CLIENT DATA INTEGRATION TECHNOLOGY OVERVIEW

〉 FactSet integrates FactSet-collected content, more than 800 commercial datasets, and client-proprietary data to provide a universe of financial intelligence.

Research reports, global news coverage, fixed income data, portfolio holdings, and many other pieces of information are combined with FactSet's unique suite of applications to provide FactSet users with unparalleled market analysis.

This technology overview outlines the five-step process for integrating your content with FactSet. We provide recommendations, examples, and in-depth discussions on technology to enable the setup of secure, robust, and automatable data integration processes. FactSet is committed to maintaining its reputation for industry-leading service, and FactSet specialists will be available to provide step-by-step assistance as necessary

CLIENT DATA INTEGRATION PROCESS OVERVIEW

Extract: You can extract your data from accounting and order management systems, databases, feeds, and other data stores into a predefined format for use in FactSet's real-time applications, Portfolio Analysis, and FactSet Research Connect. FactSet will provide detailed documentation about data fields and formats and can offer assistance in automating the extraction.

Transmit: FactSet clients can send and receive data via FTP or securely via SFTP (preferred) over the Internet. You can push files to FactSet (preferred) or FactSet can connect to you to both send and receive files using the FactSet File Transfer System (FTS).

Store:Your information is stored securely and redundantly. It can be encrypted in transit to or from FTS for additional security. FTS is a system that facilitates file transfers and is therefore subject to a retention policy of 30 days.

Process: As your data arrives on FactSet's systems, it is uploaded, transformed, and validated to meet consumption needs.

Deliver: Processed data is made available to your end-users in the interactive FactSet application. Processed reports and data can be delivered to your servers via FTP or SFTP as well as consumed by data feed subscribers. These files are also made available for pickup on FTS.

PROPRIETARY DATA INTEGRATION

Client proprietary data such as positions, returns, and transactions can be transmitted to FactSet either directly from your internal systems or from your third party vendors such as custodians. These files can be sent to FactSet via FTP or SFTP as delimited text files. FactSet will work with your IT contacts or your third party vendor to facilitate the setup of file transfer processes. A comprehensive document for portfolio upload requirements, "Guide to FactSet Parsers", is available from your account team or specialist . A FactSet specialist can provide assistance automating, transforming, and transmitting your extracted data.

RESEARCH REPORT CONTRIBUTORS

Research contributors who send reports for use in applications like FactSet Research Connect may FTP, SFTP, or email their reports as PDF or XML documents. Once these reports reach FactSet, they will be processed and made available to entitled clients through customized alerts, real-time updates, and client searches.

OTHER DATA CONTRIBUTIONS

FactSet has relationships with commercial content providers to integrate additional data sets for quantitative and fixed income analysis of custom risk models, portfolio simulations and much more. Speak with your FactSet representative to find out which content sets are available.

Moving Raw Data to FactSet: When moving files to FactSet, we recommend that you initiate the connection to FactSet (a client-initiated connection) and upload the files as soon as they are available. If FactSet is going to connect to you (a FactSet-initiated connection), we will poll for specifically named files once every 15 minutes for up to one hour until the files are successfully retrieved.

Choosing the Best Protocol for Your File Transfer Needs: FactSet recommends using SFTP to securely transmit all sensitive and proprietary data. If any of your file transfers contain information you wish to protect, SFTP should be used at all times to ensure that communication is encrypted. When choosing SFTP, there are several options for authentication:

- Key-only
- Password-only
- Key and password

ABOUT KEY-BASED ENCRYPTION

SFTP and PGP both use public-key cryptography as a means to encrypt data. This works by creating a key pair comprised of a public and private key. Anyone can use a public key to encrypt data, but only the owner of the private key can decrypt it.

FactSet FTS support for SFTP:

- SSHv2, SCP2, and SFTP (pre-RFC v3)
- SSH2 and OpenSSH key formats
- RSA and DSA keys 1024+ bits (FTS uses a 2048-bit RSA host key)
- Most modern encryption, hash, and compression algorithms

If you are sending or receiving large uncompressed files, FactSet recommends creating a compressed zip archive to use in the transmission, as this will often greatly decrease the amount of time needed to complete the transfer. Password protected zip files are not supported by FactSet. Please note that an account can only be configured for a single protocol and authentication option at any given time. This means that accounts cannot be configured to support simultaneous FTP and SFTP access. This also means that accounts enabled for SFTP will be restricted to using only a single authentication method. If you have any questions when choosing a suitable protocol and authentication method, please contact your FactSet specialist for guidance.

FactSet Server Details:

FactSet's file transfer infrastructure supports connections over the internet via FTP and SFTP protocols. FactSet's recommendation is to push files to our servers which allows for the most timely job scheduling and file processing. However, it's also possible for FactSet to retrieve files from your infrastructure at a fixed time each day.

Method	Internet
Hostnames	fts.factset.com (FTP) fts-sftp.factset.com (SFTP)
IP Address Ranges	64.209.89.0/24, 192.234.235.0/24
FTP Port	21,20
SFTP Port	6671

Please permission the firewalls in your production environment for the IP address ranges and ports listed above. The IP ranges are for both client-initiated and FactSet-initiated connections. The ports listed are for client-initiated connections to FactSet only. Additional port permissions may be needed for FactSet-initiated transfers. If you have questions, please contact FactSet.

FTS Full Public Host Key (RSA 2048-bit, IETF SECSH Format) Client-Initiated SFTP Only

---- BEGIN SSH2 PUBLIC KEY ----

AAAAB3NzaC1yc2EAAAABIwAAAQEAx7vVeiK53RXlWwfx/Ajm-fkjr5AEeXzCMg4URy0Gc0HgzWqOMN3jooEu6DECv2rjmhcM/RT8iHomqcgvhCTxPgsh8ow1C6CUhSOWkVLjS3RL/S7HVJlFX-jmseF4R5zYRR5WPmBogZdqLh/2LiyWzWl0rka4XoMsQoAZ3N-w9DvLIB3ags7bAChBbWrGh4ez5ccsihPbcCZPbuMCwPeB9L3Y-P162KaFjZQ/CBcjGbWLp9jPb6rY8YJJTTDpjhod7EeOFsm/hqlsgD+cO4MRbH0nXlyhjmjwAGGHt3m57FLVRUy2gj3ttg1l/aX3Ww3Tj1SlgN/8DZoWWTqA2My3CVVf2w==

---- END SSH2 PUBLIC KEY ----

The fingerprint (MD5) of the FactSet public SSH host key: bc:37:d9:2a:15:93:3c:a6:a0:e9:88:5e:86:81:8d:43

SSH Key Details:

- Key Exchange: Before you perform connectivity testing, please send an email to cdis@factset.com that contains the full public SSH keys for all production systems that will connect to FTS
- Key Format: FTS supports OpenSSH and SSH2 key formats only
- Key Parameters: FTS uses an RSA 2048-bit SSH key by default but can support DSA or RSA keys of 1024 bits and above
- SSH Protocols: FTS supports SSHv2, SCP2, and SFTP (pre-RFC v3)

File Retention Policy Most user accounts on FTS are subject to a file retention policy of 30 days. Files uploaded to some accounts, such as research contributors, may be deleted from FTS immediately after being moved to backend systems.

IP ADDRESS RESTRICTIONS

For additional security, connectivity to FactSet's FTP and SFTP infrastructure is restricted to a defined range of IP addresses.

Managing IP Addresses:

You can whitelist ranges of IP addresses, view the past 30 days of FTP and SFTP for your organization's file transfer accounts, and view which, if any, connections are attempted outside your defined ranges. Contact your FactSet representative to obtain access to FactSet Control Center, if you do not already have it.

- Login to FactSet Control Center with your factset.net ID
- Expand **Security** section of the sidebar and select **File Transfers**

Whitelisting IP addresses:

This process will be required if you intend to transmit data directly to FactSet and should be updated whenever there is a change of IP address(es).

- Under **File Transfers** page, navigate to **New IP Range** section
- Fill in **Description** and **Range**, thereafter select **Add Rule**

FACTSET 〉 SEE THE ADVANTAGE

FACTSET FILE TRANSFER SYSTEM (FTS) QUESTIONNAIRE

This document will help FactSet specialists identify requirements and configure FTS to best suit your needs. FTS facilitates file transfers between FactSet's backend systems and outside sources and supports bi-directional FTP and SFTP with a number of different authentication options. While FactSet is fully capable of supporting PGP file encryption and decryption, FactSet strongly recommends the use of SFTP to protect your data transfers.

Contact Name: _____

Company Name: _____

Contact Phone Number: _____

Contact Email: _____

FactSet will contact this person once this form is received and the setup can proceed.

You may need to enable the Adobe JavaScript option if you are presented with a prompt.

Optional (if known)

FactSet Contact: _____

FactSet Account: _____

Purpose (e.g. portfolio uploads):

_____

_____

Please include your FactSet contact in emails, including this questionnaire response.

☐ **I would like to connect to FactSet…**

Choose One:

◯ SFTP – SSH (Secure) File Transfer Protocol
◯ FTP - FactSet will provide password via phone

Name and version of your file transfer client:

_____

_____

Choose One SFTP Authentication Option:

◯ Key-only (Please provide your full public key(s))
◯ Password-only *(FactSet will provide via phone)*
◯ Password and key *(Both steps above are necessary)*

PGP Encryption for FTP (Optional):

◯ FactSet will decrypt *(FactSet will provide a public key)*
◯ You will decrypt *(Please provide your public key)*

Files may also be signed for additional protection.

Full Public Key(s): _____
(SFTP and PGP Only): _____

You may be prompted to accept the FactSet public SSH key (host key). The fingerprint (MD5) of this key is

bc:37:d9:2a:15:93:3c:a6:a0:e9:88:5e:86:81:8d:43

☐ **I would like FactSet to connect to our server(s)…**

Choose One:

◯ SFTP – SSH (Secure) File Transfer Protocol
◯ FTP

Name and version of your file transfer server:

_____

_____

Choose One SFTP Authentication Option:

◯ Key-only (FactSet will provide a public key)
◯ Password-only *(Please provide to FactSet via phone)*
◯ Password and key *(Both steps above are necessary)*

PGP Encryption for FTP (Optional):

◯ FactSet will decrypt *(FactSet will provide a public key)*
◯ You will decrypt *(Please provide your public key)*

Files may also be signed for additional protection.

Primary Server
Account Name: _____
Address/Port: _____
Host Key (SFTP-Only): _____

Secondary Server
Account Name: _____
Address/Port: _____
Host Key (SFTP-Only): _____

Please provide your account password (if applicable) via phone.
Example: fts-sftp.factset.com#6671.

Once this form is complete, please contact your network/firewall team to ensure that your firewalls are properly configured.
Email completed form to your FactSet specialist.