

## File Transfer (WinSCP version)

Last Update: Feb 5, 2021 (verified with WinSCP 5.17.10)

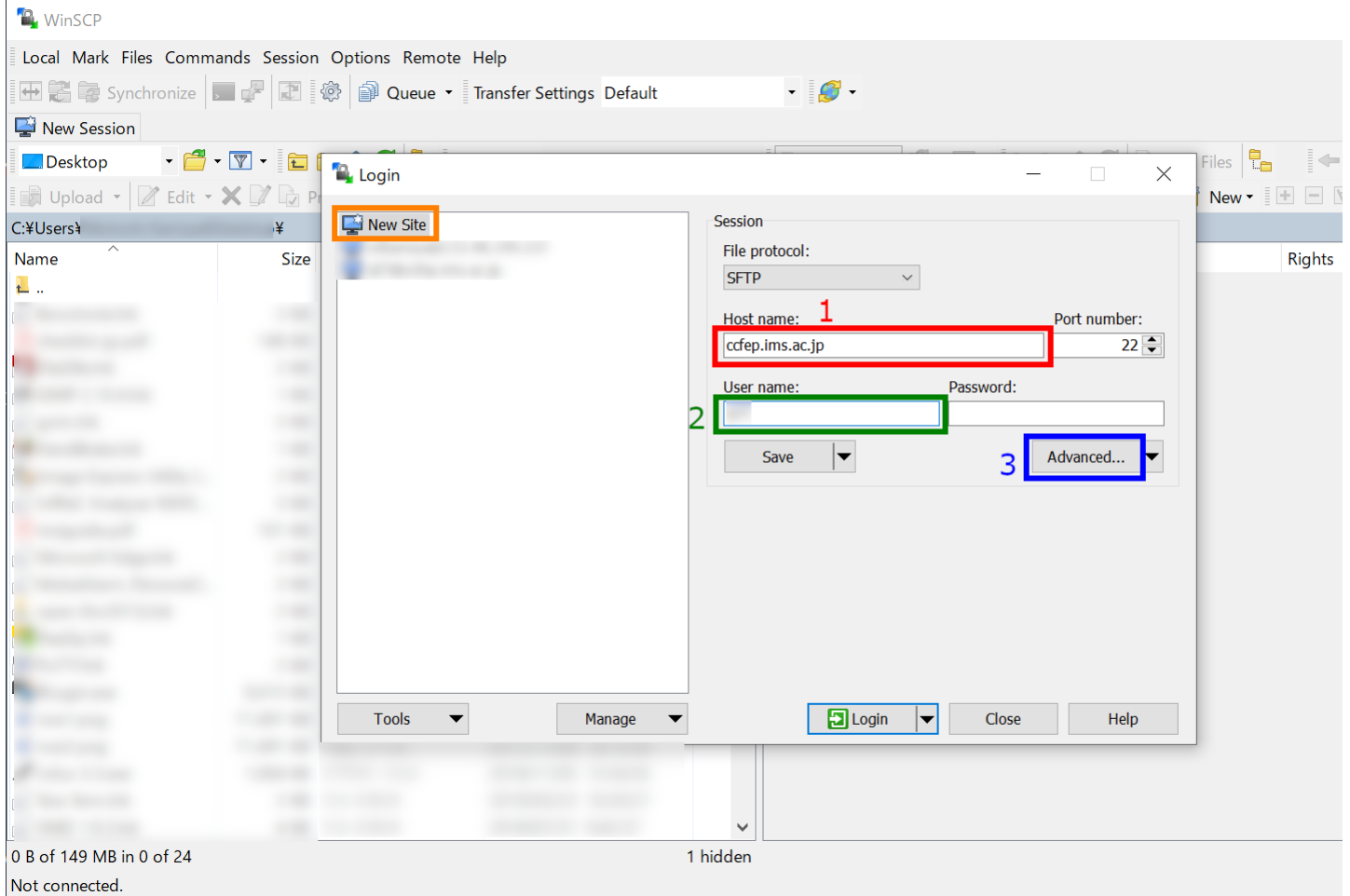
### Installation of WinSCP

You can download WinSCP at <https://winscp.net>. Please install according to the guide.

If you don't have SSH keys, please generate ones first. There are some guides in [Quick Start Guide](#) page.

### How To

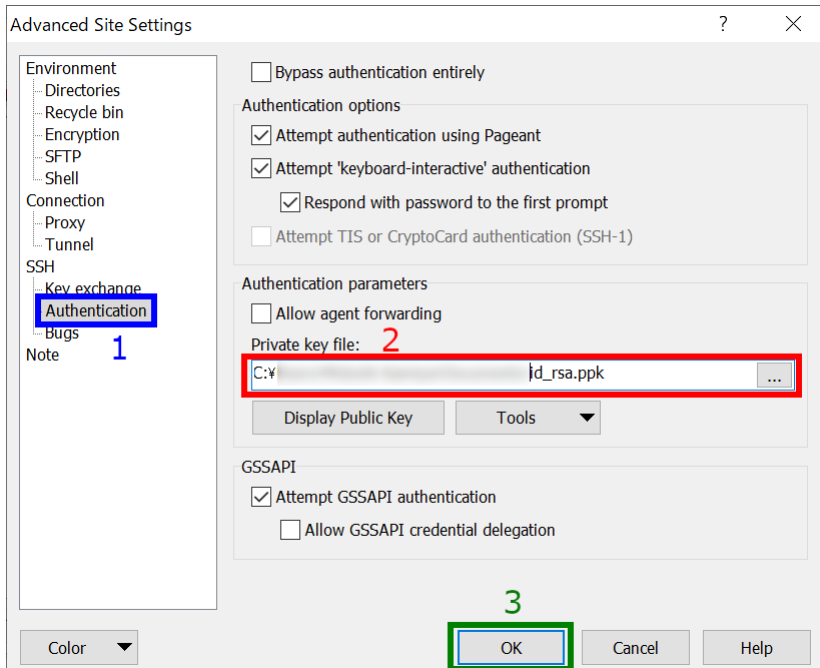
#### 1. Launch WinSCP and Begin Setup



Launch WinSCP and begin configuration as a "New Site".

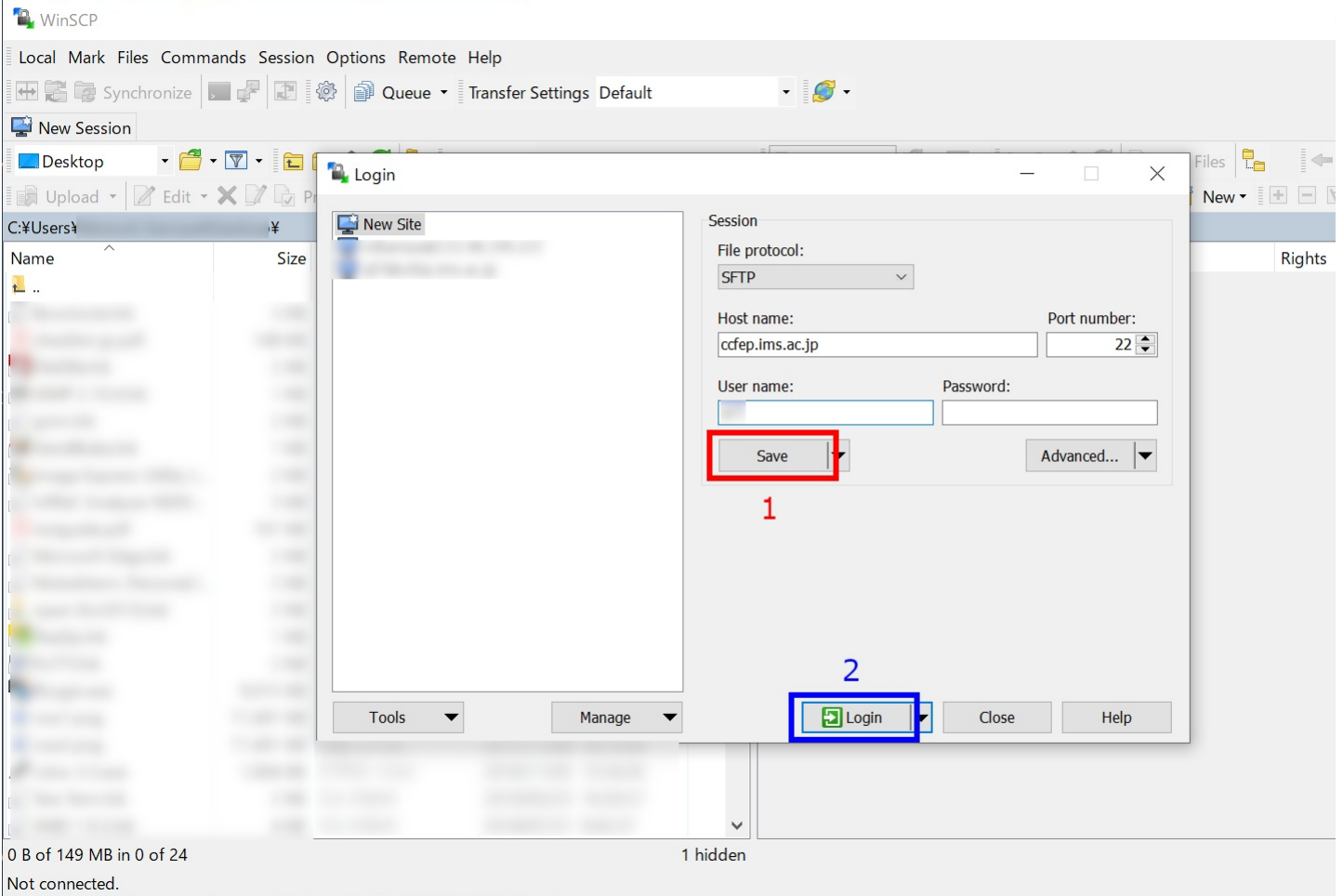
1. input `ccfep.ims.ac.jp` in Host name box
2. input RCCS user name here (3 letter ID)
3. Click Advanced... button for private key setting

#### 2. Specify Private Key



In the "Advanced Site Settings" window, select "Authentication" item inside "SSH" menu, and then specify private key file. (Both of OpenSSH (including Tera Term) and PuTTY formats will be accepted; OpenSSH one will be converted into PuTTY format.) After the private key setup, click "OK" to go back to the initial window.

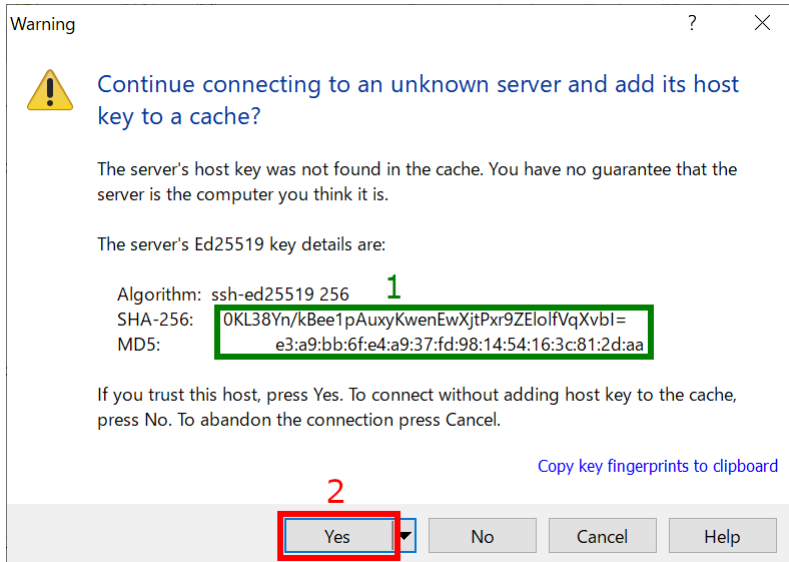
### 3. Save Config and Begin Connection



The screenshot shows the WinSCP application interface. A 'Login' dialog box is open, displaying session configuration. The 'File protocol' is set to 'SFTP'. The 'Host name' is 'ccfep.ims.ac.jp' and the 'Port number' is '22'. The 'User name' and 'Password' fields are empty. A red box highlights the 'Save' button, with a red '1' below it. A blue box highlights the 'Login' button, with a blue '2' above it. The background shows a file explorer window with a 'New Site' dialog open.

At this point, you can begin connection to the frontend server. However, we recommend you to save configuration here. Then, click "Login" to begin connection.

### 4. Security Warning upon first Connection



The warning dialog box contains the following text:

**Warning**

**Continue connecting to an unknown server and add its host key to a cache?**

The server's host key was not found in the cache. You have no guarantee that the server is the computer you think it is.

The server's Ed25519 key details are:

Algorithm: ssh-ed25519 256 **1**

SHA-256: **0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZEloIfVqXvbl=**

MD5: **e3:a9:bb:6f:e4:a9:37:fd:98:14:54:16:3c:81:2d:aa**

If you trust this host, press Yes. To connect without adding host key to the cache, press No. To abandon the connection press Cancel.

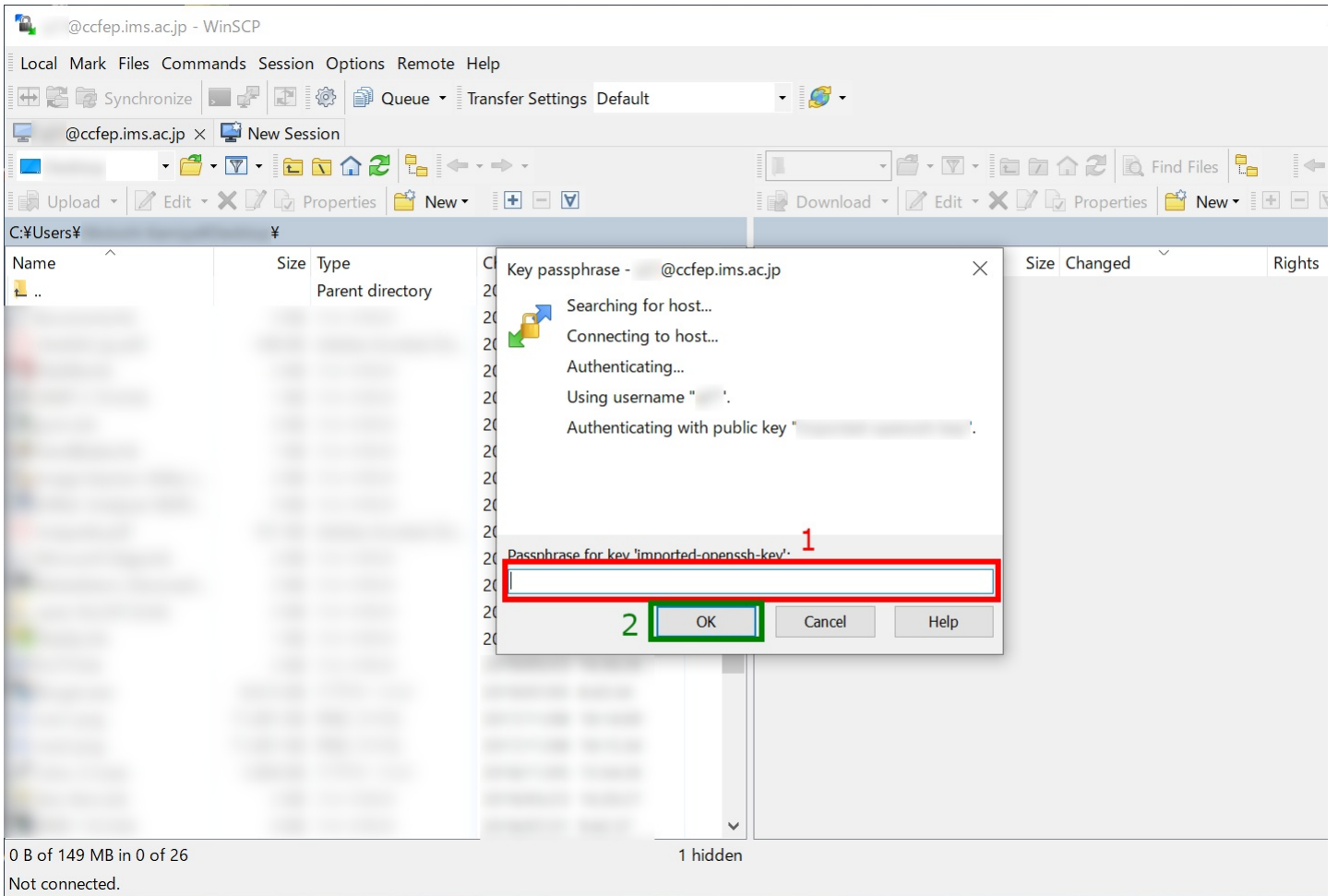
[Copy key fingerprints to clipboard](#)

A red box highlights the 'Yes' button, with a red '2' above it.

You may see warning window like above upon first connection. You need to verify the fingerprint of the server. The fingerprint must match either one in the following list. Then, click "Yes" to continue.

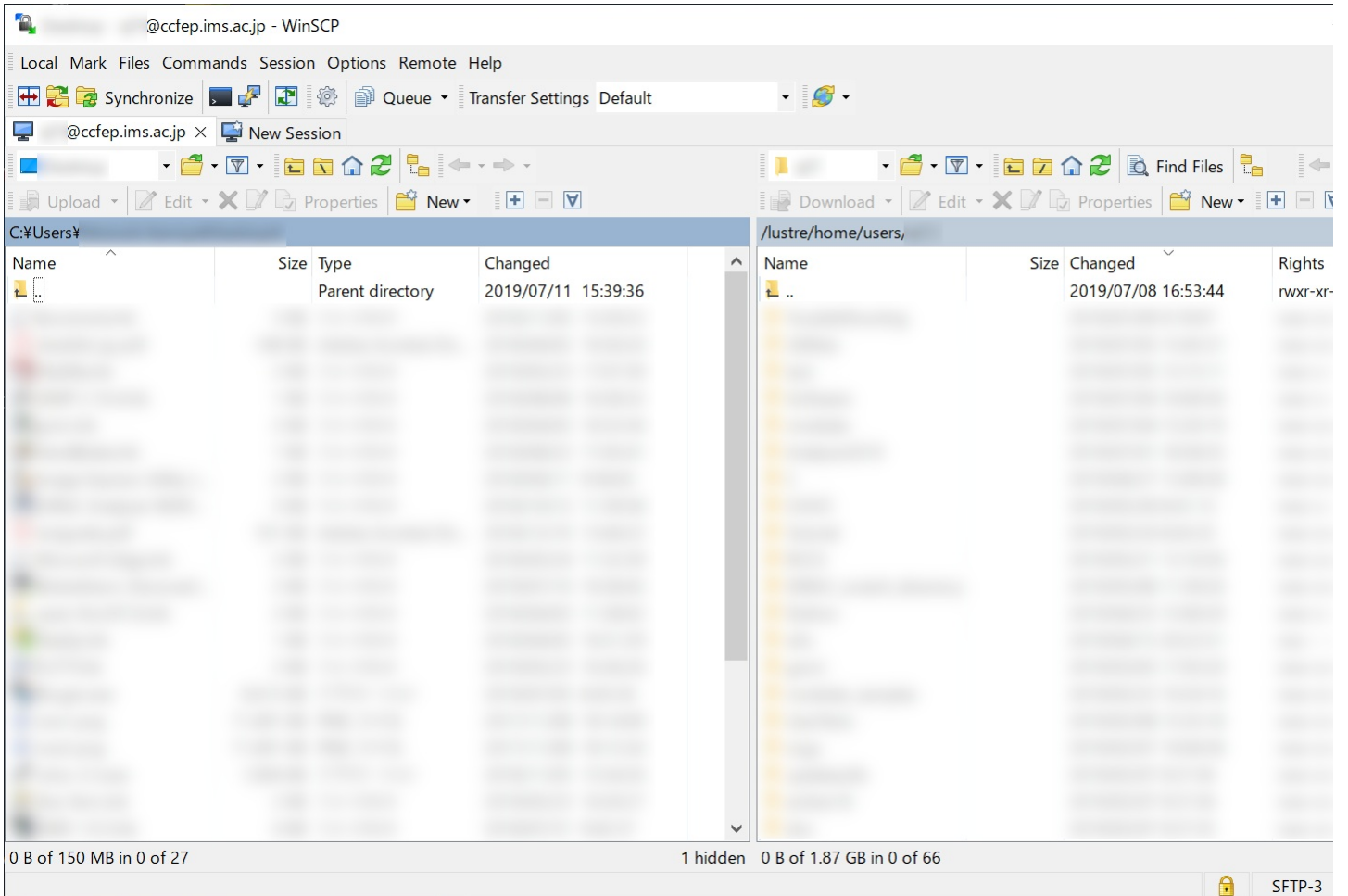
- ▶ ad:de:79:30:81:b0:b1:6a:17:f5:6f:ea:f4:b4:3b:de (MD5)
- ▶ e3:a9:bb:6f:e4:a9:37:fd:98:14:54:16:3c:81:2d:aa (MD5)
- ▶ 07:7e:df:7b:16:47:a8:f5:7c:48:b0:a3:d3:86:71:6a (MD5)
- ▶ wnEM30z4AxyDJ9XI/DdGr2PINEoivFR8v5krXHEmdU (SHA256)
- ▶ 0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZEloIfVqXvbl (SHA256)
- ▶ Nhg+9Lgij3XeuW//A/77qgUJllxWehryCtSlp1Dir (SHA256)

### 5. Input Passphrase of Private Key



Input passphrase of private key and then click OK. (If you are using Pageant and the key is registered correctly, this skip may be skipped.)

6. Completed!



If everything works fine, you will successfully logging in to the frontend node.