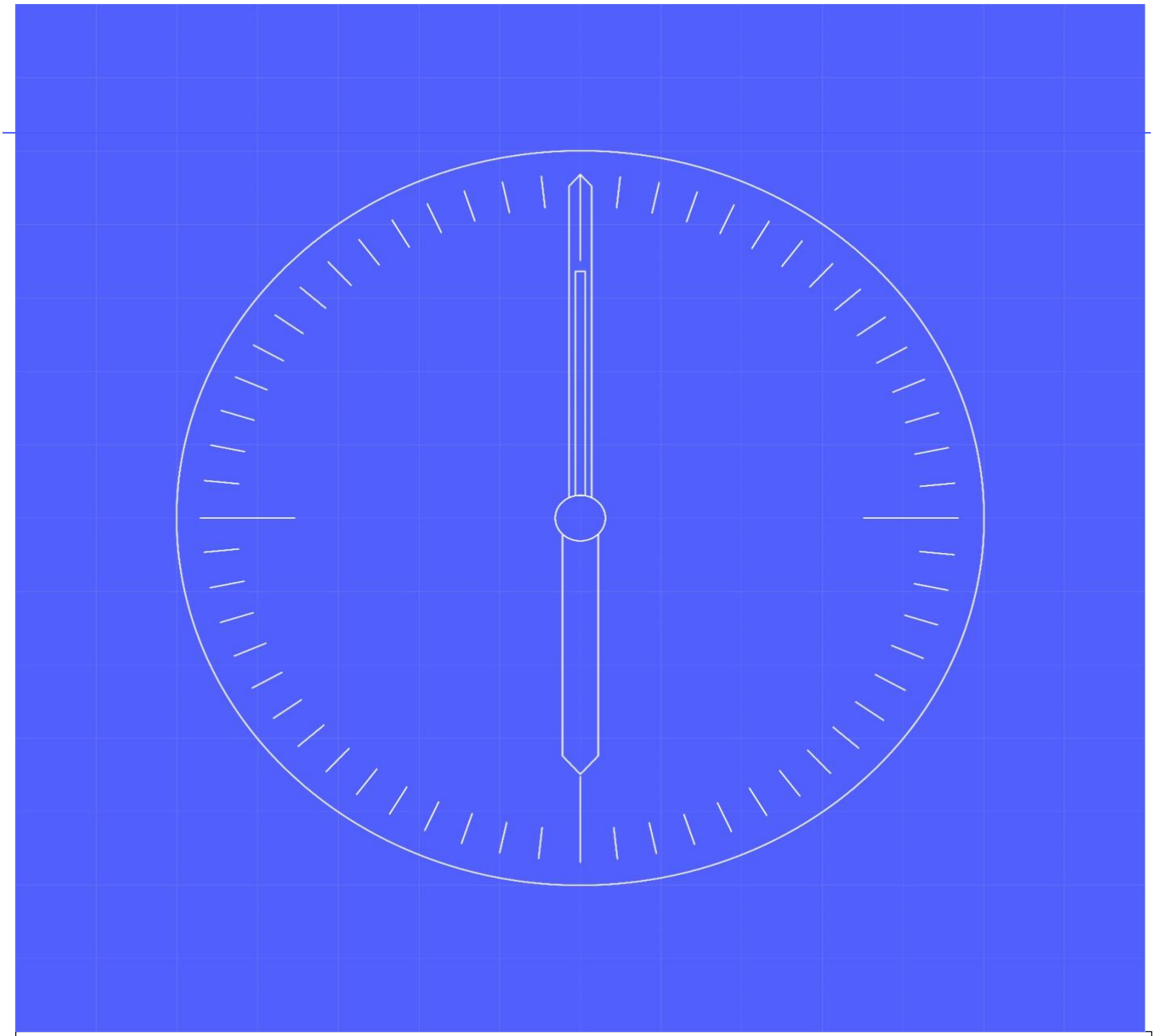
MHHS PROGRAMME
Industry-led, Elexon facilitated

SFTP Guide



Document owner	Document number	Version
Cesar Lopes	**MHHS-DEL1556**	**1.2**
Status:	Date	Classification
Issued	**23 February 2024**	**Public**

MHHS PROGRAMME
Industry-led, Elexon facilitated

Contents

1.1 Change Record

Date	Author(s)	Version	Change Detail
22/08/2023	Cesar Lopes	0.1	Initial Draft
25/08/2023	Cesar Lopes	1.0	Initial version issued
15/09/2023	Atarebi Khurshid Aishwarya Sunderrajan	1.1	Included Step-by-Step guideline for different tools and FQA
23/02/2024	Atarebi Khurshid	1.2	Updates following LDSO SFTP

1.2 Reviewers

Reviewer	Role
Richard Puddephatt	SI DataTest Manager
Simon Berry	SI Environment Manager
John Wiggins	SI Migration Manager

1.3 References

Ref No.	Document/Link	Publisher	Published	Additional Information
REF-01	MHHS-DEL813 Overarching Test Data Approach & Plan	SI Testing	24th May 2023	

1.4 Terminology

Term	Description
Various	For terminology, see Programme Glossary on the MHHS portal: Programme Glossary (SharePoint.com)

1.5 Summary of Changes

Updated document after receiving feedback from the industry:

Section 4.3.3: Added alternatives to create Public/Private keys

4.3.3.1: Terminal – Openssl

Section 5.3: Include step by step process to connect and transfer data using FilleZilla

Section 5.4: Include step by step process to connect and transfer data using Command Line on Windows

Section 5.5: Included Frequent Questions and Answers

2 Introduction to SFTP

Secure File Transfer Protocol (SFTP) is a network protocol for securely accessing, transferring and managing large files and sensitive data.

Advantages of using SFTP:

- **Security** – SFTP protects data in transit through data security, encryption and public key authentication.
- **Speed** – SFTP supports large and multiple file transfers from one server to another simultaneously
- **Integration** – SFTP integrates well with VPN's and Firewall
- **Management** – SFTP can be managed through SFTP GUI clients.
- **Platform independent** – SFTP clients are available to Windows, macOS and Linux, facilitating the transfer between different platforms. No additional software is required since most operating systems come with SFTP clients pre-installed.

2.1 MHHS Data SFTP Environment

The MHHS Programme has a SFTP Service configured to transfer Data between the Programme and the participants. Table 1 contains a summary of the technical description of the environment. It might be useful for IT departments to understand the service involved, obtain and confirm the server fingerprint.

Table 1: SFTP Technical Description

<table>
<tr><th>#</th><th>Item</th><th>Description</th></tr>
<tr><td>1</td><td>Data Storage – SI – Intra server security</td><td>- Secure transfer for REST API operations only: any connections to the data inside the cloud infrastructure will allow only HTTPs encrypted connections using Transport Layer Security (TLS) protocol with asymmetric public key infrastructure.
- Minimum TLS Version: 1.2</td></tr>
<tr><td>2</td><td>Data Storage – SI – Data in rest encryption</td><td>All data in the storage shall be encrypted using 256-bit AES encryption</td></tr>
<tr><td>3</td><td>Data Storage – SI – Data Transfer Protocol</td><td>SSH File Transfer Protocol (SFTP)</td></tr>
<tr><td>4</td><td>Data Storage – SI – SSH Authentication methods</td><td>SSH Public Private Key pair

Host key encryption using one of the following algorithms:
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- rsa-sha2-256
- rsa-sha2-512
SI to provide to participants the host SHA256 fingerprint and public keys.</td></tr>
<tr><td>5</td><td>SSH Client algorithms</td><td>Connecting clients must use algorithms specified in table below:
<table>
<tr><th>Type</th><th>Algorithm</th></tr>
<tr><td>Host key [1]</td><td>rsa-sha2-256*
rsa-sha2-512*
ecdsa-sha2-nistp256
ecdsa-sha2-nistp384</td></tr>
<tr><td>Key exchange</td><td>ecdh-sha2-nistp384
ecdh-sha2-nistp256
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group-exchange-sha256</td></tr>
<tr><td>Ciphers/encryption</td><td>aes128-gcm@openssh.com
aes256-gcm@openssh.com
aes128-ctr
aes192-ctr
aes256-ctr</td></tr>
<tr><td>Integrity/MAC</td><td>hmac-sha2-256
hmac-sha2-512
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com</td></tr>
<tr><td>Public key</td><td>ssh-rsa*
ecdsa-sha2-nistp256
ecdsa-sha2-nistp384</td></tr>
</table>
*RSA keys must be minimum 2048 bits in length.</td></tr>
</table>

<table>
<tr><th>#</th><th>Item</th><th>Description</th></tr>
<tr><td>6</td><td>Data Storage – SI – Restricted IPs access</td><td>Enable access to the data only from the selected Participants IP addresses and SI.</td></tr>
<tr><td>7</td><td>SFTP Server Fingerprint</td><td>MHHS SFTP – Valid host keys

<table>
<tr><td>Region</td><td>UK South</td></tr>
<tr><td>Host Key type</td><td>ecdsa-sha2-nistp256</td></tr>
<tr><td>SHA 256 fingerprint</td><td>weMVzOmQnlMdMp5XBoU9SdN5meBbx/8nvA8dB45w8Ck=</td></tr>
<tr><td>Public key</td><td>AAAAE2VjZHNhLXNoYTItbmlzdHA
yNTYAAAAIbmlzdHAyNTYAAABBBEnBl
lEm4/HsTP+ZMhlc8YnSAYWF23tibZDqGxf0yBRT
U/ncuaavuQdIJ5TcJb0NcXG7skEmq3StwHT0FPMWN8Y=</td></tr>
</table>

<table>
<tr><td>Region</td><td>UK South</td></tr>
<tr><td>Host Key type</td><td>ecdsa-sha2-nistp384</td></tr>
<tr><td>SHA 256 fingerprint</td><td>HpsZ8zoOCCsUbpD3nAOtxpuKIvn0L8KGyg1KMLuMUqU=</td></tr>
<tr><td>Public key</td><td>AAAAE2VjZHNhLXNoYTItbmlzdHAzODQAAAAIbmlzdHAzODQAAAB
hBGd/672brwX1kOhH31ZTdBRj+bcEmemcdmTEe0J8
8cJ3RRQy7nDFs25UrnR+h3P0ov9Uq24EJQ
S8auxRgNCUJ3i3ZH9QjcwX/MDRFPnUrNosH8NkcPmJ/pezVeMJLqs3Qw==</td></tr>
</table>

<table>
<tr><td>Region</td><td>UK South</td></tr>
<tr><td>Host Key type</td><td>rsa-sha2-256</td></tr>
<tr><td>SHA 256 fingerprint</td><td>3nrDdWUOwG0XgfrFgW27xhWSizttjabHXTRX8AOHmGw=</td></tr>
<tr><td>Public key</td><td>AAAAB3NzaC1yc2EAAAADAQABAAABAQCdLm+9OROp5zrc6nLKBJWNrTnUeCeo8
n1v9Y3qWicwYMqmRs/sS9t5V3ABWnus4TxH3bqgnQW3OqWLgO
Hse/3S+K1wGERmBbEdKOl7A7kQ9QgDkWEZoftwJ9hp+AMVTfCYhcOOsG+gW021d
ifNx+WW2O5TldL31pk+UvdhnQKRHLX31cqx5vuUmiwq4mlbBx+rY8B/xngP2bzx/oYXdy1
I9fZbWWAQ6FwJBav1sSWL0l7snRdOsy5ASeMnYollEw1IATwYeUv8g
3PzrryZuru+7gu/Ku9w8d5jbFyI6Up4KLwj
s/gZNuqQ5dif7utiQYbVe4L0TPWOmuLA25JJRZaF</td></tr>
</table>

<table>
<tr><td>Region</td><td>UK South</td></tr>
<tr><td>Host Key type</td><td>rsa-sha2-512</td></tr>
<tr><td>SHA 256 fingerprint</td><td>Csnl8SFblkdpVVsJC1jNVSyc2eDWdCBVQj9t6J3KHvw=</td></tr>
<tr><td>Public key</td><td>AAAAB3NzaC1yc2EAAAADAQABAAABAQDIwNE
frP6Httmm5GoxwprQ57AyD6b3EOVe5pTGQWIOzxnrIw2KnDPL07KNa33xZOmtXro5P
Yyhr5eNXUkFiQMEe+RblilZSNAvc4MHbp2TVD0L9N7Pdy2SetoF4m5BCXdC48kZntqgkpzXoDbFiaAV
ln5zQCHB5fOuBPS1id8+k3zqG0o+K0MHb6qcbYV8gdQeOn/PlJzKE4M0Ie8na3
aWHdGvfJjDdK/hNN0J+eUK8qIb9KCJkSMDj/l3rnue9L8Xge
KKA2Pkvh3nch4VBXCcCsDVhgSf+aoiJ0Fy8GVOTk2s7QDMzD9y37D9V2OPl66q4
pjFGOfK0mJmrgqxWNy5</td></tr>
</table>
</td></tr>
</table>

3 MHHS – SFTP User Guide

This section of the document contains the guidelines, and step-by-step procedure, for connecting and using the MHHS Programme Data SFTP Environment.

3.1 Step 2: Obtain and inform IP Addresses – Allow List

The access to the MHHS Programme Data SFTP environment is by default blocked for all public IP addresses. The first step to get access to the environment is to inform the Programme with the IP Addresses the organisation will use to access and transfer data.

It is highly recommended that the IP address be the company IP address (including VPN IP address), instead of the employee's home network IP address.

The form sent to the programme participant in Step 1 contains an item to include the user's desired IP addresses to include in the Programme "allow list".

3.2 Step 3: Generate Private/Public Keys

The MHHS Programme Data SFTP Environment uses a public-private key to ensure security.

Public-private key pairs provide a higher level of security compared to traditional password-based authentication. With keys, there are no passwords exchanged over the network, reducing the risk of password interception or brute-force attacks. The public-private keys are also used to asymmetrically encrypt the data being transferred during the SFTP session, ensuring confidentiality and integrity.

To increase security, the MHHS Programme will never have access to the user's private key. The pair public-private key will need to be generated by the user, and only the public key will be provided to the MHHS Programme.

Follow the steps in the next sections to generate the keys on MacOS or Windows.

3.2.1 Windows – Generate Private/Public Keys

Open the Command Prompt (click on the Windows icon, type “Command Prompt” and open the application:

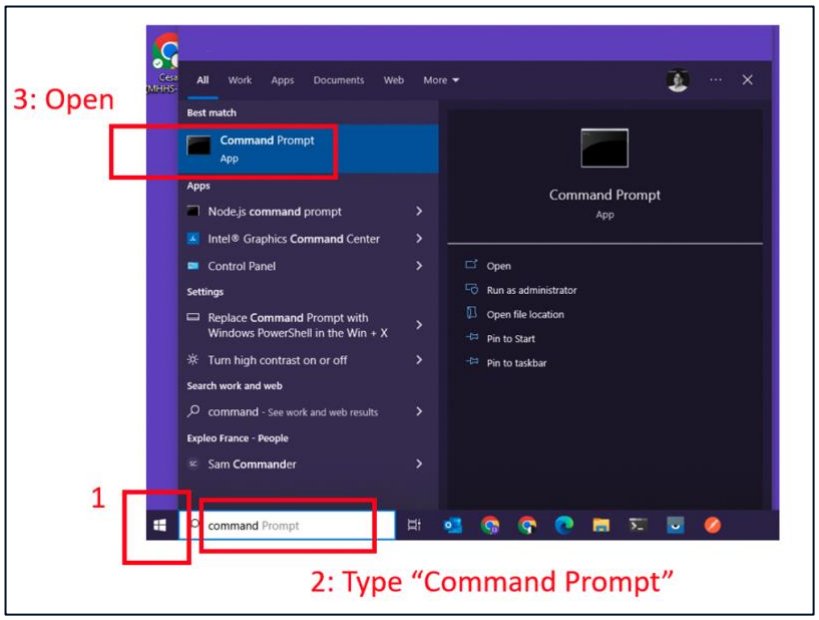


Figure 1: Windows - Open Command Prompt

On the Command Prompt, copy and paste the following command to generate the key:

```
ssh-keygen -m PEM -t rsa -b 4096
```

Figure 2: Windows - Command to generate public-private keys

The Terminal will show a message similar to Figure 2. Type a file name to create your key files and press “enter”. Example: “`mhhs_sftp_key`”.

The system will ask you to create a passphrase for the files or leave it empty. You can leave it empty. Press Enter, following the instructions on the screen. The system will then generate the keys and show messages similar to the Figure 3.

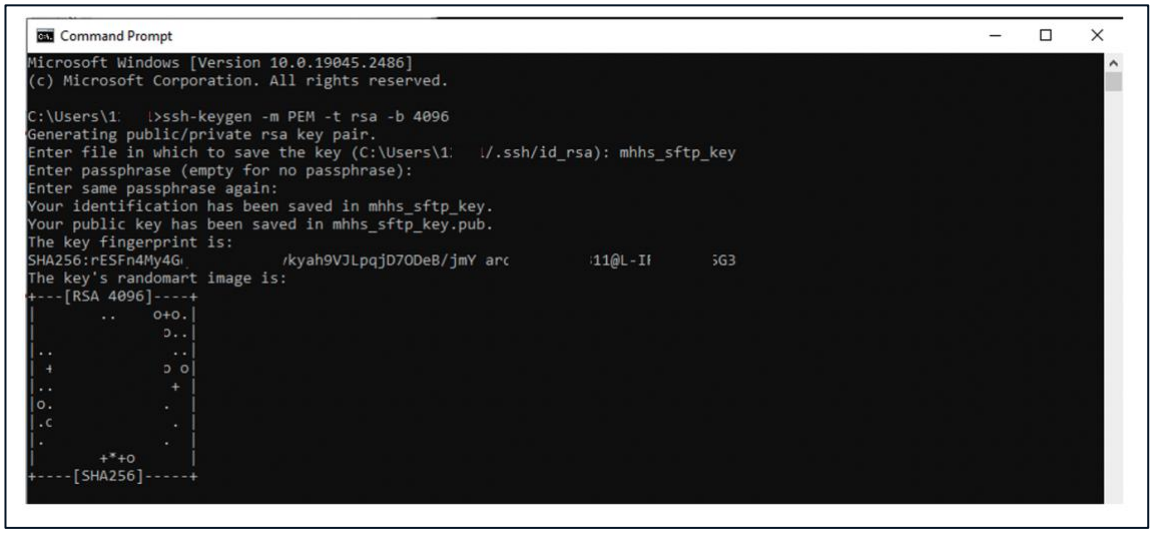


Figure 3: Public-private keys generated

Your keys were generated and saved in the location you provided in the steps above.

If you followed exactly the steps above and the file names given, you will locate your file following the steps in Figure 4.

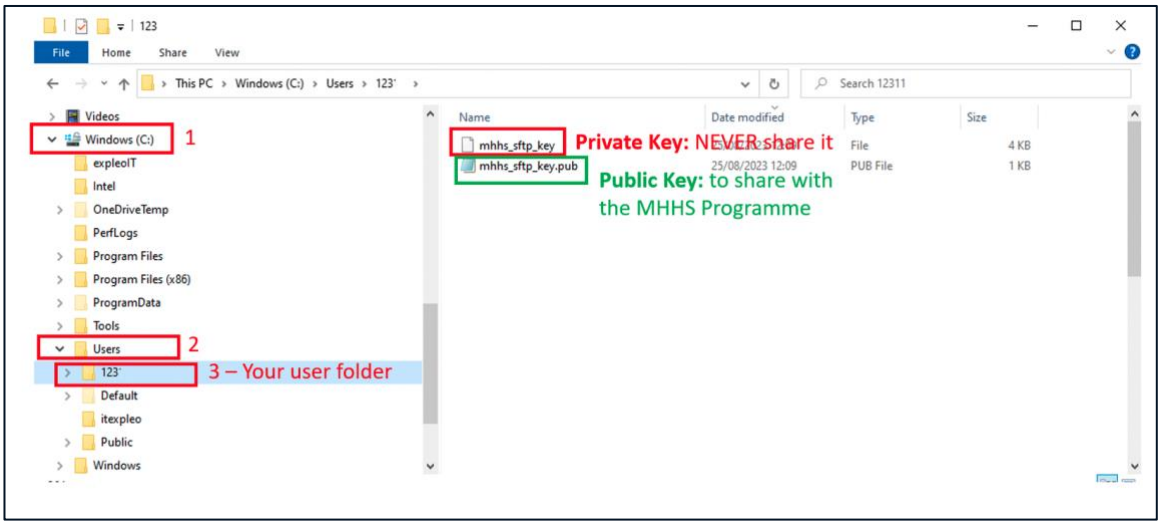


Figure 4: Keys generated - the public key can be shared to the MHHS Programme

The MHHS Programme will request the participant to provide the public key (".pub" file) to be registered in the SFTP MHHS Data Environment. During the SFTP access creation, the MHHS Programme will contact the participants who required the access via the email informed in the Step 1 of this guide (section **Error! Reference source not found.**).

3.2.2 MacOS - Generate Private/Public Keys

Open the Finder and Navigate to the Applications folder:

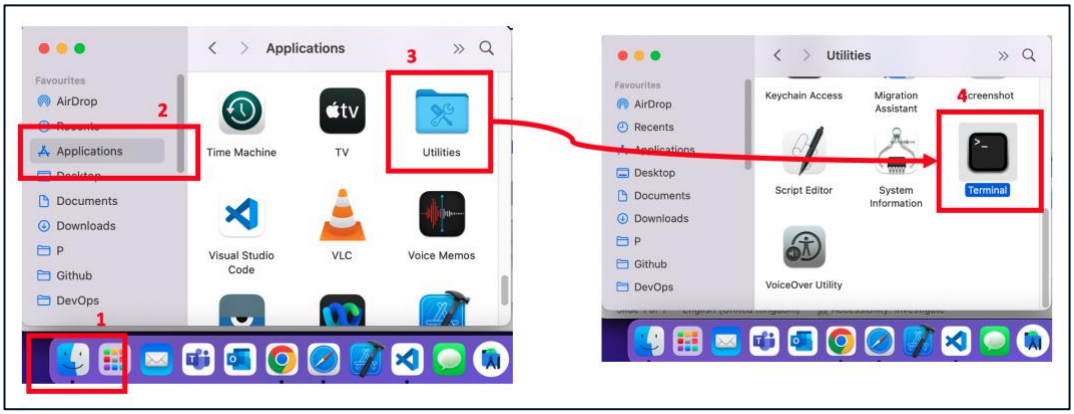


Figure 5: MacOS - Open Terminal

On the Terminal, copy and paste the following command to generate the key:

```
ssh-keygen -m PEM -t rsa -b 4096
```

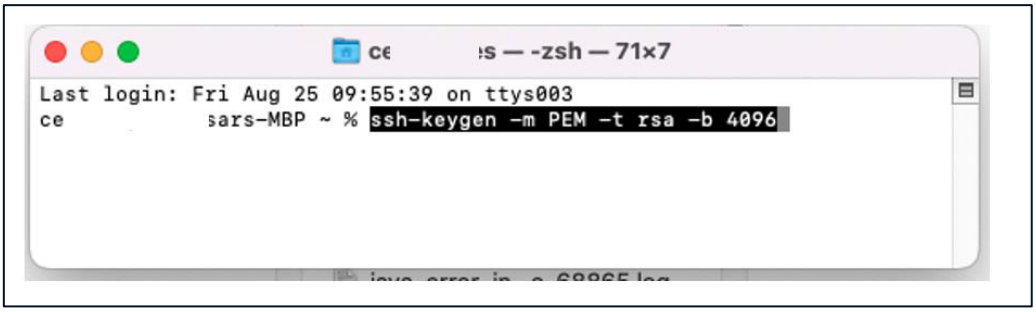


Figure 6: MacOS - Command to generate public-private keys

The Terminal will show a message similar to Figure 7. Type a file name to create your key files and press “enter”. Example: “`mhhs_sftp_key`”.

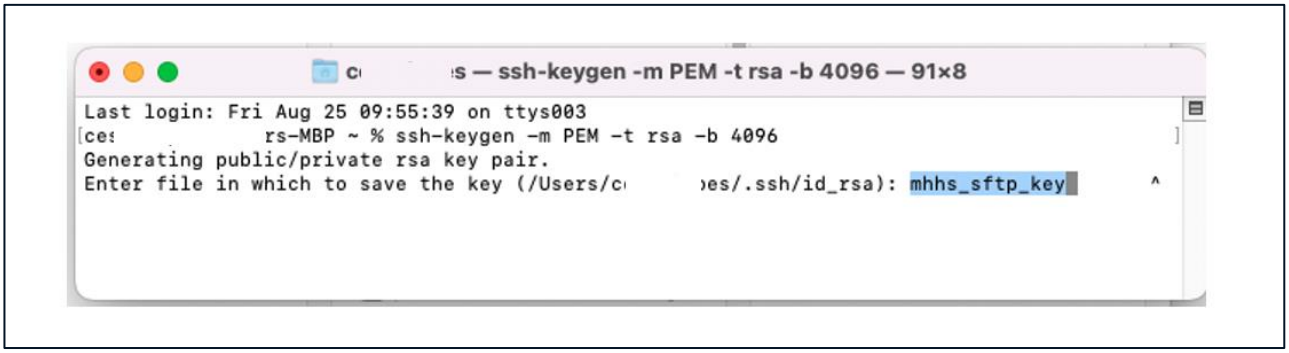


Figure 7: MacOS - Generating keys files

The system will ask you to create a passphrase for the files or leave it empty. You can leave it empty. Press Enter, following the instructions on the screen. The system will then generate the keys and show messages similar to the **Error! Reference source not found.**.

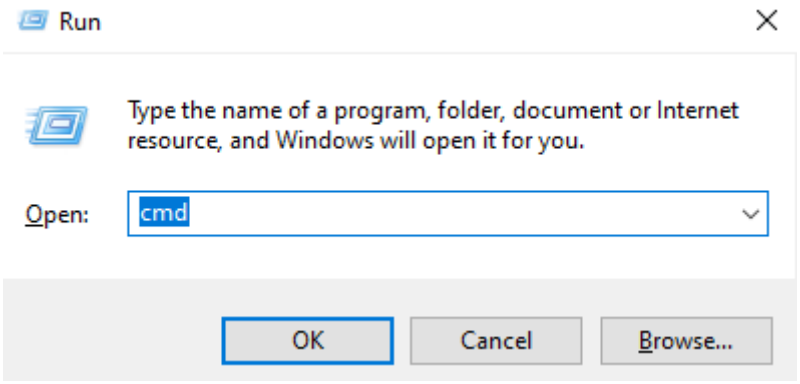
3.2.3 Added Alternatives to create Public/Private Keys

4.3.3.1- Terminal- OpenSSL

You can generate private and public keys using OpenSSL, a versatile open-source tool for working with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. Here's how you can generate a private key and then derive a public key from it using OpenSSL:

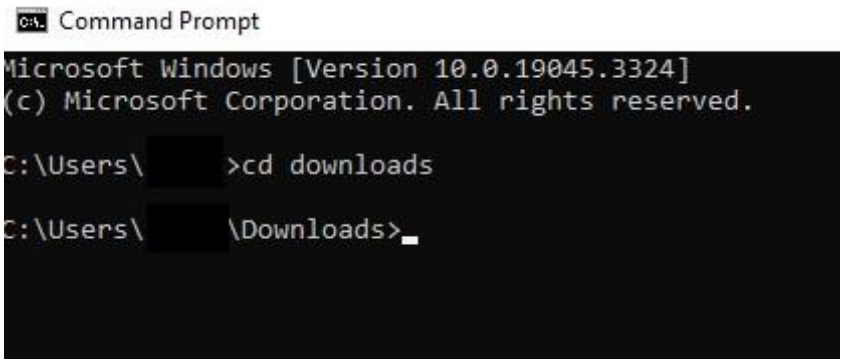
1. **: Open the Windows Command Prompt**

   Press Win + R, type cmd, and press Enter.



Now navigate to a directory to which you would like your public/private keys saved.

In this example, changed my directory to Downloads



2. . Generate a Private Key:

   You can generate a private key using the openssl genpkey command. The most common algorithm used for generating private keys is RSA. Here's how to generate an RSA private key with a specific key length (e.g., 2048 bits):

   In this example, private_key.pem is the name of the output file for the private key (This can be changed to your preference)

```
openssl genrsa -out private_key.pem 2048
```

   Once, this runs, the key will be stored in the current working directory.

3. Generate the Corresponding Public Key

   You must ensure to type out the same name of the private key for a correct public key to be generated

```
openssl rsa -pubout -in private_key.pem -out public_key.pem
```

   You will now have a public key in the directory as well as a private key

4.3.3.2 - Generating and storing public and private key pairs in Azure Portal

The generation of SSH key pairs can be simplified by integrating them into Azure. Key pairs aren't tied to a specific virtual machine and can be used in future applications. Keys can even be created in the portal separate from a virtual machine and also externally and then uploaded for use in Azure. Here's how you can generate new keys using Azure portal:

1. Open the Azure portal

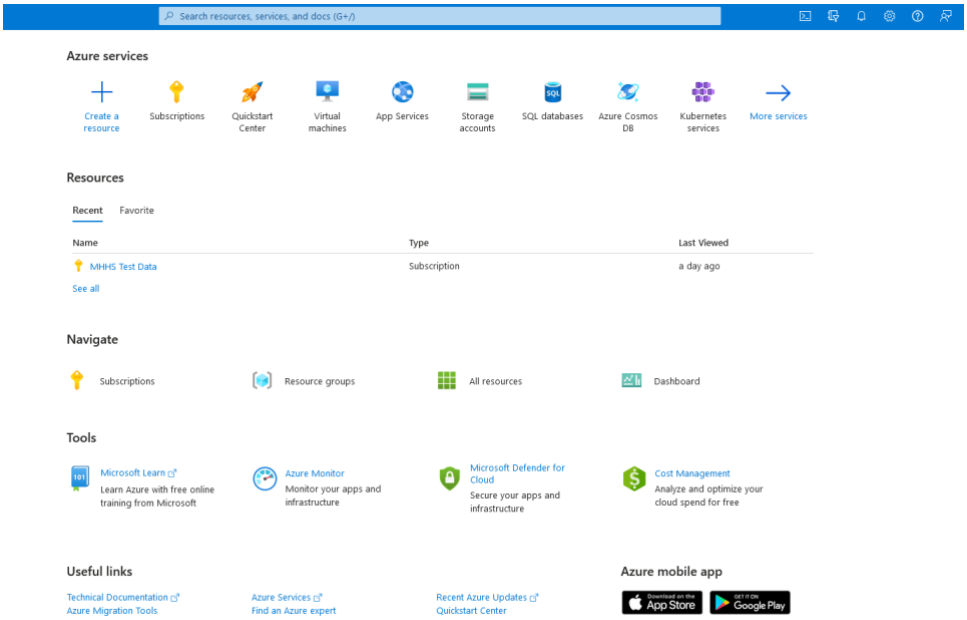


Figure 8: Azure portal

2. At the top of the page, type SSH to search. Under Marketplace, select 'SSH keys'

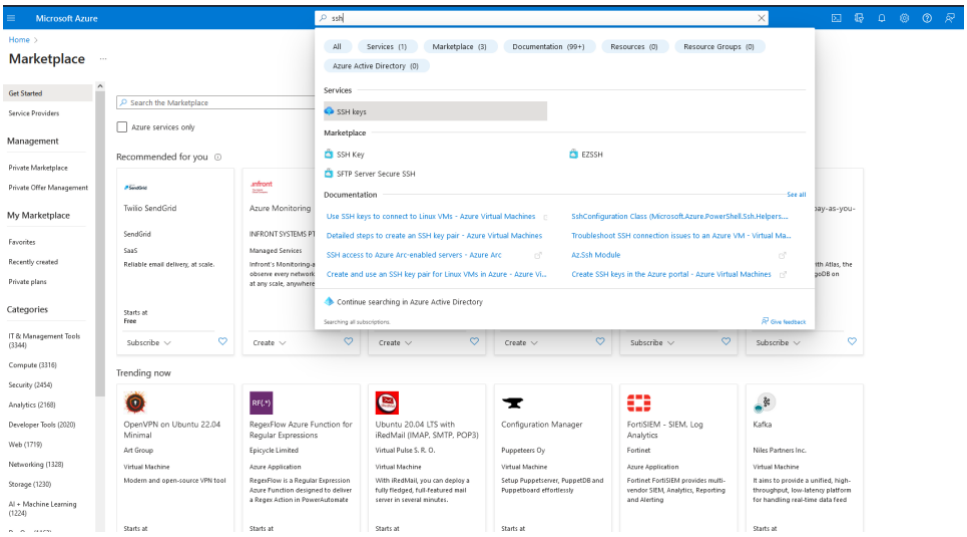


Figure 9: SSH in the marketplace

3. On the SSH Key page select 'Create'.
4. In 'Resource group' select 'Create new'' to create a new resource group to store your keys. Type a name for your resource group and select 'Ok'.
5. In 'Region' select a region to store your keys. You can use the keys in any region, this option is just the region where you store them.
6. Type a name for your key in 'Key pair name'. In 'SSH public key source', select 'Generate public key source'

7. When you''re done, select ‘Review + create’

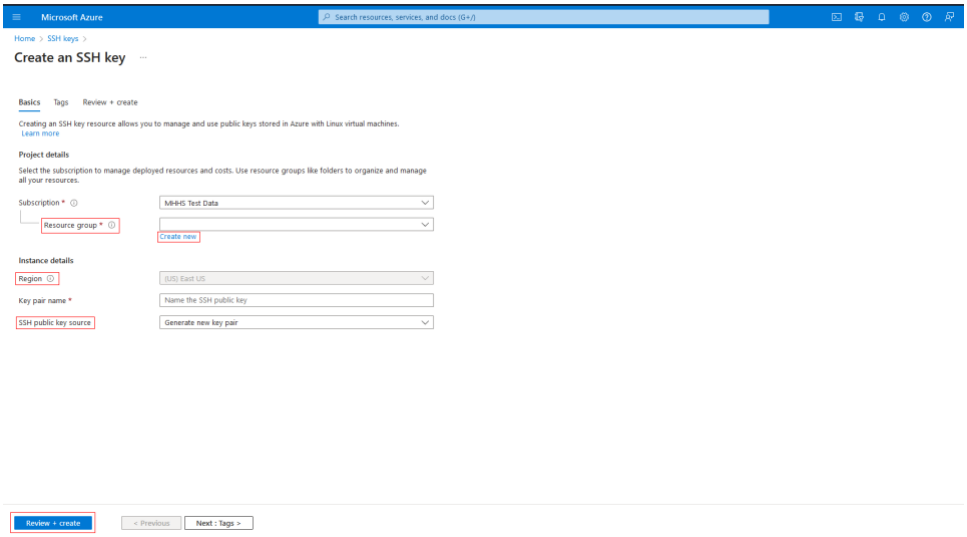


Figure 10: Creating an SSH Key Pair

8. After It passes validation, select ‘Create’
9. You’ll get a pop-up window, select ‘Download private key and create resource’ that downloads the SSH key as a .pem file

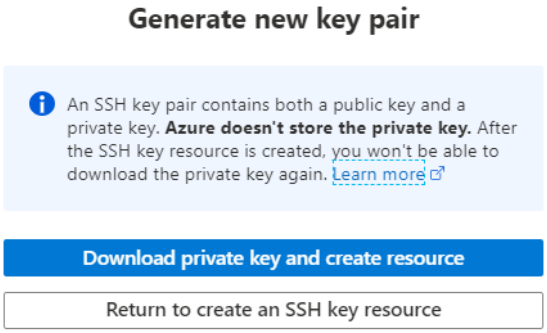


Figure 11: Downloading and saving an SSH Key Pair

10. Once you’ve downloaded the .pem file, you can move it somewhere on your computer where it’s easy to point from your SSH client.

3.3 Step 4 – Access the SFTP to download and upload files

With the keys Private-Public keys pair generated in the Step 3 and the public key shared with the MHHS Programme, the users will be ready to access the MHHS Data SFTP Environment.

The MHHS Programme will provide to the users via the email informed in Step 1 of this guide (section **Error! Reference source not found.**):

Table 2: Data needed to access the MHHS Data SFTP Environment

#	Item	Description
1	Access Protocol	SFTP – SSH File Transfer Protocol

#	Item	Description
2	Host address	Provided by the MHHS Programme. • URL to be provided via user email
3	Login Type	Key file
4	User Name	Provided by the MHHS Programme. • User name to be provided via user email
5	Key File	The user will use the Private Key generated in the Step 3 of this guide (section 3.2)

The participant can access the SFTP environment using the information described in Table 2 without installing any tool to their operating system.

To access it, the user just new to use the command in the Command Prompt (on Windows) or Terminal (on MacOS):

```
sftp -i <path/private_key_file> <user_name>@<Host address>
```

To download and upload files using the default command line tool, use the interactive commands get and put. A full list of commands available is available on:

https://man7.org/linux/man-pages/man1/sftp.1.html

While the default command line tools available on most of users' machines are complete and powerful, they are not as user-friendly as SFTP Client Applications with rich and interactive User Graphical Interfaces. Please, refer to the Appendix to get more information on SFTP Client Software.

4 Appendix

4.1 Known supported SFTP Clients

An SFTP Client is a software application that allows you to securely transfer files between a local computer and a remote server using the SFTP protocol. The SFTP client provides a user-friendly interface for managing file transfers. It allows you to:

1. Connect to SFTP Remote Server: You can input the server's connections string and your credentials, to establish a secure connection.
2. Browse remote directories: Once connected, you can navigate through the remote server's directory structure, similar to how you would navigate through directories on your local computer.
3. Upload and download files: You can transfer files between your local computer and the remote server by dragging and dropping files, using context menus, or issuing file transfer commands.
4. Monitor transfer progress: Most SFTP clients provide real-time information about the progress of ongoing file transfers and estimated time remaining.

The most popular SFTP client software includes:

1. **FileZilla**: a free and open-source SFTP client with a user-friendly interface, available for various platforms including Windows, macOS, and Linux.
2. **WinSCP**: Free and open-source SFTP client for Windows, known for its dual-pane interface and integration with PuTTY.
3. **Cyberduck**: A free SFTP client for macOS and Windows that offers a simple and intuitive interface.
4. **PuTTY**: While primarily an SSH client, PuTTY also includes an SFTP client called "PSCP" for Windows users who prefer a command-line approach.

The Table 3 contains a extensive list of known supported SFTP Clients that can be used to transfer Data within the MHHS Programme.

Table 3: Known SFTP Supported Clients

#	Item
1	AsyncSSH 2.1.0+
2	Axway
3	Cyberduck 7.8.2+
4	edtFTPjPRO 7.0.0+
5	FileZilla 3.53.0+
6	libssh 0.9.5+
7	Maverick Legacy 1.7.15+
8	Moveit 12.7
9	OpenSSH 7.4+
10	paramiko 2.8.1+
11	phpseclib 1.0.13+
12	PuTTY 0.74+
13	QualysML 12.3.41.1+
14	RebexSSH 5.0.7119.0+
15	Salesforce
16	ssh2js 0.1.20+
17	sshj 0.27.0+
18	SSH.NET 2020.0.0+
19	WinSCP 5.10+
20	Workday
21	XFB.Gateway
22	JSCH 0.1.54+
23	curl 7.85.0+

4.2 Windows Users – SFTP Guide using WinSCP

This section of the guide includes the specific steps to connect, download and upload files using a computer with a Windows Operating System and installing the SFTP Client WinSCP.

4.2.1 SFTP – How to Connect using WinSCP

- Download WinSCP using the following link: https://winscp.net/eng/download.php

Figure 8: Link to Download WinSCP

- Follow the installation instructions through the setup file and download WinSCP
- Once installed go to the start menu and open WinSCP
- Once WinSCP is opened the login window should appear, as shown in the image below

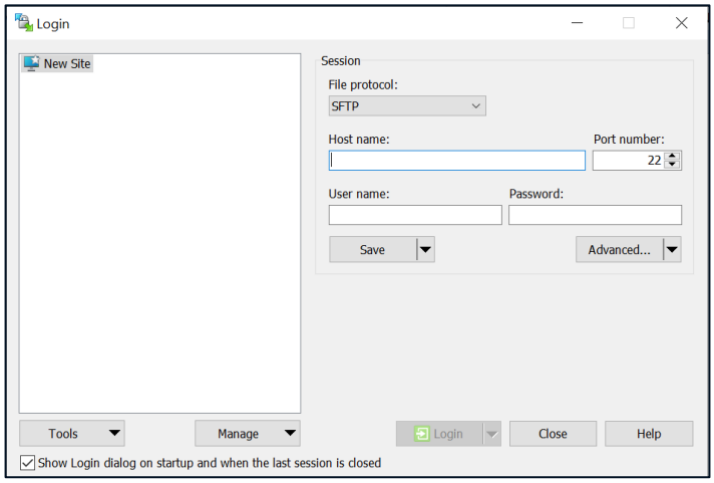


Figure 9: WinSCP Login Screen

- Fill “Host name”, “Port number” and “User name” with the information provided in Table 2.
- Click on “Advanced…”

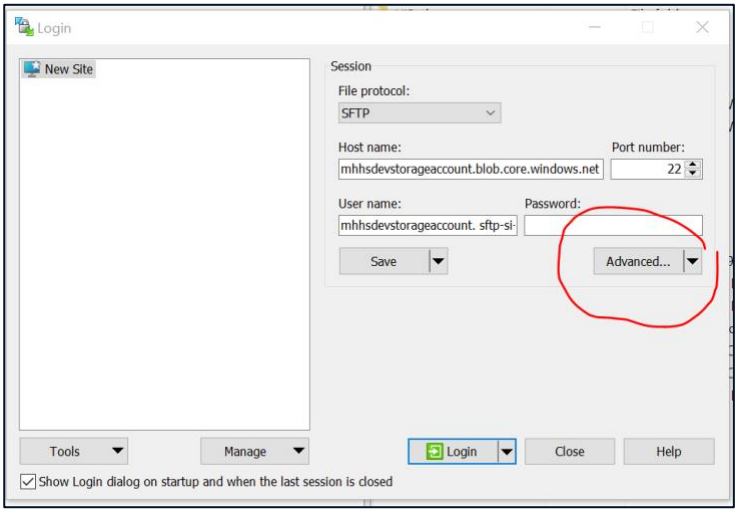


Figure 10: Advanced View

- Click on Authentication

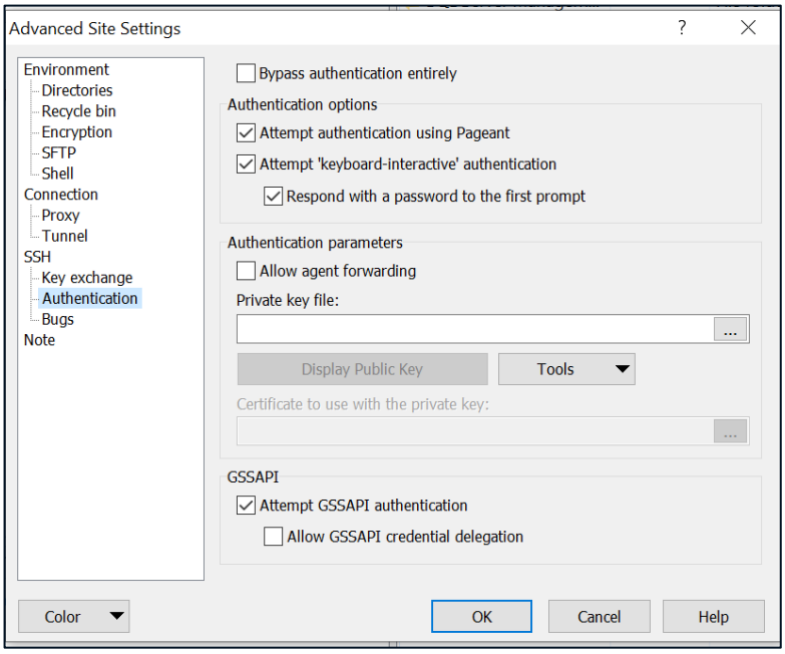


Figure 11: Advanced Settings

- On “Private key file”, select the private key file generated in the Step 3 of this guide (section 3.2) and press “OK”.
- Next press “login” as highlighted below:

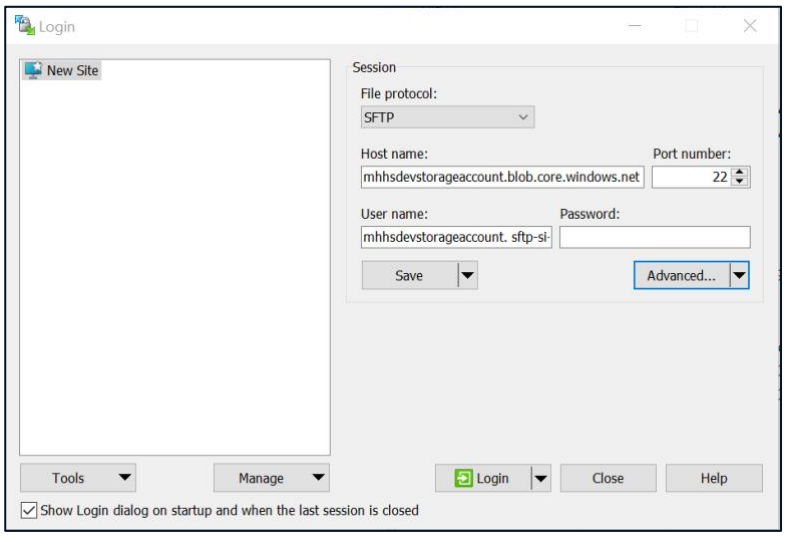


Figure 12: Login Screen

- Once the connection is set, you should see a screen like the one below, containing the files already uploaded to the SFTP environment or empty (if no file was already before):

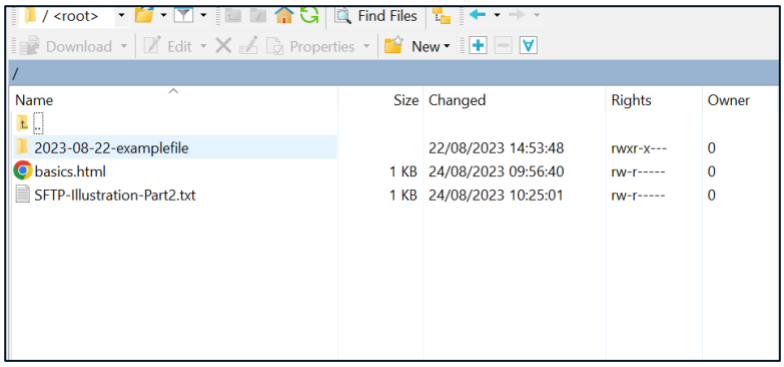


Figure 13: WinSCP Screen with Files

4.2.2 SFTP – How to Download a file using WinSCP

As shown in the image below, right-click on any of the files to download it:

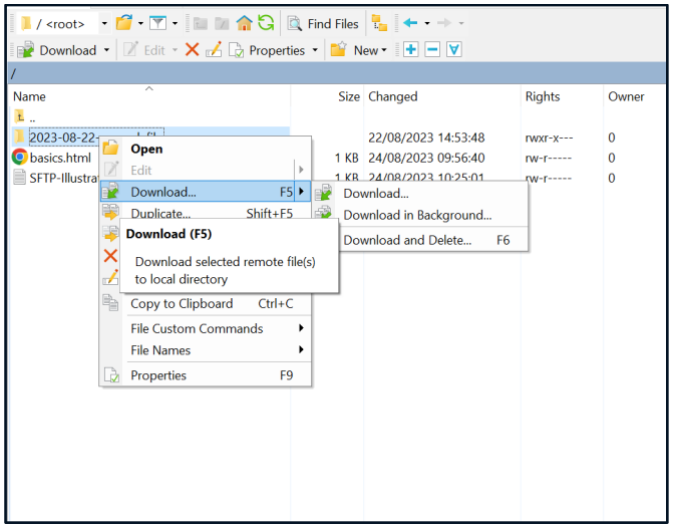


Figure 14: SCP – Downloading the file

4.2.3 SFTP – How to Upload a file using WinSCP

Upload any file copying it on the Windows Explorer and Upload it by right-clicking in WinSCP white area and paste.

Alternatively, the user can simply drag and drop files using the WinSCP:

1. On the left section, you can see the list of files on the user local computer.
2. The user can right-click on the desired files on the local user computer and select “copy to Clipboard” and right-click on the right side (remote/SFTP location) and select “Paste”.
3. The user can also just drag-and-drop the desired files from the left (local computer) to the right (remote/SFTP location)

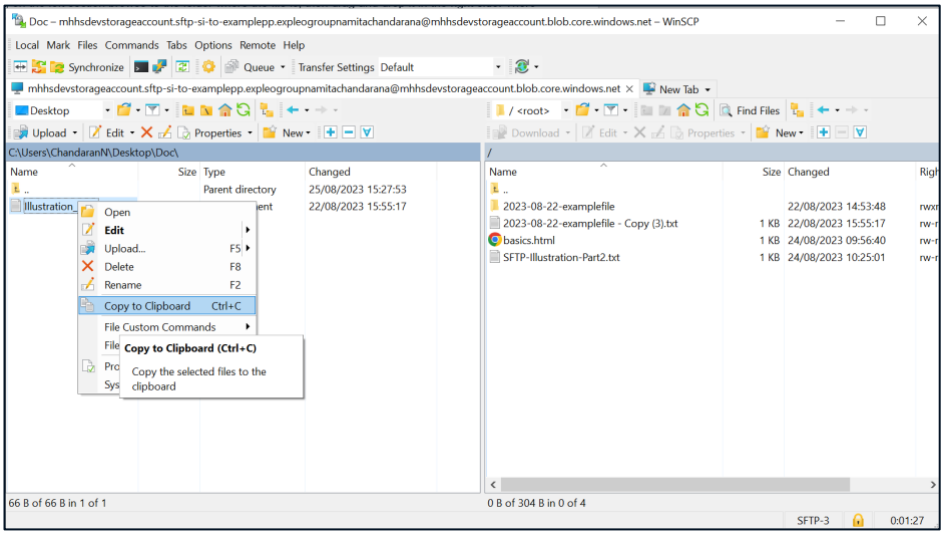


Figure 15: Copy File

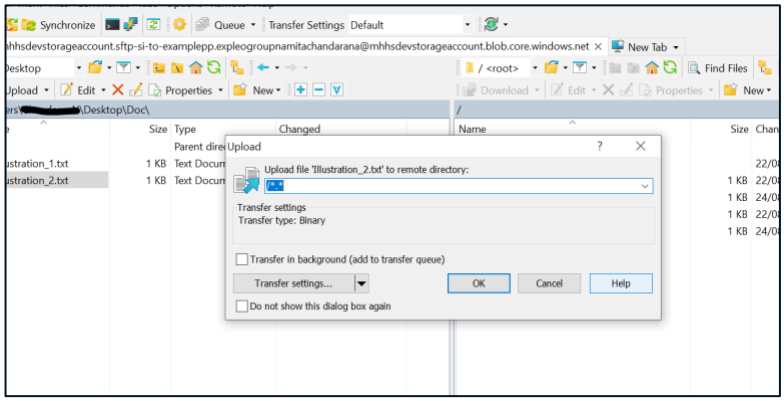


Figure 16: Uploading File

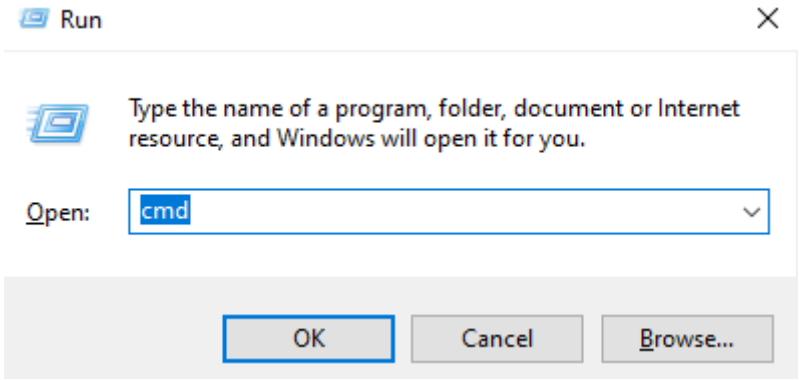
4.4 Windows Users- Connect and transfer data using Command Line

Using the command line to connect to an SFTP server provides a reliable and efficient way to manage files and directories. In this section, you can understand how to connect to an SFTP server using the command line step by step.

Before doing this step, you will need your private and public key generated and have had sent the public keys to the MHHS programme who would have reached out to you.

1. Open the Windows Command Prompt

Press Win + R, type cmd, and press Enter.



2. Connect to the SFTP Server

Run the sftp command with the -i option, specifying your private key, username, and server hostname or IP:

Example where myuser is your username, example.com is the hostname

```
sftp -i C:\Users\YourUsername\.ssh\id_rsa myuser@example.com
```

3. Navigate and Transfer Files

You should now be connected and can run the following commands to navigate/transfer files:

ls: List remote files and directories.

cd: Change the remote directory.

put: Upload a file to the remote server.

get: Download a file from the remote server.

exit: Close the SFTP session.

For example, if there is a file called ‘example.txt’ in the folder sftp_example, then

You would do the following :

First you must change the directory to where the file is located

```
cd sftp_example
```

Next you must type get followed by the file name

```
get example.txt
```

If you would like to now specifiy where you would like to download your file you must provide the full path. For instance, to download the file to C:\Downloads on a Windows machine:

```
get example.txt C:\Downloads\
```

Now the SFTP client will start the download and once complete, you will receive a message indicating that the file transfer was complete

Here is how the full session would look like

```
sftp myuser@example.com
Connected to example.com.
sftp> cd sftp_example
sftp> get example.txt
Fetching /sftp_example/example.txt to example.txt
/sftp_example/example.txt                100%  123KB   4.5MB/s   00:00
```

4. Exit the SFTP Session

Type exit to close the SFTP session and return to the Command Prompt.

4.5 Windows Users- Connect and transfer data using FileZilla

This section of the guide includes steps to connect, download and upload files using a computer with a Windows Operating System.

1. Download FileZilla using the following link: https://filezilla-project.org/download.php?platform=win64

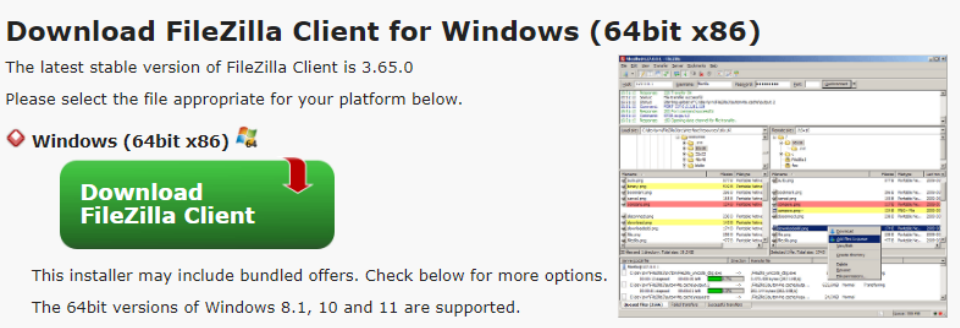


Figure 20: Downloading FileZilla

2. Follow the instructions through the setup file and download FileZilla.

3. Once installed go to the start menu and open FileZilla

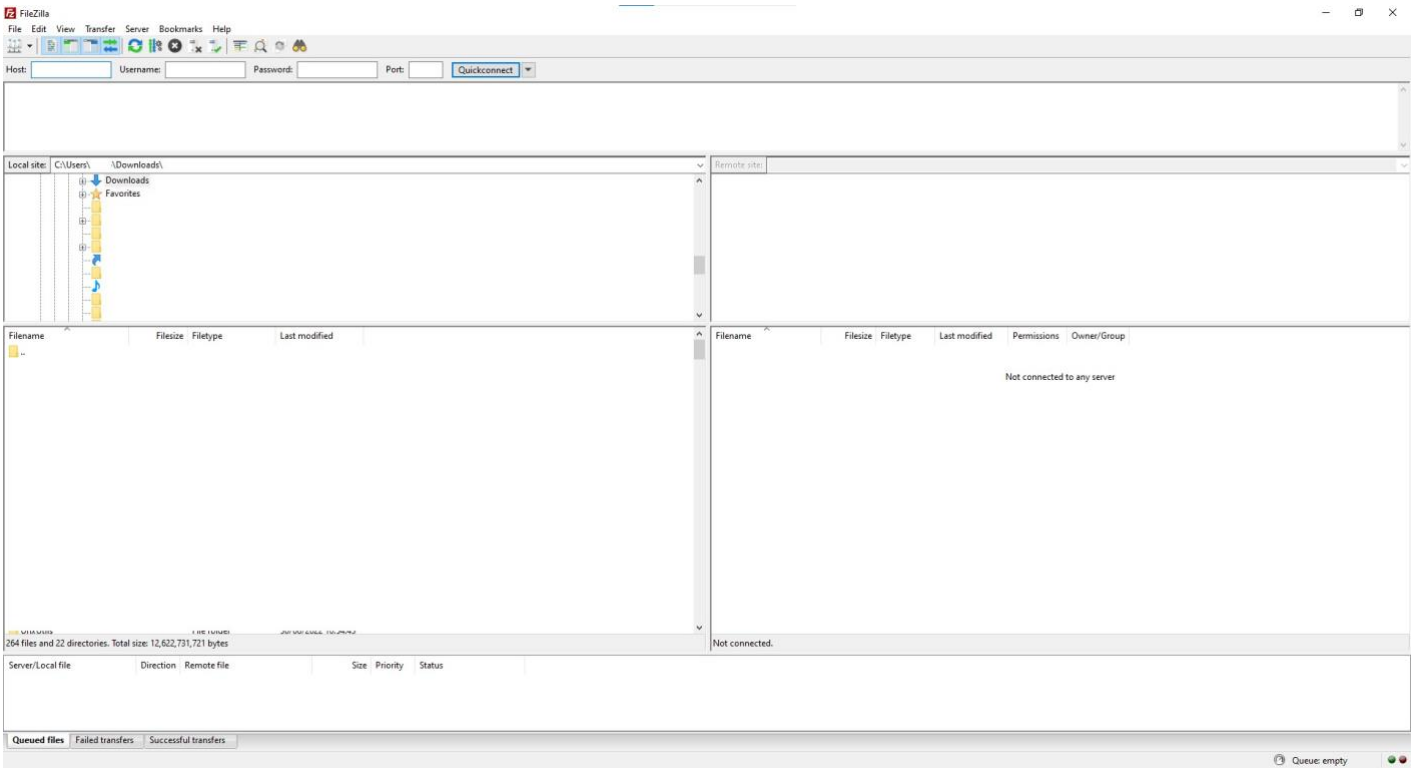
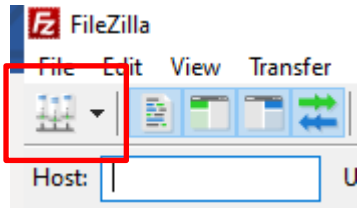
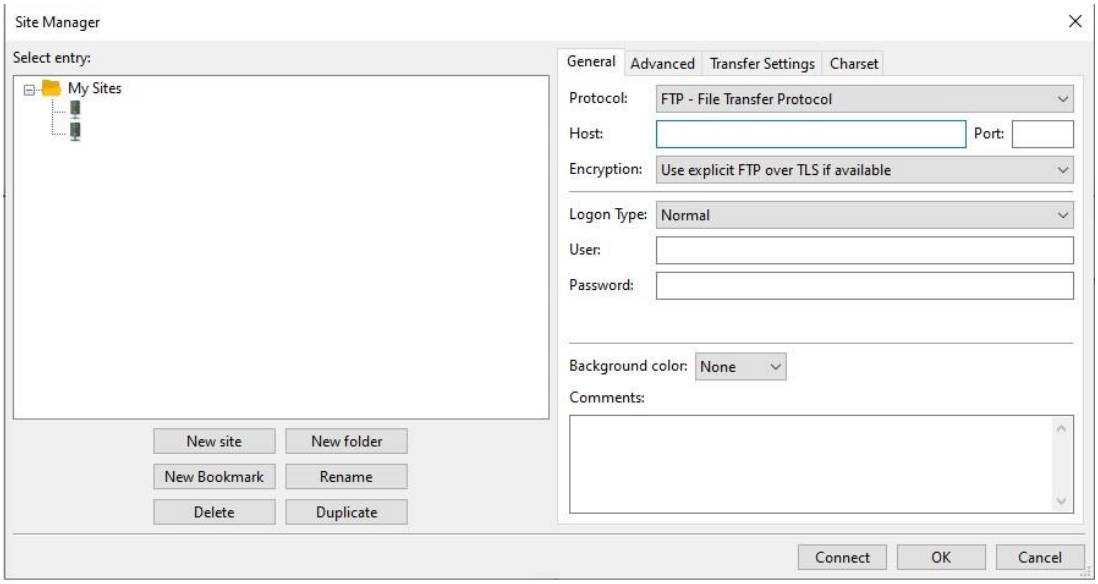


Figure 21: Opening FileZilla

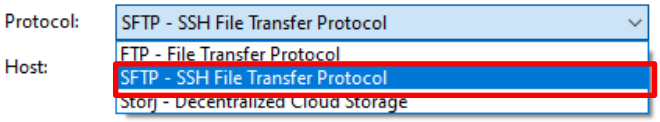
4. Press the following icon on the top left of FileZilla



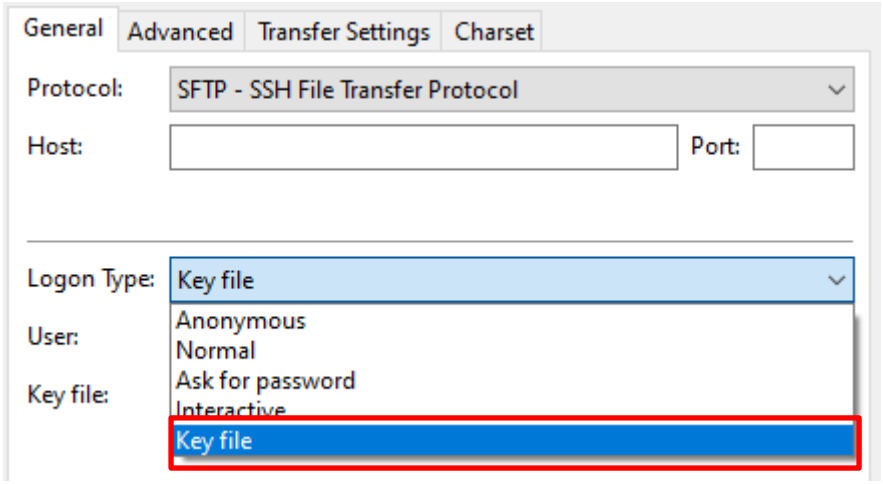
5. You should now be presented with the following pop-up



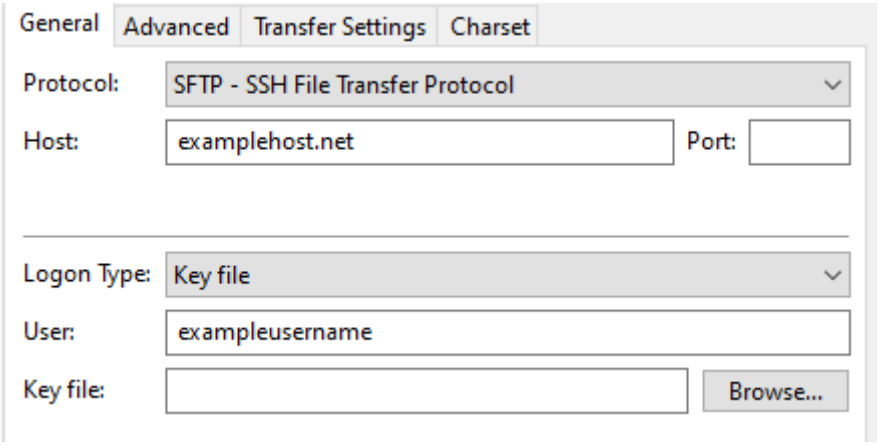
6. You will need to change the following settings from the general tab
    - Change the protocol to SFTP – SSH File Transfer Protocol



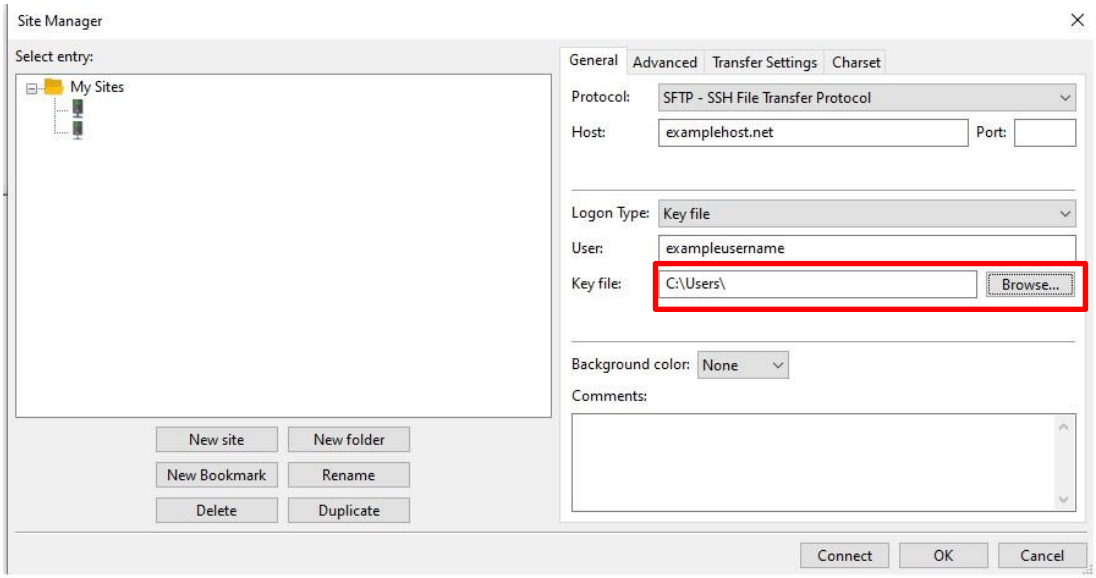
    - Change the logon type to Key file



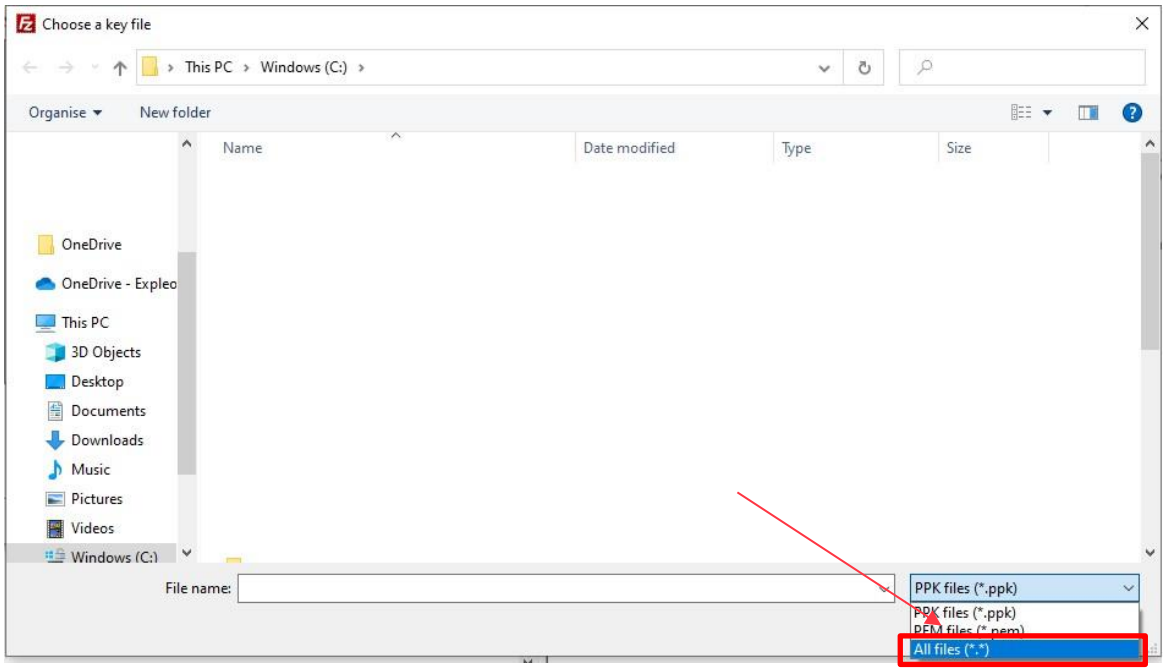
7. You will next need to type your host name and username



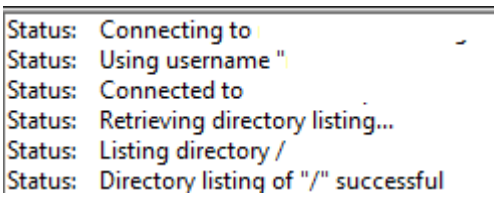
8. Next, you will need to locate where your Key file and input its directory in the Key file section

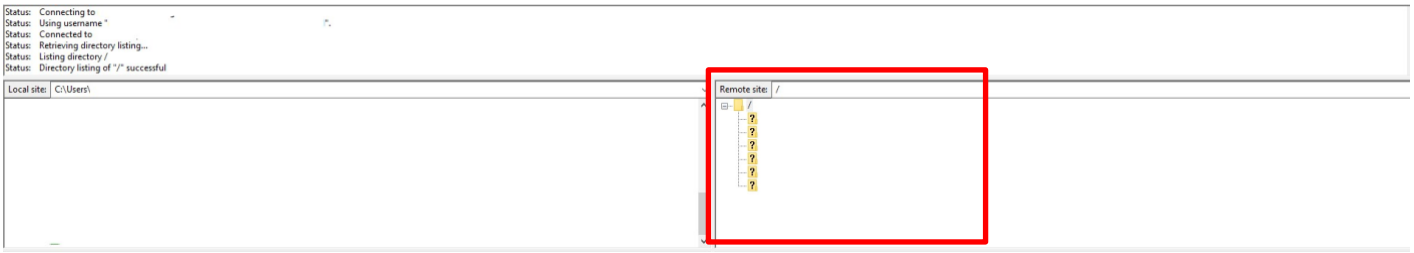


When browsing for your key, ensure to set the file type to all files, this is because your key file may not be recognised otherwise

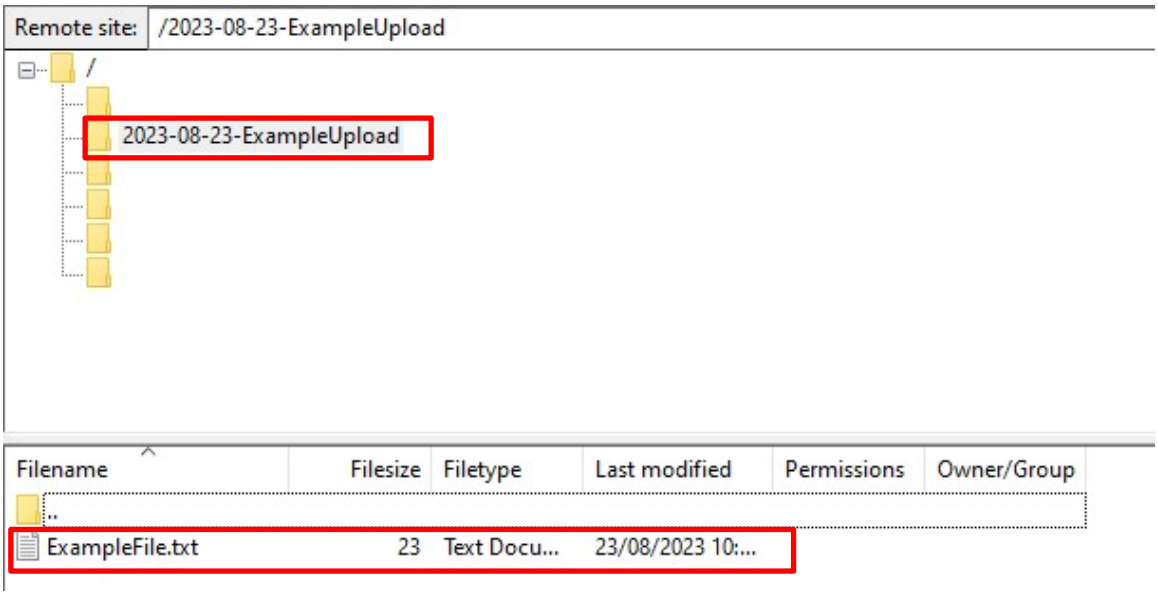


9. Once complete, you can now press connect and you should successfully connect. On the right side of FileZilla, you should now see a new directory.

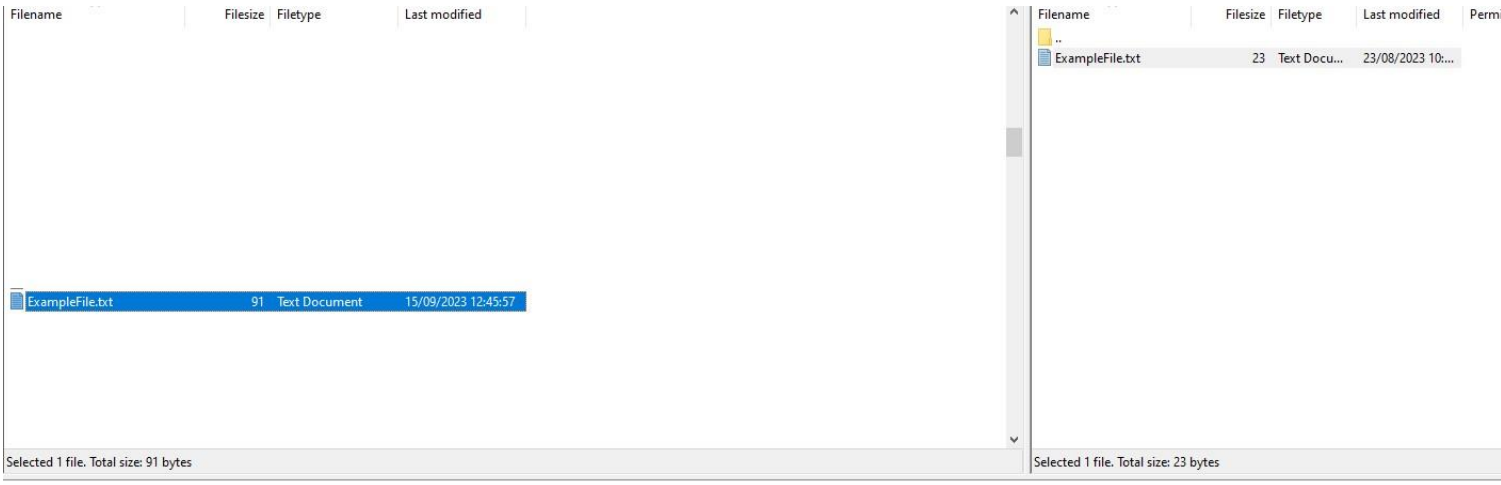




10. To download a file to your local machine, you must click on the specific folder which you want to download a file from



11. You must now chose to which directory you would like to save the file from the left side of FireZilla. Once that's complete, double click on the file you would like to download, and the file will be downloaded to your local machine.



4.6 Frequent Questions and Answers

- **Can a PP request access for Service Providers users?**

  Yes. No restrictions.

- **If a PP assign different users or Service Providers to their different MPID/Market Roles?**

  Yes. Different sftp containers (or folders) will be created per MPID/Market Role combination when different access is required.

- **Is there a limit on the number of users?**

  No

- **Do I need to have my private and public keys ready before using SFTP from the command line?**

  Yes, you should have your private and public keys generated beforehand. Additionally, you should have sent your public keys to the MHHS program, as they would have instructed you.

- **What happens if I forget my private key file or passphrase?**

  A new private-public key pair will need to be generated. Contact the MHHS Testing mailbox to register a new key.

- **How do I contact support or get assistance if I encounter issues with SFTP access or file transfers?**

  Send an email to the testing mailbox: testing@mhhsprogramme.co.uk