

NAS4Free - Basic FTP Client Configuration

Installed Version - NAS4Free-x64-LiveCD-9.0.0.1.43.ISO

Introduction

While CIFS and NFS are file system protocols, which means that whole file systems can be shared on the network, and other computers can use those file systems as if they were attached locally, FTP ([File Transfer Protocol](#)) is a TCP protocol for uploading and downloading files between computers. FTP works on a client/server model. The server component is called an FTP daemon. It continuously listens for FTP requests from remote clients. When a request is received, it manages the login and sets up the connection. For the duration of the session it executes any of commands sent by the FTP client.

Access to an FTP server can be managed in one of two ways:

1. Anonymous.
2. Authenticated.

In the Anonymous mode, remote clients can access the FTP server by using the default user account called "anonymous" or "ftp" and sending an email address as the password.

In the Authenticated mode a user must have an account and a password. User access to the FTP server directories and files is dependent on the permissions defined for the account used at login. As a general rule, the FTP daemon will hide the root directory of the FTP server, and provide access only to the FTP Home directory. This hides the rest of the file system from remote sessions.



Warning - Enabling anonymous FTP upload can be an extreme security risk. It is best to not enable anonymous upload on servers accessed directly from the Internet.

Traditional FTP is rather insecure. When you login, your *username* and *password* are transmitted in clear text, raising the possibility of your credentials being 'sniffed' by a malicious person. Fortunately there's an easy answer to this. You can quite easily configure your FTP server to use OpenSSL encryption, so that username & password, and even data files, are encrypted during transfer. For details see:

- [SUG Section 2.6.2-Secure SFTP Configuration](#)
- [SUG Section 2.6.2-Secure FTPES Configuration](#)

Prerequisites

Before deploying FTP on NAS4Free you should be familiar with:

- Linux file and directory permissions.
- Mounting and detaching (unmounting) filesystems.
- Changing File Permissions and File Ownership.

Open a Terminal (Console, CLI) on your client PC and make sure you understand these commands:

- man mount
- man umount
- man chown
- man chmod
- man ftp

You can also look them up on [FreeBSD.org's Man Pages](https://www.freebsd.org/man/).

Install NAS4Free, if you already haven't.

See [SUG Section 2.3-Installing NAS4Free on disk](#).

Or you may run it from the CDROM as required for testing.

See [SUG Section 2.2-Using NAS4Free with the CDROM and a removable disk](#) (LiveCD mode).

Basic FTP COMMANDS

The following are basic commands you can use with a CLI to manage your FTP session. These commands should work on Windows and Linux clients.

- delete - Deletes the file in the remote directory.
- lcd - Changes directory on your local machine.
- mkdir - Makes a new directory within the current remote directory.
- mget - Copies multiple files from the remote machine to the local machine. You will be prompted for a Y/N answer before transferring each file, unless you use the "Prompt Off" command before hand.
- mput - Copies multiple files from the local machine to the remote machine. You will be prompted for a Y/N answer before transferring each file, unless you use the "Prompt Off" command before hand.
- put - Copies a file from the local machine to the remote machine.
- pwd - Displays the current working directory on the remote machine.
- rmdir - Deletes a directory in the current remote machine.
- quit - Exits ftp.

Server Configuration

For details about the FTP service please see [SUG Section 6.2-FTP-File Transfer Protocol](#).

Services | FTP

Settings **Modules**

File Transfer Protocol **Enable**

TCP port	<input type="text" value="21"/> Default is 21.
Number of clients	<input type="text" value="10"/> Maximum number of simultaneous clients.
Max. conn. per IP	<input type="text" value="6"/> Maximum number of connections per IP address (0 = unlimited).
Max. login attempts	<input type="text" value="1"/> Maximum number of allowed password attempts before disconnection.
Timeout	<input type="text" value="300"/> Maximum idle time in seconds.
Permit root login	<input checked="" type="checkbox"/> Specifies whether it is allowed to login as superuser (root) directly.
Anonymous users only	<input type="checkbox"/> Only allow anonymous users. Use this on a public FTP site with no remote FTP access to real accounts.
Local users only	<input checked="" type="checkbox"/> Only allow authenticated users. Anonymous logins are prohibited.
Banner	<div style="border: 1px solid #ccc; height: 80px; width: 100%;"></div> <p>Greeting banner displayed by FTP when a connection first comes in.</p>

1 - Enable FTP, and select the parameters/options you want to use for access.

Advanced settings	
Create mask	<input type="text" value="077"/> Use this option to override the file creation mask (077 by default).
Directory mask	<input type="text" value="022"/> Use this option to override the directory creation mask (022 by default).
FXP	<input type="checkbox"/> Enable FXP protocol. FXP allows transfers between two remote servers without any file data going to the client asking for the transfer (insecure!).
Resume	<input checked="" type="checkbox"/> Allow clients to resume interrupted uploads and downloads.
Default root	<input checked="" type="checkbox"/> chroot() everyone, but root. If default root is enabled, a chroot operation is performed immediately after a client authenticates. This can be used to effectively isolate the client from a portion of the host system filesystem.
Ident protocol	<input type="checkbox"/> Enable the ident protocol (RFC1413). When a client initially connects to the server the ident protocol is used to attempt to identify the remote username.
Reverse DNS lookup	<input type="checkbox"/> Enable reverse DNS lookup. Enable reverse DNS lookup performed on the remote host's IP address for incoming active mode data connections and outgoing passive mode data connections.
Masquerade address	<input type="text"/> Causes the server to display the network information for the specified IP address or DNS hostname to the client, on the assumption that that IP address or DNS host is acting as a NAT gateway or port forwarder for the server.
Passive ports	<input type="text" value="51000"/> The minimum port to allocate for PASV style data connections (0 = use any port).
	<input type="text" value="51500"/> The maximum port to allocate for PASV style data connections (0 = use any port). Passive ports restricts the range of ports from which the server will select when sent the PASV command from a client. The server will randomly choose a number from within the specified range until an open port is found. The port range selected must be in the non-privileged range (eg. greater than or equal to 1024). It is strongly recommended that the chosen range be large enough to handle many simultaneous passive connections (for example, 49152-65534, the IANA-registered ephemeral port range).
Local user bandwidth	<input type="text"/> Local user upload bandwidth in KB/s. An empty field means infinity.

2 - Then click the **“Save and Restart”** Button.

Verify Connection to Server

Connect your Client to the Network, and use [W PING](#) to verify that you can reach the Server's IP Address. You can also try to open the NAS4Free WebGUI, if you are successful then you have a working connection.

Client Software

Linux and Windows both have built-in, CLI based, FTP clients. Most people will probably prefer a GUI based client. A popular client is [Filezilla](#), and Filezilla supports a version for most Operating Systems. There are many others and you can use Google to find one that's right for you.

Testing your FTP service and connection.

The FTP service should now be running, so let's test the FTP Connection manually, with the CLI, before trying to use Filezilla. If you can't login, it's likely that there is no account created for you.

1 - Open a Terminal Window (Console, CLI).

2 - Type the following:

```
ftp 192.168.1.250
```

3 - Logon to FTP: If Anonymous Users was selected, your username will be *anonymous*, otherwise for local users, enter your *username* and press the “**ENTER**” key. Enter your Password and press the “**ENTER**” key. You should see something like this:

```
Connected to 192.168.1.250
220 ProFTPD 1.3.2e Server (ldknas4free FTP Server) [::ffff:192.168.1.250]
Name (192.168.1.250:larry): ldk
331 Password required for ldk
Password:
230-Welcome to NAS4Free FTP Server
230 User ldk logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

4 - Type the following:

```
ls
```

5 - You should see the following:

```
ftp> ls200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxrwxrwx 3 root wheel 512 Jul 18 12:24 CF_Data_Part2
drwxrwxrwx 8 root wheel 7680 Jul 25 12:51 mysata
drwxr-xr-x 4 root wheel 512 Jul 21 13:45 ramdisk1
drwxr-xr-x 3 root wheel 512 Jul 21 13:45 ramdisk2
226 Transfer complete
ftp>
```

6 - Exit FTP:

```
ftp>quit
```

This procedure just verified that you can connect manually using ftp. You will use the Menu's from Filezilla to transfer files.

REF: [Basic FTP Commands](#)

Configuring FTP Access Behind a Firewall

If you want to use NAS4Free behind a NAT box (router or firewall) that does not support FTP you should:

1. Configure your NAT box (router or firewall) to forward port (TCP 21 and a RANGE of TCP ports) to your NAS4Free
2. Add your public IP address on the 'Passive IP address' field
3. Add your lower TCP port of your configured range on the 'pasv_min_port' field
4. Add your high TCP port of your configured range on the 'pasv_max_port' field
5. Enable 'NAT Mode'

You will be opening several ports, these are generic instructions and it may be wise for you to consult the manufacturers' manual for information specific to your equipment and application. Port 21 may be blocked by some ISP's and therefore you may need to use another unassigned port, which probably would be a wise decision. For best results don't use known port numbers at all, use unassigned, private ports per [IANA](#) recommendations. If you have trouble configuring your router or getting it to work, look for help on the manufacturers' website or Google.

How-to access NAS4Free FTP server from internet.

The diagram illustrates the network setup for accessing a NAS4Free FTP server from the internet. It shows an ISP cloud connected to a Modem, which is connected to a Router. The Router is connected to a NAS4Free server. A computer is also connected to the Router. The Router's IP address is 192.168.1.1 / 24, and the NAS4Free server's IP address is 192.168.1.250 / 24. The computer's IP address is 192.168.1.2 / 24.

On your Router

1. You must forward port 21 to **NAS4free 192.168.1.250.**
2. You must forward a port range to **.NAS4Free IP port range 51000 to 51010**
3. Find your external IP address from: <http://checkip.dyndns.org:8245/>

On NAS4free Server

1. WebGUI - System - GeneralSetup - DNS servers
Enter your router IP (192.168.1.1) & save
2. WebGUI - Interfaces - Lan - Default Gateway
Enter your router IP (192.168.1.1) & save & reboot
3. WebGUI - Services - FTP
Passive IP address: **your external IP**
pasv_min_port: **51000**
pasv_max_port: **51010**

From: <https://www.xigmanas.com/wiki/> - XigmaNAS

Permanent link: https://www.xigmanas.com/wiki/doku.php?id=documentation:setup_and_user_guide:basic_client_configuration

Last update: 2018/07/08 16:57

