

WWW Service Properties

You use the **Service** property sheet to control who can use your server and to specify the account used for anonymous client requests to log on to the computer. If you allow anonymous logons, then all user permissions for the user, such as permission to access information, will use the IUSR_*computername* account. To use your current security system to control information access, change the anonymous logon account from IUSR_*computername* to an existing account on your network.

This property sheet also sets the comment in the main Internet Service Manager window.

TCP Port

Determines the port on which the WWW service is running. The default is port 80. You can change the port to any unique TCP port number. For a new port number to take effect, you must restart your computer.

Connection Timeout

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

Maximum Connections

Sets the maximum number of simultaneous connections to the WWW service.

Anonymous Logon

Sets the Windows NT user account to grant permissions to all anonymous connections. By default, Peer Web Services creates and uses the account IUSR_*computername*. Note that the password is used only within Windows NT; anonymous users do not log on by using a user name and password.

When you installed Internet Information Server, Setup created the account IUSR_*computername* in the Windows NT User Manager and in the Internet Service Manager. This account was assigned a random password. The password for this account must be the same, both in Internet Service Manager and in the Windows NT User Manager. If you change the password, you must change it in both places and make sure it matches. **Note:** This account must have a password. You cannot assign a blank password.

The IUSR_*computername* is granted **Log on locally** user rights by default. This right is necessary as long as you want to grant anonymous logon access to your site. **Note:** To grant access to a specific user, you must grant that user **Log on locally** rights in Windows NT Workstation **User Manager**.

Password Authentication

Specifies the authentication process to use if anonymous access is not allowed or the remote client requests authentication.

Basic authentication is encoded. Basic authentication is often used in conjunction with Secure Sockets Layer (SSL) to ensure that user names and passwords are encrypted before transmission. Most browsers support Basic authentication. Note that, when not used in conjunction with SSL, Basic authentication sends passwords in clear (unencrypted) text.

Windows NT Challenge/Response authentication automatically encrypts user names and passwords.

Note: At least one option must be selected.

Comment

Specifies the comment displayed in Internet Service Manager **Report** view.

See also: The Peer Web Services *Installation and Administration Guide*. Choose Help Topics from Internet Service Manager, or click the Product Documentation icon in the Microsoft Peer Web Services program group.

WWW Directories

The WWW **Directories** property sheet sets directories and directory behavior for the WWW service.

Directory listing box

Lists the directories used by the WWW service.

Directory lists the path of directories used by the WWW service.

Alias is the path used for virtual directories.

Address lists the Internet Protocol (IP) address using that directory.

Error indicates system errors, such as difficulty reading a directory.

Add, Remove, and Edit buttons

To set up a directory, press the **Add** button or select a directory in the Directories listing box and press the **Edit** button. The **Remove** button removes the directories that you select.

Enable Default Document and Directory Browsing Allowed

The **Default Document** and **Directory Browsing** settings in the **Directories** property sheet for the WWW service are used to set up default displays that will appear if a remote user does not specify a particular file. Directory browsing means that the user is presented with a hypertext listing of the directories and files so that the user can navigate through your directory structure.

You can place a default document in each directory so that when a remote user does not specify a particular file, the default document in that directory is displayed. A hypertext directory listing is sent to the user if directory browsing is enabled and no default document is in the specified directory.

Note that virtual directories will not appear in directory listings; users must know a virtual directory's alias and type in its Uniform Resource Locator (URL) address, or click a link in a HyperText Markup Language (HTML) page, to access virtual directories.

See also: The Peer Web Services *Installation and Administration Guide*. Choose Help Topics from Internet Service Manager, or click the Product Documentation icon in the Microsoft Peer Web Services program group.

WWW Directory Properties

Configure the WWW service directories by using this dialog box. Press the **Add** button on the **Directories** property sheet to set up new directories.

Directory

Sets the path to the directory to use for the WWW service.

Browse button

Use to select the directory to use for the WWW service.

Home Directory

Choose this to specify the root directory for the WWW service.

Peer Web Services provides a default home directory, \Wwwroot, for the WWW service. The files that you place in the WWW home directory, and its subdirectories, are available to remote browsers. You can change the location of the default home directory.

Virtual Directory

Choose this to specify a subdirectory for the WWW service. Enter the directory name or alias that service users will use to gain access.

You can add other directories outside the home directory that are accessed by browsers as subdirectories of the home directory. That is, you can publish from other directories and have those directories accessible from within the home directory. Such directories are called "virtual directories."

The administrator can specify the physical location of the virtual directory and the virtual name (alias), which is the directory name used by remote browsers.

Note that virtual directories will not appear in WWW directory listings; you must create explicit links in HTML files in order for users to access virtual directories. Users can also type in the URL if they know the alias for the virtual directory.

The published directories can be located on local or network drives. If the virtual directory is a network drive, provide the user name and password with access to that network drive. Virtual directories on network drives must be on computers in the same Windows NT domain as the computer running Peer Web Services.

Account Information

This box is active only if the directory specified in the first line of this dialog box is a Universal Naming Convention (UNC) server and share name, for example, \\Webserver\Htmlfiles. Enter the user name and password that has permission to use the network directory. Virtual directories on network drives must be on computers in the same Windows NT domain as the Peer Web Services.

Important If you specify a user name and password to connect to a network drive, all Peer Web Services access to that directory will use that user name and password. You should use care when using UNC connections to network drives to prevent possible security breaches.

Access check boxes

The **Access** check boxes control the attributes of the directory. If the files are on a Windows NT File System (NTFS) drive, NTFS settings for the directory must match these settings.

Read must be selected for information directories. Do not select this box for directories containing programs.

Execute allows clients to run any programs in this directory. This box is selected by default for the directory created for programs. Put all your scripts and executable files into this directory. Do not select this box for directories containing static content.

Require secure SSL channel select this box if using Secure Sockets Layer (SSL) security to encrypt data transmissions.

See also: The Peer Web Services *Installation and Administration Guide*. Choose Help Topics from Internet Service Manager, or click the Product Documentation icon in the Microsoft Peer Web Services program group.

WWW Logging Properties

The **Logging** property sheet sets logging for the selected information service.

Logging provides valuable information about how a server is used. If you have multiple servers or services on a network, you can log all their activity to a single file on any network computer.

You can specify how often to create new logs and which directory put the log files in. The **Convlog.exe** command prompt command converts log files to either EMWAC log files or the common log file format.

Enable Logging

Select this box to start or stop logging for the selected service.

Log to File

Choose this option to log to a text file for the selected service.

Log Format

Click the down arrow and choose either Standard format or National Center for Supercomputing Applications (NCSA) format.

Automatically open new log

Select this box to generate new logs at the specified interval. If not selected, the same log file will grow indefinitely.

Log file directory

Shows the path to the directory containing all log files. To change directories, click Browse and select a different directory.

Log file name

Names the log file. Lowercase letters **yy** will be replaced with the year, **mm** will be replaced with the month, and **dd** will be replaced with the day.

See also: The Peer Web Services *Installation and Administration Guide*. Choose Help Topics from Internet Service Manager, or click the Product Documentation icon in the Microsoft Peer Web Services program group.

Internet Service Manager Authentication Options

In addition to the "anonymous logon" user name and password fields, the **Service** property sheet of Internet Service Manager contains the following authentication options:

WWW

Allow Anonymous When this check box is selected, anonymous connections are processed, and the "anonymous logon" user name and password are used for these connections. When this check box is unchecked, all anonymous connections are rejected, and basic or Windows NT Challenge/Response authentication protocol is required to access content.

Basic When this check box is selected, the WWW service will process requests using basic authentication. **WARNING:** Basic authentication sends Windows NT user names and passwords across the network without encryption. This check box is cleared by default for security reasons.

Windows NT Challenge/Response When this check box is selected, the service will honor requests by clients to send user account information using the Windows NT Challenge/Response authentication protocol. This protocol uses a one-way hash (a function with no inverse function, for instance X2) to prevent passwords from being transmitted across the network. The Windows NT Challenge/Response authentication process is initiated automatically as a result of an "access denied" error on an anonymous client request.

Note: If the **Basic** and **Windows NT Challenge/Response** check boxes are both cleared (and the **Allow Anonymous** check box is selected), all client requests are processed as anonymous requests. In this case, if the client supplies a user name and password in the request, this user name and password are ignored by the WWW service. The "anonymous logon" user account will be used to process the request.

See also: The Peer Web Services *Installation and Administration Guide*. Choose Help Topics from Internet Service Manager, or click the Product Documentation icon in the Microsoft Peer Web Services program group.

Select the directory you want or create a new directory by typing a name in the **New Directory Name** box.

Help not available.

Help not available.

Help not available.

