FileSender Technical Questions and Answers

This document covers more technical Q&A:

1. What reporting is available for FileSender users?
2. How to use FileSender from the command line?
3. How to use the FileSender API?
4. How to clear FileSender logs and stored information?
5. How to delete your FileSender account?
6. How does FileSender encrypt files?

1) What reporting is available for FileSender users?

REANNZ institutions and organisations who are FileSender users can request reports from the REANNZ engagement team (engagement@reannz.co.nz). These reports include:

- the number of files uploaded and their total size (in bytes)
- the number of files downloaded and their total size (in bytes)
- a time series showing data from the past 30 days or a selected time range
- a list of the top downloaders, broken down by country, file size, and number of files downloaded
- upload stats for external users (outside your organization)
- upload stats for guests using vouchers, categorized by location
- upload stats for users uploading files with guest vouchers.

2) How to use FileSender from the command line?

You can use a command line Python script to send files and folders with FileSender. You'll need:

- The command line tool
- Your API key
- Configuration for the command line tool. This is optional; it is a custom file that includes the FileSender URL, your username, and your API key.

Prerequisites

To use the FileSender command line tool, you will need to have Python 3 installed on your device. Download the latest version from the Python site or install Python directly from your Operation System if available.

Download and set up the FileSender command line tool

1. Log on to FileSender in a web browser and click **My Profile** in the top navigation menu.
2. Scroll down to Python CLI Client.
3. Right click Download Python CLI Client and click Save Link As… or Download Linked File, depending on your browser.
4. Create a folder on your device to keep the command line tool in.
5. Go to your downloads folder, find the **filesender.py** file you downloaded earlier, and copy it to the new folder.
6. If you want to use FileSender's default client configuration – recommended so that you can avoid specifying every parameter in every command:

a. Create a subfolder called .filesender

- For Windows, create this in your user folder, typically found on C:/Users/[your local username]
- For macOS, create this in your user folder, typically found on /Users/[your local username]
- For Linux, create this in your user folder, typically found on /home/[your local username] Users/[your local username]

b. Under Python CLI Client, right click Download Python CLI Client configuration and click Save Link As… or Download Linked File, depending on your browser.

c. Go to your downloads folder, find the **filesender.py.ini** file downloaded, and copy it to the new .filesender folder.

3) How to use the FileSender API?

Prerequisites

To use the FileSender API, you'll need your unique API key. To retrieve your API key:

1. Click **My Profile** on the side navigation panel.
2. Copy the long string displayed under **API secret**.

If you have not previously created an API secret, click **New API secret** and

agree to the Acceptable Use Policy for remote authentication.
If you want to delete your current API secret, click **Clear API secret**.

Host URL

The host URL for the FileSender API is https://filesender.reannz.co.nz/rest.php

API documentation

You can find the documentation for FileSender's API at https://docs.filesender.org/filesender/v3.0/rest/.

Please note that this is an external website; not administered by REANNZ.

Sample API scripts

Example scripts can be found here: https://github.com/filesender/filesender/tree/master3/scripts/client. Please note that this is an external website; not administered by REANNZ.

4) How to clear FileSender logs and stored information?

Clear logs

To remove all transfer logs from the FileSender system:

1. Log in to FileSender in a web browser.
2. Click **My Profile** in the top navigation menu.
3. Scroll down to **Logs** under **Actions**.
4. Click **Clear logs**.

Clear email address autofill

FileSender will suggest to autofill email addresses while you are typing based on those you've previously sent files to. To reset this feature:

1. Log in to FileSender in a web browser.
2. Click **My Profile** in the top navigation menu.
3. Scroll down to **Saved information** under **Actions**.
4. Click **Clear recipient emails**.

Clear stored transfer options

FileSender will default to the same options you used on your previous send. To reset this feature:

1. Log in to FileSender in a web browser.
2. Click **My Profile** in the top navigation menu.
3. Scroll down to **Saved information** under **Actions**.
4. Click **Clear transfer settings**.

5) How to delete your FileSender account?

If you no longer need your FileSender account profile or want to delete all of your data associated with it, you can use the **Delete my account** feature.

Note: *using this feature will not affect your institution account or remove your access to FileSender. All of the data you have stored in FileSender will be removed, including active transfers, information about past transfers, FileSender vouchers, and logs.*

Delete your account

1. Log in to FileSender in a web browser.
2. Click **My Profile** in the top navigation menu.
3. Scroll down and click **Delete my account**.
4. Click **OK**.

   You will then be logged out of FileSender.

Note: *If you want to use FileSender again, you can log back in and a new FileSender account will be created for you.*

6) How does FileSender encrypt files?

The FileSender application has two main parts:

- The script that runs in your browser. This is responsible for setting up file uploads and downloads, encryption, and password generation.
- The server application. This stores your files and sends invitations to people you want to share them with.

This allows FileSender to separate out any encryption-related activities from file storage. This has the following benefits:

- The server doesn't see exactly what the browser-based script does to encrypt your files. Hacking attacks on the server are pointless; if someone gained access to the FileSender server, they might be able to access your encrypted files – but they'd have no data available on how to decrypt them, because the FileSender server doesn't know how.
- If the files are intercepted in transit – for example, if your Wi-Fi network is compromised – then they're already encrypted while they're moving. This means that any interceptors can't decrypt your files.
- Separating the file encryption and decryption functions from storage helps to keep your files safer.

Encryption used

FileSender supports full end-to-end encryption using AES-GCM with PBKDF2 to protect the integrity of encrypted files. This ensures the information you encrypt is exactly the same when it is decrypted. Once data is encrypted in your browser, it cannot be intercepted and modified without FileSender detecting the change when it decrypts the files and halting the process.

Note: If you've enabled encryption when sending files, you must record the password that you used. FileSender uses this to encrypt the files, and without it, the recipient won't be able to read the files. If you lose this password, your only option is to resend the files; REANNZ Support cannot help you to decrypt the files.

How it works

You can send one or more encrypted files in FileSender.

Upload:

- Add files to FileSender in your browser window.

- Specify an encryption password.
- FileSender encrypts the files before it reaches the server.
- Your browser uploads the encrypted files to the FileSender server.

Password communication:

- Manually send the encryption password to the person who needs to download the files.

Download:

- Visit the unique file link provided by FileSender or the person who uploaded the files.
- Enter the encryption password.
- Your browser downloads the encrypted files.
- FileSender decrypts the files in your browser and checks them.
- Your browser saves the decrypted files to your device.

Create a password

FileSender can generate a password for you. Remember to copy the password to a safe location.

Alternatively, use a dedicated password manager with a password generation feature. Many password managers will allow you to:

- Automatically save your password on a secure server.
- Share specific passwords with other people, without ever sending the password in clear text.

Performance impacts

Encryption can affect your processing, upload, and download speeds.

FileSender encrypts and decrypts files in your web browser, so batches of files larger than 4 GB may not transfer. If you need to send more than 4 GB of encrypted files, we recommend sending them in multiple batches.

Encrypt your FileSender files

1. Add your files and fill out the recipient details. Either of the two methods of sending files below have encryption options.
2. Under **Transfer settings**, toggle **File Encryption**.
3. Enter a unique password that you can send to the recipient after you upload and send your files. We advise that you do this via a separate communication channel, preferably one that is secure or encrypted.

Use a dedicated password manager with a password generation feature. Many password managers will allow you to:

- Automatically save your password on a secure server.
- Share specific passwords with other people, without ever sending the password in clear text.

If you send the password to the same email address as the FileSender invitation, you negate most of the security you gain by encrypting the files – anyone with access to the recipient's email can also decrypt the files you send.

4. Click **Generate password** to have FileSender automatically generate a password for you.
5. Finish your configuration and click **Send**.