

Help does not exist for this dialog.

FTP Site Properties - FTP Site Property Sheet

On this property sheet, you set the identification parameters for your server. The server and domain names and the IP address are optional.

Identification

Description

You can use any name you want for the server name. This name is primarily for your own identification and organizational purposes.

IP Address

For an address to appear in this box, it must have already been defined for use in Control Panel. See your Windows NT documentation for more information.

TCP Port

Determines the port on which the service is running. The default is port 21. 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. For a new port number to take effect, you must restart your computer.

Connection

Unlimited

Allows an unlimited number of simultaneous connections to the server.

Limited To

Sets the maximum number of simultaneous connections allowed to the server.

Connection Timeout

Sets the length of time 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 FTP 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 FTP 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.

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**.

Current Sessions

Click this button to view a list of users currently connected to your site. This feature is not available on Internet Service Manager (HTML).

FTP Site Properties - Security Accounts Property Sheet

Use the **Security Accounts** property sheet to control who can use your server and specify the account used for anonymous client requests to log on to the computer. Most Internet sites allow anonymous logons. 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.

Allow Anonymous Connections

Select the **Allow Anonymous Connections** check box to allow users using the username "anonymous" to log into your FTP server. Use the **User Name** and **Password** dialog boxes to establish the Windows NT user account to use for permissions for all anonymous connections. By default, Internet Information Server creates and uses the account IUSR_*computername* for all anonymous logons. Note that the password is used only within Windows NT ; anonymous users do not log on using this user name and password.

Typically, anonymous FTP users will use "anonymous" as the user name and their e-mail address as the password. The FTP service then uses the IUSR_*computername* account as the logon account for permissions.

When you installed Internet Information Server, Setup created the account IUSR_*computername* in the Windows NT User Manager for Domains and in Internet Service Manager. This account was assigned a random password for both in Internet Service Manager and in the Windows NT User Manager for Domains. 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 if you want to grant anonymous logon access to your site.

Note

To grant access only to specific users, you must grant those users **Log on locally** rights in User Manager for Domains.

Allow only anonymous connections

Select this check box to allow only anonymous connections. With this box selected, users cannot log on with user names and passwords. This option prevents access by using an account with administrative permission; only the account specified for anonymous access is granted access.

Enable Automatic Password Synchronization

When you create a new anonymous account, you must make sure that your FTP site and Windows NT password settings are identical. Select this option to enable your FTP site to automatically synchronize your anonymous password settings with those set in Windows NT. This option is enabled by default if the anonymous account exists on your FTP site, and not on a remote computer.

FTP Site Operators

Note

In order to administer virtual FTP sites, you must be a member of the Windows NT user accounts Administrative group. Adding Windows NT user accounts in the Operators list box will not enable users to administer this FTP site.

Use the **Operators** list box to designate the user accounts you want to be able to administer this FTP site. To add a user account to the current list of accounts which have administrative privileges, click **Add**. To remove a user account from this list, select the account you want to remove in the **Operators** list box, then click **Remove**.

FTP Site Properties - Messages Property Sheet

Use this property sheet to create your own messages that will be displayed to browsers that contact your site.

Welcome message

Displays this text to clients when they first connect to the FTP server. The message is blank by default.

Exit message

Displays this text to clients when they log off the FTP server. The message is blank by default.

Maximum connections message

Displays this text to clients that try to connect when the FTP service already has the maximum number of client connections allowed. The message is blank by default.

FTP Site Properties - Virtual Directory Property Sheet

Use this property sheet to change the properties of a virtual directory in your FTP 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 FTP site. To add a new virtual directory to an FTP site, right-click the FTP site, select **Create 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.

FTP Site Directory

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.

Browse button

Click the **Browse** button to select a local directory rather than typing the directory path in the **Path** text box.

Access check boxes

Use the **Access** 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 FTP server returns an error. This permission must be selected for FTP directories.

Write Enables Web clients to upload files to the enabled directory on your server. Select this permission only for directories that are intended to accept files from users.

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 FTP site. Logging is enabled by default. To turn off logging, select the FTP site, open its property sheets, click the **FTP Site** tab, and then clear the **Enable Logging** check box.

FTP Site Properties - Directory Security Property Sheet

The **Directory Security** property sheet sets access by specific IP address to block individuals or groups from gaining access to your server.

TCP/IP Access Restrictions

You can control access to each Internet service by specifying the IP address, subnet mask, or domain name of the computer or computers to be granted or denied access.

If you choose to *grant* access to all users by default, you can then specify the computers to be denied access. For example, if you discover that a particular user on the Internet is trying to download restricted files from your FTP server, you can prevent the computer at that IP address from connecting to your site. Conversely, if you choose to *deny* access to all users by default, you can then specify which computers are allowed access.

Granted Access

Select this button, then click **Add** to list computers that will be denied access.

Denied Access

Select this button, then click **Add** to list computers that will be granted access.

Add

To add computers that you want to deny access to, select the **Granted Access** button and click **Add**. Conversely, to add computers that you want to grant access to, select the **Denied Access** button, and click **Add**.

Note

You can configure Security properties at the FTP Site and virtual directory level.

FTP Site Properties - Home Directory Property Sheet

Use this property sheet to change the home directory for your FTP site or to modify its properties. The home directory is the central location for the published files in your FTP site. A default home directory, called \Ftproot, was created when you installed the FTP 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.

FTP Site Directory

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.

Access check boxes

Determines 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 FTP server returns an error. This permission must be selected for FTP directories.

Write Enables Web clients to upload files to the enabled directory on your server. Select this permission only for directories that are intended to accept files from users.

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 FTP site. Logging is enabled by default. To turn off logging, select the FTP site, open its property sheets, click the **FTP Site** tab, and then clear the **Enable Logging** check box.

Directory Listing Style

Changes the directory listing style to send to FTP users. Because many browsers expect UNIX format, you should select **UNIX** for maximum compatibility.

Basic Authentication Warning

In addition to the "anonymous logon" user name and password fields, the **Security Accounts** property sheet contains the following authentication options:

Allow Anonymous Connections

When this check box is selected, FTP logons in which the user enters a user name of "anonymous" will be processed. These anonymous connections will be processed on behalf of the Windows NT user account specified on the Security Accounts property sheet. When this check box is cleared, users will be required to enter valid Windows NT user names and passwords to log onto the FTP service.

Allow only anonymous connections

When this check box is selected, all user logons except "anonymous" will be rejected.

Warning

FTP user names and passwords are sent across the network in clear text. When this check box is cleared, Windows NT passwords will be sent to the server without encryption. This check box is checked by default for security reasons.

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 radio 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.

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

Domain Name Select this radio button to add access rights for a specific internet domain. Type the 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 to, by default, grant access to all users, you are specifying that these computers to be denied access. If you choose to, by default, deny access to all users, you are then specifying that these specific computers be allowed access. You should fully understand TCP/IP networking, IP addressing, and the use of subnet masks before you use this option.

Select Windows NT User Account

Use this dialog box to grant administration privileges for this FTP 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 Name

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.

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.

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 Name** in the **Select Windows NT User Account** 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 **Select Windows NT User Account** dialog box.

Members

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

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. For tighter security, use the `IUSR_computername` account (the anonymous user) for the computer on the network.

Logging Properties - General Properties Property Sheet

This property sheet 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 property sheet 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.

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.

Server Port The port number the client is connected to.

Time Taken The length of time the action took.

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).

FTP User Sessions

This dialog box displays a list of all currently connected users. To disconnect a single user, select the user and click **Disconnect**. To disconnect all current users, click **Disconnect All**.

FTP Service Master Properties - IIS 3.0 Admin Property Sheet

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

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 higher level, or parent node. By default, child nodes inherit properties that are set at the higher level; that is, the child nodes do not automatically override the values that you set at the parent node with their current settings unless those settings have been previously explicitly set at the child node level. 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.

