Live Distribution

Welcome to the documentation for using the Live Distribution feature for distributing data files securely through the EGA platform. This guide will walk you through the process of downloading encrypted files and decrypting them using **Crypt4GH**. Please follow the steps below to ensure a smooth experience.

Before Downloading

1. Create an **EGA user**.
2. Make sure that you have the permissions to download the dataset of interest. In case you don't have access, **request access** to the dataset.
3. Add your **Crypt4GH-compatible public key** to your EGA account. Please allow a few hours for your public key to be synced with your profile. Afterwards, you will be able to connect to your EGA outbox using the SFTP protocol.

Download

Graphical User Interface (GUI)

You can use any GUI that supports SFTP connections, such as **FileZilla**, an open-source FTP client. For Filezilla as your GUI, follow these steps to download files:

1. Open FileZilla and access Site Manager (File > Site Manager).
2. Create a new connection with the following settings (*Figure 1*):
   - **Protocol:** `SFTP - SSH File Transfer Protocol`
   - **Host:** `outbox.ega-archive.org`
   - **Logon Type:** `Key file`
   - **User:** your `EGA username`
   - **Key file:** `path/to/your/private_key`

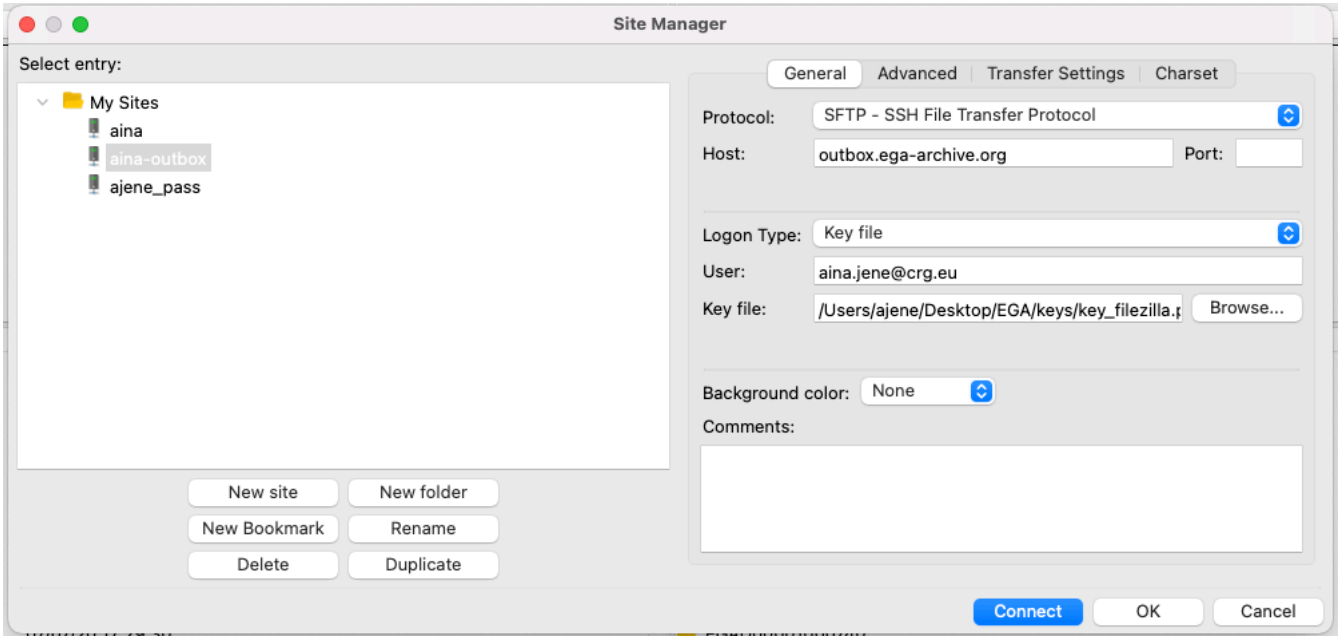

Figure 1: Process of establishing a new connection to outbox.ega-archive.org using a key file as the logon method in FileZilla. The figure showcases the FileZilla version 3.52.2 operating on IOS v11.2.3. By following the depicted steps, users can create a secure and efficient connection to the EGA outbox, ensuring seamless data transfers.

3. Click Connect to access your Outbox. This folder serves as your storage space within the EGA cloud, containing files accessible for download in a secure way.

4. Browse the remote directory on the right side of the FileZilla screen. Select the files you wish to download, right-click, and choose Download (*Figure 2*).

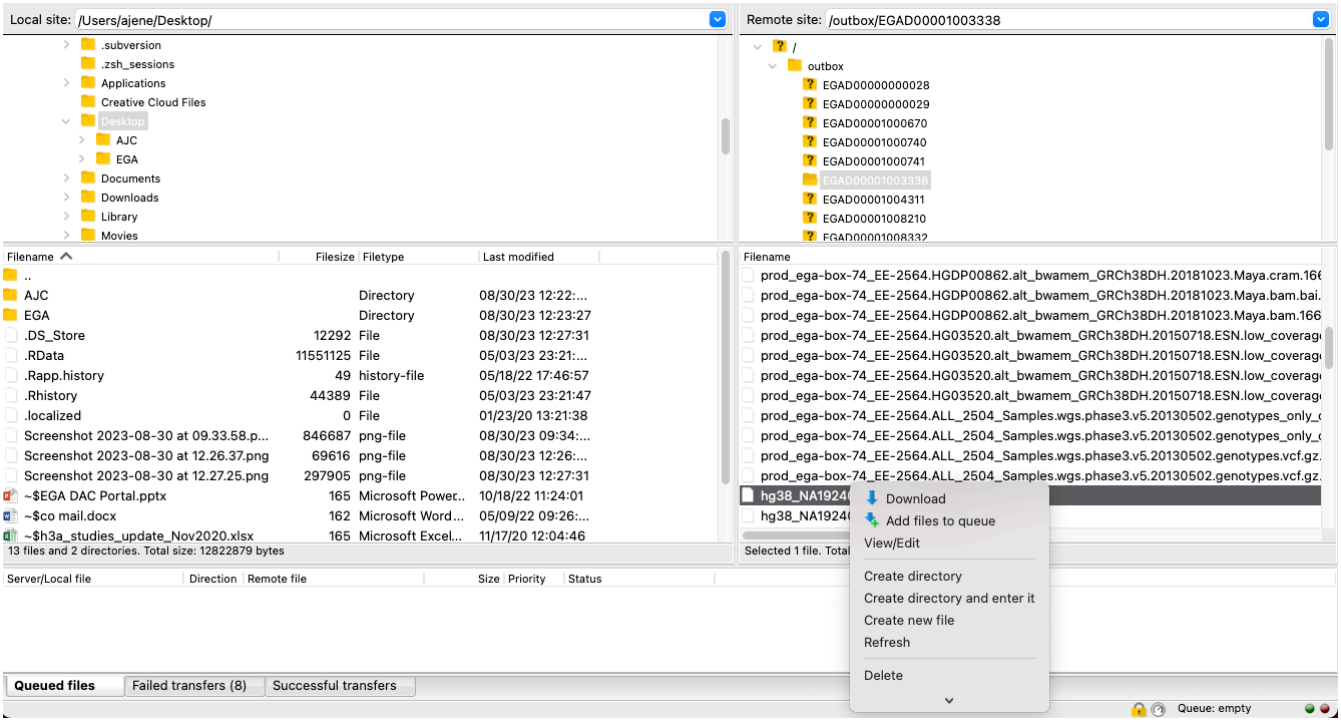

Figure 2: Step-by-step process of manually downñoad files from outbox.ega-archive.org using FileZilla, with FileZilla version 3.52.2 operating on IOS v11.2.3. The figure demonstrates how users can downñoad data from the EGA outbox to their local storage by following the depicted steps

SFTP command line

You can also use the SFTP command line to securely download files from the EGA Outbox.

Using SFTP command line client in Linux/Unix

1. Open a terminal window
2. Enter the following command to connect: `sftp username@hostname`
3. Enter your EGA password
4. To see a list of available sftp commands type `help`
   - sftp> `put` – Upload file
   - sftp> `get` – Download file
   - sftp> `cd path` – Change remote directory to 'path'
   - sftp> `pwd` – Display remote working directory
   - sftp> `lcd path` – Change the local directory to 'path'
   - sftp> `lpwd` – Display local working directory
   - sftp> `ls` – Display the contents of the remote working directory
   - sftp> `lls` – Display the contents of the local working directory
5. Type get command to download files. For example: `get encrypted_file.c4gh`
6. Use the `bye` command to close the connection (SFTP session).

Convenient SSH settings

Include the following settings in your SSH config file, located in `~/.ssh/config`

```
Host outbox.ega-archive.org EGA-outbox
    hostname outbox.ega-archive.org
    User username
    IdentityFile path/to/the/private/key
```

Replace *username* and *path/to/the/private/key* with the appropriate settings, and you will be able to connect to the outbox.ega-archive.org simply using `sftp EGA-outbox`.

How to decrypt

Files archived at the EGA are encrypted based on **Crypt4GH**. Hence, to decrypt the files you need to install Crypt4GH. You can install a python implementation of it, with

```
pip install crypt4gh
```

or directly from the **Github repository**

```
pip install git+https://github.com/EGA-archive/crypt4gh.git
```

After installing Crypt4GH, decrypt files using the following command:

```
crypt4gh decrypt --sk /path/private/key < encrypted_file.c4gh > decrypted_filename
```

The command reads the encrypted file from `stdin` (with `<`) and output the decrypted version to `stdout` (with `>`).
Replace `encrypted_file.c4gh` and `decrypted_filename` with the appropriate filenames but make sure to not use the same filename for both reading and writing because your SHELL would then truncate both files before you even read or write.

Frequently Asked Questions

What username should I use to log in to my outbox? +

I see that some files in my dataset have 'unavailable' as extension. What should I do? +

Specific to using keys

Can I access one EGA account from different devices? +

I have several keys and I don't remember which one is which +

What if I can't find my SSH keys for uploading files with a key file, and how can I use new keys? +

I don't want to type the passphrase every time I use the key. What can I do? +

Can I use my password for authentication (without my private key)? +

Why is it better to use my key and not my password? +

DISCOVERY

Studies Datasets DACs

TOOLS

Submitter Portal DAC Portal All Tools

CONNECT WITH US

Blog Twitter LinkedIn Youtube

The European Genome-phenome Archive (EGA) is part of the ELIXIR infrastructure.

EGA is an Elixir Core Data Resource. Learn more...