



[SFTP] No matching host key type found

Last updated by | Shenwang Zeng | Feb 16, 2023 at 7:37 PM PST

ERRORS KEX_FAILURE Message="no matching host key type found" Kex=ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,ssh-dss"

Symptom	Customer is using SshPublicKey auth but can not create a connection
Server log	ERRORS KEX_FAILURE Message="no matching host key type found" Kex=ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,ssh-dss"
Cause	the host key algorithm which sftp server is using doesn't supported by sftp connector underlying sdk, below is the host key algorithm list
Resolution	Use another host key algorithm which is supported by both sftp connector and sftp server to generate key-pair

Follow these steps:

1. Find a substitute host key algorithm which is supported by both sftp connector and sftp server. Connector sdk support algorithm list can be found in github <https://github.com/sshnet/SSH.NET> , sftp server algorithm need to contact server administrator.(we use ed25519 as example below)
2. Prepare local environment to connect to SFTP server through Ubuntu. <https://windowsloop.com/add-ubuntu-to-windows-terminal/>  (if have local linux environment, then can skip this step)

3. Create a new SSH key pair on local machine: **ssh-keygen -t ed25519**

```
shenwang@WIN-7J1LOR5L37H:~$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/shenwang/.ssh/id_ed25519):
/home/shenwang/.ssh/id_ed25519 already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/shenwang/.ssh/id_ed25519
Your public key has been saved in /home/shenwang/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:XV96mmFa2HmYiHT13YrapKx5tDZikvB/j/kbgR0k19A shenwang@WIN-7J1LOR5L37H
The key's randomart image is:
+--[ED25519 256]--+
|      . ++.      |
|      + .E.o     |
|      . +  =     |
|      o * B B    |
|      S + B % o   |
|      .  ..= = *  |
|      o . .+. + o |
|      + oo*o .    |
|      ++=o++     |
+-----[SHA256]-----+
shenwang@WIN-7J1LOR5L37H:~$
```

4. Copy Public Key to Remote Machine, you can find the public key in ***/.ssh

```
shenwang@WIN-7J1LOR5L37H:~$ cd .ssh/
shenwang@WIN-7J1LOR5L37H:~/.ssh$ ls
id_dsa      id_ed25519    id_rsa      id_rsa.pub   known_hosts.old  shenwang_rsa.pub
id_dsa.pub  id_ed25519.pub id_rsa.ppk  known_hosts  shenwang_rsa
shenwang@WIN-7J1LOR5L37H:~/.ssh$
```

the command is in this format: **ssh-copy-id -i algorithm.pub remote_user@remote_IP**, we use ed25519 in this doc and then replace **algorithm.hub** to **id_ed25519.pub**

5. Login the remote sftp server: **ssh remote_user@remote_IP**, if above steps are successful, then you can login in to sever without password

You may encounter cyphers error when use ed25519, **Invalid Sftp credential provided for 'SshPublicKey' authentication type.cipher name aes256-ctr for openssh key file is not supported**, then you can change encryption cypher by adding -Z parameter: **ssh-keygen -t ed25519 -Z aes256-cbc**

<https://github.com/sshnet/SSH.NET/issues/742> 