

Frequently Asked Questions: SFTP Push Transfers

1. Who hosts the SFTP server, and who initiates the file transfer?

hMetrix hosts the SFTP server. The partner/client acts as the connecting entity and must utilize an SFTP PUSH method to upload files to our endpoint. Our systems will never query, pull, or grab files directly from your network.

2. What information must a partner provide before an account is provisioned?

To onboard, partners must complete the **FTS Partner Onboarding Document** and provide:

1. A 2048-bit RSA (or stronger) SSH Public Key for account authentication.
2. A **Static Source IP / Routing Range** so we can allow-list your servers in our AWS Firewalls/Security Groups.
3. Technical Point of Contact (PoC) details for troubleshooting.

3. What is the hostname for the SFTP server?

The hostname is files.hmetrix.com (IP 54.144.103.108).

4. What network port and protocols are required?

All connections must use **Native SFTP/SSH only** over **Port 22**. Standard FTP or FTPS protocols are not supported.

5. How is the partner's folder structure secured on our AWS backend?

We use a **Logical Home Directory mapping** mechanism via AWS Transfer Family. This architecture ensures absolute isolation. When a partner logs in, they are securely locked into a predefined root folder path labeled simply as */*. They cannot see our internal S3 bucket names, AWS paths, or any other partner folders.

6. What subdirectories should the partner use to transfer data?

Within their isolated root directory (*/*), partners are granted access to a standard subdirectory structure designed to separate data tiers:

1. **/Test:** Map initial onboarding connections, structural tests, and test file batches here. Files dropped in this folder validate end-to-end handshake syntax but bypass live production databases.
2. **/Inbound:** Route all official, live 837P/837I transaction sets or final production Flat Files to this directory for active processing.
3. **/Outbound:** Monitor this directory to pull automated data quality reports (DQR), structural validation exceptions, and transaction acknowledgments (TA1/999 for X12 submissions, or a response status CSV for Flat File submissions).

7. What are the expectations and testing patterns for the /Test folder?

The /Test directory is intended for validating end-to-end connectivity and file syntax. Partners are expected to successfully transmit sample files that mirror production volume and structure to verify full integration. All test batches must undergo validation against the expected schema to ensure structural compliance before any production data is routed. Once testing is successfully completed and confirmed, coordinate with hMetrix to transition to production workflows.

8. What file formats are accepted?

We accept **X12 Standard** (837P and 837I transaction sets) and **Flat File Standard** (pipe-delimited granular service lines). For further details, please refer to the Technical Submission Guidance: [EHN - CRISP](#)

9. Are there specific file compression requirements?

Yes, batch file compression is **mandatory**. Files must be compressed prior to transfer using one of the following formats: **.zip**, **.gz**, **.tar.gz**, or **.tgz**.

10. Are there volume limits on how many claims can be sent in a single file?

1. **X12 Submissions:** A single logical file must not contain more than 50,000 Transaction Sets (Claims/ST-SE envelopes).
2. **Flat File Submissions:** A single logical file must not exceed 50,000 line items, excluding headers.

11. Is there a maximum size cap for uncompressed data payloads?

Regardless of the actual claim count, the uncompressed size of any single file must not exceed 1000MB. For example, a 100MB compressed GZIP file that expands to over 5000MB

will be automatically rejected by the processing gateway for exceeding the uncompressed buffer threshold.

12. What should we do if our monthly transmission volume exceeds these thresholds?

You must split large monthly volumes into multiple smaller files. Keep in mind that 837P (Professional) and 837I (Institutional) transactions must be split separately. Each separate file must be compressed individually and named sequentially using the required format (e.g., _001_01, _002_01, _003_01).

13. What is the "Incomplete Ingestion Buffer" rule?

To prevent our backend automated processing engines from attempting to read a file while it is still actively uploading, our ingestion gateway filters out temporary files.

1. Files arriving with active transfer extensions (e.g., **.filepart**, **.tmp**, **.upload**) are isolated and ignored.
2. Partners must configure their transfer systems to upload using a temporary extension and then perform an **atomic rename** to a clean, finalized file extension (like **.zip**) once the transfer is completely finished.
3. The file name must be constructed using the following pattern:
[SENDERID]_[SUBMISSIONDATE]_[FILETYPE]_[SEQUENCE]_[VERSION].[EXTENSION].

14. Is additional data encryption required for sensitive files?

While SFTP secures the data in transit, the **OpenPGP encryption standard** is strongly suggested for all file transfers containing Protected Health Information (PHI) or Personally Identifiable Information (PII) to secure the data at rest. The standard practice is to compress the file first, then encrypt it. Our public PGP key can be requested from the onboarding team.

15. Who should partners contact if a transfer fails or credentials need to be updated?

For immediate connection troubleshooting, firewall issues, credential updates, or file delivery validation failures, partners should contact the centralized technical support queue directly at crisp.ehn.support@hmetrix.com.