**What Are the Top File Transfer Protocols?**

Tags: [**PeSIT**](https://www.goanywhere.com/blog/tag/pesit), [**FTP**](https://www.goanywhere.com/blog/tag/ftp), [**FTPS**](https://www.goanywhere.com/blog/tag/ftps), [**SFTP**](https://www.goanywhere.com/blog/tag/sftp), [**HTTPS**](https://www.goanywhere.com/blog/tag/https), [**AS2**](https://www.goanywhere.com/blog/tag/as2), [**AS3**](https://www.goanywhere.com/blog/tag/as3), [**AS4**](https://www.goanywhere.com/blog/tag/as4), [**MFT**](https://www.goanywhere.com/blog/tag/mft), [**GoAnywhere MFT**](https://www.goanywhere.com/blog/tag/goanywhere-mft), [**XML**](https://www.goanywhere.com/blog/tag/xml), [**EDI**](https://www.goanywhere.com/blog/tag/edi) | Categories: [**FTP**](https://www.goanywhere.com/blog/category/ftp)

**And the Top File Transfer Protocols Are...**

Before implementing the secure managed file transfer solution of your choice, it’s a good idea to have a basic understanding of the file sharing protocols involved that allow for transfers to remain safe and secure. Brush up on the introductory file sharing protocol facts below

**1. FTP**

The original file transfer protocol, [**FTP**](https://www.goanywhere.com/managed-file-transfer/file-server/ftp-server), is a popular file transfer method that has been around for decades. FTP exchanges data using two separate channels known as the command channel to authenticate the user, and the data channel to transfer the files.

With FTP, both channels are unencrypted, leaving any data sent over these channels vulnerable to being taken advantage of. However, it does require an authenticated username and password for access.

**Related Reading:**[**Replace Your FTP Scripts to Increase Security**](https://www.goanywhere.com/blog/replace-your-ftp-scripts-to-increase-security)

**2. FTPS**

Short for FTP over SSL/TLS (Secure Sockets Layer/ Transport Layer Security), [**FTPS**](https://www.goanywhere.com/managed-file-transfer/connectivity/ftps) is a secure file transfer protocol that allows you to transfer files securely with trading partners, customers, and users. The transfers can be authenticated through FTPS-supported methods like client certificates, server certificates, and passwords.

**Related Reading:**[**SFTP vs. FTPS: The Key Differences**](https://www.goanywhere.com/blog/2016/11/23/sftp-vs-ftps-the-key-differences)

**3. SFTP**

[**SFTP**](https://www.goanywhere.com/managed-file-transfer/connectivity/sftp) stands for FTP over SSH (Secure Shell). It is a secure FTP protocol and a great alternative to unsecure FTP tools or manual scripts. SFTP exchanges data over an SSH connection and provides organizations with a high level of protection for file transfers shared between their systems, trading partners, employees, and the cloud.

**Related Reading:**[**Are SFTP and FTP the Same?**](https://www.goanywhere.com/blog/are-sftp-and-ftp-the-same)

[Request a Demo](https://www.goanywhere.com/demo)

**4. SCP**

An older protocol, [**SCP**](https://www.goanywhere.com/managed-file-transfer/connectivity/scp) or Secure Copy Protocol, is a network protocol that supports file transfers between hosts on a computer network. It’s somewhat similar to FTP, however, SCP supports encryption and authentication features.

**Related Reading:**[**SCP vs. SFTP: Which is Better?**](https://www.goanywhere.com/blog/scp-vs-sftp-which-is-better)

**5. HTTP & HTTPS**

As the backbone of the WWW (World Wide Web), [**HTTP**](https://www.goanywhere.com/managed-file-transfer/connectivity/https) (Hyper Text Transfer Protocol) is the foundation of data communication. It defines the format of messages through which web browsers and web servers communicate and defines how a web browser should response to a web request. HTTP uses TCP (Transmission Control Protocol) as an underlying transport and is a stateless protocol. This means each command is executed independently and no session information is retained by the receiver.

[**HTTPS**](https://www.goanywhere.com/managed-file-transfer/file-server/web-client) (Hyper Text Transfer Protocol Secure) is the secure version of HTTP where communications are encrypted by TLS or SSL.

**Related Reading:**[**Comparing Transfer Methods: HTTP vs. FTP**](https://www.goanywhere.com/blog/comparing-transfer-methods-http-vs-ftp)

**6. AS2, AS3, & AS4**

[**AS2, AS3, and AS4**](https://www.goanywhere.com/solutions/as2-transfers) (Applicability Statement 2, 3, and 4) are all popular protocols used to send and secure critical file transfers.

AS2 is used to transmit sensitive data securely and reliably over the internet. AS2 utilizes digital certificates and encryption standards to protect critical information while it’s in transit across systems, networks, and locations. AS2 messages can be compressed, signed, encrypted, and sent over a secure SSL tunnel.

AS3 is a standard that can be used to transmit virtually any file type. It provides a layer of security for data transmission through digital signatures and data encryption. It was created initially to transfer data files like [**XML**](https://www.goanywhere.com/managed-file-transfer/translation/xml) and [**EDI**](https://www.goanywhere.com/resource-center/electronic-data-interchange) documents for business-to-business data. Unlike AS2, which is a defined transfer protocol, AS3 is a message standard and focuses on how a message should be formatted when transmitting from server to server. Once an AS3 message has been composed, it can be transmitted via any other protocol (FTP, SFTP, HTTPS, etc.) as long as both parties can access the location in which the message has been placed.

AS4 is a protocol that allows businesses to securely exchange data with their partners. It builds on the foundations originally set by AS2 but works with web services and provides improved delivery notifications. As a business-to-business standard, AS4 helps make exchanging documents over the internet secure and simple.

**Related Reading:**[**What’s the Difference Between AS2, AS3, and AS4?**](https://www.goanywhere.com/blog/whats-the-difference-between-as2-as3-and-as4)

**7. PeSIT**

[**PeSIT**](https://www.goanywhere.com/managed-file-transfer/connectivity/pesit), short for Protocol d'Echanges pour un Systeme Interbancaire de Telecompensation, is an end-to-end file transfer protocol that was developed in by the French Interbank Teleclearing Systems Economic Interest Grouping (GSIT). It's less widely used in North America and is primarily used to meet European banking standards and transfer communications to and from banks in Europe.

**Related Reading:** [**What is PeSIT?**](https://www.goanywhere.com/blog/what-is-pesit)

**What Do These Protocols Have in Common? - GoAnywhere MFT**

MFT, short for Managed File Transfer, is a tool that centralizes multiple file sharing protocols on a single pane of glass. With an emphasis on security and automation for file transfer protocols, it's the souped-up [**version of FTP**](https://www.goanywhere.com/blog/ftp-vs-mft-whats-the-difference), and a top choice for IT professionals across all industries.

One of the biggest benefits of MFT is that it utilizes all of these industry-standard file sharing protocols to secure data exchange. Explore how an [**MFT solution**](https://www.goanywhere.com/solutions/managed-file-transfer) like **[GoAnywhere MFT](https://www.goanywhere.com/managed-file-transfer)** can help you automate, simplify, and streamline all aspects of file transfers all while simultaneously supporting each of the above-mentioned protocols.