---

title: Hosting your own XFTP Server

revision: 31.07.2023

Hosting your own XFTP Server

Overview

XFTP is a new file transfer protocol focussed on meta-data protection - it is based on the same principles as SimpleX Messaging Protocol used in SimpleX Chat messenger:

- asynchronous file delivery - the sender does not need to be online for file to be received, it is stored on XFTP relays for a limited time (currently, it is 48 hours) or until deleted by the sender.
- padded e2e encryption of file content.
- content padding and fixed size chunks sent via different XFTP relays, assembled back into the original file by the receiving client.
- efficient sending to multiple recipients (the file needs to be uploaded only once).
- no identifiers or ciphertext in common between sent and received relay traffic, same as for messages delivered by SMP relays.
- protection of sender IP address from the recipients.

Installation

1. First, install `xftp-server`:
    - Manual deployment (see below)
    - Semi-automatic deployment:
        - Offical installation script
        - Docker container

Manual installation requires some preliminary actions:

1. Install binary:
    - Using offical binaries:

      ```
      sh curl -L https://github.com/simplex-chat/simplexmq/
      releases/latest/download/xftp-server-ubuntu-20_04-x86-64
      -o /usr/local/bin/xftp-server
      ```

    - Compiling from source:

      Please refer to Build from source: Using your distribution

2. Create user and group for `xftp-server`:

   ```
   sh sudo useradd -m xftp
   ```

3. Create necessary directories and assign permissions:

   ```
   sh sudo mkdir -p /var/opt/simplex-xftp /etc/opt/simplex-xftp
   /srv/xftp sudo chown xftp:xftp /var/opt/simplex-xftp /etc/
   opt/simplex-xftp /srv/xftp
   ```

4. Allow xftp-server port in firewall:

   ```sh

   # For Ubuntu

   sudo ufw allow 443/tcp

   # For Fedora

   sudo firewall-cmd --permanent --add-port=443/tcp && \ sudo firewall-cmd --reload ```
   ```

5. **Optional** — If you're using distribution with `systemd`, create `/etc/systemd/system/xftp-server.service` file with the following content:

   ```sh [Unit] Description=XFTP server systemd service

   [Service] User=xftp Group=xftp Type=simple ExecStart=/usr/local/bin/xftp-server start +RTS -N -RTS ExecStopPost=/usr/bin/env sh -c '[ -e "/var/opt/simplex-xftp/file-server-store.log" ] && cp "/var/opt/simplex-xftp/file-server-store.log" "/var/opt/simplex-xftp/file-server-store.log.$(date +'%FT%T')"' LimitNOFILE=65535 KillSignal=SIGINT TimeoutStopSec=infinity AmbientCapabilities=CAPNETBIND_SERVICE

   [Install] WantedBy=multi-user.target ```

   And execute `sudo systemctl daemon-reload`.

## Tor installation

xftp-server can also be deployed to serve from tor network. Run the following commands as `root` user.

1. Install tor:

   We're assuming you're using Ubuntu/Debian based distributions. If not, please refer to offical tor documentation or your distribution guide.

   - Configure offical Tor PPA repository:
   ```

```
sh CODENAME="$(lsb_release -c | awk '{print $2}')" echo
"deb [signed-by=/usr/share/keyrings/tor-archive-
keyring.gpg] https://deb.torproject.org/torproject.org $
{CODENAME} main deb-src [signed-by=/usr/share/keyrings/
tor-archive-keyring.gpg] https://deb.torproject.org/
torproject.org ${CODENAME} main" > /etc/apt/
sources.list.d/tor.list
```

- Import repository key:

```
sh curl --proto '=https' --tlsv1.2 -sSf https://
deb.torproject.org/torproject.org/
A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89.asc | gpg --
dearmor | tee /usr/share/keyrings/tor-archive-
keyring.gpg >/dev/null
```

- Update repository index:

```
sh apt update
```

- Install `tor` package:

```
sh apt install -y tor deb.torproject.org-keyring
```

2. Configure tor:

- File configuration:

  Open tor configuration with your editor of choice (`nano`,`vim`,`emacs`,etc.):

  ```
  sh vim /etc/tor/torrc
  ```

  And insert the following lines to the bottom of configuration. Please note lines starting with #: this is comments about each individual options.

  ```sh
  # Enable log (otherwise, tor doesn't seemd to deploy onion address)
  ```

  Log notice file /var/log/tor/notices.log

Enable single hop routing (2 options below are dependencies of third). Will reduce latency in exchange of anonimity (since tor runs alongside xftp-server and onion address will be displayed in clients, this is totally fine)

SOCKSPort 0 HiddenServiceNonAnonymousMode 1 HiddenServiceSingleHopMode 1

xftp-server hidden service host directory and port mappings

HiddenServiceDir /var/lib/tor/simplex-xftp/ HiddenServicePort 443 localhost:443 ```

- Create directories:

  ```
  sh mkdir /var/lib/tor/simplex-xftp/ && chown debian-tor:debian-tor /var/lib/tor/simplex-xftp/ && chmod 700 /var/lib/tor/simplex-xftp/
  ```

3. Start tor:

   Enable `systemd` service and start tor. Offical `tor` is a bit flunky on the first start and may not create onion host address, so we're restarting it just in case.

   ```
   sh systemctl enable tor && systemctl start tor && systemctl restart tor
   ```

4. Display onion host:

   Execute the following command to display your onion host address:

   ```
   sh cat /var/lib/tor/simplex-xftp/hostname
   ```

Configuration

To see which options are available, execute `xftp-server` without flags:

```sh sudo su xftp -c xftp-server

... Available commands: init Initialize server - creates /etc/opt/simplex-xftp and /var/opt/simplex-xftp directories and configuration files start Start server (configuration: /etc/opt/simplex-xftp/file-server.ini) delete Delete configuration and log files

```

You can get further help by executing `su xftp -c "xftp-server <command> -h"`

After that, we need to configure `xftp-server`:

```sh sudo su xftp -c "xftp-server init -h"

... Available options: -l,--store-log Enable store log for persistence -a,--sign-algorithm ALG Signature algorithm used for TLS certificates: ED25519, ED448 (default: ED448) --ip IP Server IP address, used as Common Name for TLS online certificate if FQDN is not supplied (default: "127.0.0.1") -n,--fqdn FQDN Server FQDN used as Common Name for TLS online certificate -p,--path PATH Path to the directory to store files -q,--quota QUOTA File storage quota (e.g. 100gb) -h,--help Show this help text ```

You should determine which flags are needed for your use-case and then execute `xftp-server init`:

```
sh sudo su xftp -c "xftp-server init -<your flag> <your option>"
```

For example, run:

```
sh sudo su xftp -c "xftp-server init -l --ip 192.168.1.5 -q '20gb' -p /srv/xftp/"
```

to initialize your `xftp-server` configuration with:

- restoring connections when the server is restarted (`-l` flag),
- IP address `192.168.1.5` (`--ip` flag),
- set overall storage quota to 10Gb (`-q` flag),
- store files in `/srv/xftp` directory (`-p` flag).

To password-protect your `xftp-server`, change it in the configuration:

1. Open configuration with:

   ```
   sh sudo su xftp -c "vim /etc/opt/simplex-xftp/file-server.ini"
   ```

2. Under `[AUTH]` section uncomment `create_password` and change it:
   ```

```sh ... [AUTH] # Set newfiles option to off to completely prohibit uploading new files. # This can be useful when you want to decommission the server, but still allow downloading the existing files. newfiles: on

# Use createpassword option to enable basic auth to upload new files. # The password should be used as part of server address in client configuration: # xftp://fingerprint:password@host1,host2 # The password will not be shared with file recipients, you must share it only # with the users who you want to allow uploading files to your server. createpassword: yourverysecure_password ...

```

After that, your installation is complete and you should see in your teminal output something like this:

```sh Certificate request self-signature ok subject=CN = 192.168.1.5 Server initialized, you can modify configuration in /etc/opt/simplex-xftp/file-server.ini.

# Run `file-server start` to start server.

You should store CA private key securely and delete it from the server. If server TLS credential is compromised this key can be used to sign a new one, keeping the same server identity and established connections. CA private key location:

# /etc/opt/simplex-xftp/ca.key

SimpleX XFTP server v0.1.0 Fingerprint: ioyYeRyy4SqJkNvb7nM04MuLasOM4c-acVyVnqw248= Server address: xftp://ioyYeRyy4SqJkNvb7nM04MuLasOM4c-acVyVnqw248=@ ```

The server address above should be used in your client configuration and if you added server password it should only be shared with the other people when you want to allow them to use your server to upload files. If you passed IP address or hostnames during the initialisation, they will be printed as part of server address, otherwise replace `&lt;hostnames&gt;` with the actual server addresses.

# Documentation

All necessary files for `xftp-server` are located in `/etc/opt/simplex-xftp/` folder.

Stored messages, connections, statistics and server log are located in `/var/opt/simplex-xftp/` folder.
```

Location of uploaded files is configured by the user. In our guide we're using `/srv/xftp/`

XFTP server address

XFTP server address has the following format:

```
xftp://
<fingerprint>[:<password>]@<public_hostname>[,<onion_hostname>]
```

- `<fingerprint>`

  Your `xftp-server` fingerprint of certificate. You can check your certificate fingerprint in `/etc/opt/simplex-xftp/fingerprint`.

- **optional** `<password>`

  Your configured password of `xftp-server`. You can check your configured pasword in `/etc/opt/simplex-xftp/file-server.ini`, under `[AUTH]` section in `create_password:` field.

- `<public_hostname>`, **optional** `<onion_hostname>`

  Your configured hostname(s) of `xftp-server`. You can check your configured hosts in `/etc/opt/simplex-xftp/file-server.ini`, under `[TRANSPORT]` section in `host:` field.

Systemd commands

To start `xftp-server` on host boot, run:

```sh sudo systemctl enable xftp-server.service

Created symlink /etc/systemd/system/multi-user.target.wants/xftp-server.service → /etc/systemd/system/xftp-server.service. ```

To start `xftp-server`, run:

```
sh sudo systemctl start xftp-server.service
```

To check status of `xftp-server`, run:

```sh sudo systemctl status xftp-server.service

● xftp-server.service - XFTP server systemd service Loaded: loaded (/etc/systemd/system/xftp-server.service; enabled; vendor preset: enabled) Active: active (running) since Sat 2023-03-11 13:11:55 UTC; 1 months 10 days ago Main PID: 110770 (xftp-server) Tasks: 14 (limit: 4611) Memory: 2.4G CGroup: /system.slice/xftp-server.service └─110770 /usr/local/bin/xftp-server start +RTS -N -RTS

Feb 27 19:21:11 localhost systemd[1]: Started XFTP server systemd service. Feb 27 19:21:11 localhost xftp-server[2350]: SimpleX XFTP server v0.1.0
```
```

Feb 27 19:21:11 localhost xftp-server[2350]: Fingerprint: ioyYeRyy4SqJkNvb7nM04MuLasOM4c-acVyVnqw248= Feb 27 19:21:11 localhost xftp-server[2350]: Server address: xftp://ioyYeRyy4SqJkNvb7nM04MuLasOM4c-acVyVnqw248=@ Feb 27 19:21:11 localhost xftp-server[2350]: Store log: /var/opt/simplex-xftp/file-server-store.log Feb 27 19:21:11 localhost xftp-server[2350]: Uploading new files allowed. Feb 27 19:21:11 localhost xftp-server[2350]: Listening on port 443... Feb 27 19:21:11 localhost xftp-server[2350]: [INFO 2023-02-27 19:21:11 +0000 src/Simplex/FileTransfer/Server/Env.hs:85] Total / available storage: 64424509440 / 64424509440 ```

To stop `xftp-server`, run:

```
sh sudo systemctl stop xftp-server.service
```

To check tail of `xftp-server` log, run:

```sh sudo journalctl -fu xftp-server.service

Feb 27 19:21:11 localhost systemd[1]: Started XFTP server systemd service. Feb 27 19:21:11 localhost xftp-server[2350]: SimpleX XFTP server v0.1.0 Feb 27 19:21:11 localhost xftp-server[2350]: Fingerprint: ioyYeRyy4SqJkNvb7nM04MuLasOM4c-acVyVnqw248= Feb 27 19:21:11 localhost xftp-server[2350]: Server address: xftp://ioyYeRyy4SqJkNvb7nM04MuLasOM4c-acVyVnqw248=@ Feb 27 19:21:11 localhost xftp-server[2350]: Store log: /var/opt/simplex-xftp/file-server-store.log Feb 27 19:21:11 localhost xftp-server[2350]: Uploading new files allowed. Feb 27 19:21:11 localhost xftp-server[2350]: Listening on port 443... Feb 27 19:21:11 localhost xftp-server[2350]: [INFO 2023-02-27 19:21:11 +0000 src/Simplex/FileTransfer/Server/Env.hs:85] Total / available storage: 64424509440 / 64424509440 ````

## Monitoring

You can enable `xftp-server` statistics for `Grafana` dashboard by setting value `on` in `/etc/opt/simplex-xftp/file-server.ini`, under `[STORE_LOG]` section in `log_stats:` field.

Logs will be stored as `csv` file in `/var/opt/simplex-xftp/file-server-stats.daily.log`. Fields for the `csv` file are:

```
sh
fromTime,filesCreated,fileRecipients,filesUploaded,filesDeleted,dayCount,w
```

- `fromTime` - timestamp; date and time of event
- `filesCreated` - int; chunks created
- `fileRecipients` - int; number of file chunks recipients
- `filesUploaded` - int; chunks uploaded
- `filesDeleted` - int; chunks deleted
```

- `dayCount` - int; uploaded chunks in a day
- `weekCount` - int; uploaded chunks in a week
- `monthCount` - int; uploaded chunks in a month
- `fileDownloads` - int; chunks downloaded
- `filesCount` - int; count of stored file chunks
- `filesSize` - int; total size of uploaded file chunks

To import `csv` to `Grafana` one should:

1. Install Grafana plugin: Grafana - CSV datasource
2. Allow local mode by appending following:

   ```
   sh [plugin.marcusolsson-csv-datasource] allow_local_mode = true
   ```

   ... to `/etc/grafana/grafana.ini`
3. Add a CSV data source:
   - In the side menu, click the Configuration tab (cog icon)
   - Click Add data source in the top-right corner of the Data Sources tab
   - Enter "CSV" in the search box to find the CSV data source
   - Click the search result that says "CSV"
   - In URL, enter a file that points to CSV content
4. You're done! You should be able to create your own dashboard with statistics.

For further documentation, see: CSV Data Source for Grafana - Documentation

Configuring the app to use the server

Please see: SMP Server: Configuring the app to use the server.