Remote Copy Help Contents

Introducing Remote Copy

What is Remote Copy?

The Remote Copy application lets you quickly copy files or directories between your PC and another computer on the network. If you know the location of the files that you want to transfer, Remote Copy provides a fast way to transfer those files without having to log in to the remote host.

You can use wildcards to transfer multiple files, and verify your identity on the remote host by using the Rsh or Rexec authentication protocol. (Unlike the FTP application, you cannot rename, view, or delete files with Remote Copy.)

Related Topics

Getting Started
Step-by-Step Instructions
Concepts

Getting Started

Before you start copy files with Remote Copy, be sure that

- You know the hostname or Internet Protocol (IP) address of the <u>remote host</u> that you want to use for file transfers.
- The appropriate account information (for example, username and password) is established for you on that host. You need this login information when you make a connection to that remote host for Remote Copy transfers that use authentication.
- On UNIX hosts, you can examine the /etc/hosts and /etc/hosts.equiv files to be sure your host is listed. If you have any questions about this procedure, or about your account on a remote host, contact your system administrator.
- You have permission to access the files that you want to copy.
- On remote UNIX systems, you can examine the file permissions if you are uncertain about them, using the UNIX **ls -l** command with the Remote Command application or similar utility.
- You are familiar with file naming conventions, case sensitivity rules, and <u>wildcard</u> syntax on the remote host and your PC.

Related Topic

<u>What is Remote Copy?</u>
<u>Step-by-Step Instructions</u>
<u>Concepts</u>

Step-by-Step Instructions

Preparing to Use Remote Copy

Copying Files with Remote Copy

Choose the Authentication Protocol

Choose the <u>authentication protocol</u> from either the Authentication menu or the toolbar.

Related Topics

<u>The Authentication Menu</u>
<u>The Toolbar</u>

<u>Introduction</u>
<u>Step-by-Step Instructions</u>
<u>Concepts</u>

Copy Files to a Remote Computer from Your PC

1. In the Copy To box, select Remote.

2. In the Username box, enter the <u>username</u> required on the remote host.

3. In the Hostname box, enter the remote <u>hostname</u>.

4. In the File Name(s) box, enter the name(s) of the files you want to copy.

   Note: To specify more than one file, enter each name in the File Name box and separate each name with a space. You can also choose Select Files and use the Select Local Files for   Transfer dialog box to select multiple files.

5. To copy the file(s) into a remote directory other than the default login directory, in the Remote Directory box, enter the name of the directory on the remote hostinto which you want to copy files.

6. In the Local Directory box, enter the name of the directory on your PC in which the files you want to copy reside.

7. Choose Start.

   If a <u>password</u> is required, the Password dialog box appears. Enter the password on the remote host, and choose OK.

Related Topics

<u>Introduction</u>
<u>Step-by-Step Instructions</u>
<u>Concepts</u>

Copy Files from a Remote Computer to Your PC

1. In the Copy To box, select Local.

2. In the Username box, enter the <u>username</u> required on the remote host.

3. In the Hostname box, enter the remote <u>hostname</u>.

4. In the File Name(s) box, specify the files on the remote host that you want to copy to your PC. (Use wildcard syntax to specify multiple files.)

5. If the files on the remote host reside in a directory other than the default login directory, in the Remote Directory box, enter the name of the directory that contains the file(s) you want to copy.

6. In the Local Directory box, enter the name of the directory on your PC into which you want to copy files.

7. Choose Start.

    If a <u>password</u> is required, the Password dialog box appears. Enter the password on the remote host, and choose OK.

    The Start button changes to Stop. Choose Stop at anytime to cancel the operation in progress. When the process is fully executed, the button changes back to Start.

Related Topics

<u>Introduction</u>
<u>Step-by-Step Instructions</u>
<u>Concepts</u>

Copy All Files in a Directory

1. In the Copy To box, select Local or Remote.

2. In the Username box, enter the <u>username</u> required on the remote host.

3. In the Hostname box, enter the remote <u>hostname</u>.

4. In the File Name(s) box, use wildcard syntax to specify all files in the directory. For example, enter
   `*.*`.

5. If you are copying files to your local PC and the files on the remote host reside in a directory other than the default login directory, in the Remote Directory box, enter the name of the directory that contains the file(s) you want to copy.
   --or--
   If you are copying files to the remote host and you want to copy the files into a remote directory other than the default login directory, in the Remote Directory box, enter the name of the directory on the remote hostinto which you want to copy files.

6. If you are copying files to your local PC, in the Local Directory box, enter the name of the directory on your PC into which you want to copy files.
   --or--

. If you are copying files to the remote host, in the Local Directory box, enter the name of the directory on your PC in which the files you want to copy reside.

7. Choose Start.

Related Topics

Set Options for Copying Files

1. In the Type of Transfer box, choose <u>ASCII</u> or <u>Binary</u> to specify the type of files you are copying to/from the remote host.

2. In the Umask box, enter the <u>umask value</u> to set UNIX permissions for new files that you transfer from your PC to the remote host.

3. Choose OK.

Dialog Box Items

<u>ASCII</u>
<u>Binary</u>

<u>UMASK</u>

Related Topics

<u>Introduction</u>
<u>Step-by-Step Instructions</u>
<u>Concepts</u>

Concepts

The Authentication Menu

Use the Authentication Menu to choose the type of <u>authentication protocol</u> you want to use, either Rsh or Rexec.

Use this command	To do this
Do Not Request a Password	Use the Rsh protocol.
Request a Password	Use the Rexec protocol.

Related Topic

<u>The Toolbar</u>
<u>Introduction</u>
<u>Step-by-Step Instructions</u>
<u>Concepts</u>

The Edit Menu

Use the Edit menu to cut, copy, and paste information to and from the Windows clipboard.

Use this command	To do this
Cut	Cut information from the edit fields (Username, Hostname, File Name(s), Remote/Local Directory).
Copy	Copy information from the edit fields.
Paste	Paste information into the edit fields.

Related Topics

Introduction
Step-by-Step Instructions
Concepts

The Settings Menu

Use the Settings menu to customize Remote Copy. You can display the Status bar to view information about the progress being made by Remote Copy, and to display information pertinent to debugging.

Use this command	To do this
Display Icon Bar	Alternate between viewing and hiding the toolbar.
Display Status Bar	Alternate between viewing and hiding the status bar.
Save Settings on Exit	Save settings when you exit the application.

Related Topics

Introduction
Step-by-Step Instructions
Concepts

The File Menu

Use the File menu to exit the Remote Copy application.

Related Topics

[Introduction](#)
[Step-by-Step Instructions](#)
[Concepts](#)

The Toolbar

The toolbar gives you quick access to commands.

Use this button   To do this

Use the Rsh protocol; do not request a password

Use the Rexec protocol; request a password

Exit the Remote Copy application

Use the Settings menu to alternate between viewing and hiding the toolbar.

Related Topics

Introduction
Step-by-Step Instructions
Concepts

Umask values

The **umask** (User's Mask) command creates or returns the current <u>permissions</u> of files and directories on a UNIX system. It is like the UNIX **chmod** command, except that it masks or removes permissions from new files that you create.

In the Options dialog box, you can use the Umask box to set the default permissions for new files that you transfer from your PC to the remote host.

An octal value in the Umask box represents read (r), write (w), and execute (x) file permissions for the user (creator of the file), "group" and "other" classes of users. The first digit specifies the user's file permissions and is always zero (0). The default value is 0700.

Note: In most cases, the remote host is already set up with a default umask value for new files that you copy to that host. Typically, the default value provides the user with all permissions (0) and prevents write access (2) for group and others.

The octal values and the corresponding permission values are as follows:

Octal value	File Permissions
0	rwx (no restrictions)
1	rw-
2	r-x
3	r--
4	-wr
5	-w-
6	--x
7	(none)

For more information about **umask** values and file permissions, refer to your UNIX documentation.

Related Topics

<u>Introduction</u>
<u>Step-by-Step Instructions</u>
<u>Concepts</u>

Using Remote Copy

You use Remote Copy to quickly copy files or directories between your PC and another computer on the network. If you know the location of the files that you want to transfer, Remote Copy provides a fast way to transfer those files without having to log in to the remote host.

Dialog Box Items

Local
Remote

Username
Hostname
File Name(s)
Remote Directory
Local Directory

Select File(s)

Start/Stop
Options

Related Topics

Introduction
Step-by-Step Instructions
Concepts

Entering a Password

If you are using the Rexec <u>authentication protocol</u> or the remote host requires a password, enter your <u>password</u> in the Password box and choose OK.

Dialog Box Items

<u>Password required for *username*</u>

Related Topics

<u>Introduction</u>
<u>Step-by-Step Instructions</u>
<u>Concepts</u>

wildcard: One or more special characters that specify multiple files. For example, myfile.* on a PC matches myfile.exe, myfile.ini, myfile.bat, etc. UNIX wildcards are more powerful and more complex. Refer to your UNIX documentation for complete details about UNIX wildcards.

umask: An octal number that specifies default file permissions for new files on UNIX file systems.

file permissions: Determine whether you can read (r), write (w), or execute (x) a file.

authentication protocol: A communications protocol that sets up authentication for the connection between your PC and the remote host.

With Remote Copy, you can choose either Rsh (do not request a password) or Rexec (request a password).

hostname: The name assigned to the IP address of the remote host. You can identify the host by its name or by its IP address.

ASCII: An acronym for American Standard Code for Information Interchange and their standard computer character set used to encode text file; specifies the file transfer mode for a text file.

binary: A transfer mode for a file that contains both data and programming instructions; for example, a file that contains a compiled program. Binary mode can also be used for ASCII (text) files.

Indicates that you wish to copy file from a
remote host to your PC.

Indicates that you wish to copy file from
your PC to a remote host.

Type the username required to log in to the
remote host.

Type the password required to log in to the
remote host.

Type the name of the directory on the
remote host into which or from which you
wish to copy files. Leave blank to specify
the default login directory.

Type the name of the file to be copied. Use
wildcards to specify multiple files.

Type the name of the directory on your PC into
which or from which you wish to copy files.

Opens a standard dialog box that allows you to
browse your PCs file system to select one or
more local files for transfer.

Indicates that you wish to transfer ASCII (i.e.,
text) files.

Indicates that you wish to transfer binary files
(for example, program executables). You can
use this setting for ASCII (text) files as well.

Sets UNIX file permissions for new files that you transfer from
your PC to the remote host. The octal value in the Umask box
represents read (r), write (w), and execute (x) file permissions for
the user (creator of the file), "group" and "other" classes of users.
The first digit specifies the user's file permissions and is always
zero (0). The default value is 0700.

account name: The name or word that identifes who is billed for this session on a computer system.

case sensitivity: The ability of a program to evalutate the difference between the capitalized and non-capitalized versions of a character. Case sensitive programs treat for example, *cat* and *Cat*, as distinct items.

It matters how you enter file and variable names on a case sensitive operating system (such as the UNIX operating system). If you want to view a file named *Cat*, and you enter the characters *cat*,   the system displays the file named *cat* if one exists, or gives you an error message. It does not display a file named *Cat*. Case sensitivity also effects the way that files are listed when sorted in alphabetical order.
.

filename conventions: A TCP/IP network usually contains computers that run different operating systems. Each operating system has different conventions for naming files. For example, both the number and kinds of characters that can be used in a name are often subject to limits.

When you use some TCP/IP supported services such as telnet and ftp, use the filenaming conventions in effect on the host system to work with files that are on the host.

hostname: The name of a networked computer.

The hostname is one form of the computers TCP/IP network address; the other is its complete numeric network address.You can access a computer by its hostname or its numeric network address.

toolbar: A group of buttons that appears below the menu bar. These buttons let you gain access quickly to the application's features.

IP address: A number (in the form *n.n.n.n*   where each *n* is a value in the range 0 to 255) that uniquely identifies a networked computer that uses the TCP/IP communication protocol. (The Internet Protocol is defined in RFC 791.)

MIB-II: The Management Information Base (MIB) database used by an SNMP MIB agent to store information about the network operations of your PC. MIB-II (or MIB version 2) is the second version of the Internet-standard MIB. RFC 1213 defines the format of MIB-II.

packet: A single network message with its associated header, addressing information, data, and optional trailer. Also known as a "frame" or "datagram".

password: A word or string of characters that you supply in order to login to another system on a network. Systems that accept the username "anonymous" often require you to provide your e-mail address as the password.

permissions: On UNIX systems, settings that control who has access to a file and what rights (read, write, or execute) are given. NFS uses UNIX-style permissions to control access to network files.

protocol window: Some OnNet applications support a window dedicated to displaying the interactions between your PC and the remote host (the protocol). You can display the window usually from a View, Settings, or Options menu.

remote host: A networked computer that makes a service available to other computers on the network. Typical host services include transferring files, printing files, and managing logins from remote users.

SNMP community: A relationship between an SNMP agent and one or more SNMP management stations.

SNMP community name: A unique name shared by the members of an SNMP community.

SNMP message: A packet of data, consisting of an SNMP community name and SNMP commands and operands.

status bar: A message area, typically at the bottom of the application window, that provides information about the component that is currently selected, or the state of the application.

session: A session comprises the interactions between your PC and a remote host   beginning with the initial connection and ending when you or the host explicitly disconnect.

Some OnNet applications allow you to configure sessions, that is, automatically send parameters such as your username and password to the remote host..

session definition: The configuration settings for a particular session or host connection. A session definition might include such settings as the hostname of a computer on the network and your login name for that computer, as well as other values that you specify. The set of session parameters you can specify differs with each program.

TCP (Transmission Control Protocol): A Transport layer, connection-oriented, end-to-end protocol that provides reliable, sequenced, and nonduplicated delivery of bytes to a remote or a local user. TCP provides reliable byte stream communication between pairs of processes in hosts attached to interconnected networks.

time out: A period of time when a connection between a PC and a host computer is allowed to be idle or unused, or when a PC can attempt to make a connection to a networked host..

When the time period elapses, the host closes the idle connection, or the PC reports that it failed to connect to a host.

UDP (User Datagram Protocol): A Transport layer, connection-less mode protocol providing a (potentially unreliable, unsequenced, and/or duplicated) datagram communication for delivery of packets to a remote or a local user. UDP provides a procedure for a process to send messages to other processes with a minimum of protocol mechanism.

username: A name required for login to a remote system.

wildcard: A character such as * or ? that represents one or more characters in a filename. In a network, each operating system supports

its own wildcard characters and syntax. When you use wildcards on a remote host, follow the conventions that apply to that host.

Displays or hides additional elements of this dialog box.

Returns to the previous dialog box.

Displays the Open dialog box so that you can search for a specific file.

Cancels your selection(s) and close the dialog box without taking any action.

Closes the dialog box.

Exits the application.

Displays Help about the contents of this dialog box.

Does not proceed as indicated.

Proceeds to the next dialog box.

Confirms your selection(s) and close the dialog box.

Opens the Options dialog box.

Enter a word or string of characters to log in to another system, workgroup, or domain on a network.

Protects the contents of the file from modification.

Starts the operation.

Stops the operation.

Starts or stops the operation.

Enter the hostname or IP address of the remote host that you are trying to reach.

Enter the name that you use to log in to a computer on a network.

Proceeds as indicated.

Proceeds as indicated and avoids further prompts for confirmation.

Click this to set up options,

Saves all the changes you have made without closing the dialog box.

Context-sensitive help for this item is not yet implemented.

Help for this dialog box is not yet implemented.

Technical assistance

Users in the U.S. and Canada, and worldwide resellers   Contact FTP Software®:

    Telephone: **(800) 382-4387**
                      (508) 685-3600
    E-mail: **support@ftp.com**
    Fax: **(508) 794-4484**

 or

Users outside of the U.S. and Canada   Contact your local reseller.

Tip

For FREE online technical services, see:

    World Wide Web: **http://www.ftp.com**
    Anonymous Ftp Server: **ftp.ftp.com**
    Bulletin Board System: **(508) 684-6240** (settings   8,N,1)
    CompuServe: **GO FTPSOFT** (PCVENJ Section 8)