

# CREATING SSH USER AND SSH KEY

## CREATING STORAGE STRUCTURE

In a terminal window, su to the root user (type `su` and then, when prompted, type the root user password), and then issue the following two commands:

```
mkdir -p /si-data/_sftp
chmod 701 /si-data/_sftp
```

## ADD SFTP GROUP

Create a group for SFTP users.

```
groupadd sftp_users
```

## ADD SFTP USER(S)

Create a user that doesn't have regular login privileges, but does belong to our newly created `sftp_users` group.

```
useradd -g sftp_users -d /x-change -s /sbin/nologin USERNAME
```

Where `USERNAME` is the name of the user.



All users must have random 10 character suffix for example `bifiles_S6qQ4YzptQ` Use this [link](#) for quick generation of the random string.

Create password (to be replaced with SSH key)

```
passwd USERNAME
```

## CREATE USER ENVIRONMENT

Create an upload directory, specific to the new user, and then give the directory the proper permissions.

```
mkdir -p /si-data/_sftp/USERNAME/x-change
chown -R root:sftp_users /si-data/_sftp/USERNAME
chown -R USERNAME:sftp_users /si-data/_sftp/USERNAME/x-change
```

## CONFIGURE SFTP

Add to the bottom of the `/etc/ssh/sshd_config` file the following configuration options

```
Match Group sftp_users
  ChrootDirectory /si-data/_sftp/%u
  ForceCommand internal-sftp
  RSAAuthentication yes
  PubkeyAuthentication yes
  AuthorizedKeysFile /si-data/_sftp/%u/.ssh/authorized_keys
```

Restart SSH with the command:

```
systemctl restart sshd
```

## CREATING SSH KEY

Create a folder to store the key.

```
mkdir /si-data/_sftp/USERNAME/.ssh  
mkdir /si-data/_sftp/USERNAME/x-change/keys  
chmod 700 /si-data/_sftp/USERNAME/.ssh
```

Create a key for a user


```
ssh-keygen -t rsa -b 4096 -C "USERNAME"
```

Point to the `keys` folder `/si-data/_sftp/USERNAME/x-change/keys/id_rsa`

When key is generated, copy .pub key to .ssh folder as authorized\_keys and apply corresponding ownership

```
cp  
/si-data/_sftp/USERNAME/x-change/keys/id_rsa.pub  
/si-data/_sftp/USERNAME/.ssh/authorized_keys  
  
chmod 644 /si-data/_sftp/USERNAME/.ssh/authorized_keys
```

Download and post private key in Engage.

 Remove the keys folder from the server.

After confirmation from a client, remove key file from Engage.

## PASSWORD USE

 Not recommended

`chage -l USERNAME` will show user password settings

`chage -M -1 USERNAME` will remove password restrictions

---

🔄Revision #14

★Created Fri, Jun 17, 2022 8:40 PM by Dennis Ayzin

✎Updated Wed, Aug 10, 2022 6:32 PM by Dennis Ayzin