SSH File Transfer Protocol

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#mw-head)[Jump to search](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#searchInput)

*Not to be confused with*[*Simple File Transfer Protocol*](https://en.wikipedia.org/wiki/Simple_File_Transfer_Protocol)*,*[*FTP over SSH*](https://en.wikipedia.org/wiki/File_Transfer_Protocol#FTP_over_SSH)*, or*[*FTPS*](https://en.wikipedia.org/wiki/FTPS)*.*

In [computing](https://en.wikipedia.org/wiki/Computing), the **SSH File Transfer Protocol** (also **Secure File Transfer Protocol**, or **SFTP**) is a [network protocol](https://en.wikipedia.org/wiki/Network_protocol) that provides [file access](https://en.wikipedia.org/wiki/File_access), [file transfer](https://en.wikipedia.org/wiki/File_transfer), and [file management](https://en.wikipedia.org/wiki/File_management) over any reliable [data stream](https://en.wikipedia.org/wiki/Data_stream). It was designed by the [Internet Engineering Task Force](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force) (IETF) as an extension of the [Secure Shell](https://en.wikipedia.org/wiki/Secure_Shell) protocol (SSH) version 2.0 to provide secure file transfer capabilities. The IETF [Internet Draft](https://en.wikipedia.org/wiki/Internet_Draft) states that, even though this protocol is described in the context of the SSH-2 protocol, it could be used in a number of different applications, such as secure file transfer over [Transport Layer Security](https://en.wikipedia.org/wiki/Transport_Layer_Security) (TLS) and transfer of management information in [VPN](https://en.wikipedia.org/wiki/VPN) applications.

This protocol assumes that it is run over a [secure channel](https://en.wikipedia.org/wiki/Secure_channel), such as SSH, that the server has already authenticated the client, and that the identity of the client user is available to the protocol.



**Contents**

* [1Capabilities](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#Capabilities)
* [2History and development](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#History_and_development)
  + [2.1Versions 0–2](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#Versions_0%E2%80%932)
  + [2.2Version 3](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#Version_3)
  + [2.3Version 4](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#Version_4)
  + [2.4Version 5](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#Version_5)
  + [2.5Version 6](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#Version_6)
* [3Software](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#Software)
  + [3.1SFTP client](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#SFTP_client)
  + [3.2SFTP server](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#SFTP_server)
  + [3.3SFTP proxy](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#SFTP_proxy)
* [4See also](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#See_also)
* [5References](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#References)
* [6External links](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#External_links)

Capabilities[[edit](https://en.wikipedia.org/w/index.php?title=SSH_File_Transfer_Protocol&action=edit&section=1)]

Compared to the [SCP](https://en.wikipedia.org/wiki/Secure_copy) protocol, which only allows file transfers, the SFTP protocol allows for a range of operations on remote files which make it more like a remote [file system](https://en.wikipedia.org/wiki/File_system) protocol. An SFTP [client](https://en.wikipedia.org/wiki/Client_(computing))'s extra capabilities include resuming interrupted transfers, directory listings, and remote file removal.[[1]](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_note-Barrett2001-1)

SFTP attempts to be more platform-independent than SCP; with SCP, for instance, the expansion of [wildcards](https://en.wikipedia.org/wiki/Wildcard_character) specified by the client is up to the server, whereas SFTP's design avoids this problem. While SCP is most frequently implemented on [Unix](https://en.wikipedia.org/wiki/Unix) platforms, SFTP servers are commonly available on most platforms. The file transfer is fast in SCP when compared to the SFTP protocol due to the back and forth nature of SFTP protocol. In SFTP, the file transfer can be easily terminated without terminating a session like other mechanisms do.

SFTP is not [FTP](https://en.wikipedia.org/wiki/File_Transfer_Protocol) run over [SSH](https://en.wikipedia.org/wiki/Secure_Shell), but rather a new protocol designed from the ground up by the [IETF](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force) SECSH [working group](https://en.wikipedia.org/wiki/Working_group). It is sometimes confused with [Simple File Transfer Protocol](https://en.wikipedia.org/wiki/Simple_File_Transfer_Protocol).[[1]](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_note-Barrett2001-1)

The protocol itself does not provide authentication and security; it expects the underlying protocol to secure this. SFTP is most often used as subsystem of [SSH](https://en.wikipedia.org/wiki/Secure_shell) protocol version 2 implementations, having been designed by the same working group. It is possible, however, to run it over SSH-1 (and some implementations support this) or other data streams. Running an SFTP server over SSH-1 is not platform-independent as SSH-1 does not support the concept of subsystems. An SFTP client willing to connect to an SSH-1 server needs to know the path to the SFTP server binary on the server side.

Uploaded files may be associated with their basic attributes, such as time stamps. This is an advantage over the common [FTP](https://en.wikipedia.org/wiki/FTP) protocol.

History and development[[edit](https://en.wikipedia.org/w/index.php?title=SSH_File_Transfer_Protocol&action=edit&section=2)]

The Internet Engineering Task Force (IETF) working group "Secsh" that was responsible for the development of the [Secure Shell](https://en.wikipedia.org/wiki/Secure_Shell) version 2 protocol ([RFC 4251](https://tools.ietf.org/html/rfc4251)) also attempted to draft an extension of that standard for secure file transfer functionality. [Internet Drafts](https://en.wikipedia.org/wiki/Internet_Draft) were created that successively revised the protocol into new versions.[[2]](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_note-tools.ietf.org-2) The software industry began to implement various versions of the protocol before the drafts were standardized. As development work progressed, the scope of the Secsh File Transfer project expanded to include [file access](https://en.wikipedia.org/wiki/File_access) and [file management](https://en.wikipedia.org/wiki/File_management). Eventually, development stalled as some committee members began to view SFTP as a [file system](https://en.wikipedia.org/wiki/File_system) protocol, not just a [file access](https://en.wikipedia.org/wiki/File_access) or [file transfer](https://en.wikipedia.org/wiki/File_transfer) protocol, which places it beyond the purview of the working group.[[3]](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_note-3) After a seven-year hiatus, in 2013 an attempt was made to restart work on SFTP using the version 3 draft as the baseline.[[4]](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_note-4)

**Versions 0–2**[[edit](https://en.wikipedia.org/w/index.php?title=SSH_File_Transfer_Protocol&action=edit&section=3)]

Prior to the IETF's involvement, SFTP was a proprietary protocol of [SSH Communications Security](https://en.wikipedia.org/wiki/SSH_Communications_Security), designed by Tatu Ylönen with assistance from Sami Lehtinen in 1997.[[5]](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_note-5) Differences between versions 0–2 and version 3 are enumerated upon in [section 10 of draft-ietf-secsh-filexfer-02](http://tools.ietf.org/html/draft-ietf-secsh-filexfer-02#section-10).

**Version 3**[[edit](https://en.wikipedia.org/w/index.php?title=SSH_File_Transfer_Protocol&action=edit&section=4)]

At the outset of the IETF Secure Shell File Transfer project, the Secsh group stated that its objective of SSH File Transfer Protocol was to provide a secure file transfer functionality over any reliable data stream, and to be the standard file transfer protocol for use with the SSH-2 protocol.

Drafts 00–02 of the IETF Internet Draft define successive revisions of version 3 of the SFTP protocol.

* [SSH File Transfer Protocol, Draft 00, January 2001](http://tools.ietf.org/html/draft-ietf-secsh-filexfer-00)
* [SSH File Transfer Protocol, Draft 01, March 2001](http://tools.ietf.org/html/draft-ietf-secsh-filexfer-01)
* [SSH File Transfer Protocol, Draft 02, October 2001](http://tools.ietf.org/html/draft-ietf-secsh-filexfer-02)

**Version 4**[[edit](https://en.wikipedia.org/w/index.php?title=SSH_File_Transfer_Protocol&action=edit&section=5)]

Drafts 03–04 of the IETF Internet Draft define version 4 of the protocol.

* [SSH File Transfer Protocol, Draft 03, October 2002](http://tools.ietf.org/html/draft-ietf-secsh-filexfer-03)
* [SSH File Transfer Protocol, Draft 04, December 2002](http://tools.ietf.org/html/draft-ietf-secsh-filexfer-04)

**Version 5**[[edit](https://en.wikipedia.org/w/index.php?title=SSH_File_Transfer_Protocol&action=edit&section=6)]

Draft 05 of the IETF Internet Draft defines version 5 of the protocol.

* [SSH File Transfer Protocol, Draft 05, January 2004](http://tools.ietf.org/html/draft-ietf-secsh-filexfer-05)

**Version 6**[[edit](https://en.wikipedia.org/w/index.php?title=SSH_File_Transfer_Protocol&action=edit&section=7)]

Drafts 06–13 of the IETF Internet Draft define successive revisions of version 6 of the protocol.

* [SSH File Transfer Protocol, Draft 06, October 2004](http://tools.ietf.org/html/draft-ietf-secsh-filexfer-06)
* [SSH File Transfer Protocol, Draft 07, March 2005](http://tools.ietf.org/html/draft-ietf-secsh-filexfer-07)
* [SSH File Transfer Protocol, Draft 08, April 2005](http://tools.ietf.org/html/draft-ietf-secsh-filexfer-08)
* [SSH File Transfer Protocol, Draft 09, June 2005](http://tools.ietf.org/html/draft-ietf-secsh-filexfer-09)
* [SSH File Transfer Protocol, Draft 10, June 2005](http://tools.ietf.org/html/draft-ietf-secsh-filexfer-10)
* [SSH File Transfer Protocol, Draft 11, January 2006](http://tools.ietf.org/html/draft-ietf-secsh-filexfer-11)
* [SSH File Transfer Protocol, Draft 12, January 2006](http://tools.ietf.org/html/draft-ietf-secsh-filexfer-12)
* [SSH File Transfer Protocol, Draft 13, July 2006](http://tools.ietf.org/html/draft-ietf-secsh-filexfer-13)

Software[[edit](https://en.wikipedia.org/w/index.php?title=SSH_File_Transfer_Protocol&action=edit&section=8)]

**SFTP client**[[edit](https://en.wikipedia.org/w/index.php?title=SSH_File_Transfer_Protocol&action=edit&section=9)]

The term **SFTP** can also refer to [Secure file transfer program](https://en.wikipedia.org/wiki/Secure_file_transfer_program), a [command-line](https://en.wikipedia.org/wiki/Command-line) [program](https://en.wikipedia.org/wiki/Computer_program) that implements the [client](https://en.wikipedia.org/wiki/Client_(computing)) part of this protocol. As an example, the sftp program supplied with [OpenSSH](https://en.wikipedia.org/wiki/OpenSSH) implements this.[[6]](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_note-6)

Some implementations of the [scp](https://en.wikipedia.org/wiki/Secure_copy" \l "SCP_program" \o "Secure copy) *program* support both the SFTP and SCP protocols to perform file transfers, depending on what the server supports.

**SFTP server**[[edit](https://en.wikipedia.org/w/index.php?title=SSH_File_Transfer_Protocol&action=edit&section=10)]

Some [FTP server implementations](https://en.wikipedia.org/wiki/List_of_FTP_server_software) implement the SFTP protocol; however, outside of dedicated file servers, SFTP protocol support is usually provided by an [SSH server implementation](https://en.wikipedia.org/wiki/Comparison_of_SSH_servers), as it shares the default port of 22 with other SSH services. SFTP implementations may include an SSH protocol implementation to leverage integration of SSH connection details with preexisting FTP server access controls, where an alternative SSH server is tolerable or where alternative ports may be used. An SSH-2 server which supports subsystems may be leveraged to keep a uniform SSH implementation while enhancing access controls with third party software, at the cost of fine-grained integration with connection details, and SSH-1 compatibility.

**SFTP proxy**[[edit](https://en.wikipedia.org/w/index.php?title=SSH_File_Transfer_Protocol&action=edit&section=11)]

It is difficult to control SFTP transfers on security devices at the network perimeter. There are standard tools for logging [FTP](https://en.wikipedia.org/wiki/FTP) transactions, like TIS [fwtk](https://en.wikipedia.org/w/index.php?title=Fwtk&action=edit&redlink=1" \o "Fwtk (page does not exist)) or SUSE FTP proxy, but SFTP is encrypted, rendering traditional proxies ineffective for controlling SFTP traffic.

There are some tools that implement man-in-the-middle for SSH which also feature SFTP control. Examples of such a tool are Shell Control Box from [Balabit](https://en.wikipedia.org/wiki/Balabit" \o "Balabit)[[7]](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_note-7) and CryptoAuditor from [SSH Communications Security](https://en.wikipedia.org/wiki/SSH_Communications_Security)[[8]](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_note-8) (the original developer of the Secure Shell protocol) which provides functions such as SFTP transaction logging and logging of the actual data transmitted on the wire.

See also[[edit](https://en.wikipedia.org/w/index.php?title=SSH_File_Transfer_Protocol&action=edit&section=12)]

* [Comparison of SSH clients](https://en.wikipedia.org/wiki/Comparison_of_SSH_clients)
* [Comparison of SSH servers](https://en.wikipedia.org/wiki/Comparison_of_SSH_servers)
* [Comparison of file transfer protocols](https://en.wikipedia.org/wiki/Comparison_of_file_transfer_protocols)
* [FISH](https://en.wikipedia.org/wiki/Files_transferred_over_shell_protocol)
* [FTPS](https://en.wikipedia.org/wiki/FTPS)
* [Lsh](https://en.wikipedia.org/wiki/Lsh)—a [GNU](https://en.wikipedia.org/wiki/GNU_Project) SSH-2 and SFTP server for [Unix-like](https://en.wikipedia.org/wiki/Unix-like) OSes
* [SSHFS](https://en.wikipedia.org/wiki/SSHFS)—Mounting remote filesystem using SFTP and SSH
* [Category:FTP clients](https://en.wikipedia.org/wiki/Category:FTP_clients)
* [Category:SFTP clients](https://en.wikipedia.org/wiki/Category:SFTP_clients)

References[[edit](https://en.wikipedia.org/w/index.php?title=SSH_File_Transfer_Protocol&action=edit&section=13)]

* 1. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_ref-Barrett2001_1-0) [***b***](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_ref-Barrett2001_1-1) *Barrett, Daniel; Silverman, Richard E. (2001), SSH, The Secure Shell: The Definitive Guide, Cambridge: O'Reilly,*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*0-596-00011-1*](https://en.wikipedia.org/wiki/Special:BookSources/0-596-00011-1)
  2. [**^**](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_ref-tools.ietf.org_2-0) [*"Secsh Status Pages"*](http://tools.ietf.org/wg/secsh/draft-ietf-secsh-filexfer/)*. Tools.ietf.org. Retrieved 2012-08-20.*
  3. [**^**](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_ref-3) [*"ietf.secsh—Formal consultation prior to closing the secsh working group—msg#00010—Recent Discussion"*](https://web.archive.org/web/20120320214102/http:/osdir.com/ml/ietf.secsh/2006-07/msg00010.html)*. Osdir.com. 2006-08-14. Archived from*[*the original*](http://osdir.com/ml/ietf.secsh/2006-07/msg00010.html)*on 2012-03-20. Retrieved 2012-08-20.*
  4. [**^**](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_ref-4) [*"SSH File Transfer Protocol—draft-moonesamy-secsh-filexfer-00"*](http://permalink.gmane.org/gmane.ietf.secsh/6904)*. Gmane.org. 2013-07-12.*
  5. [**^**](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_ref-5) <ftp://ftp.ietf.org/ietf-mail-archive/secsh/2012-09.mail>
  6. [**^**](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_ref-6) [*"OpenBSD manual page for the "sftp" command: "See Also" section"*](https://man.openbsd.org/sftp.1#SEE_ALSO)*. OpenBSD.org. Retrieved 2018-02-04.*
  7. [**^**](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_ref-7) [*"Record SSH/RDP/Citrix into Audit Trail—Activity Monitoring Device"*](http://www.balabit.com/network-security/scb/)*. Balabit.com. Retrieved 2012-08-20.*
  8. [**^**](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol#cite_ref-8) [*"Privileged Access Control and Monitoring"*](http://www.ssh.com/products/crypto-auditor)*. SSH.com. Retrieved 2014-11-25.*

External links[[edit](https://en.wikipedia.org/w/index.php?title=SSH_File_Transfer_Protocol&action=edit&section=14)]

* [Chrooted SFTP with Public Key Authentication](https://archive.is/20130103130850/http:/www.ipsure.com/blog/2010/chrooted-sftp-with-public-key-authentication) – Integrating SFTP into FreeBSD production servers using the public key cryptography approach
* [User-based chrooted SFTP in GNU/Linux](http://wiki.gilug.org/index.php/How_to_mount_SFTP_accesses)