

SFTP Guide





Contents

1.1	Change Record	2
1.2	Reviewers	2
1.3	References	2
1.4	Terminology	2
1.5	Summary of Changes	2
2	Introduction to SFTP	3
2.1	MHHS Data SFTP Environment	3
3	MHHS – SFTP User Guide	4
3.1	Step 1: Request Access to SFTP Environment	5
3.2	Step 2: Obtain and inform IP Addresses – Allow List	4
3.3	Step 3: Generate Private/Public Keys	5
3.	3.1 Windows – Generate Private/Public Keys	5
3.	3.2 MacOS - Generate Private/Public Keys	6
3.	3.3 Added Alternatives to create Public/Private Keys	7
3.4	Step 4 – Access the SFTP to download and upload files	10
4	Appendix	11
4.1	Known supported SFTP Clients	11
4.2	Windows Users – SFTP Guide using WinSCP	12
4.2	2.1 SFTP – How to Connect using WinSCP	12
4.2	2.2 SFTP – How to Download a file using WinSCP	14
4.2	2.3 SFTP – How to Upload a file using WinSCP	15
4.4	Windows Users- Connect and transfer data using Command Line	16
4.5	Windows Users- Connect and transfer data using FileZilla	18
4.6	Frequent Questions and Answers	23

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	1.1	Included Step-by-Step guideline for different tools and FQA
	Sunderrajan		
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	24 th 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.

#	Item	Description						
1	Data Storage – SI – Intra server security	 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 						
2	Data Storage – SI – Data in rest encryption	All data in the stor	All data in the storage shall be encrypted using 256-bit AES encryption					
3	Data Storage – SI – Data Transfer Protocol	SSH File Transfer	SSH File Transfer Protocol (SFTP)					
4	Data Storage – SI – SSH Authentication methods	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						
5	SSH Client algorithms		rticipants the host SHA256 fingerprint and put must use algorithms specified in table below:					
		Type Host key ¹	Algorithm rsa-sha2-256* rsa-sha2-512* ecdsa-sha2-nistp256 ecdsa-sha2-nistp384					
		Key exchange	ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group-exchange-sha256					
		Ciphers/encryption	aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-ctr aes192-ctr aes256-ctr					
		Integrity/MAC	hmac-sha2-256 hmac-sha2-512 hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com					
		Public key	ssh-rsa* ecdsa-sha2-nistp256 ecdsa-sha2-nistp384					
		*RSA keys must be m	inimum 2048 bits in length.					

Table 1: SFTP Technical Description

	Description						
Data Storage – SI – Restricted IPs access	Enable access to the data only from the selected Participants IP addresses and SI.						
SFTP Server Fingerprint	MHHS SFTP – Valid host keys						
	Region	UK South					
	Host Key type	ecdsa-sha2-nistp256					
	SHA 256 fingerprint	weMVzOmQn1MdMp5XBoU9SdN5meBbx/8nvA8dB45w8Ck=					
	Public key	AAAAE2VjZHNhLXNoYTItbmlzdHA yNTYAAAAIbmlzdHAyNTYAAABBBEnBl lEm4/HsTP+ZNhlc8YnSAYWF23tibZDqGxf0yBRT U/ncuaavuQdIJSTcJb0NcXG7skEmq3StwHT0FPMWN8Y=					
	Region	UK South					
	Host Key type	ecdsa-sha2-nistp384					
	SHA 256 fingerprint	HpsZ8zoOCCsUbpD3nAOtxpuKIvn0L8KGyg1KMLuMUqU=					
	Public key	AAAAE2VjZHNhLXNoYTItbmlzdHAzODQAAAAIbmlzdHAzODQAAAB h6Gd/672brwX1kOhH31Z1dBRj+bcEmemcdmTEe038 8cJ3RRQYJD6525UnRHA7bPOx9Uq24EJQ S8auxRgNCUJ313ZH9QjcwX/MDRFPnUrNosH8NkcPmJ/pezVeMJLqs3Qw==					
	Region	UK South					
	Host Key	rsa-sha2-256					
	SHA 256	3nrDdWUOwG0XgfrFgW27xhWSizttjabHXTRX8AOHmGw=					
	Public key	AAAAB3NzaC1yc2EAAAADAQABAAABAQCdLm+90R0p5zrc6nLKBJWNrTnUeCeo8 n1v9Y3QMicwYMqmKs/s59t5V3ABWnus4TXH3bqgnQW30QWLg0 Hse/35KLWGERmBbEdK01J7ArQ9QQBVMEZoftW3DPhrAWVTfCYhc0Os6+gW021d ifNx+WW2O5T1dL31pk+UvdhnQKRHLX31cqx5vuUmiwq4m1bBx+rY8B/xngP2bzx/oYXdy1 19fZbWMAQ6FwJBavIs5WL017snRd0sy5A5eMrYo11Ew11ATwYeUv8g 3PzrryZur+7gu/KJw9463j5PjfUD9HCKWj s/gZNuqQ5dif7utiQYbVe4L0TPWOmuLA25JJRZaF					
	Region	UK South					
	Host Key type	rsa-sha2-512					
	SHA 256 fingerprint	Csn18SFb1kdpVVsJC1jNVSyc2eDWdCBVQj9t6J3KHvw=					
	Public key	AAAAB3NzaC1yc2EAAAADAQABAAABAQDIwNE frP6Httmm5GoxwprQ57AyD6b3EOVe5pTGQWIOzxnrIw2KnDPL07KNa33xZOmtXro5P Yyhr5eKNLKFiQMEerkB11IZSNAvc4Whb0pZVD0L9N7Pdy2SetoF4m5BCXdC48kZntqgkpzXoDbFiaAV In52QCHB5fOuBP51id8+k3zqG0o+K0MHb6qcbYV8gdQeOn/PlJzKE4M0Ie8na3 akHd6vf3jOdK/hNN03+eUK8q159KCJKSMDj/J3rnue9L8Xge KKA2PkvH3ncH4VBXCCSUDkg5f+aoiJ0Fy8GV0Tk2s7QDMzD9y37D9V20P166q4 pjFG0FK0mJmrgqxWNy5					
	Restricted IPs access	Restricted IPs access SFTP Server Fingerprint MHHS SFT Region Host Key Host Key SHA 256 fingerprint Public key SHA 256 fingerprint Public key SHA 256 SHA 256 fingerprint Public key SHA 256					

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:



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.

💷 Run	×
	Type the name of a program, folder, document or Internet resource, and Windows will open it for you.
<u>O</u> pen:	<mark>cmd ~</mark>
	OK Cancel <u>B</u> rowse

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

In this example, changed my directory to Downloads

	ndows [Version 10.0.19045.3324] t Corporation. All rights reserved.
C:\Users\	>cd downloads
C:\Users∖	\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

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

₽ Searce	h resources, servic	es, and docs (G+/)						E	Ę	Q	۲	0
Azure services												
+ 📍	×	.	۲		SQL	S	**	\rightarrow				
Create a Subscription resource	s Quickstart Center	Virtual machines	App Services	Storage accounts	SQL databases	Azure Cosmos DB	Kubernetes services	More services				
Resources												
Recent Favorite												
Name			Туре				Last Viewed					
📍 MHHS Test Data			Subscripti	ion			a day ago					
See all												
Subscriptions	[)	Resource groups		All resources								
				-	,	<mark>∐li</mark> Da	shboard					
Tools				-	,	<mark>∐l</mark> Da	shboard					
Tools Microsoft Learn C ² Learn Azure with free on	line	Azure Monitor Monitor your apps	and	Microsoft De	efender for		st Management alyze and optimiz					
Microsoft Learn 📑	line 🏵		and	Microsoft De	efender for apps and		st Management					
Microsoft Learn e* Learn Azure with free on	line	Monitor your apps	and	Microsoft De Cloud Secure your	efender for apps and	s co An do	st Management alyze and optimiz					

Figure 8: Azure portal

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

Microsoft Azure			P ssh				~	E 6	ψw
Home > Marketplace			All Azure Ad	Services (1) Marketplace (3) tive Directory (0)	Documentation (99+) R	esources (0) Resource Groups	(0)		
Set Started			Services						
Service Providers	Search the Marketplace	-	🗢 SSH key	5					
danagement	Azure services only		Marketplac						
management	Recommended for you		🚊 SSH Key		EZSSH				
Private Marketplace			🙆 SFTP Se	rver Secure SSH					
Private Offer Management	#Sindhe	anfront 2000-	Documenta	tion			See all		
dy Marketplace	Twilio SendGrid	Azure Monitoring		ys to connect to Linux VMs - Azure Vir	tual Machines n SshConfigura	tion Class (Microsoft Azure PowerShell		say-as-you-	
	SendGrid	INFRONT SYSTEMS PT		eps to create an SSH key pair - Azure \		SSH connection issues to an Azure VN	4 - Virtual Ma		
avorites	SauS	Managed Services		to Azure Arc-enabled servers - Azure					
lecently created	Reliable email delivery, at scale.	Infront's Monitoring-a						ith Atlas, the	
Private plans		observe every network at any scale, anywhere	Create and	use an SSH key pair for Linux VMs in a	Azure - Azure Vi Create SSH k	eys in the Azure portal - Azure Virtual	Machines 📴	20DB on	
ategories			🚸 Continu	e searching in Azure Active Directory					
aregones	Starts at Free		Searching all su	bscriptions.			R Give feedback		
T & Management Tools (3344)	Subscribe 🗸 🗢	Create \lor	Ø	Create 🗸 🗢	Create 🗸 💙	Subscribe 🗸 💙	Subscribe \lor	\heartsuit	
Compute (3316)	Trending now								
Security (2454)	Irending now								
Analytics (2168)	0	RF(.*)			Ŧ	0	- 34		
Developer Tools (2020)	OpenVPN on Ubuntu 22.04	RegexFlow Azure Fi		Ubuntu 20.04 LTS with	Configuration Manager	FortiSIEM - SIEM, Log	Kafka		
Neb (1719)	Minimal Art Group	Regular Expressions Epicycle Limited	•	iRedMail (IMAP, SMTP, POP3) Virtual Pulse S. R. O.	h	Analytics	Niles Partners Inc.		
letworking (1328)	Art Group Virtual Machine			Virtual Pulse S. R. O. Virtual Machine	Puppeteers Oy Virtual Machine		Niles Partners Inc.		
	Virtual Machine Modern and open-source VPN tool	Azure Application RepexFlow is a Repular	Expression	Virtual Machine With iRedMail, you can deploy a	Virtual Machine Setup Puppetserver, PuppetDB and	Azure Application Fortinet FortiSIEM provides multi-	R aims to provide a	unified high-	
itorage (1230)		Azure Function design a Regex Action in Powe	ed to deliver	fully fiedged, full-featured mail server in several minutes.	Puppetboard effortlessly	vendor SiEM, Analytics, Reporting and Alerting	throughput, low-la for handling real-ti	tency platform	
N + Machine Learning (1224)									

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'

	,P Search resources, services, and docs (G+/)	5 6 0 6 A
iome > SSH keys >		
Create an SSH key		
Basics Tags Review + create		
Creating an SSH key resource allows you to manage and use p Learn more	sublic keys stored in Azure with Linux virtual machines.	
Project details		
Select the subscription to manage deployed resources and co all your resources.	sts. Use resource groups like folders to organize and manage	
Subscription * 💿 MHHS Test Data	✓	
Resource group * ()	\checkmark	
Create new		
Instance details		
Region (US) East US		
Key pair name * Name the SSH put	dic key	
SSH public key source Generate new key	pair V	
Review + create < Previous Next : Ta		

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
Γ	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	Ахway
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: <u>https://winscp.net/eng/download.php</u>



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

🔒 Login 🕎 New Site		Session File protocol:		_	
		SFTP Host name: User name:	~	Password:	Port number:
		Save	 		Advanced 🖛
Tools 🔹	Manage 🔻		🔁 Login 🛛 👻	Close	Help
Show Login dialog on sta	_			Close	

Figure 9: WinSCP Login Screen

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

New Site		Session		
		File protocol:		
		SFTP	-	
		Host name:		Port number:
		mhhsdevstorageaccount.blo	b.core.windows.net	22 🗘
		User name:	Password:	
		mhhsdevstorageaccount. sft		
		Save 🔻		Advanced
			~	~
	Manage 🔻	Login	Close	Help

Figure 10: Advanced View

- Click on Authentication

Advanced Site Settings		?	\times
Environment - Directories - Recycle bin - Encryption - SFTP - Shell Connection - Proxy - Tunnel SSH - Key exchange - Authentication - Bugs Note	□ Bypass authentication entirely Authentication options ☑ Attempt authentication using Pageant ☑ Attempt 'keyboard-interactive' authentication ☑ Respond with a password to the first prompt Authentication parameters ☐ Allow agent forwarding Private key file:		
	Display Public Key Tools Certificate to use with the private key: GSSAPI Attempt GSSAPI authentication Allow GSSAPI credential delegation		
Color 🔻	OK Cancel	He	elp

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:

New Site	Session	
	File protocol:	
	SFTP ~	
	Host name:	Port number:
	mhhsdevstorageaccount.blob.core.windows.net	22 🖨
	User name: Password:	
	mhhsdevstorageaccount. sftp-si-	
	Save 💌	Advanced

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):

📕 / <root> 🔹 🎽 🛛 🐨 💟 🔹 🖾 🏠 🗌</root>				
📲 📝 Download 👻 📝 Edit 🔹 🗙 🛃 Download	ties 🔹 📫 N	lew - 🕇 🚽 🗸		
1				
Name	Size	Changed	Rights	Owner
2023-08-22-examplefile		22/08/2023 14:53:48	rwxr-x	0
O basics.html	1 KB	24/08/2023 09:56:40	rw-r	0
SFTP-Illustration-Part2.txt	1 KB	24/08/2023 10:25:01	rw-r	0

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:

	_			_		_				
		🖥 • 🍸 • 🛯 🖬 🕅 🏫								
Download	•	📝 Edit 🝷 🗙 🏑 🕞 P	Propertie	es	-	Î N	ew 🕶 🛨 🗖 🤝			
1										
Jownload / Name 2023-08-22- basics.html		Open Edit Download	F5 hift+F5 mote fi Ctrl+C	<pre>> le(s) </pre>		Size KB KR Dov Dov	W • • • • • • • • • • • • • • • • • • •	F6	Rights rwxr-x rw-r	Owner 0 0

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:

Is: 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



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: <u>https://filezilla-project.org/download.php?platform=win64</u>



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

lost: Username: Password: Port: Quickconn	*	
iii 🕹 Downloads	Remote site:	
0) ** Fivorites 0) 0 	~	
Filename Filesize Filetype Last modified	Filename Filesize Filetype Last modified Permissions Owner/Group	
н	Not connected to any server	
64 files and 22 directories. Total size: 12,622,731,721 bytes	V Not connected.	
ever/Local file Direction Remote file Size Priority Status	luor connecter	

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

elect entry:			General Advanced Transfer Settings Charset	
⊡ <mark></mark> My Sites			Protocol: FTP - File Transfer Protocol Host: Port: Encryption: Use explicit FTP over TLS if available	``
			Logon Type: Normal User: Password:	~
			Background color: None V Comments:	^
	New site	New folder		
	New Bookmark	Rename		
	Delete	Duplicate		~

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

Protocol:	SFTP - SSH File Transfer Protocol 🗸
11-st	FTP - File Transfer Protocol
Host:	SFTP - SSH File Transfer Protocol
	Storj - Decentralized Cloud Storage

• Change the logon type to Key file

General	Advanced Transfer Settings Charset
Protocol	SFTP - SSH File Transfer Protocol 🗸
Host:	Port:
Logon Ty	rpe: Key file 🗸 🗸
User:	Anonymous
o sen	Normal
Key file:	Ask for password
	Key file

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

General Adv	Advanced Transfer Settings Charset							
Protocol: SFTP - SSH File Transfer Protocol								
Host:	examplehost.net Port:							
Logon Type:	Key file \checkmark							
User:	exampleusername							
Key file:	Browse							

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

elect entry:			General Ad	vanced	Transfer Settings Charset				
□ My Sites			Protocol:	Protocol: SFTP - SSH File Transfer Protocol					
1			Host:	examp	plehost.net	Port:			
			Logon Type:	Key file	e		Ŷ		
			User:	2	pleusername		_		
			Key file:	C:\Use	ers\	Brows	e		
			Background Comments:	color: [None 🗸				
	New site	New folder					0		
	New Bookmark	Rename							
	Delete	Duplicate					V		

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

Z Choose a key file				×
\leftarrow \rightarrow \checkmark \bigstar This PC \Rightarrow Windows (C:) \Rightarrow		ٽ ~	Q	
Organise 🔻 New folder				0
^ Name ^	Date modified	Туре	Size	
OneDrive				
OneDrive - Expleo				
This PC 3D Objects				
Desktop				
Documents				
Uownloads				
👌 Music				
Pictures				
Videos				
🟥 Windows (C:) 🎽 🗕				
File name:			PPK files (*.ppk)	~
			PPK files (*.ppk) PEM files (*.pem)	- 1
			All files (*.*)	

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.

-

 Status:
 Connecting to

 Status:
 Using username "I

 Status:
 Connected to

 Status:
 Retrieving directory listing...

 Status:
 Listing directory /

 Status:
 Directory listing of "/" successful

Status: Connecting to Status: Using unsamme Status: Connected to Status: Retrieving directory isting Status: Listing directory // Status: Directory for successful		
Local site C/UserN	Remote size / - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2	

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

Remote site: /2023-08-23-	d			
Filename	Filetype	Last modified	Permissions	Owner/Group

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.

	Ų					
ExampleFile.txt 91 Text Document 15/09/2023 12:45:57						
	-					
		ExampleFile.txt	23	Text Docu	23/08/2023 10:	
Filename Filesize Filetype Last modified	^	Filename	Filesize	Filetype	Last modified	Perm

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