

# XFTP 6 User Guide

A Powerful SFTP/FTP File Transfer Program

*NetSarang Computer Inc.*

Copyright © 2018 NetSarang Computer, Inc. All rights reserved.

## Xftp™ Manual

This software and various documents have been produced by NetSarang Computer, Inc. and are protected by the Copyright Act. Consent from the copyright holder must be obtained when duplicating, distributing or citing all or part of this software and related data.

This software and manual are subject to change without prior notice for product functions improvement.

Xlpd™ and Xftp™ are trademarks of NetSarang Computer, Inc. Xmanager® and Xshell® are registered trademarks of NetSarang Computer, Inc. Microsoft Windows® is a registered trademark of Microsoft®. UNIX® is a registered trademark of AT&T Bell Laboratories. SSH® is a registered trademark of SSH Communications Security. Secure Shell is a trademark of SSH Communications Security.

This software includes software products developed through the OpenSSL Project and used in OpenSSL Toolkit.

NetSarang Computer, Inc.

4701 Patrick Henry Dr. BLDG 22 Suite 137 Santa Clara, CA 95054

<http://www.netsarang.com/>

# Contents

<b>About Xftp .....</b>	<b>3</b>
Key Functions .....	4
Recommendations .....	5
Install and Uninstall .....	5
<b>Start .....</b>	<b>7</b>
Create Session .....	7
Connect to Remote Host with SFTP .....	8
Connect to Remote Host with FTP .....	9
Transfer File .....	10
Move Tab to another Tab Group .....	11
Exit Xftp .....	11
<b>Session Management .....</b>	<b>12</b>
Session Management .....	12
Session Properties .....	13
General Tab .....	13
SFTP Advanced Options Dialog Box .....	16
Export .....	16
Import .....	17
<b>Connection .....</b>	<b>19</b>
Connection without Session files .....	19
Quick Connect Bar .....	20
Connection with Session files .....	20
Disconnect and Reconnect .....	21
Connection in Passive Mode .....	21
Connection in Active Mode .....	22
Connection with Kerberos .....	22
Connection with PKCS#11 .....	23
Set Startup Folder .....	23
<b>Security .....</b>	<b>25</b>
Public Key User Authentication .....	25
User Keys Dialog Box .....	26
Master Password .....	28
<b>File Transfer .....</b>	<b>31</b>
Download .....	31
Upload .....	32
Synchronize Folder .....	33
Synchronization Options .....	33
Synchronize Options Dialog Box .....	34
Transfer Queue Management .....	34

Set Transfer Types .....	35
Set File Transfer Options .....	36
Resume File Download and Upload .....	37
<b>File Management.....</b>	<b>39</b>
<b>Session Log.....</b>	<b>41</b>
<b>Window Management.....</b>	<b>43</b>

# About Xftp

**Xftp** is a powerful SFTP and FTP file transfer program operating on the Windows platform. Windows users can transfer files securely and conveniently with UNIX/Linux hosts using **Xftp**. SFTP (Secure Shell File Transfer Protocol) supports encryption and user authentication for secure Internet connections and can replace conventional file transfer protocols, such as FTP.

# Key Functions

## General

- Supports SFTP (SSH2 only) and FTP protocol
- Supports Windows 7/8/10, Windows Server 2008, 2012, 2016
- Supports virtual environments
- Supports OpenSSH, ssh.com server and SSH servers that follow SFTP protocol standards
- Multi-user setting
- Keep alive option
- UTF-8 character strings
- Diverse proxy servers
- Supports FXP for direct transfer between servers
- Support for Kerberos(MIT Kerberos, Microsoft SSPI)

## Session Management

- Creates and manages session files for different hosts
- Open session using the Sessions dialog box, quick connect bar, session shortcuts, and links bar
- Provides default session for quick connect
- Supports URL commands in quick connect bar and connections to remote host without opening a saved session
- Shows folders and trees in Sessions dialog box
- Automatically connect to the session which was open at program exit

## Security

- RSA/DSA/ECDSA/ED25519 public key, password and keyboard interactive user authentication
- RSA/DSA/ECDSA/ED25519 new user key wizard and import/export key
- Supports SSH PKCS#11
- AES128/192/256, 3DES, BLOWFISH, CAST128, ARCFOUR and RIJNDAEL encryption algorithms
- SHA1, SHA1-96, MD5, MD5-96 and RIPEMD160 MAC algorithms
- zlib compression
- Host keys dialog box
- User keys dialog box
- User defined master password for additional session security

## Appearance

- Dockable UI for the main window
- Theme selection feature
- Simple and powerful user interface
- Multiple tabs, multiple tab group

- Customizable Standard Buttons on toolbar

### **File Transfer**

- Transfers files simultaneously
- Resumes downloading
- Pause transfer
- Resume for failed transfers
- Shows transferred folder in tree view
- Shows graphical transfer status
- Supports folder synchronization between remote and local folders

### **File Management**

- Direct editing and automatic transfers of remote files 전송
- Edit remote files using a user defined editor
- Manages several local folders
- Deletes and renames files
- Creates new folders
- Executes files
- Changes permissions

### **Interoperability**

- Interoperable with Windows Explorer
- Interoperable with Xshell® program
- Interoperable with Xagent program

## **Recommendations**

- **Operating System:** Microsoft Windows® XP SP3 or higher
- **Storage Space:** Reserve space of 50MB or more
- **Network:** TCP/IP network

## **Install and Uninstall**

The **Xftp** installation program was created using InstallShield®. A variety of installation options can be changed in the course of installation. It is sufficient in most cases to simply click [Next].

To uninstall **Xftp**, use standard Windows add/remove features. Run [Add/Remove Program] and select in the control panel to uninstall **Xftp** from the list.

Even when the program is uninstalled, the registry information, log files and user created data files are not removed. Such information and files are available for reuse when the program is reinstalled. If you want to remove all the files and registry information completely, remove the following explicitly:

### **Registry Information:**

- \HKEY\_CURRENT\_USER\Software\NetSarang\Xftp

**File and Folder:**

- 'User's Documents Folder' \Netsarang Computer\6\Xftp

# Start

This section provides directions for creating an SFTP or an FTP session and exchanging files by connecting with a UNIX/Linux host. The FTP session is very simple. The SFTP session however, occasionally requires user key registration in the server before connecting. If a user key registration is necessary, see 'Public Key User Authentication'.

## Create Session

1. Select [New] in the [File] menu. The **New Session Properties** dialog box is displayed.

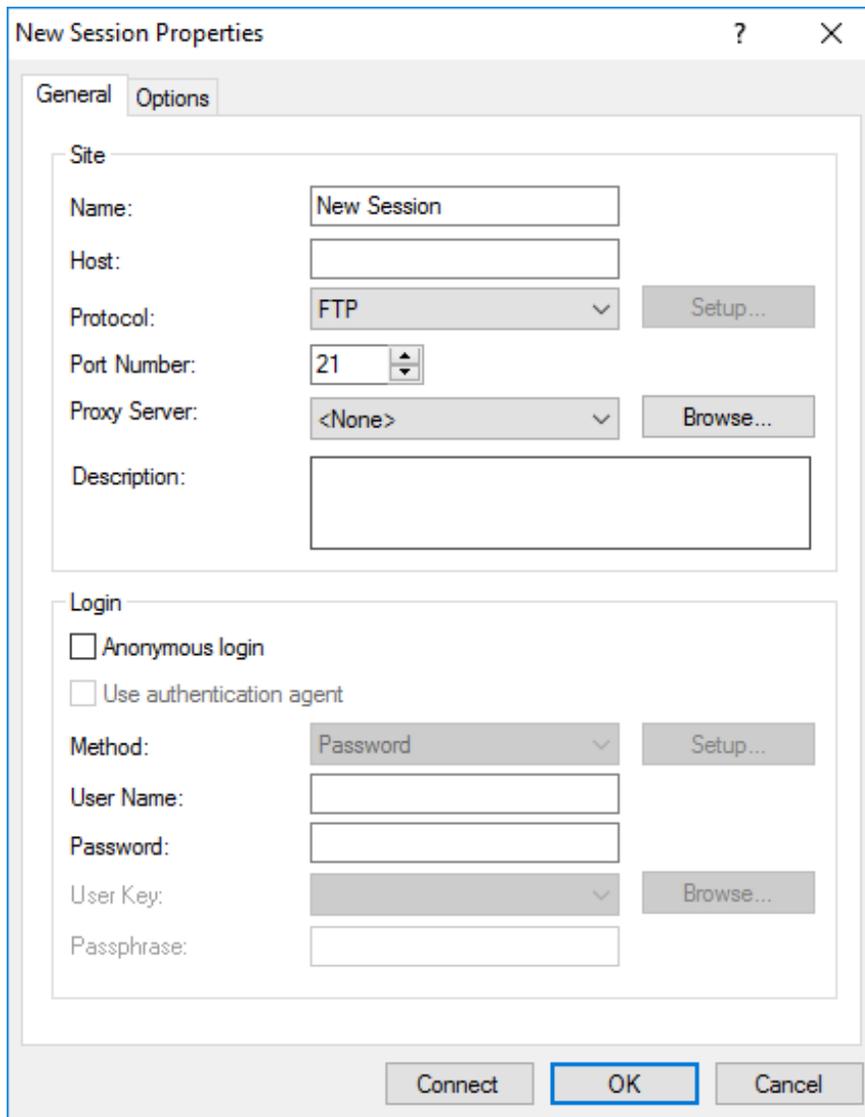


Fig. 1: New Session Properties dialog box

2. Enter session name in the [Name].
3. Enter host name or IP address in the [Host].
4. Select an appropriate protocol from the [Protocol] list.
5. Enter port number used by the remote server in the [Port Number].
6. Enter the user account of the server in the [User Name].
7. Click [OK].

## Connect to Remote Host with SFTP

When an SFTP session has been created, a connection can be made with a remote host using the SFTP protocol. If there are no sessions created, see 'Create Session' first.

1. Select [Open] in the [File] menu. Sessions dialog box is displayed.
2. Select a session for connection and click [Connect]. The **SSH User Authentication** dialog box is displayed.

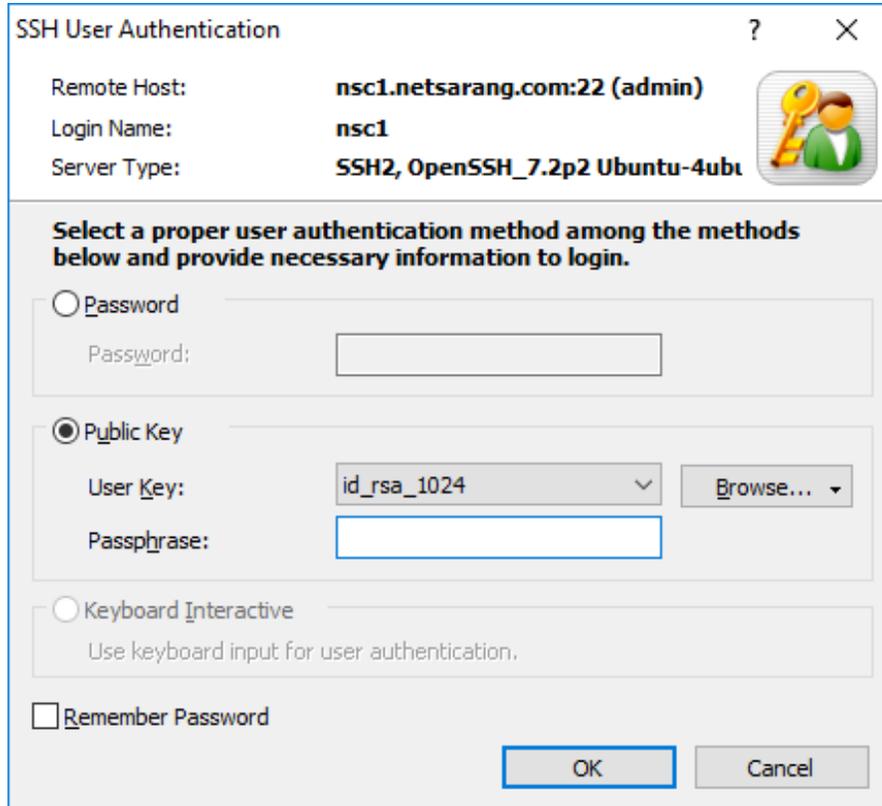


Fig. 2: SSH User Authentication dialog box

3. For *Password* authentication, enter a password in the [Password] box and click [OK].
4. For *Public Key* authentication, first select a user key from the list. Enter the passphrase for the selected user key in the [Passphrase] box and click [OK].

**Note**

If a user key is not available, see 'Public Key User Authentication'.

5. For *Keyboard Interactive* authentication, click [OK] and answer the questions given during the connection process.

## Connect to Remote Host with FTP

When an FTP session has been created, a connection can be made with a remote host using the FTP protocol. If there are no sessions created, see 'Create Session' first.

1. Select [Open] in the [File] menu. **Sessions** dialog box is displayed.
2. Select a session for connection and click [Connect]. The **FTP User Authentication** dialog box

is displayed.

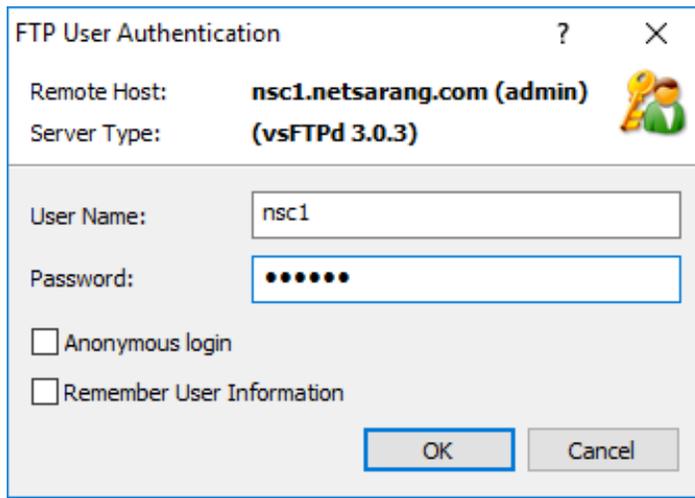


Fig. 3: FTP User Authentication dialog box

3. Enter user name in the [User Name] box, enter password and click [OK].

## Transfer File

### Transfer Files from Remote Server to Local PC

1. Select files to download from the remote folder window.
2. Drag the selected files to the local folder window.

### Transfer Files from Local PC to Remote Server

1. Select files to upload from the local folder window.
2. Drag the selected files to the remote folder window.

### Transfer Files between Local Folders

1. Select files to transfer from the local folder window.
2. Drag the selected files to the local folder window of another tab group.

### Transfer Files between Remote Folders

1. Select files to transfer from the remote folder window.
2. Drag the selected files to the remote folder window of another tab group.

#### Note

Users can also transfer files by clicking the left or right arrow buttons in the standard buttons toolbar.

## Move Tab to another Tab Group

1. If there is only one tab group, create a new tab group via the method shown in step 2 below.
2. To create a new tab group, drag a tab towards the right border of a tab group.  
A guideline is displayed at the position to which a tab is to be moved. When the tab is dropped over the guideline, a new tab group is created, which includes the selected tab.

 **Note**

You can create a new tab group by selecting [New Vertical Tab Group] in the [Window] menu.

3. If there are two or more tab groups, a tab can freely moved between tab groups by dragging and dropping the tab to the desired tab group.

## Exit Xftp

To close the tab, click its Close button or click [Close] in the [File] menu.

To end **Xftp**, select [Exit] in the [File] menu.

# Session Management

A 'session' is a file containing information about the remote host connection setup. By creating a session, a user can set different options for different remote hosts. The **Sessions** dialog box shows all sessions created and enables the creation and editing of sessions.

A user can also connect to a remote computer without creating a session. For this purpose, Xftp provides a default session which can be used concurrently with installation.

## Session Management

### To Create a New Session:

1. Open the **New Session Properties** dialog box.
2. Enter connection information.
3. Click [OK].

### To Open the Sessions Dialog Box:

- Select [Open] in the [File] menu.
- Click the standard [Open] button.

### To Edit a Session:

1. Open the **Sessions** dialog box.
2. Select a session to edit.
3. Click the standard [Properties] button.
4. Click [OK] after completing session editing.

### To Rename a Session:

1. Open the **Sessions** dialog box.
2. Right-click on a session to rename.
3. Select [Rename] in the menu.

#### Note

A session name must be a valid file name.

### To Copy a Session under a Different Name:

1. Open the **Sessions** dialog box.
2. Select a session to copy under a different name.
3. Click the standard [Save As] button.

### To Delete a Session:

1. Open the **Sessions** dialog box.
2. Select a session to delete.
3. Click the standard [Delete] button.

#### To Create a Shortcut to a Session:

1. Open the **Sessions** dialog box.
2. Select a session for which the shortcut will be created.
3. Click the standard [Create Shortcut] button.
4. Select a folder in which to save the shortcut.
5. Click [OK].

#### To Change Default Session Properties:

1. Move to the local folder tab or close all remote folder windows.
2. Select [Properties] in the [File] menu. The default Session Properties dialog box is displayed.

#### Note

Default session properties are used when connecting with SFTP and FTP via the quick connect bar.

#### To Create a New Session Folder:

1. Open the **Sessions** dialog box.
2. Select [Folder] from the list displayed when the arrow button next to the standard [New] button is clicked.
3. Enter folder name.

#### To Copy a Session File to Another Computer:

1. Open the **Sessions** dialog box.
2. Click the standard [Open Session Folder] button.
3. Copy the session file (\*.xfp) or e-mail it to another computer.
4. Save session file in the following folder:  
"%APPDATA%\NetSarang\Xftp\Sessions"

## Session Properties

Open a **Session Properties** dialog box to edit a session or create a new session .

#### To Open Session Properties dialog box:

- Select [New] in the [File] menu.
- Select [Properties] in the [File] menu.
- Click the standard [Properties] button.

## General Tab

Information about session connections can be set up under the general tab. In most cases, users can connect with a remote host just by setting information about the session connection.

#### Name

Enter a name unique to this session. The name becomes the name of the session file. It must be composed of characters valid for use in a file name.

**Host**

Enter the remote computer host name or IP address.

**Protocol**

Select a protocol to use when connecting to the remote computer. Supported protocols are SFTP and FTP.

**Setup**

Set detailed options when using the SFTP protocol. For detailed information, see 'SFTP Advanced Options Dialog Box.

**Port Number**

Enter the port number of the protocol selected above. When a protocol is selected from the list of protocols, the default protocol port number is automatically entered. If the remote computer is using another port number, the user must directly enter the port number. The defaults are 22 for SFTP and 21 for FTP.

**Proxy Server**

Select a proxy server to use in the connection.

**Anonymous Login**

Login as an anonymous user. This function is available only in the FTP protocol.

**Use Authentication Agent**

Authentication is attempted with **Xagent** for SFTP connections. **Xagent** is an SSH authentication agent. **Xagent** stores user keys used for public key user authentication and passes them to **Xftp** when requested.

**Method**

Select a method to authenticate users on the remote computer.

**User Name**

Enter the user login name. This name is the remote computer login account. If this is left blank, a dialog box requesting a user name appears during each connection.

**Password**

Enter the remote computer user password to use during connection. The password is encoded and saved in the user's PC. Keep this section blank for greater security. If this section is left blank, a dialog box requesting user authentication appears during each connection.

**User Key**

Select a user key to be used when public key authentication is selected in the SFTP protocol. If this section is left blank, a dialog box requesting user authentication appears during each connection. If there are no user keys in the list, a key must be created first and be registered in the remote SSH server.

**Passphrase**

Enter the selected user key passphrase. The entered key passphrase is encoded and saved in the user's PC. Keep this section blank for greater security.

## Options Tab

Under the options tab, detailed session options can be set. In most cases, users are not required to set options.

### **Host Type**

Select the type of remote computer operating system. Select [Auto Detect] if the remote computer type is unknown.

### **Use UTF-8 Encoding**

Communicate with a remote computer using UTF-8 character strings. This option must be selected when the remote computer uses UTF-8 character strings and the remote computer files hold character strings encoded in UTF-8.

### **Send Keep Alive Messages**

Send keep alive messages to the remote computer. This function is useful when a connection is unexpectedly closed while the connection is idle. In some network environments, the gateway or firewall system forces a disconnection if data transfer is not made for a defined period of time.

### **Auto-refresh remote folder listing**

Automatically refreshes the remote folder list after the user defined period of time (minutes).

### **Use Passive Mode**

Connect with the remote computer in passive mode for file transfers. For details, see 'Connection in Passive Mode'. This option is not necessary when an SFTP connection is selected.

### **Transfer Type**

Designate the type of file transfer in this session. For details, See 'Set Transfer Types'.

### **Multiple Transfer**

Designate the number of files to be transferred simultaneously. To use this function, the server must support a multiple connection.

### **Use Main Connection Only**

Use this option when the server allows for only a single connection. Since the main connection is used for file transfers, files can be transferred one by one. During file transfers, functions such as file list refreshing cannot be used. This option is not necessary when an SFTP connection is selected.

### **Local Folder**

Designate a folder to be displayed in the local folder window when a connection succeeds.

### **Remote Folder**

Designate a folder to be displayed in the remote folder window when a connection succeeds.

## SFTP Advanced Options Dialog Box

Set the various options necessary for connections using the SFTP protocol in the **SFTP Advanced Options** dialog box. Select the SFTP protocol in the [General] tab of **Session Properties** and click [Setup] to open.

### Encryption

Encryption algorithms are used to encrypt and decrypt network traffic. Users may select the preferred encryption algorithm from the list. If *<Cipher List>* is selected from the list, multiple algorithms are attempted in the order appearing in the list. To edit the list of *<Cipher List>*, click [Edit].

### MAC (Message Authentication Code)

MAC is added in SSH2 for greater security and to ensure data integrity. If *<MAC List>* is selected from the list, multiple algorithms are attempted in the order appearing in the list. To edit the list of *<MAC List>*, click [Edit].

### Key Exchange

Users can select the initial Key Exchange for the SSH connection. The desired algorithm can be selected from the list. If the server does not support the selected algorithm, the connection will fail.

### Use ZLIB Compression

If the network speed is slow, increase speed using ZLIB compression.

### SFTP Server: User custom SFTP server

SFTP is a subsystem of the SSH protocol. If the connection will not utilize the SSH protocol's default SFTP system, enter the path of the SFTP server program to use. This can be used when acquiring another user's rights after a connection has been made.

## Export

Sessions exported from **Xftp** are made into a single convenient file. When this file is imported by another computer with **Xftp** installed, the imported sessions can be used without additional setup.

### To Export a Session:

1. Select [Export] from the [File] menu. The **Import/Export Sessions** wizard is displayed.

#### Note

If 'Clear Password' is selected, the exported session file will not include the session password during the export. Also, even if 'Clear Password' is not selected, the password will only be available if imported into the same computer under the same user. To use the session with the session password on another device you must first set a Master Password on the computer from which the session file is being exported and the same exact Master Password must be set on the computer into which the session file is to be imported.

2. Select the path where the exported file is to be saved and click [Next]. The session export results are displayed.

3. Click [Finish] to end session export.

## Import

**Xftp** can import session files from another computer.

### To Import a Session:

1. Select [Import] in the [File] menu. The **Import/Export Sessions** wizard is displayed.
2. Directly enter the file path exported from other computer or click the [...] button to select the exported file and click [Next]. Sessions are imported and the result is displayed.
3. Select how to handle sessions with the same file names.
4. Click [Next] to select the types of sessions to import
5. Click [Finish] to end session import.



# Connection

**Xftp** provides various ways to connect to sessions, such as the **Sessions** dialog box, links bar, quick connect bar, and session shortcuts.

## Connection without Session files

### To Connect at the Quick Connect Bar:

1. Select the [Quick Connect Bar] in the [View] - [Toolbars] menu.
2. Enter the host name or IP address in addition to the protocol into the quick connect bar as follows:
  - ftp://hostname
  - sftp://hostname
  - Host Name or IP address

#### **Note**

If a protocol is not entered, the protocol defined in the default session properties is used.

3. Enter user name and password. If this process is omitted, an authentication window is displayed according to the authentication method selected in the default session properties.
4. Type Enter or click [Connect].

#### **Note**

For details on the quick connect bar, see 'Quick Connect Bar'.

## Quick Connect Bar

The quick connect bar allows users to connect to a server quickly using only minimal information, without using a session file.

### Host Name or IP Address

Enter the remote computer host name or IP address. Use the following format:

```
[protocol://][user:password@]host name[:port][/][path]
```

The available protocols are *sftp* and *ftp*. The default protocol is the one defined by the user in the default session properties. The default port number for each protocol is:

- *sftp*: 22
- *ftp*: 21

Examples are listed below.

Example	Description
foobar.com	Connect to foobar.com via the protocol and a port number defined in the default session properties.
sftp://kay@foobar.com/	Connect to foobar.com via the SFTP protocol. User account is kay and the default port number is used.
sftp://kay@foobar.com:12345/	Connect to port 12345 of foobar.com with the SFTP protocol. User account is kay.
ftp://foobar.com/	Connect to foobar.com via the FTP protocol. User account is not designated and the default connection port is port 21.

### Note

**Xshell** is executed when SSH and TELNET protocols are entered. The **Xshell** program must be installed on the user's PC.

### User Name

Enter the user name for login. The user name is the login account of the remote computer. If this section is left blank, a dialog box requesting a user name appears during connection.

### Password

Enter the remote computer user name password. If this section is left blank, a dialog box requesting user authentication appears during connection.

## Connection with Session files

If a remote host is connected to frequently, users can create session files for easy access in the future. Users can connect to remote hosts via saved session files in multiple ways.

### To Connect from the Sessions Dialog Box:

1. Open the **Sessions** dialog box.

2. Select a session file for connection.
3. Click [Connect].

**To Connect with a Shortcut:**

1. Double-click the shortcut icon of a session file.

## Disconnect and Reconnect

It is possible to disconnect or reconnect at any time without closing the remote folder window. During reconnection, user authentication information used in the previous connection is reused and therefore the user authentication process is not required.

**To Disconnect:**

1. Click the standard [Disconnect] button.

**To Reconnect:**

1. Click the standard [Reconnect] button.

 **Note**

To utilize reconnection, the remote folder window must not be closed.

## Connection in Passive Mode

For FTP connections, connections in passive mode is available. In passive mode, the remote FTP server waits for **Xftp** to establish the data connection. Select passive mode to use **Xftp** inside a firewall.

**For Connection in Passive Mode Using a Session File:**

1. Open the **Sessions** dialog box.
2. Select a session for connection.
3. Click the standard [Properties] button.
4. Click the [Options] tab in the **Session Properties** dialog box.
5. Select [Use Passive mode].
6. Click [OK].
7. Connect with the session file.

**For Connection in Passive Mode Using the Quick Connect Bar:**

1. Move to the local folder tab or close all remote folder windows.
2. Select one of the following methods:
  - Select [Properties] in the [File] menu.
  - Click the standard [Properties] button.
3. Click the [Options] tab in the default **Session Properties** dialog box.
4. Select [Use Passive mode].
5. Click [OK].
6. Connect from the quick connect bar.

## Connection in Active Mode

For FTP connection, connection in active mode is available. When a file is transferred in active mode, **Xftp** waits for the FTP server to establish the data connection. Transfer may fail if active mode is selected when using **Xftp** inside a firewall.

### For Connection in Active Mode Using a Session:

1. Open the **Sessions** dialog box.
2. Select a session for connection.
3. Click the standard [Properties] button.
4. Click the [Options] tab in a **Session Properties** dialog box.
5. Clear [Use Passive mode].
6. Click [OK].
7. Connect with session.

### For Connection in Active Mode Using the Quick Connect Bar:

1. Move to local folder tab or close all remote folder windows.
2. Select one of the following methods:
  - Select [Properties] in the [File] menu.
  - Click the standard [Properties] button.
3. Click the [Options] tab in the default **Session Properties** dialog box.
4. Clear [Use Passive mode].
5. Click [OK].
6. Connect from quick connect bar.

## Connection with Kerberos

Xftp 6 supports MIT GSSAPI Kerberos and Microsoft's SSPI Kerberos authentication. This article assumes that you have a working Kerberos server and client.

### To create a new Kerberos session

1. Select [New] from the [File] menu
2. Enter a session name in [Name].
3. Select SFTP from the [Protocols] list.
4. Select **GSSAPI** from the [Method] list in the Login section.

#### **Note**

If the PC running Xftp is utilizing an Xftp supported Kerberos module, Xftp can only automatically authenticate to the SFTP server if GSSAPI authentication is selected.

5. To change the GSSAPI settings, click the [Setup] button to open the 'Setup GSSAPI' dialog box.

#### **Note**

To connect to another server using Kerberos authentication from a server using Kerberos

authentication, select the 'Allow GSSAPI credential delegation' option.

6. Click [OK] to save the GSSAPI settings .
7. Enter the user name.
8. Click [OK] to save the session file.
9. Click [Connect] to connect immediately or select the session file from the Sessions Dialog Box to connect.

You have finished creating a session that will use the Kerberos module. When this session opens, it will try to use the Kerberos credential for the specified user. It has to be the same user you defined in the Network Identity Manager.

## Connection with PKCS#11

PKCS #11 is one of the public key cryptography standards. Xftp 6 can connect to a remote SFTP server using a PKCS #11 encrypted hardware security token (HSM) or a smart card's RSA key.

To create a new PKCS#11 session:

1. Select [New] from the [File] menu.
2. Enter a session name in [Name].
3. Select SFTP from the [Protocols] list.
4. Select **PKCS11** from the [Method] list in the Login section.
5. Click the [Setup] button to open the 'Setup PKCS11' dialog box.
6. Enter the path of the middleware program that can connect to the hardware token that contains the user key. Or click [...] to browse for it.
7. If the pin number is set in the hardware token, enter the pin number. Enter the user name.
8. Click [OK] to save the session file .
9. Click [Connect] to connect immediately or select the session file from the Sessions Dialog Box to connect.

## Set Startup Folder

Users can set remote and local folders for Xftp 6 to automatically navigate to once a connection is established. Users may find it convenient to set a frequently used folder to save time.

**To Set Local Startup Folder:**

1. Open the **Sessions** dialog box.
2. Select a session.
3. Click the standard [Properties] button.
4. Click the [Options] tab in a **Session Properties** dialog box.
5. Select one of the following methods:
  - Enter the startup folder in the [Local Folder].
  - Click [...] and select a folder from the **Browse For Folder** dialog box.
6. Click [OK].

**To Set Remote Startup Folder:**

1. Open the **Sessions** dialog box.
2. Select a session.
3. Click the standard [Properties] button.
4. Click the [Options] tab from the **Session Properties** dialog box.
5. Enter the startup folder in the [Remote Folder].
6. Click [OK].

# Security

**Xftp** supports public key user authentication.

Host keys and user key databases created in **Xftp** can be used in **Xmanager** and **Xshell** programs. Once a public key is created, it can be used in all programs without additional configuration.

## Public Key User Authentication

For public key user authentication, a pair of user keys must be created comprised of a public key and a private key. While public key authentication is carried out, the private key is used by **Xftp** to create a user signature and the public key is used by SSH server to check the signature.

A user key can be created in either the SSH server or **Xftp**. If the user key was created from the server, the private key must be registered in the **Xftp** private key repository using the **Xftp** import function. If the user key was created from **Xftp**, the public key must be registered in the server.

### To Create a User Key:

1. Select [New User Key Wizard] from the [Tools] menu.
2. Create a user key according to instructions given by the **New User Key Wizard**.

#### Note

Register a public key in a server at the last stage of key creation. Registration methods vary depending on server types.

- *SSH1*: Copy the public key text and save it to `$HOME/.SSH/authorized_keys` file. Execute the following command to turn off the write permission of the files and directories.  

```
$ cd  
$ chmod go-w . .ssh .ssh/authorized_keys
```
- *SSH2-OpenSSH*: OpenSSH servers use this format. Copy the public key text and save it to `$HOME/.SSH/authorized_keys2` file. Execute the following command to turn off the write permission of the files and directories.  

```
$ cd  
$ chmod go-w . .ssh .ssh/authorized_keys2
```
- *SSH2-IETF SECSH*: Some commercial SSH servers, such as the ssh.com server, use this format. Save the public key under an intrinsic name, such as `mypublickey.pub`, and copy it to `$HOME/.ssh2` directory. Add the following line to the `$HOME/.ssh2/authorization` file:  

```
Key mypublickey.pub
```

Execute the following command to turn off the write permission of the files and directories.  

```
$ cd  
$ chmod go-w . .ssh2  
$ chmod go-w .ssh2/authorization .ssh2/mypublickey.pub
```

### To Register a Public Key in a Server:

1. Select [User Key Manager] from the [Tools] menu and the **User Keys** dialog box is displayed.
2. Select a user key to register.
3. Click [Properties]. The **User Key Properties** dialog box is displayed.
4. Click the [Public Key] tab.
5. Select an appropriate type from the [Public Key Format] list.
6. Save user key by clicking [Save as a file] or copy the key and register it to the server according to public key registration methods above.

### To Change the User Key Passphrase:

1. Open the **User Keys** dialog box.
2. Select a user key for which to change the passphrase.
3. Click [Properties]. The **User Key Properties** dialog box is displayed.
4. Click the [General] tab.
5. Click [Change Passphrase].

#### **Note**

Import, export, rename, delete, and create a user key in the 'User Keys Dialog Box'.

## User Keys Dialog Box

The **User Keys** dialog box enables the creation and management of user keys. Open the **User Keys** dialog box by selecting [User Key Manager] from the [Tools] menu.

### Import

Select and import user key files by opening the **Open** dialog box. Currently, **Xftp** can read SSH1 protocol RSA keys, OpenSSH SSH2 protocol RSA/DSA keys, SSH.com keys, and NetSarang user keys.

### Export

Save the selected user key file by opening the **Save** dialog box. Exported file types are NetSarang user keys or the OpenSSH SSH2 format. NetSarang Computer user key format files (\*.pri) can be used in programs developed by NetSarang Computer, Inc.

### Delete

Delete the selected user key from the database.

### Rename

Rename a selected user key. Key name must be valid as file name.

### Properties

Show user key attributes. Type, length, fingerprint, and public key may be viewed, and the key passphrase may be changed.

### Generate

Open the **New User Key Wizard**.

# Host Key Management

A host key is a remote host public key, and users can verify the host via its fingerprint. The remote host sends its own public key to **Xftp** when a connection is made. For cases where a host is connected to for the first time or where the host key is not saved in the database, a **SSH Security Warning** dialog box is displayed. If the host key is valid and reliable, it can be saved in the host key database.

## SSH Security Warning Dialog Box

The **SSH Security Warning** dialog box is displayed when the remote host key is not saved in the host key database or when the fingerprints of the saved host key differs from the remote host key.

### Accept Once

Accept a host key for this connection only. The host key is not saved and the same dialog box is displayed at the next connection. This is useful when a server host key changes often or the user rarely connects to the server.

### Accept and Save

Save host key and process the connection. This dialog box does not open on the next connection. This is useful when the fingerprint is correct and the user connects to the host frequently.

### Cancel

Host key is not accepted and connection is cancelled.

## Host Keys Dialog Box

The **Host Keys** dialog box permits users to manage host keys of remote hosts to which connectoin is allowed. The **Host Keys** dialog box can be opened by selecting [Host Key Manager] in the [Tools] menu.

### Import

Import host keys by opening the **Open** dialog box. Imported host keys are saved in the host key database and displayed in the **Host Keys** dialog box. Files saved as SECSH public keys can be imported.

### Export

Export the selected host key by opening the **Save** dialog box. The exported keys are saved as SECSH public keys and can be used in other programs.

### Remove

Remove selected host key from the database.

### View

Open a selected host key file with notepad.

# Master Password

Master password can be used to save passwords more securely using the user defined master password. **Xftp** saves all password information in an encrypted format. However, since passwords are encrypted using a fixed key, it has a risk of being exploited by hackers. When the master password is enabled and set, it is mixed in during password encryption adding an additional layer of security.

Master password uses a user defined keyword to encrypt the password section of the session data. When the master password is enabled, Xftp asks for the master password every time a new Xftp instance is started and a session is open. If the correct master password is not inputted, the session's password is not able to be utilized and must be entered again manually preventing unauthorized access.

## Note

Be sure to remember your master password. If you lose your master password, there is no way to retrieve the password information stored in the session files. Master Password settings are applied simultaneously to Xmanager, Xshell, and Xftp sessions.

### To Enable Master Password:

1. Click on the **Tools** menu and then select **Set Master Password**.
2. In the **Master Password** dialog box, enter a new master password in the **New Password** field.
3. In the **Confirm Password** field, enter the new password again.
4. Click **OK** to save the changes.

Once master password is enabled, all sessions saved in the default location are re-encrypted using the new master password.

### To Change Master Password:

1. Click on the **Tools** menu and then select **Set Master Password**.
2. In the Change area click **Change** to open the Master Password Change dialog box..
3. Enter the current master password in the **Current Password** field.
4. Enter the new master password in the **New Password** field.
5. Enter the new password one more time in the **Confirm Password** field.
6. Click **OK** to save the changes.

### To Disable Master Password:

1. Click on the **Tools** menu and then select **Set Master Password**.
2. Click the **Remove** button to open the Remove Master Password dialog box.
3. In the Remove Master Password dialog box, enter the master password and click **OK**.

### To Reset the Master Password:

1. Click on the **Tools** menu and then select **Set Master Password**.
2. Click the **Reset** button to open the Reset Master Password dialog box.

3. In the Reset Master Password dialog box, click **Reset Master Password** and click **OK**.

 **Note**

Reset of the master password can be used if you forgot your master password or if you would like to clear all the passwords stored in your sessions.



# File Transfer

**Xftp** provides various transfer methods. User can transfer using the left/right buttons, drag & drop, and copy & paste. For redundant files, Xftp provides overwriting and continued downloading as well as renaming and skipping functions. In addition, **Xftp can** transfer several files simultaneously to increase overall transfer speed. For folder unit transfers, **folder lists can be displayed in a tree** so users can easily check the transfer status.

## Download

### To Download Using the Menu:

1. Select a file to download from the remote folder window.
2. Use one of the following methods:
  - Select [Transfer to Left] or [Transfer to Right] from the [Commands] menu.
  - Right-click on the remote folder window and select [Transfer].
  - Click the standard [Transfer to Left] or [Transfer to Right] buttons.

### To Download Using Drag & Drop:

1. Select a file to download from the remote folder window.
2. Drag the selected file and drop it in the local folder window.

#### Note

User can also drag files from the remote folder window and drop them directly into the desktop or Windows Explorer.

### To Download Using Copy & Paste:

1. Select a file to download from the remote folder window.
2. Use one of the following methods:
  - Select [Copy] from the [Edit] menu.
  - Right-click on the remote folder window and select [Copy].
3. Click the local folder window.
4. Use one of the following methods:
  - Select [Paste] from the [Edit] menu.
  - Right-click on the local folder window and select [Paste].

### To Download After Creating a Transfer List:

1. Select a file to download from the remote folder window.
2. Right-click on the remote folder window and select [Queue].

### To Resume Paused File/Directory Download:

Select one of the following methods:

- Right-click on the paused transfer in the transfer queue pane, and then click [Resume].
- Right-click on the transfer queue pane and select [Resume All].

## Upload

### To Upload Using the Menu:

1. Select a file to upload from the local folder window.
2. Select one of the following methods:
  - Select [Transfer to Left] or [Transfer to Right] from the [Commands] menu.
  - Right-click on local folder window and select [Transfer].
  - Click the standard [Transfer to Left] or [Transfer to Right] button.

### To Upload Using Drag & Drop:

1. Select a file to upload from local folder window.
2. Drag the selected file and drop it in remote folder window.

#### Note

User can also drag files directly from the desktop or Windows Explorer and drop them into the remote folder window.

### To Upload Using Copy & Paste:

1. Select a file to upload from the local folder window.
2. Select one of the following methods:
  - Select [Copy] from the [Edit] menu.
  - Right-click on the local folder window and select [Copy].
  - Click the standard [Copy] button.
3. Click the remote folder window.
4. Select one of the following methods:
  - Select [Paste] from the [Edit] menu.
  - Right-click on the remote folder window and select [Paste].
  - Click the standard [Paste] button.

#### Note

Users can also copy a file from Windows Explorer and paste it into the remote folder window.

### To Upload After Creating a Transfer List:

1. Select a file to upload from the local folder window.
2. Right-click on the local folder window and select [Queue].

### To Resume Paused File/Directory Upload:

Select one of the following methods:

- Right-click on the paused transfer in the transfer queue pane, and then click [Resume].
- Right-click on the transfer queue pane and select [Resume All].

# Synchronize Folder

## To Synchronize the Local and Remote Folder:

1. Open the local and remote folders to synchronize.
2. Click the standard [Synchronize Folders] button. The **Synchronization** dialog box will open.
3. To change the synchronization target folders, select the folders in the [Left] and [Right] areas.
4. Select the desired [Synchronization Direction] and click [Compare]
5. Click [Transfer]. Synchronization starts as file upload/download is carried out.

### Note

Clicking [Queue] instead of [Transfer] will not start a file transfer immediately and instead, the file is added to the transfer list. Start synchronization by selecting either [Resume] or [Resume All] from the transfer queue.

## Synchronization Options

Options provided in the **Synchronization** dialog box.

### Synchronization Direction

Select one of the following: Synchronize (Both), Left to Right (Single), Right to Left (Single), Mirror (Left Base), Mirror (Right Base).

- Synchronize (Both): File transfers occur so that the contents of the synchronization target folders are the same.
- Left to Right (Single): Among the differing files after comparison, files in the left folder will be transferred to the right folder.
- Right to Left (Single): Among the differing files after comparison, files in the right folder will be transferred to the left folder.
- Mirror (Left Base): After comparing, the right folder will exactly mirror the left folder. Files only contained in the right folder will be deleted.
- Mirror (Right Base): After comparing, the left folder will exactly mirror the right folder. Files only contained in the left folder will be deleted.

### Filter Results

	Description
	Shows files or directories that cannot be synced. These may be files with the same name but different capitalizations, etc.
	Shows files or directories that cannot be transferred. This may be a folder with the same name, or (during a single direction sync) a file with the same name, etc.
	Shows files which will be deleted. During a Mirror sync, files to be deleted will be displayed.

	Description
	Shows the files which will be transferred to the left.
	Shows the files which will be transferred to the right.
	Shows identical files which exist in both the left and right folders.
	Shows differing files which exist in both the left and right folders. The file names are the same, but the size or dates are different.
Duplicates	Shows files with the same names that exist in both the left and right folders.
Single	Shows files that exist on only one side.

### Begin Transfer

Click the [Transfer] button to begin the transfer of the list of files and folders in the specified direction.

### Place in Queue

Click the [Queue] button to add the list of files and folders into the queue. The user can then initiate the transfer from Xftp's main transfer window at any time.

## Synchronize Options Dialog Box

Click the [More Options] button to access the **Synchronization Options** dialog box:

### Include Subdirectories

Select this option to do recursive synchronization to all subfolders.

### Synchronize empty folders

Select this option to have folders without files or subfolders to be synchronized to the destination folder

### If only one object is compared, compare case-insensitively

Remote folders may contain files which are different in their capitalization (ABC.text, abc.text). If this type of duplicate file does not exist in the destination folder, turning this option on determines that the local and target files have the same name (AbC.text = abc.text.).

### Comparing by Modified Time

Files with the same name are compared by time of file modification.

### Comparison by File Size

Files with the same name are compared by file size.

## Transfer Queue Management

The Transfer Queue shows file lists and displays the transfer status as Ready, Transferring, Paused, or Finished. It also shows the logs of all transfer processes.

**To Remove All Transfers:**

1. Right-click on the transfer queue and select [Remove All].

**To Remove Some Transfers:**

1. Select files or directories to remove from the transfer queue.
2. Right-click and select [Remove].

**To Delete Completed Transfers of Files or Directories:**

1. Right-click on the transfer queue and select [Remove Finished Jobs].

**To Pause All Transfers:**

1. Right-click on the transfer queue and select [Pause All].

**To Pause Some Transfers:**

1. Select the file or directory to pause transfer in the transfer queue.
2. Right-click and select [Pause].

**To Resume All Paused Transfers:**

1. Right-click on the transfer queue and select [Resume All].

**To Resume Some Paused Transfers:**

1. Select the file or directory to resume transfer in the transfer queue.
2. Right-click and select [Resume].

**To Retry Failed Transfer:**

1. Right-click on the transfer queue and select [Retry All Failed Jobs].

**To Check Transfer Status:**

1. Select the file or directory you want to check the status of in the transfer queue.
2. Right-click and select [Status]. The **Transfer Status** dialog box is displayed.

**Note**

The **Transfer Status** dialog box provides detailed information about transfers. A list of failed transfer files and the reasons for failure are displayed.

## Set Transfer Types

Methods to express text file line feed characters differ depending on the system. When transferring the text files, **Xftp** converts line feed characters to suit the remote computer type, enabling users to view the text files of different systems. For non-text files, the binary file transfer type must be used.

**To Transfer Text Files:**

1. Select [ASCII] from [Transfer Type] in the [Commands] menu.
2. Transfer text files.

### To Transfer Binary Files:

1. Select [Binary] from [Transfer Type] in the [Commands] menu.
2. Transfer binary files.

### To Transfer Files via the Automatic Transfer Type:

1. Select [Auto] from [Transfer Type] in the [Commands] menu.
2. Click [ASCII Extensions] in the [Transfer] tab of **Options** dialog box.
3. Register the file extension to be transferred via ASCII transfer type in the **ASCII Extensions** dialog box.
4. Transfer files.

## Set File Transfer Options

**Xftp** offers overwriting, resumption, renaming, and skipping functions for redundant files during file transfers. **Xftp** also provides automatic retry options for failed transfers.

#### Note

This setting is made in [Transfer Options] field in the [Transfer] tab of the **Options** dialog box and therefore applies to all sessions.

### To Select a Transfer Operation for Redundant Files:

1. Open the **Options** dialog box.
2. Click the [Transfer] tab.
3. Click [Advanced Options] in the [Transfer Options] field.
4. Select a redundant file operation from the download options in the [Overwrite File] field.

#### Note

Options for redundant files are as follows:

- *Prompt For Action*: Opens the **Confirm File Transfer Actions** dialog box.
- *Skip*: Do not transfer file.
- *Resume*: Resumes downloading an existing file from where it was left off. Overwrites the file if the existing file is larger than the file to be transferred.
- *Overwrite*: Overwrites the existing file.

### To Change All Transferred File Names to Small Letters:

1. Open the **Options** dialog box.
2. Click the [Transfer] tab.
3. Click [Advanced Options] in the [Transfer Options] field.
4. Select [Lowercase] as the download or upload option in the [File Name] field.

### To Change All Transferred File Names to Capital Letters:

1. Open the **Options** dialog box.
2. Click the [Transfer] Tab.
3. Click [Advanced Options] in the [Transfer Options] field.
4. Select [Uppercase] as the download or upload option in the [File Name] field.

**To Capitalize All Transferred File Names:**

1. Open the **Options** dialog box.
2. Click the [Transfer] Tab.
3. Click [Advanced Options] in the [Transfer Options] field.
4. Select [Capitalize] as the download or upload option in the [File Name] field.

**To Set Automatic Retry for Failed Transfer:**

1. Open the **Options** dialog box.
2. Click the [Transfer] tab.
3. Click [Advanced Options] in the [Transfer Options] field.
4. Enter [Maxretry attempts] in the [Retry Transfer] field.
5. Designate a standby time from transfer failure to retry in [Retry interval].

## Resume File Download and Upload

Files paused during transfer may continue to be downloaded. Download resumption is enabled when a file to transfer already exists, but its size is larger than the file of the target folder. To resume a folder download, compare the sizes of all files in the folder and download only the necessary files.

**To Resume Downloading a File or a Folder:**

1. Select and download a file you wish to resume downloading.
2. When the **Confirm File Transfer Actions** dialog box is displayed, select [Resume Downloading].

**To Resume Uploading a File or a Folder:**

1. Select and upload a file or a folder you wish to resume uploading.
2. When the **Confirm File Transfer Actions** dialog box is displayed, select [Resume Uploading].



# File Management

With **Xftp**, users can execute/rename/delete files, create new files, or directly edit files in a remote folder. In addition, **Xftp** offers the capability to edit files with a user defined editor. Not only does **Xftp** utilize the same user interface as Windows Explorer so Windows users can conveniently manage files, it allows users to use the Windows context menu for local files and folders. This way, context menu commands installed on Windows for file types can be utilized directly within Xftp.

## To Change Between the Xftp and Windows Context Menu for Files/Folders:

1. From the [Tools] menu, select Options to open the Options dialog box.
2. From the [Right-click Menu] under the [General] tab, select either Xftp or the Windows System.

## To Execute a File:

1. Select a file to execute in the local or remote folder window.
2. Right-click and select [Open].

### Note

A remote file is executed after it is downloaded to a temporary folder. When a local folder is executed, the File Explorer for the folder opens.

## To Rename a File or a Folder:

1. Select a file or a folder to rename from the local or remote folder window.
2. Select one of the following methods:
  - Select [Rename] from the [Commands] menu.
  - Right-click and select [Rename].
3. When the input box appears, enter a new file name.
4. Press Enter.

## To Delete a File or a Folder:

1. Select a file or a folder to delete from the local or remote folder window.
2. Select one of the following methods:
  - Select [Delete] from the [Commands] menu.
  - Right-click and select [Delete].
3. Select [Yes] when the **Delete File** dialog box is displayed.

## To Change Remote Computer File Permissions:

1. Select the file whose permissions are to be changed from the remote folder window.
2. Select one of the following methods.
  - Select [Change Permissions] from the [Commands] menu.
  - Right-click and select [Change Permissions].
3. Select permissions to change from the **Change Permissions** dialog box.

4. Click [OK].

 **Note**

This function is provided via the UNIX remote computer and therefore the remote computer operating system must be compatible with UNIX. Changing permissions may fail depending on remote computer type.

**To Edit a Remote Text File:**

1. Select a file to edit from the remote folder window.
2. Right-click and select [Edit with Notepad].

 **Note**

Instead of Notepad, a custom editor can be designated by the user in the **Options** dialog box [Advanced] tab.

**To Create a New Folder:**

1. Click the local or remote folder window.
2. Select one of the following methods:
  - Select [New Folder] from the [Commands] menu.
  - Right-click and select [New Folder].
3. When an input box appears, enter the name of the new folder.
4. Press Enter.

**To View File Attributes:**

1. Select the file whose the attributes are to be checked from the local or remote folder window.
2. Right-click and select [Properties].

# Session Log

**Xftp** has two types of log files. One is for file management, such as renaming or deleting, and the other is for transfers. In the log folder, **Xftp** creates new folder for each execution date. In each folder, a file management log and a file transfer log are created for each session.

## To Change Log Display in the Logs Window:

1. Open the **Options** dialog box.
2. Click the [Log] tab.
3. Enter the maximum display lines in the remote log window of [Max lines].

## To Create a Log File:

1. Open the **Options** dialog box.
2. Click the [Log] tab.
3. Click [Save log messages to files].
4. Click [OK].

## To Delete a Log File:

1. Open the **Options** dialog box.
2. Click the [Log] tab.
3. Click [Delete all log files].

## To Designate Log File Storage Duration:

1. Open the **Options** dialog box.
2. Click the [Log] tab.
3. Enter the storage duration in the [Days to keep logs].
4. Click [OK].

## To Designate a Log File Storage Folder:

1. Open the **Options** dialog box.
2. Click the [Log] tab.
3. Click the browser button ([...]) for [Log folder location].
4. Select a folder in which to save logs from the **Browse For Folder** dialog box.
5. Click [OK].



# Window Management

**Xftp** offers convenient local and remote folder window management.

## To Move between Folder Windows:

- Select a folder window to move from by clicking the Session tab.
- Navigate folder windows in order using Ctrl+Tab.

## To Refresh a Folder Window:

1. Do one of the following:
  - Select [Refresh] from the [View] menu.
  - Right-click on the folder window and select [Refresh].
  - Click the standard [Refresh] button in the folder window.

## To Arrange Folder Window Contents:

1. Do one of the following:
  - Select [Arrange Icons by] from the [View] menu.
  - Right-click on the folder window and select [Arrange Icons by].

## To Change the Double-click Actions in a Folder Window:

1. Open the **Options** dialog box.
2. Click the [General] tab.
3. Select [Double-click Action].

### **Note**

Double-click Actions are *Transfer, Open, Properties, and Edit*.

