# FDS manual

## File Delivery Services

SFTP file transfer

# Publisher

Post CH Ltd
IT
Webergutstrasse 12
CH-3030 Berne (Zollikofen)

# Contact

Post CH Ltd
IT
Webergutstrasse 12
CH-3030 Berne (Zollikofen)
IT17.34 FDS Operation
E-mail: fds@post.ch

Version 8.5 / January 2023

Download the latest version from: https://www.post.ch/fds

# Table of contents

# 1. Introduction

File Delivery Services (FDS) is a service provided by the IT service unit of Post CH Ltd.

FDS acts as a gateway in the IT security system between Swiss Post's Intranet and external networks. It enables files and applications to be exchanged among internal and external partners of Post CH Ltd.

This manual describes how files can be transferred via the FDS server of Post CH Ltd. The service is available to anyone who has a file transfer client installed on his or her computer and the required account.

Swiss Post IT assumes no responsibility for the accuracy of the information in this manual. Subject to errors and amendments.

# 2. Swiss Post FDS model

## 2.1 Overview

FDS was introduced in 1993. It was launched in the context of the data transmission and communication project of the then PostFinance organisation. The first files were transferred via Kermit, FTP and FTAM. In 1995, the service was extended for file transfer with CONNECT:Direct™. In 2002, FDS was expanded to include the FDS-SSH system (FTP over SSH sometimes called Secure FTP), while the FTAM and Kermit protocols were discontinued.

SFTP (SSH File Transfer Protocol) was introduced in 2007 and marked the change to a new technology and a new generation. The FDS-SSH service became obsolete as a result and, as of mid-2010, was no longer continued.

The use of the protocol FTP over the internet is disallowed for security reasons for new customers since June 2015. Existing customers have migrated to the protocol SFTP since December 2018.

## 2.2 Supported protocols

- SFTP (SSH File Transfer Protocol)

## 2.3 Connection types

Three types of connections are available:

- Internet
- MPLS/IPSS — leased connections, IPSS Swisscom network
- Intranet — for Post CH Ltd internal partners/applications

The installation dates of the network provider have to be taken into consideration when coordinating new-leased connections and MPLS. Leased connections are only used if another type of connection is more expensive than a leased connection, or in the event that special security requirements make them necessary. ADSL connections are only possible in combination with a provider via the Internet. The use of SFTP makes the utilisation of leased lines and VPN unnecessary, as both do not offer additional security.

# 3. FDS service

## 3.1 File Delivery System

The file delivery system is based on a special mail-boxing system, which accommodates the tightened security requirements that pertain to the Internet, extranet and intranet.

## 3.2 Where are the file delivery services?

FDS constitutes an application server, database server and several perimeter servers. All of the components are located in different zones (DMZ) of the IX platform. The IX platform is a security zone protected by firewalls and is located between the Post CH Ltd network (Intranet) and the external networks (Internet, leased connections). The file transfer and database servers are located in a highly protected zone: access to this zone is highly restricted. The perimeter servers are in zones of lesser security, in which access via clients is permitted. The client/server connections from external networks and from the internal Post CH Ltd network always run via the perimeter servers. The FDS service is geographically redundant and is configured to remain available even after the complete outage of one data center.

## 3.3 File Transfer Protocols

For more detailed information please consult our "file transfer clients manual" on https://www.post.ch/fds

### 3.3.1 SFTP

SFTP (SSH Secure File Transfer Protocol) is a safe file transfer protocol. An uninterrupted, encrypted connection is established between the client and the server and renders data, usernames and passwords illegible to attackers. The integrity and privacy of the exchanged files is ensured via public-key authentication. Public-key authentication enables clients to log in to the server without any user interaction. SSH guarantees that data is transmitted from the sender to the recipient in full and unchanged. Only SSH-2 (version 2) is supported, exclusively in combination with public-key authentication.

With an **SFTP** client, a connection with the FDS SFTP server can be established and the necessary commands executed.

Please note: SFTP should not be confounded with FTPS (FTP over SSL) or FTP over SSH (sometimes called SecureFTP).

## 3.4 Delivery and collection from an external server

If the FDS server is required to deliver files or collect them from the customer, a number of requirements will need to be fulfilled. These prerequisites are listed in chapter 6 .

Delivery and distribution of a file takes place in an events-based manner. When the file arrives, it is forwarded by the FDS server to the pre-specified destination. Specification of a certain time for the action to be executed is not possible.

## 3.5 Using the File Delivery Service

Administrative registration to use the FDS service is via the customer services of the service unit or business unit of Post CH Ltd.

By urgent problems, you can contact our hotline: +41 (0)848 800 030
For queries with regard to the File Delivery Services, please use the following e-mail address: fds@post.ch

# 4. Security

## 4.1 User name (login)

External participants receive their own username for the respective service and business unit. If a customer uses the same username for several business units of his company, Post CH Ltd assumes no liability for any damage that is incurred. This refers to damage that could occur in the event of data subsequently being accessed on Post CH Ltd.'s file transfer server.

## 4.2 Link encryption

Link encryption is not a standard service provided by the FDS services. However, it can be used as a network option. The use of SFTP with an adequate key length makes the utilisation of a link encryption unnecessary, as it does not offer additional security.

### 4.2.1 For all connection types

Client-to-server encryption is provided via the SFTP protocol and is available for all connection types.

### 4.2.2 MPLS/IPSS

Link encryption is also supported by MPLS/IPSS.

### 4.2.3 LAN-LAN

With LAN-LAN connections, link encryption can be established with both routers.

# 5. Configurations

## 5.1 FDS client-server configuration

### 5.1.1 File transfer server

| Zone | Host name |
|---|---|
| Internet and leased lines | fdsbc.post.ch |
| Post CH network/DMZ | fdsbc.pnet.ch |

The distribution of the communications on two locations is accomplished with a DNS load balancing (Round-Robin). This means that, alternately, the IP addresses of the two locations are returned.

It must be ensured that the communication to or from FDS is allowed in your network. Usually the network team has to allow the communication with the appropriate firewall rules. Two IP addresses are used. Those IP addresses may only be used for the configuration of the firewall rules. For the connection to FDS from your application, it is essential that you use the domain name.

**Both IP addresses can be determined with several DNS lookup requests.**

FDS supports IPv4 and IPv6. The use of IPv6 requires a continuous support of IPv6 in your infrastructure.

### 5.1.2 DNS caching

The FDS service is operating in active/active mode on two locations. The failover mechanism is guaranteed by a Global Server Load Balancing (GSLB) infrastructure. In order for you to benefit quickly from this failover mechanism, you must ensure that no additional DNS caching is done in your environment. The Time to live (TTL) specification given from the Post CH DNS has to be respected.

### 5.1.3 Ports

The FDS SFTP server is running on standard port 22.

### 5.1.4 User name (login)

Usernames are defined and communicated to the customers during the initiation of the service.

### 5.1.5 Directories

The name of the directories on the FDS server are always written in small letters with the following restrictions

- Characters: [ a-z ], [ 0-9 ], [ . - ] ( dot, hyphen)
- Start: the first character has to be [ a-z ], [ 0-9 ]

### 5.1.6 File names

The following guidelines must be observed for the names of files in the directories on the FDS server:

- Characters: [ A-Z ], [ a-z ], [ 0-9 ], [ . - _ ] (dot, hyphen, underscore)

## 5.2 SFTP

### 5.2.1 General information

Detailed information can be found in our “file transfer clients manual” on https://www.post.ch/fds

### 5.2.2 Send public key to Post CH Ltd

A copy of the public key has to be sent to Post CH Ltd by e-mail at fds@post.ch. To verify the identity of the sender, the e-mail has to be sent by the registered contact person or this one has to appear at the least as cc in the e-mail exchange.

If needed, there is the possibility to configure more than one public key for one username. Likewise, different usernames may use the same key if needed.

The length of the generated SSH key must be at least **4096** bits.

### 5.2.3 Dealing with keys

Treat your private key like your personal credit card! Protect it against unauthorised access.

# 6. Annex A. Information about using FDS

The following succinct information describes how data is exchanged and details the FDS functions. It lays down the generally applicable rules and stipulations for transmitting files via the FDS file transfer servers. It is intended for FDS users in business units and Group companies of Post CH Ltd and their external customers.

### 6.1 General terms and conditions/restrictions

a) FDS is not an archiving system. Collected files, which the customer has not yet deleted, are removed automatically by the server after a period of 9 days.

b) Each file can be downloaded maximum 20 times.

c) FDS follows a 1-minute processing rhythm. Delivered files appear 1 minute after completion of the file transfer in the recipient's mailbox. If the configuration requires that the files are forwarded to a target computer, the process can take longer depending on the size and the number of the files.

d) Large files (usually ASCII files) must be transmitted in a compressed form. The sender and recipient (end-to-end) shall agree on the compression method (e.g. ZIP, GZIP).

e) A large number of files has to be transmitted with a correspondingly large number of file transfers (put/get) per FTP/SFTP login session. Example for 1200 files: 10 FTP connections/logins composed of 120 file transfers each. If the number of logins is too big within a certain unit of time, the Intrusion Prevention System of Post CH Ltd automatically blocks the Source IP address during 15 minutes.

f) FDS does not confirm the file transfer with regard to the sender. Creation and sending confirmation is the responsibility of the recipient and is not ensured by FDS.

g) If the file transfer involves data being forwarded, no order of transmission can be guaranteed. Files of different sizes can overtake each other if the data transmissions are taking place at the same time. The recipient system in the end-to-end relation is responsible for restoring the correct order of the transmitted files.

h) Forwarding and distributing files is performed in an event-based manner. Time-scheduled management is not supported.

i) IT must be notified in good time about the size, frequency and changes in volume of files involved in file transfers that are performed via the FDS server. This is the only way to ensure that the required capacity is made available at the requested time.

j) IT must be informed about priorities for all file transfers that are performed via the FDS server and that must be adhered to in the event of escalation. Standard SLA comes into effect in all other cases.

### 6.2 Restrictions in data delivery (Client → FDS server)

- When a file transfer client carries out an upload function (put) to an FDS mailbox (folder), the files from these processes are attended to on the FDS server as soon as the file transfer has been completed. Entries in the files in the upload mailboxes remain visible to the customer for two minutes (display of files via "dir" and "ls"). **Deleting or renaming a sent file will have no effect: this file is forwarded to the recipient under its original file name.**
- FDS guarantees that only completely transferred file will be processed. In case of a breakup of the connection during transfer the partially transferred file will be rejected.
- It is not possible to change a file attribute on FDS after the file transfer.

### 6.3 Data delivery requirements (FDS server → target system)

To enable the FDS service to deliver files, the following requirements must be in place at both the internal and external Post CH Ltd recipients:

– Permanent network connections such as WAN Access (MPLS) or Internet
– The system must be available 24/7
– Operative Computer Centre operation must be ensured

– Contact persons for support (phone numbers, e-mail) and availability must be ensured.

### 6.4 Requirements and restrictions in data collection on third-party systems

FDS is able to collect files automatically via FTP and SFTP on third-party systems.
This function should only be used in exceptional cases.

**Requirements:**
– Permanent network connections such as WAN Access (MPLS) or Internet
– The system must be available 24/7
– Operative Computer Centre operation must be ensured
– Contact persons for support (phone numbers, e-mail) and availability must be ensured.

**Restrictions:**
– This service is not offered if time-critical data have to be collected at intervals shorter than 30 minutes.
– The files to be downloaded have to be placed in directories having invariable names. FDS does not support the download of files from variable directories (e.g. directories names which contain the actual date).

# 7. Annex B. Glossary

| | | |
|---|---|---|
| **D** | DMZ | Demilitarised Zone – A DMZ is located at a separate LAN connection in the firewall between an internal network and an insecure network, e.g. the Internet. Servers that provide services for users of the Internet (e.g. www or e-mail) are often set up in a DMZ. Ideally the DMZ is between two physically separated firewalls. The outer firewall protects against attacks from outside and monitors all attempts to access the DMZ from the Internet. The inner firewall checks attempts to access the internal network from the DMZ and vice versa. It represents the second line of defence in case the outer firewall is penetrated. The advantage of this is that the internal network continues to be protected even if an attacker gets through to the web server. |
| | DNS | The Domain Name System (DNS) is one of the most important services on the Internet. Its main task is to translate "Internet addresses" names into the respective IP address. |
| **E** | End-to-end | The relation between an application (e.g. EGA-B) of a business unit at Post CH Ltd (e.g. PostFinance Ltd) and the application belonging to the external customer. |
| **F** | FDS | File Delivery Services is a service provided by the Post CH Ltd Information Technology (IT) service unit. FDS acts as a proxy in the IT security system between Post CH Ltd's Intranet and external networks. It enables files and applications to be exchanged among internal and external partners of Post CH Ltd. |
| | FTP | File Transfer Protocol is a network protocol specified in RFC 959 from 1985 to transfer files across TCP/IP networks. The protocol enables files to be exchanged between different computers, regardless of their operating system and physical location. |
| **I** | IPSS | LAN Interconnect over IPSS is a service provided by Swisscom. It connects local networks to form a single corporate-wide communication infrastructure. IPSS is Swisscom's own solution and applies cutting-edge technology. The MPLS technology applied here (Multi Protocol Label Switching) enables greater flexibility with respect to the bandwidth. The service is provided completely by Swisscom Enterprise Solution. http://www.swisscom.com/es/ |
| **M** | MPLS | Multi Protocol Label Switching (MPLS) is an implementation of Label Switching. These technique takes the burden off the routers involved in transporting a data package, as the level of complexity is reduced to a single switch. The aim here is to establish a specific connection channel at the beginning of the data transmission. In this process the routers no longer need to check the recipients of the data packages being forwarded, instead they simply forward the packages in accordance with the previously specified connection, without any further processing. |
| **S** | SFTP | SSH File Transfer Protocol (SFTP) is a further development of SCP and enables secure data transmission and allows clients to access files on remote systems. The protocol has no authentication procedure or any encryption. These functions have to be taken over the underlying SSH protocol. SFTP should not be confused with Secure FTP or with FTP over SSL. |
| | SSH | SSH enables cryptographically secure communication in insecure and secure networks. It provides a high level of security. Reliable mutual authentication of the partners as well as integrity and privacy of the exchanged data is supported. SSH guarantees the complete and unchanged transmission of the data from the sender to the recipient. |
| **T** | Time to live | Time to Live (TTL) is a mechanism that limits the lifespan or lifetime of data in a computer or network. TTL may be implemented as a counter or timestamp attached to or embedded in the data. Once the prescribed event count or timespan has elapsed, data is discarded |