SFTP Account Configuration

Contents

Introduction

UKG HR Service Delivery provides a transit area for various mass actions on the platforms. You can access this space through a secure SFTP connection.

The purpose of this document is to describe the different steps required to set up an SFTP account as well as the ways to connect to it.

Setting up an SFTP account

Step 1: Create an SSH key

An SSH key (Secure Shell key) allows you to authenticate securely. Keys are generated via a command line, see Creating an SSH key via a command line (Secure Shell).

Step 2: Share your information

In order to create an SFTP account for you, we need the following information:

- Your public IP address(es) (workstation and/or server)
- Your public key

Check with your IT department to find out which public IP addresses will be used.

Step 3: Receive your identifiers

UKG HR Service Delivery grants you access, then provides you with the information you need to log in to your account:

- Your username
- The IP address of the SFTP server
- The server port

Check with your IT department to make sure you can access the server at the requested IP address and port.

Step 4: Configure your SFTP client

Once all the information has been transmitted, you can configure your client to connect.

- Example of configuration with FileZilla: Configuring an SFTP client (FileZilla)
- Example of an automation script in Python: Example of an automation script

You can find all the connection information to the UKG HR Service Delivery SFTP servers in the documentation available at this address: https://doc.people-doc.com/client/guides/synchronization/.

Principles of key-based authentication

Key-based authentication involves 3 components:

- A private key: Allows you to prove your identity to the SFTP server.
  The private key should not be sent to us. It must be kept and installed on your workstations/servers that will connect to our server.

- A passphrase (optional): Used to secure the private key.

- A public key: Allows the server to authorize the corresponding private key.
  The **public key (ending in ".pub")** is to be provided to UKG HR Service Delivery in order to configure your access. **UKG HR Service Delivery only accepts public SSH keys in OpenSSH format.**

For more information about security related to the use of SSH keys:
https://www.ssh.com/ssh/openssh/#sec-What-Risks-Are-Associated-with-SSH-Keys

Creating an SSH key via a command line (Secure Shell)

The **ssh-keygen** tool exists on Windows, Linux and Mac, so the syntax for generating a key is common.

In a Windows terminal or command prompt, you can use the wizard by typing only:

- *ssh-keygen*

Or use the following syntax by modifying the values according to the table below:

- *ssh-keygen -t **KEY_TYPE** -b **BITS** -C "**COMMENT**" -f "**LOCATION_&_NAME**"*

We recommend that you use the full syntax so that you can explicitly specify the characteristics of your key (see the recommendations in the table below).

In addition, it is recommended that you assign a passphrase to the generation of your SSH key to ensure its security. This passphrase should only be known to you. The two commands mentioned above will prompt you to define it.

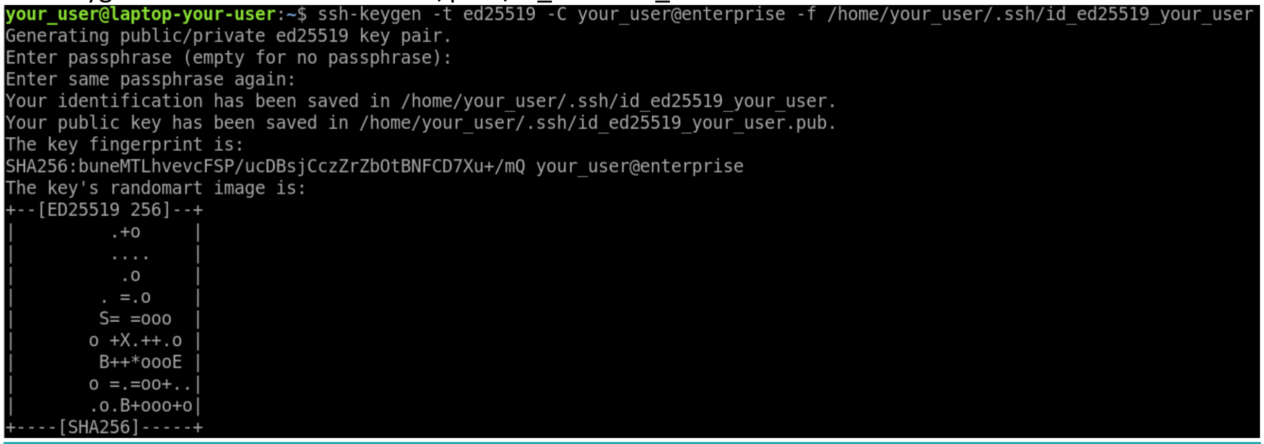
Assign a comment to each of your SSH keys to differentiate them, making it easier to communicate when multiple public keys are authorized.

Section	Key Features
KEY_TYPE	See our online documentation for supported and recommended key types and formats, and associated sizes.
COMMENT	• Identification of the owner of the key (email address) *Example:* *martin_doe@company.com*
LOCATION_&_NAME	Location where keys are created • Windows: *c:\users\Martin_Doe\id_rsa_martin_doe* • Linux / Mac: */home/martin_doe/.ssh/id_rsa_martin_doe*

# Examples via full syntax

## SSH key ed25519

ssh-keygen -t ed25519 -C "email" -f /path/id_ed25519_owner



```
your_user@laptop-your-user:~$ ssh-keygen -t ed25519 -C your_user@enterprise -f /home/your_user/.ssh/id_ed25519_your_user
Generating public/private ed25519 key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/your_user/.ssh/id_ed25519_your_user.
Your public key has been saved in /home/your_user/.ssh/id_ed25519_your_user.pub.
The key fingerprint is:
SHA256:buneMTLhvevcFSP/ucDBsjCczZrZbOtBNFCD7Xu+/mQ your_user@enterprise
The key's randomart image is:
+--[ED25519 256]--+
|         .+o     |
|         ....    |
|          .o     |
|        . =.o    |
|        S= =ooo  |
|       o +X.++.o |
|        B++*oooE |
|       o =.=oo+..|
|       .o.B+ooo+o|
+----[SHA256]-----+
```

## SSH key rsa-sha2-512

ssh-keygen -b 4096 -t rsa-sha2-512 -C "email" -f /path/id_rsa-sha2-512_owner

## SSH key rsa-sha2-256

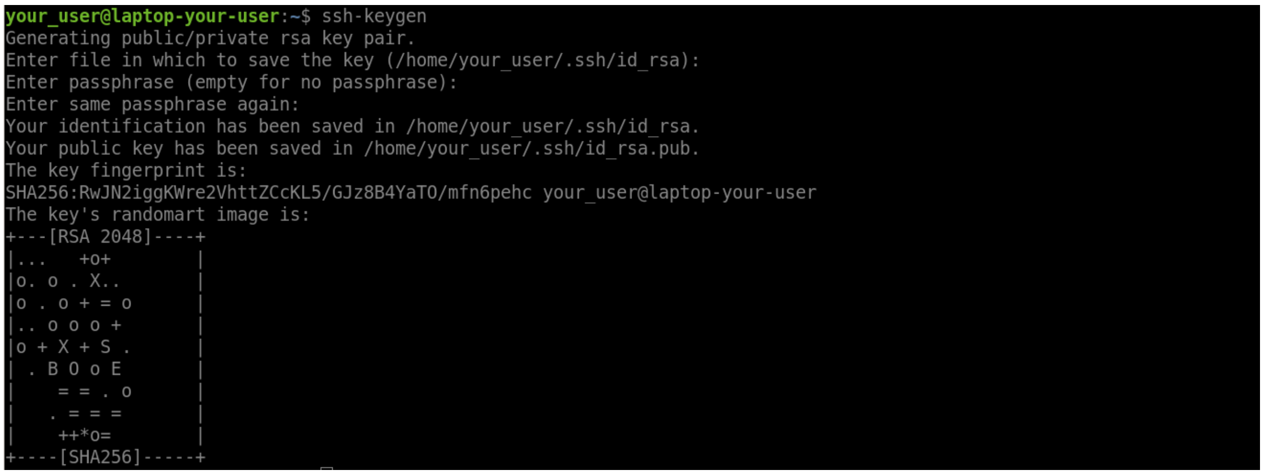
ssh-keygen -b 4096 -t rsa-sha2-256 -C "email" -f /path/id_rsa_sha2-256_owner

## SSH key rsa

ssh-keygen -b 4096 -t rsa -C "email" -f /path/id_rsa_owner

# Example via the assistant

ssh-keygen wizard



```
your_user@laptop-your-user:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/your_user/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/your_user/.ssh/id_rsa.
Your public key has been saved in /home/your_user/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:RwJN2iggKWre2VhttZCcKL5/GJz8B4YaTO/mfn6pehc your_user@laptop-your-user
The key's randomart image is:
+---[RSA 2048]----+
|...   +o+        |
|o. o . X..       |
|o . o + = o      |
|.. o o o +       |
|o + X + S .      |
| . B O o E       |
|    = = . o      |
|   . = = =       |
|    ++*o=        |
+----[SHA256]-----+
```

Configuring an SFTP Client (FileZilla)

Download and install FileZilla: https://filezilla-project.org/download.php?type=client

Click File -> Site Manager -> New Site.

Fill in the fields according to the server you want to connect to.

Protocol	SFTP
Host	SFTP server (DNS) address *example: sftp_server_address.ukg.com*
Port	9030
Logon Type	Key file
User	Your login, transmitted by UKG HR Service Delivery
Key file	Path to your private key *example: c:\users\Martin_Doe\id_rsa_Martin_Doe*

Finally, click on Connect (the Site profile is automatically saved).

If a passphrase was defined when creating your key pair (public and private), FileZilla prompts you to fill it in at the time of login.

During the first connection, a warning is displayed to ensure that you are connecting to the desired server.

If the fingerprint is the same as the server you want to access [RSA key fingerprint or SSH public key (PEM format) of the server on the official documentation], you can trust this server and associate it with the connection.

If not, please let us know.

Example of an automation script

For production, it is highly recommended to automate the transfer of files from your servers to our SFTP server.

Example of a Python script using the paramiko module.

```
 #!/usr/bin/env python

import paramiko
 paramiko.util.log_to_file('/tmp/paramiko.log')

# Connection

host = 'sftp_server_address.ukg.com’
port = 9030
 transport = paramiko. Transport((host, port))

# Authentication

username = 'xxxx'
key_path = '/home/xxx/.ssh/id_rsa'
key_pass = ''

my_key = paramiko. RSAKey.from_private_key_file(key_path, key_pass)
transport.connect(username=username, pkey=my_key)

# SFTP client

sftp = paramiko. SFTPClient.from_transport(transport)

# Upload using .filepart extension to prevent remote processing during the transfer

local_path = '/home/xxxx/ndmat_yyyy_zzzz_sal_20150909.csv'
remote_path = 'in/will/ndmat_yyyy_zzzz_sal_20150909.csv'
sftp.put(local_path, remote_path + '. filepart')
sftp.rename(remote_path + '. filepart', remote_path)

# Stop gracefully

sftp.close()
transport.close()
```