASP scripts to use relative paths to the parent directory of the current directory (paths using the .. syntax). If you enable this option, do not give the parent directories Execute access; otherwise, a script could attempt to run an unauthorized program in a parent directory.

Default ASP Language

Specifies the primary script language for Active Server Pages, the language used to process commands within ASP delimiters (<% and %>). To choose a different primary script language for all pages in the selected application, type the name of the language in the text box. ASP comes with two ActiveX script engines: Microsoft Visual Basic Scripting Edition (**vbscript**) and Microsoft JScript (**jscript**). The initial value of **Default ASP Language** is **vbscript**. You can specify the name of any language for which an ActiveX script engine is installed on your server; be sure to use the exact keyword required for your engine as documented by your script engine provider. You can override default language on an ASP page by using the <%@ LANGUAGE %> directive.

ASP Script Timeout

Specifies the length of time ASP will allow a script to run. If the script does not finish running by the end of the timeout period, ASP stops the script and writes an event to the Windows NT event log. You can set the timeout period to a value between 1 and 2147483647. You can override this option in an ASP script by using the **Server.ScriptTimeout** method.

Note

You can set Application Configuration properties at the Web site, virtual directory, and directory level.

Application Configuration - App Debugging Property Sheet

Use this property sheet to set debugging options for ASP scripts run in the selected application.

Enable ASP Server-Side Script Debugging

Select this check box to enable the Web server to enter the Microsoft Script Debugger while processing ASP scripts. You can then use the debugger to examine your scripts.

Enable ASP Client-Side Debugging

This check box is reserved for future use and has no effect on the current version of ASP.

Send Detailed ASP Error Messages to Client

Select this option to send specific debugging information (including the file name, error message, and line number) to the browser.

Send Text Error Message to Client

Select this option to send a default error message to the browser when any error prevents the Web server from processing the ASP script. A specific error message is written to the error log. You can change the default error message by typing a new message in the text box.

Note

You can set Application Configuration properties at the Web site, virtual directory, and directory level.

Application Configuration - App Mappings Property Sheet

Use this property sheet to map file name extensions to the program or interpreter that processes those files. Mapped applications include Internet Server API (ISAPI) applications, Active Server Pages (ASP) applications, Internet Database Connector (IDC) applications, and files that use server-side include directives. For example, when the Web server receives a request for a page with an .asp extension, it uses the application mapping to determine that the executable file asp.dll should be called to process the page.

Cache ISAPI Applications

Internet Server API DLLs can be loaded and cached so that further requests can be processed without calling the application again. Most ISAPI applications (including Active Server Pages) benefit from caching. You should clear this option only for special circumstances, such as debugging ISAPI applications.

If the same ISAPI application has been loaded and cached by more than one Web site on a server, then clearing this option for the server does not unload the application from memory. You must clear this option for all Web sites that use the application. Clearing this option does not unload running applications. Only subsequent requests are not cached.

Application Mappings

The table lists the file name extension associated with an executable file and the name of the executable file. Click the **Add**, **Edit**, and **Remove** buttons to modify application mappings.

Note

You can set Application Configuration properties at the Web site, virtual directory, and directory level.

Application Configuration - Process Options Property Sheet

Use this property sheet to change settings for the applications running in a single process. You can use this property sheet to change settings for two types of processes: the Web server process and isolated application processes. Options set for the Web site affect all applications running in the Web server process. Options set for an isolated application affect only that application.

Write Unsuccessful Client Requests to Event Log

Select this check box to instruct the Web server to write unsuccessful client requests to the Windows NT event log.

Enable Debug Exception Handling

When this check box is selected, ASP sends a general error message when it cannot create an instance of an object provided by an ActiveX component (a call to **Server.CreateObject**). When this check box is deselected, ASP passes on the specific error message from the component. Deselect this option when you are debugging a component. When you have finished debugging, select the option again.

Number of Script Engines Cached

Specifies the maximum number of ActiveX script engines that Active Server Pages will keep cached in memory.

Script File Cache Options

Use these options to specify the number of preprocessed .asp files to cache in memory. Increasing the number of cached files improves Active Server Pages performance. To cache all .asp files, select **Cache All Requested ASP Files**. To specify the maximum number of script files to cache, select **Max ASP Files Cached** and type a value in the text box.

CGI Script Timeout

You can set or change the timeout value, which is the amount of time a CGI script is given to execute and return a value before the operation is stopped.

Note

You can set Application Configuration properties at the Web site, virtual directory, and directory level.

Web Site Properties - Documents Property Sheet

Enable Default Document

Select this check box to show the user a default document when a browser request does not include a specific HTML file name. Default documents can be a directory's home page, or an index page, that provides links to the documents in the directory. You can specify more than one default document; to add a new default document, click **Add**. The Web server searches the directory for the default documents, following the order in which the names appear in the list. The server returns the first document it finds. To change the search order, select a document and click the arrows.

Enable Document Footer

Select this option to configure your Web server to automatically insert an HTML-formatted file to the bottom of every Web document sent by your Web server. The footer file should be not be a complete HTML document, rather, it should only include HTML tags necessary for formatting the appearance and function of your footer content.

You must provide the full path and file name for your footer file.

Note

You can configure Documents properties at the Web site, virtual directory, and directory level.

Web Site Properties - Directory/File Security Property Sheet

Use this property sheet to set your Web server's security features.

Anonymous Access and Authentication Control

Click **Edit** to configure your Web server's authentication and anonymous access features. Use these features to configure you Web server to confirm the identity of users before granting access to restricted content.

Before your server can authenticate users, however, you must first create valid Windows NT user accounts and then configure Windows NT File System (NTFS) directory and file permissions for those accounts.

Secure Communications

Click **Key Manager** to create an SSL key pair and server certificate request. You cannot use your Web server's secure communications features until you have installed a valid server certificate and bound this certificate to your server key pair. For more information, consult your the Web server documentation.

After creating a server key, under Secure communications, click **Edit** (this button previously displayed the words "Key Manager") to configure your Web server's Secure Sockets Layer (SSL) secure communications features (your Web server also supports the Private Communication Technology (PCT) 1.0 standard for secure communications.). You can use these features to do the following:

- Require user to establish a secure (encrypted) link in order to connect to your directory or file.
- Configure your Web server's client certificate mapping and authentication features.
- Configure Key Manager.

TCP/IP and Domain Name Restrictions

(This feature is only available for Windows NT Server installations.)

Click **Edit** to enable or prevent specific users, computers, or domains from accessing this Web site, directory, or file.

WWW Service Master Properties - IIS 3.0 Admin Property Sheet

Use this property sheet to designate a single Web site that can be administered by previous versions of Internet Service Manager. Only one Web site per IIS 4.0 installation can be administered by the version of Internet Service Manager shipped with IIS 3.0 or earlier.

Content Ratings - Ratings Property Sheet

Use this property sheet to configure your Web server's content rating features for a particular Web site, directory, or files. Your Web server's default Platform for Internet Content Selection (PICS) based rating system uses a system developed by the Recreational Software Advisory Council (RSAC), which rates content according to levels of violence, nudity, sex, and offensive language. On the **Rating Service** property sheet, you can fill out a RSAC ratings questionnaire to obtain recommended ratings for your Web site.

To configure your content ratings, select the **Enable Ratings for this resource** check box. Select a rating system from the **Category** list box. Select the appropriate value (or label) by using the slider bar. Under **Optional Information**, type the name of person who rated the content. Click **Date** to choose a expiration date for the rating settings.

IP Address and Domain Name Restrictions

Use these properties to provide or prevent specific users from accessing this Web site, directory, or file.

By default, all computers will be:

Granted Access Select this button to allow all computers access to this virtual directory, except those computers specifically listed as exceptions. For example, you can exclude a particular individual or group by denying access to your server from a particular IP address, or prevent entire networks from accessing your server, while allowing all others to have access.

Denied Access Select this button to deny access to all remote users except those whose IP addresses have been specifically granted access. IP address security is probably most useful on the Internet, to exclude everyone except known users.

Except those listed below:

To grant or deny access to a specific computer or group of computers:

1 Click **Add**. If the **Granted Access** button is selected, the **Deny Access On** dialog box appears; if the **Denied Access** button is selected, the **Grant Access On** dialog box appears.

2 In the appropriate (either **Deny Access On** or **Grant Access On**)window, select **Single Computer**, **Group of Computers**, or **Domain Name** to restrict or allow access by that method.

3 In the **IP Address** box, type the IP address of the computer to be granted or denied access to your site.

Logging Properties - General Properties Property Sheet

This dialog box allows you to specify how log files will be created and saved.

New Log Time Period

Choose the criterion that the software uses when starting a new file.

Note

For the **Daily**, **Weekly**, or **Monthly** criteria for new log files, "midnight" is defined in the time zone used by the chosen log format. This means that for NCSA Common Log File Format (or for IIS only, ODBC Logging), "midnight" is on local time; for Microsoft IIS Log Format and W3C Extended Log File Format, "midnight" is on Greenwich Mean Time.

Daily Log files created daily, starting with the first entry that occurs after midnight.

Weekly Log files created weekly, starting with the first entry that occurs as Sunday begins (after midnight).

Monthly Log files created monthly, starting with the first entry that occurs as the month begins (after midnight).

Unlimited file size Data is always appended to the same log file. You can only access this log file after stopping the server (that is, selecting the server and clicking the Stop button).

When file size reaches A new log file is created when the current log file reaches a given size; specify the size you want.

Log file directory

Type the directory in which log files should be saved, or click **Browse** and locate the directory.

A filename is displayed beneath the **Log file directory** box; this name is determined by the log file format and the criterion used for starting new log files.

Extended Logging Properties - Extended Properties Property Sheet

This dialog box allows you to customize W3C Extended logging, by choosing the fields (items) to be recorded in the log. You can gather detail using fields important to you, while limiting log size by omitting unneeded fields. The fields are as follows:

Date The date on which the activity occurred.

Time The time the activity occurred.

Client IP Address The IP address of the client that accessed your server.

User Name The name of the user who accessed your server.

Service Name The Internet service that was running on the client computer.

Server Name The name of the server on which the log entry was generated.

Server IP The IP address of the server on which the log entry was generated.

Server Port The port number the client is connected to.

Method The action the client was trying to perform (for example, a GET command).

URI Stem The resource accessed: for example, an HTML page, a CGI program, or a script.

URI Query The query, if any, the client was trying to perform; that is, one or more search strings for which the client was seeking a match.

Http Status The status of the action, in HTTP terms.

Win32 Status The status of the action, in terms used by Windows NT.

Bytes Sent The number of bytes sent by the server.

Bytes Received The number of bytes received by the server.

Time Taken The length of time the action took.

Protocol Version The protocol (HTTP, FTP) version used by the client. For HTTP this will be either HTTP 1.0 or HTTP 1.1.

User Agent The browser used on the client.

Cookie The content of the cookie sent or received, if any.

Referrer The site on which the user clicked on a link that brought the user to this site.

ODBC Logging Properties - ODBC Properties Property Sheet

Before you can begin ODBC logging from IIS or PWS, there are several steps to take. First, use ODBC-compliant database software (such as Microsoft Access or Microsoft SQL Server) to create a database. Within the database, create a table containing the fields listed at the end of this topic. Next, use the Control Panel to access the ODBC option and give the database a system Data Source Name (DSN), so that the ODBC software-layer can recognize the database. Finally, supply IIS or PWS with the Data Source Name and Table name by using this dialog box. If a user name and password are required for accessing the database, supply them as well. The options in this dialog box are as follows:

ODBC Data Source Name (DSN)

Type the system Data Source Name for the database to which logging entries will be sent. The Data Source Name must be defined in the Control Panel by using the **ODBC** option and the **System DSN** property sheet. Be sure to type the same name here as you type in the **System DSN** property sheet.

Table

Type the name of the database table to which logging entries will be sent. Type the same name as the one you assigned the table within the database program. See the list below for the fields that must be part of the table in order for it to receive logging entries.

User Name

If a user name and password are required for accessing the ODBC-compliant database, type the user name here.

Password

If a user name and password are required for accessing the ODBC-compliant database, type the password here.

Fields to Include in the Database You Create

Before ODBC logging can begin, you must create an appropriate table within the database that is specified in this dialog box. The table must have the following fields: **ClientHost** varchar(255), **Username** varchar(255), **LogTime** datetime, **Service** varchar(255), **Machine** varchar(255), **ServerIP** varchar(50), **ProcessingTime** int, **BytesRecvd** int, **BytesSent** int, **ServiceStatus** int, **Win32Status** int, **Operation** varchar(255), **Target** varchar(255), **Parameters** varchar(255).

Basic Authentication Domain

Users logging on with the Basic authentication method must belong to a specific *domain*. A domain is a computer or a network of computers managed as a single administrative entity. When users attempt to log on without specifying a domain, you can configure you server to assume that the users belongs to a domain different from the default local domain. For example, if your server contains a Web site accessed exclusively by members of the *Sales* domain, but your server belongs to the *Shipping* domain, then you can configure that Web site's Basic authentication default domain to be the *Sales* domain.

If your Web server does not belong to a network, then the default local domain is the name of your computer.

Client Certificate Authorities

Certificate authorities are mutually trusted, third-party authorities that issue client certificates to a user (usually for a fee) after verifying the user's identity. You can configure your server to authenticate users by mapping client certificates to Windows NT accounts by matching a client certificate issuing authority against your server's list of trusted authorities. Alternatively, you can authenticate users by matching against specific authorities, rather than every authority on the list. To select an authority, click **Toggle**. Click **OK**.

Account Mappings - Advanced

Client certificates contain fields that identify a user, an organization affiliated with the user, and the authority that issued the certificate; some fields also contain certificate serial numbers and expiration dates. Based on these fields, you can define rules for accepting and mapping certificates to user accounts. For example, you can define a rule that automatically maps all client certificates issued by a particular organization, to a Windows NT account, regardless of the user's identity.

Enable Wildcard Client Certificate Matching

Select this check box to enable custom mapping rules that check whether client certificate fields match a pre-defined criteria. (You must explicitly create the rules by which certificates are mapped.)

Edit Rule

Select a custom matching rule that want to modify, then click this button.

Add

Click this button to create a custom rule for checking a client certificate's fields for specific information before mapping the certificate to a Windows NT account.

Delete

Select a custom matching rule that want to remove, then click this button.

Move Up and Move Down

Click these buttons to scroll up or down the matching rules list in order to select a rule.

Rules

You can create mapping rules that check whether certain client certificate fields match pre-defined criteria. If the a field or subfield matches the criteria, the certificate is mapped to an account. For example, you can create a rule that automatically maps any client certificate issued by a particular authority, regardless of any other information contained on the certificate.

New

Click this button to create new certificate field and match criteria with the **Edit Rule Element** dialog box.

Edit

Click this button to modify certificate field and match criteria for the selected certificate.

Delete Button

Click this button to delete the selected certificate field and match criteria.

Anonymous User Account

Use this dialog box to set the Windows NT user account used for anonymous connections. By default, the server creates and uses the account IUSR_*computername*.

Username

Type the name of the anonymous account you created with the Windows NT User Manager for Domains utility in this box.

Password

Type in the anonymous user account password in this box. When you installed the server, Setup created the account IUSR_*computername* in Windows NT User Manager for Domains and in Internet Service Manager.

Note

Enabling automatic password synchronization disables this box. The password is used only within Windows NT; anonymous users do not log on by using a user name and password.

Enable Automatic Password Synchronization

When you create a new anonymous account, you must make sure that your Web site and Windows NT password settings are identical. Select this option to automatically synchronize your anonymous password settings with those set in Windows NT.

Important

Password synchronization should only be used with anonymous user accounts defined on the local computer, not with anonymous accounts remote computers.

Add Users and Groups

Use this dialog box to grant administration privileges for this Web site to Windows NT users and groups.

List Names From

Select the Windows NT domain that contains the user or group you want to add from this list box, which includes the name of the computer you are administering.

Names

Select the user or group you want to add, then click **Add** to add that user or group. If you select a group, you can click **Members** to view a list of the group's members. Click **Search** to search for users and groups by domain.

Add Names

The users and groups you added using the **Names** dialog box appear in this dialog box. Click **OK** to verify these are the users and groups you want to add.

Local Group Membership

Lists the user accounts and global groups that are members of the selected local group.

Members Of Local Group

Lists the members of the selected local group.

Add

Adds the user accounts or global groups selected in **Members Of** in the **Local Group Membership** dialog box to **Add Names** in the **Add Users And Groups** dialog box.

Members

Displays the members of the selected global group (that is itself a member of this local group).

Global Group Membership

Lists the user accounts that are members of the selected global group.

Members of Global Group

Lists the members of the selected global group.

Add

Adds the user accounts or global groups selected in **Members Of** in the **Local Group Membership** dialog box to **Add Names** in the **Add Users And Groups** dialog **box.**

Find Account

Use this feature to search domains for a specific user or group.

Find User or Group

Type the user or group that you want to search for in the text box.

Search All

Select this option to search every domain for the user or group you specified in the **Find User or Group** text box.

Search Only In

To limit your user or group search to specific domains, select this option button. Select a domain to search from the list box. To select multiple domains, press the CTRL key while selecting.

Search Results

This box displays the user accounts and groups found by a search. This list is continuously filled as a search progresses.

The list presents the matching users in the form *domainname**username* (full name) description, or *computername**username* (full name) description.

The list presents the matching groups in the form *domainname**groupname* description, or *computername**groupname* description.

Add

Closes the **Find Account** dialog box and adds the accounts selected in **Search Results** to **Add Names** text box in the previous dialog box.

Inheritance Overrides

Use this dialog box to determine whether the properties you set at one level in the tree view of Internet Service Manager are inherited by the levels below that level, or parent node. By default, lower, or child nodes, inherit properties that are set at a higher level; however, if you have previously changed a child node, the child node does not automatically inherit the new parent value. This dialog box allows you to designate which child nodes should inherit the changed value of the parent node.

To designate which child nodes should inherit the value that is being set at the parent node level, select the nodes in the list box and click **OK**.

Click **Select All** to indicate that all child nodes should inherit the new value that is being set at the parent node level.