|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Company Sending Files** | Click or tap here to enter text. | | | | | | |
| **Client Names on Files**  **(If different then Company)** | Click or tap here to enter text. | | | | | | |
| **Contact Full Name** | Click or tap here to enter text. | | | **Title** | | Click or tap here to enter text. | |
| **Contact Email** | Click or tap here to enter text. | | | **Contact Phone** | | Click or tap here to enter text. | |
| **Product Type(s)** | **FSA** | **DCA** | **Commuter** | | **HRA** | **HSA** | **COBRA** |

**MoneyWise Solutions SFTP Access Request Form**

**Options for SFTP Transmission** – **Must Select One**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Key based authentication (Recommended)** | | | | **Password based authentication** | | |
|  | **Option 1 (Recommended)**  Client generated SSH Key pair (public key provided to MoneyWise) | | |  | **Option 3**  Password Authentication | |
|  | **Step 1** | Create SSH Public and Private Key Pair  (see next page for accepted algorithms) | | **Step 1** | Send this completed form to Moneywise Solutions to contact listed below |
|  | **Step 2** | Client to securely email Public Key along with this request form to MoneyWise Solutions to contact listed below. | | **Step 2** | Moneywise will supply the connection credentials for the user. |
|  | **Step 3** | Moneywise will provide connection information needed to submit files. | | **Step 3** | Moneywise will provide connection information needed to submit files. |
|  | **Step 4** | Client to send test file. | | **Step 4** | Client to send test file. |
|  | **Option 2**  MoneyWise generated SSH Key pair (private key provided to client) | | |  | | |
|  | **Step 1** | | Send this completed form to Moneywise Solutions to contact listed below |  | | |
| **Step 2** | | Moneywise will supply the private key for the user |
| **Step 3** | | Moneywise will provide the connection information needed to submit files |
| **Step 4** | | Client to send test file |
|  | **File Naming Conventions**  Please use the following File Naming Conventions when sending files to MoneyWise Solutions  **ClientName\_ProductType\_mmddyyyy** (date of transmission)  **Example: ABCcomany\_FSA\_02062024**  *When sending test files, please add TEST after the date, i.e.* ABCcomany\_FSA\_02062024\_TEST | | | | | |

|  |
| --- |
| **Option 1, 2, and 3 General Info**  *Full Details will be emailed to you at completion of set up.* |
| **Server: moneywisesftpstorage.blob.core.windows.net**  Port: 22  Login: moneywisesftpstorage.<TBDUsername>  Password (if applicable): TBD |

**Please email this completed form to the contact below. Additionally, if you are selecting Option 1, please email the SSH Public Key. You can expect to receive your connection details within 3-5 business days.**

|  |  |  |
| --- | --- | --- |
| **SFTP Contact Information:** | Carter Boaze | [csboaze@moneywisesolutions.com](mailto:csboaze@moneywisesolutions.com) |

## **MoneyWise Solutions SFTP Overview**

## **Introduction**

MoneyWise Solutions maintains a network protocol called Secure File Transfer Protocol (SFTP) to provide secure file transfers for its clients. The main use of the MoneyWise SFTP is to transfer eligibility/enrollment data. It is also used to transfer other sensitive files to and from clients.

The purpose of this document is to provide instructions for clients who need to establish a connection with the Moneywise Solutions’ SFTP service in order to transfer eligibility/enrollment data or other files.

Users must request an SFTP account to securely transfer files. You can authenticate users connecting via SFTP by using a password or a Secure Shell (SSH) public-private keypair.

## **Authentication**

Authentication to the SFTP server occurs by means of a cryptographically linked pair of keys called a secure shell (SSH) key pair. This method, more secure than standard username/password authentication, is called SSH key-based authentication. One key in the pair is public and the other key is private. The public key can be freely shared. The private key should never be shared. A security action performed by one key in the pair can be verified only by the other key in the pair. Proof of identity is one such action. In this way, MoneyWise can validate a user’s identity assertion using the user’s public key without ever needing the private key. One distinct advantage of SSH key-based authentication is that the user can automate file transfers without needing to hardcode a password in a script or program.

**SSH key-based Authentication**

A public-private key pair is the most common form of authentication for Secure Shell (SSH). The private key is secret and should be known only to the local user. The public key is stored in Azure. When an SSH client connects to the storage account using a local user identity, it sends a message with the public key and signature. Our SFTP server validates the message and checks that the user and key are recognized by the storage account.

If you choose to authenticate with private-public key pair (option 1), you will need to generate the key pair and provide us the public key. Supported algorithms can be found here: <https://learn.microsoft.com/en-us/azure/storage/blobs/secure-file-transfer-protocol-support#supported-algorithms>. An example of generation can be found here <https://learn.microsoft.com/en-us/azure/virtual-machines/linux/ssh-from-windows#create-an-ssh-key-pair>

**Passwords**

You can't set custom passwords, so we will generate one for you. If you choose password authentication, then your password will be provided with the other connection information. Make sure to copy that password and save it in a location where you can find it later. If you lose the password, we'll have to generate a new one. For security reasons, you can't set the password yourself.