Beginner's Guide to Secure FTP (SFTP/FTPS)

In today's digital-first world, cybersecurity has become a paramount consideration – and transferring files safely between systems is essential. Secure File Transfer Protocol (SFTP) is designed to do just that, helping businesses and other organisations securely exchange sensitive data.

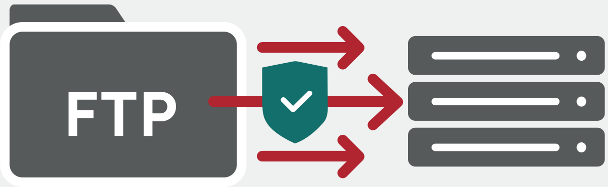
As organisations grow and handle more confidential information, protecting that data during transfer is crucial to avoid security breaches and maintain client trust. Whether you're new to SFTP or are simply exploring data transfer options for your organisation, understanding how it works can help you make more informed choices.

This beginner's guide will cover the basics of SFTP: how it works, what it is commonly used for, how it compares to other file transfer methods and why it's often considered the best choice for organisations that need a safe and secure way of transferring files/exchanging data.

What is SFTP?

SFTP, or Secure File Transfer Protocol, is a secure way to transfer files over a network and is specifically designed to protect data from unauthorised access. It encrypts both the files and the commands used to transfer them, keeping third parties out, and works by creating a secure 'tunnel' through which data can travel safely from one computer to another.

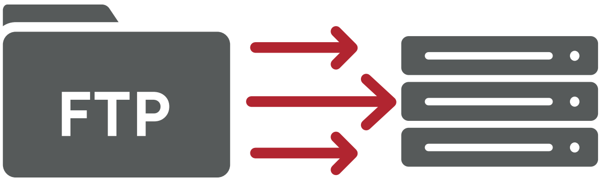
Imagine sending a highly sensitive document through a private, guarded pathway where only trusted individuals have access. SFTP uses encryption to scramble data, making it unreadable to anyone except the intended recipient. This combination of encryption and authentication secures data against interception or tampering.



In sectors like finance, healthcare and the public sector, contractors are often required to provide proof that data will be handled securely as a prerequisite when bidding for contracts. SFTP meets those standards, protecting sensitive information and upholding regulatory requirements.

What is FTP?

File Transfer Protocol (FTP) is one of the oldest methods of transferring files over a network. Developed in the early days of the internet, FTP was designed to move files between systems quickly and easily. However, it has one significant drawback: without proper configuration it lacks built-in security.



The primary difference between FTP and SFTP, therefore, lies in security. While FTP relies on a basic, unencrypted connection, SFTP was specifically created to address basic FTP's security weaknesses, encrypting all data as it travels between a client and a server.

Due to these differences, FTP without encryption is generally suitable only for non-sensitive file transfers within secure networks, whereas SFTP is suitable for the transmission of any data requiring privacy protection, especially across public networks or the internet.

Which sectors use SFTP – and how?

Secure FTP is widely used across industries requiring secure and efficient data transfers. Here are some of the sectors that use SFTP, and a selection of the documents they share via this method:

Retail, wholesale and manufacturing

- Stock, order data and sales reports.
- Customer data, memberships and statistics.
- Usage data for e-commerce and store reporting.
- Product documentation, compliance documentation and imagery.
- Marketing asset distribution.

Software and technology

- Secure transfer of software updates and system logs.
- Distribution of software and firmware updates.
- Storage and transfer of source code, software usage statistics and bug reports.

Hospitality

- Sharing availability and booking data.
- Sharing promotional content with graphic designers and printers.
- Travel aggregator data transfer.

Media, print and distribution

- Editorial collaboration involving graphic assets, videos and photos.
- Exchanging customer and distribution list data.
- Post-production transfer of raw and processed media.
- Stock photography/asset distribution and content licensing.

Transport and logistics

- Sharing shipment data.
- Performance statistics and reports.
- Collection of telematics data.
- Product and stock data for dropshipping and freight forwarding.
- Secure transmission of customs and regulatory documents.

Education and research

- Research data inputs and results.
- Distribution of course or project data.
- Compliance and grant application data.

Internet of Things (IoT) and data collection

- Collection of sensor and reading data.
- Energy usage, environmental and IoT device data.
- CCTV and automated number plate recognition (ANPR) images and data.

Government and public sector

- Inter-agency/department communication of sensitive data.
- Tender documentation and response collection.
- Service performance data collection.
- Disaster management collaboration.
- Tax and revenue collections (DWP, HMRC).

Utilities and construction

- Sharing and collaborating on CAD drawings and blueprints.
- Construction project data sharing with suppliers and clients.
- Compliance, permit and environmental data.
- Property and dilapidation data and evidence storage.
- Systems and hardware monitoring data.

Financial services, law and insurance

- Sharing audited financial and legal reports.
- Policy and contract data sharing and storage.
- Fraud and sensitive data exchange between departments.
- Real-time analysis data and report storage.
- Claims management, evidence and call recordings.

Charities and not-for-profits

- Donation records and data management.
- Prospect data collection and collaboration.
- Exchanging compliance data.
- Volunteer and event management.
- Managing and sharing campaign assets.

General uses of SFTP include the following:

- Transferring stock and order data between clients and suppliers.
- Exchanging messaging between systems (known as Electronic Data Interchange, or EDI).
- Transferring highly sensitive transaction data through a common secure location (push and pull data).
- Centralised backup storage, hosting files/data for recovery and business resilience.
- Cross-team or client-supplier collaboration, providing a secure area for sharing project files across distributed teams.

Is Standard FTP secure – and how can I make it secure?

FTP was developed for simplicity and speed, but its security limitations make it unsuitable for transferring sensitive data. Because standard FTP without extra configuration transmits data in plain text, this can make it vulnerable to interception so that anyone with a compromised internet connection could potentially view or tamper with the data being transferred.

There are, however, several ways to secure FTP in order to reduce this risk:

Use FTP Secure (FTPS)

FTPS adds encryption through SSL/TLS, which is the same technology used to secure websites with HTTPS. By encrypting the data, FTPS protects it from being easily intercepted during transfer.

Use strong credentials

For further security on top of FTPS consider implementing very strong passwords and non-generic usernames such as "staff".

Implement IP whitelisting and access controls

Limiting FTP access to specific IP addresses or ranges can reduce the risk of unauthorised access. Additionally, restricting access permissions ensures only authorised users can modify or view sensitive files.

Regularly monitor or audit activity

Regularly auditing FTP activity logs can help you detect any unusual or unauthorised access attempts. Monitoring access patterns helps identify potential security breaches or attempts sooner, giving you time to take preventative action. We have a specific Reporting & Monitoring System (RMS) to assist with this.

SFTP vs. FTP vs. FTPS

To understand SFTP's value, it helps to know how it compares to other file transfer protocols – specifically, FTP and FTPS. Each protocol offers varying levels of security, usability and reliability, and understanding this can help you make a more informed choice.

File Transfer Protocol (FTP)

FTP is the most basic file transfer method, allowing users to send files over a network. However, **these files are not encrypted,** which means data could be exposed during transit. This can be risky when the data being sent is sensitive.

FTP Secure (FTPS)

FTPS is an upgraded version of FTP using **SSL/TLS encryption**, similar to HTTPS websites. It can require complex configurations which may make it unsuitable for certain types of businesses, but with a hosted solution your provider will do this for you.

Secure File Transfer Protocol (SFTP)

SFTP uses **Secure Shell (SSH) technology to ensure secure data transfer, encrypting files** and keeping data out of the wrong hands. SFTP is, therefore, a robust and user-friendly solution, and one that's ideal for businesses and other organisations seeking a reliable and secure method of file transfer.

Because of it's built-in encryption and options for user authentication, SFTP is often considered the most secure and dependable option for organisations that need to protect their data. This is particularly important for compliance purposes and can help prevent issues with regulators.

Key benefits of SFTP

SFTP offers a range of advantages for organisations needing secure and dependable file transfer capabilities.

Security

SFTP's encryption and authentication features protect sensitive data, ensuring it can't be accessed by unauthorised users.

Platform compatibility and collaboration

SFTP works across different operating systems – including Windows, macOS and Linux – enabling seamless collaboration. In addition, users can access files in real time and see updates as they're made.

Reliability

SFTP is equipped with features to maintain data integrity such as checksums, which ensure that files aren't corrupted during transfer. This makes SFTP highly reliable, even for large files.

Integrates with your processes

SFTP provides a common protocol for systems and businesses to transfer data, including through CRMs, workflows, cloud services and bespoke software and scripts.

Compliance and tendering

Many industries require secure data transfer methods like SFTP for regulatory compliance. It's often a minimum standard for tendering contracts in sectors like finance, healthcare and the public sector, making SFTP valuable for businesses needing to meet these requirements.

Common uses of SFTP

SFTP is widely used across industries where secure and reliable data transfer is essential. Its ability to protect sensitive information makes it the preferred choice for businesses that handle confidential data, must comply with strict regulations, require large, uncorrupted file transfers, or manage highly transactional data between systems.

From highly regulated sectors like finance and healthcare to collaborative environments involving external partners, SFTP meets diverse data transfer needs. Here are some of the most common ways in which it's used:

Secure transfer of sensitive client data

Many organisations, in industries such as law, healthcare and finance, use SFTP to protect client data during transfer. Its robust encryption and authentication protocols mean SFTP keeps confidential information safe.

Meeting compliance requirements

Increasingly, in some industries, SFTP is a requirement as stipulated by regulatory bodies. This helps organisations in these industries meet strict data protection standards and reduce the risk of non-compliance, helping them to avoid the fines and reputational damage that can go with it.

Automated data transfers and scheduled backups

SFTP is a common protocol or language between many systems. As such, it can integrate with transfer scheduling, automation and workflow systems. These can include tools to automate regular file transfers (stock or order data, for example) and data backups, reducing the risk of data loss and human error.

Transferring large files without data corruption

SFTP is ideal for transferring large files such as reports, blueprints, technical specifications and video content. Built-in integrity checks, like checksums, help to ensure that data is not corrupted during transfer.

Bidding for contracts

In some sectors, including government, SFTP is a prerequisite when trying to win contracts. Using SFTP helps organisations to demonstrate their commitment to data security, enhancing their eligibility for these opportunities and building trust with potential clients.

Secure collaboration with partners and clients

SFTP allows organisations to securely share files – including stock and order data – with external partners, including clients and suppliers. This helps to foster closer collaboration and efficiency on products and services while ensuring that data and intellectual property are protected.

SFTP security best practices

For organisations using SFTP, it's important to be aware of best practices to maximise security and keep the risk of unauthorised access to a minimum. Here are some practical tips to follow.

✓ Use strong extra layers of authentication

Public key authentication provides an extra layer of security beyond passwords. Public/Private keys allow you to have combinations of username, password and/or key file. This ensures that only authorised users can access files.

✓ Apply strong encryption standards

To prevent data from being intercepted and read by online criminals, businesses should ensure that their SFTP configuration uses strong encryption standards like AES-256.

✓ Implement access controls

Define and isolate user roles and permissions to limit access to sensitive files. This helps to minimise the risk of data breaches by ensuring that only people who genuine need access to data can do so.

✓ Regular auditing and monitoring

By monitoring file transfers and conducting regular audits, organisations are more likely to detect suspicious activity early and address security vulnerabilities, thereby reinforcing the security of their SFTP system.

✓ Encryption at rest storage

Further reassure your users by encrypting "data at rest" as well as "in transit".

How can I set up a secure FTP server?

Configuring an SFTP server requires careful setup and ongoing management & maintenance to ensure that it's both functional and secure. From isolated user accounts to firewall configuration and software updates, every element plays a role in protecting your data.

There are two main options for setting up an SFTP server: self-hosting within your own network or using a hosting provider. Here, we'll go through the pros and cons involved.

Self-hosting a secure FTP server

Setting up an SFTP server in-house gives you full control over your data and access settings, but it also requires a dedicated IT infrastructure and skilled personnel to maintain security. Key setup considerations include the following:

Isolated user accounts

Isolating user accounts means setting up a 'chroot' environment, where each user is restricted to a designated area within the server. This setup ensures that users can only access the files they need to have access to, helping to prevent unauthorised access and data leakage.

Firewall configuration

Self-hosting requires configuring your firewall to allow SFTP traffic into your network. This process involves setting specific port permissions and ensuring that only trusted IPs can access the server, which helps to prevent unauthorised connections. However, incorrectly configured firewalls can leave your network open to security risks.

Ongoing maintenance and software updates

Hosting an SFTP server in-house requires continuous monitoring and regular software & hardware updates to keep it secure. Outdated software can expose your system to vulnerabilities, which is why it's essential to ensure that all security patches are applied promptly.

Self-hosting can be a good solution for organisations with existing or spare infrastructure and strong in-house IT teams with the required knowledge & experience, but it can be time-consuming, complex and expensive for organisations to implement. Many organisations are also hesitant to open their networks to allow inbound traffic from other businesses or the public internet.

Using a hosting provider for SFTP

For many organisations, hosting an SFTP server in-house is prohibitively expensive and time consuming. Using an SFTP hosting provider, therefore, is a simpler and more realistic option. By outsourcing your SFTP server hosting, you gain access to robust infrastructure, expert management and enhanced security without the need for extensive IT resources. Key benefits include:

Reduced network exposure

When you use a hosting provider, you avoid opening up your internal network to allow external access to the SFTP server. This reduces security risks as the hosting provider's network is typically isolated and protected by advanced security measures.

Firewall and security configurations are managed for you

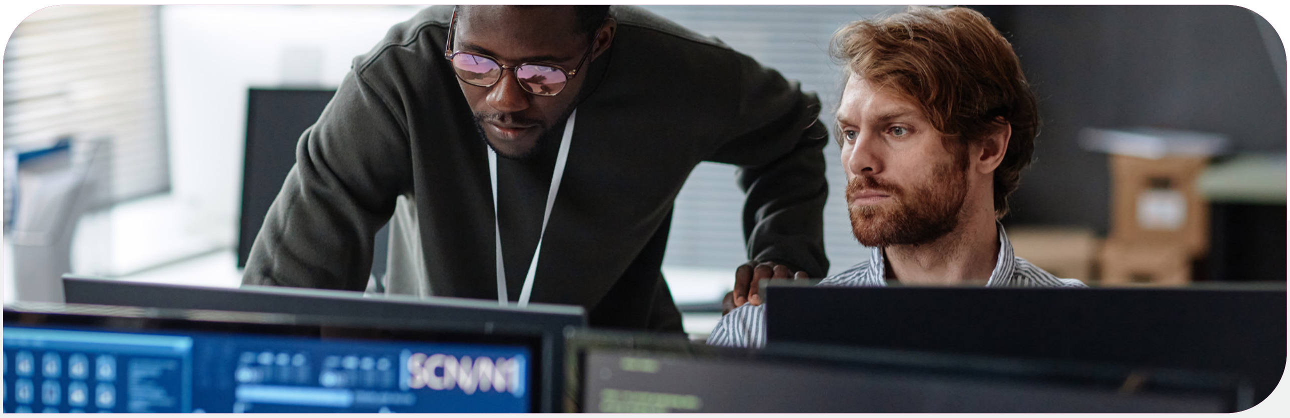
SFTP hosting providers handle complex security configurations like firewalls and access control, saving you the hassle of managing them yourself. Providers often offer additional features, such as IP whitelisting, automated backups and advanced encryption.

Automatic software updates and security patches

A managed hosting provider will handle software updates and apply necessary security patches to keep your server secure. This removes the burden of continually monitoring for updates and maintaining the server yourself.

Scalability and added features

Many hosting providers offer features like multi-user support, advanced reporting and monitoring tools, and support for compliance with specific industry regulation. These added features can simplify data management and provide peace of mind that your SFTP setup meets all the necessary requirements.



Reporting and monitoring

Effective reporting and monitoring are essential elements of a secure and compliant SFTP setup. Monitoring provides real-time visibility over user activity, file transfers and any potential security threats, while reports allow organisations to track historical data and prove their compliance with relevant regulatory requirements.

Ridgeon Network's Reporting and Monitoring System (RMS) add-on provides comprehensive tracking and reporting capabilities to simplify the oversight of your SFTP server hosting. It provides detailed logs and insights on each file transfer, user access and system event, so that any unusual patterns or potential breaches can be dealt with quickly. Here are some of some of the features it offers.

Audit trail for compliance

For many industries, particularly finance, health and government departments, maintaining an audit trail of all file transfers and access activity is often a regulatory necessity. RMS automatically records each transfer, login and logout, making it easier to demonstrate compliance and pass audits.

Enhanced security monitoring

Real-time monitoring detects and proactively blocks suspicious activity and unusual data transfers. With RMS, you gain visibility into every action taken on the server, allowing for quick responses to potential threats before they can escalate.

Customisable reporting

With RMS, you can generate custom reports tailored to your organisation's specific needs. These reports give your team a fine-grained understanding of when and where data is being transferred to and from, as well as monitoring data flow between your business processes.

Data integrity

By continuously monitoring transfer statuses, RMS helps confirm that files reach their destination without errors or corruption. This feature is important for businesses handling large files or mission-critical data, as it ensures that information is transferred intact and available for immediate use as required.

Setting up reporting and monitoring

Implementing reporting and monitoring can be challenging, especially for businesses managing a self-hosted setup. Comprehensive monitoring requires specialised tools and, often, custom configurations requiring considerable technical expertise.

Managing these capabilities can be time-consuming and complex. Partnering with a specialist hosting provider, however, can simplify the process, saving you time and resources as well as significantly reducing the risk of any oversight.

How can I access data on a secure FTP server?

Accessing data on an SFTP server is straightforward, but it requires secure authentication so that only authorised users can access the files. With SFTP, data access is protected through encryption and various authentication methods, such as passwords and/or public keys, which help maintain system and process security.

Accessing files on an SFTP server generally involves using SFTP client software, which provides an interface for users to browse, upload and download files safely. Here's a step-by-step overview of how to securely access data on an SFTP server.

1 Use an SFTP client

To access data on an SFTP server, you'll need an SFTP client application. This application will create a secure connection with the SFTP server, allowing you to navigate file directories, transfer files and manage data with ease (e.g FileZilla Client, WinSCP, Fetch).

2 Accessing files via command line or scripts (advanced users)

For the more tech-savvy users, the command line provides a more flexible way to access an SFTP server. With a few simple commands, you can connect to the server, list files and download or upload data securely. This method is popular among IT professionals who need to automate file transfers or work with large datasets, where SFTP transfers are a part of the workflow.

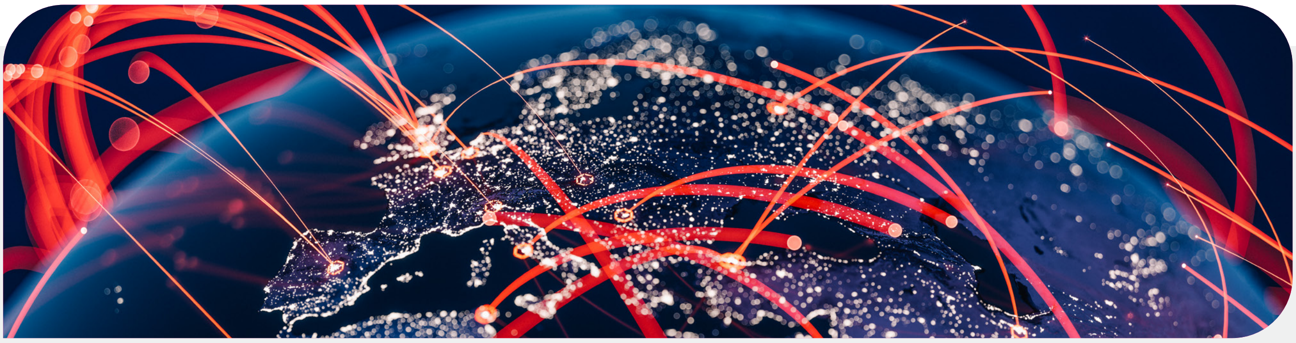
3 Use automation software or services

Connect software or cloud/internet services to your SFTP hosting to provide a user-friendly method of exchanging data between systems.

4 Web based access

Some SFTP hosting providers have the ability for users to access through a user-friendly web-based interface with the same account, with added 2FA (2-Factor Authentication) for additional security. This can be useful for less technical users who still need to upload/download or manage data on the same system as automated processes, for example.

By following these steps/using these options, you can access data securely on an SFTP server without compromising your organisation's security or the confidentiality of sensitive data. Whether you're downloading client files, collaborating with external partners or backing up critical data, the entire process is designed to uphold data integrity and keep your file transfers secure.



What if I need help and support?

When technical issues arise or you need additional guidance, it's crucial to have reliable support on hand. Ridgeon Network offers comprehensive, UK-based support for its clients – so whenever you need help, our team is only an email or a telephone call away. We listen to your requirements and processes to help you set up or configure a solution tailored to your needs.

Our experts can quickly diagnose and resolve technical issues, such as connectivity problems, access or permissions issues. This means you can speak to knowledgeable professionals who'll walk you through solutions step-by-step, ensuring a quick and comprehensive solution.

We also understand that many of our clients operate in sectors with stringent compliance standards. Ridgeon Network are ISO27001 and ISO9001 compliant so our team can provide insights on security practices to help you meet industry standards, maintain data security and ensure that your organisation remains in line with regulatory requirements.

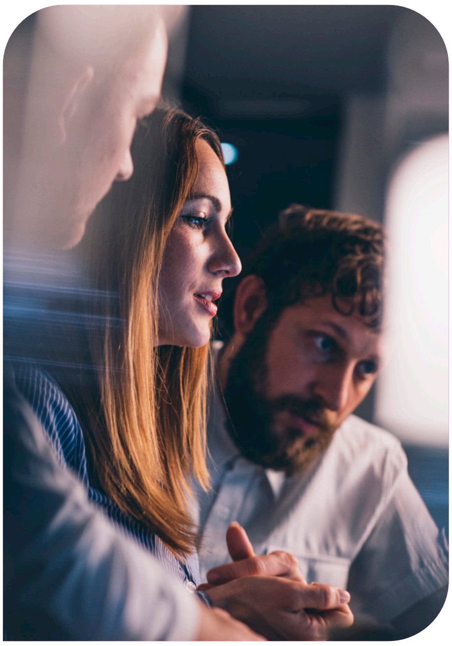
Ridgeon Network's UK-based support gives you peace of mind knowing that expert help is there when you need it. Our dedication to excellent customer service and support makes us an outstanding partner for any organisation needing secure, compliant and hassle-free SFTP hosting solutions.

Conclusion

For businesses focused on data security and regulatory compliance, SFTP is a powerful and practical solution. It offers robust protection for sensitive data, meets compliance standards and enables closer and automated collaboration without compromising security.

Choosing the right SFTP hosting solution can also give companies a competitive edge, particularly when bidding for contracts, as it makes them more attractive to clients with strict security requirements (such as ISO27001). Its comprehensive security features and cross-platform compatibility therefore mean that SFTP helps businesses protect their data transfer process while enhancing overall efficiency.

Ridgeon Network's team of experts provides in-depth guidance to help you find the best SFTP hosting solution for your needs and budget. Contact us today to find out more.



Ridgeon NETWORK

+44 (0)1455 221 645 | info@ridgeon-network.co.uk | www.ridgeon-network.co.uk

Ridgeon Network Ltd, Alma Park, Woodway Lane, Lutterworth, Leicestershire, LE17 5BH

CYBER ESSENTIALS

Cyber Essentials
Certification

ISO

ISO 27001
Certified

ISO

ISO 9001
Certified

Google ★★★★★

Rated 5 Stars
on Google