

**NAME**

**psftp** – interactive SFTP (secure file transfer protocol) client

**SYNOPSIS**

**psftp** [*options*] [*user@*]*host*

**DESCRIPTION**

**psftp** is an interactive text-based client for the SSH-based SFTP (secure file transfer) protocol.

**OPTIONS**

The command-line options supported by **psftp** are:

- V** Show version information and exit.
- pgpfp** Display the fingerprints of the PuTTY PGP Master Keys and exit, to aid in verifying new files released by the PuTTY team.
- b batchfile**  
Use specified batchfile.
- bc** Output batchfile commands.
- be** Don't stop batchfile processing on errors.
- v** Show verbose messages.
- load session**  
Load settings from saved session.
- P port** Connect to port *port*.
- proxycmd command**  
Instead of making a TCP connection, use *command* as a proxy; network traffic will be redirected to the standard input and output of *command*. *command* must be a single word, so is likely to need quoting by the shell.  
  
The special strings **%host** and **%port** in *command* will be replaced by the hostname and port number you want to connect to; to get a literal **%** sign, enter **%%**.  
  
Backslash escapes are also supported, such as sequences like **\n** being replaced by a literal new-line; to get a literal backslash, enter **\\**. (Further escaping may be required by the shell.)  
  
(See the main PuTTY manual for full details of the supported **%**- and backslash-delimited tokens, although most of them are probably not very useful in this context.)
- l user** Set remote username to *user*.
- batch** Disable interactive prompts.
- no-sanitise-stderr**  
By default, PSFTP will filter control characters from the standard error channel from the server, to prevent remote processes sending confusing escape sequences. This option forces the standard error channel to not be filtered.
- pw password**  
Set remote password to *password*. **CAUTION:** this will likely make the password visible to other users of the local machine (via commands such as **'w'**).
- 1** Force use of SSH protocol version 1.
- 2** Force use of SSH protocol version 2.
- 4, -6** Force use of IPv4 or IPv6 for network connections.
- C** Enable SSH compression.
- i keyfile**  
Private key file for user authentication. For SSH-2 keys, this key file must be in PuTTY's PPK format, not OpenSSH's format or anyone else's.

If you are using an authentication agent, you can also specify a *public* key here (in RFC 4716 or OpenSSH format), to identify which of the agent's keys to use.

**-noagent**

Don't try to use an authentication agent.

**-agent** Allow use of an authentication agent. (This option is only necessary to override a setting in a saved session.)

**-hostkey *key***

Specify an acceptable host public key. This option may be specified multiple times; each key can be either a fingerprint (**99:aa:bb:...**) or a base64-encoded blob in OpenSSH's one-line format.

Specifying this option overrides automated host key management; *only* the key(s) specified on the command-line will be accepted (unless a saved session also overrides host keys, in which case those will be added to), and the host key cache will not be written.

**-sshlog *logfile***

**-sshrawlog *logfile***

These options make **psftp** log protocol details to a file. (Some of these may be sensitive, although by default an effort is made to suppress obvious passwords.)

**-sshlog** logs decoded SSH packets and other events (those that **-v** would print). **-sshrawlog** additionally logs the raw encrypted packet data.

## COMMANDS

For a list of commands available inside **psftp**, type **help** at the **psftp>** prompt.

## MORE INFORMATION

For more information on **psftp** it's probably best to go and look at the manual on the PuTTY web page:

<https://www.chiark.greenend.org.uk/~sgtatham/putty/>

## BUGS

This man page isn't terribly complete. See the above web link for better documentation.