10 Essential Tips for Securing FTP and SFTP Servers

1

Disable standard FTP

FTP is over 30 years old. It's not designed to withstand modern security threats.

2

Use Strong Encryption and Hashing

Encryption ciphers are used in both SFTP and FTPS protocols to protect data in transmission.

3

Place Behind a Gateway

If the FTP server is in the DMZ, trading partners' data files & user credentials are also stored there—a big risk even if files are encrypted.

4

Implement IP Blacklists & Whitelists

IP blacklists deny a range of IP addresses from accessing the system (temp or permanent).

5

Harden Your SFTP Server

Don't use Explicit FTPS unless you force encryption for authentication & data channels. Don't use any version of SSL or TLS 1.0. Do use Elliptic curve Diffie- Hellman key exchange algorithms.

6

Utilize Good Account Management

Don't allow anonymous users or shared accounts.

7

Use Strong Passwords

Establish complex passwords (including numeric, alphanumeric characters and at least one special character).

8

Implement File & Folder Security

Trading partners should only have folder access they absolutely need. Encrypt files at rest.

9

Lock Down Administration

Restrict admin duties to a limited number of users; require multi-factor authentication. Consider PAM.

10

Follow these SFTP Best Practices

- Keep the FTPS or SFTP server software up-to-date
- Using U.S. government data? Use only FIPS 140-2 validated encryption ciphers
- Don't use default SFTP software version
- Keep any backend databases on a different server
- Require re-authentication of inactive sessions
- Implement good key management

SSH

Learn more at ssh.com