Published on *Research Center for Computational Science* (https://ccportal.ims.ac.jp)

SSH Key Generation (MobaXterm version)

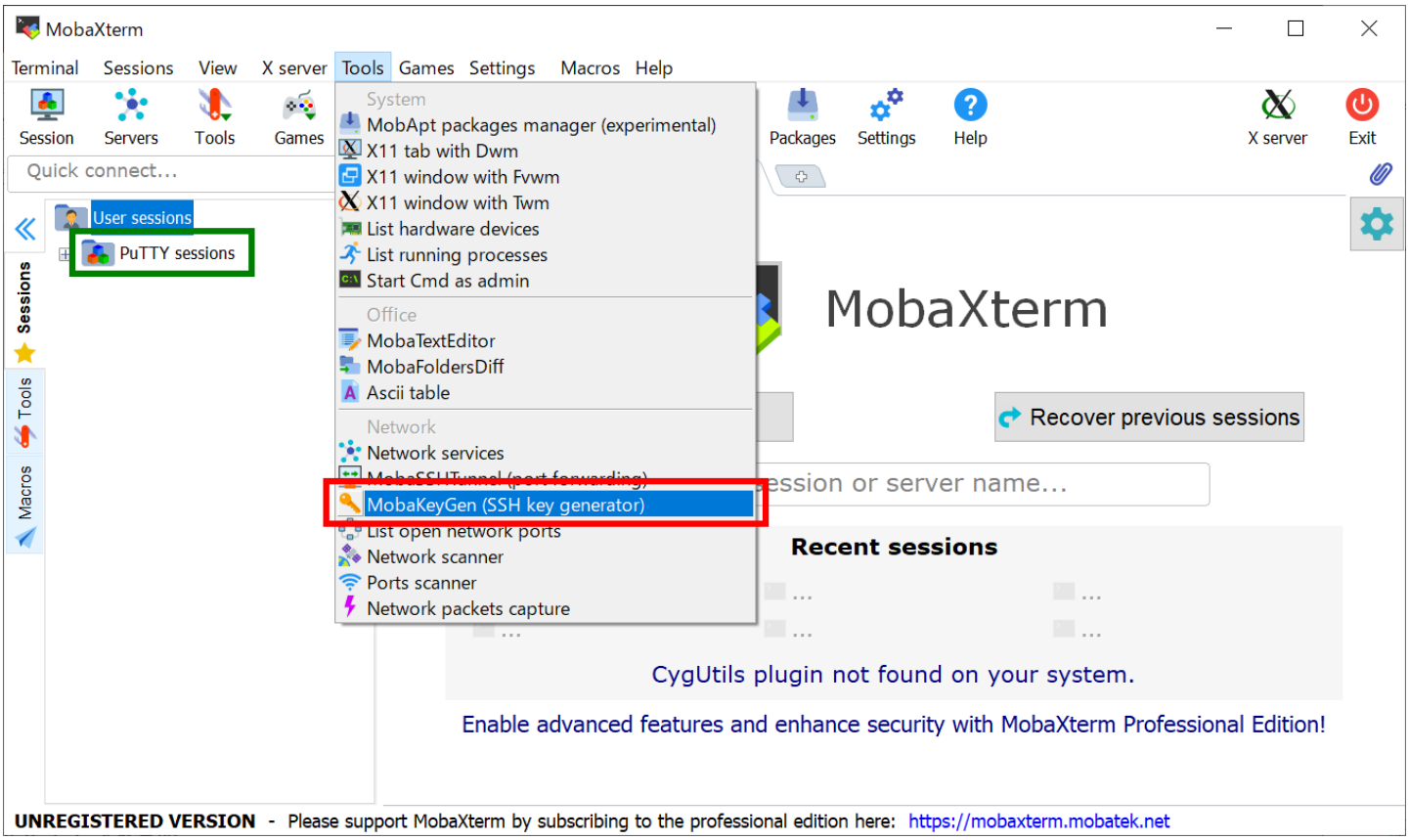
Last update: Feb 4, 2021 (verified with MobaXterm 20.6 Personal)

Introduction

The aim of this page is to explain how to login to RCSS supercomputer using MobaXterm.

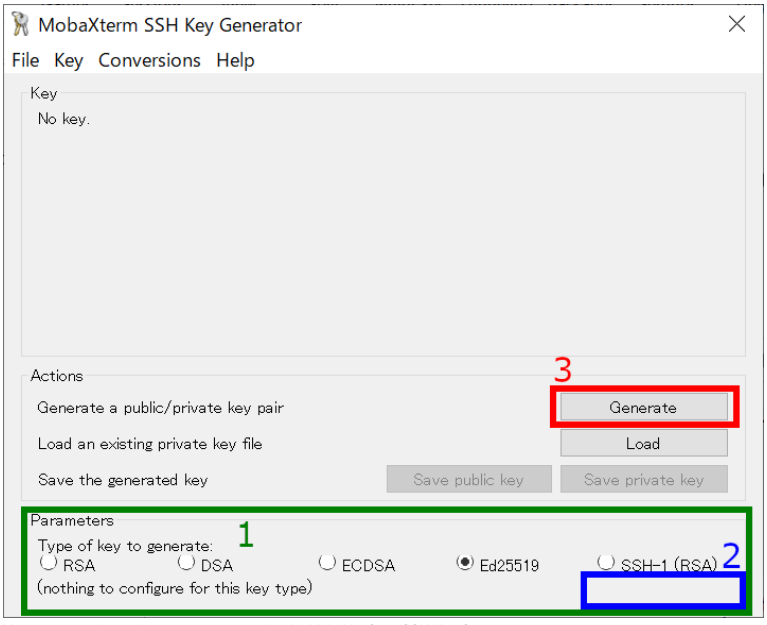
SSH Key Generation using MobaKeyGen

Invoke Key Generator of MobaXterm



Launch MobaXterm and select MobaKeyGen (SSH key generator) from "Tools" menu. If you already have PuTTY session settings (in registry?), they will be automatically loaded on left pane of the window. This PuTTY setting may be usable.

Key Generation (1) - choose key type



You may see window like above when you invoke MobaKeyGen (SSH Key Generator).

1. Choose Key Type

Ed25519, ECDSA (256, 384, 521 bits), and RSA 4096 bits * of keys are recommended in RCCS. Please choose Ed25519 if you have no preference.

*MobaXterm Personal 20.6 does not support SHA2 algorithms of RSA (rsa-sha2-256/512). Therefore, if SHA1 algorithm (ssh-rsa) is disabled in the near future, it may cause an RSA authentication problem. (Note: the RSA key format itself is not related with those SHA1 and SHA2 algorithms. Once RSA-SHA2-capable MobaXterm is relased, you may be able to login to ccfep.ims.ac.jp without extra settings/operations; just updating MobaXterm is enough.)

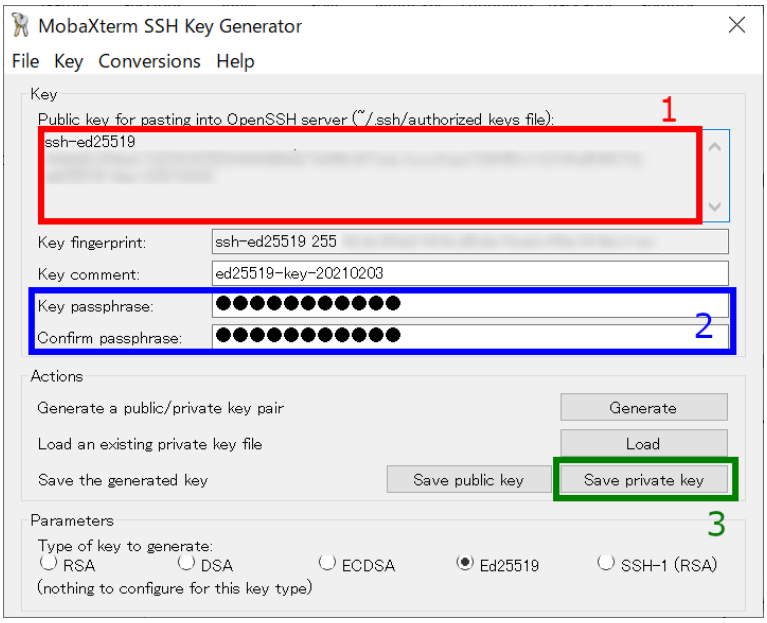
2. Choose Key Length (ECDSA or RSA case)

In case of ECDSA or RSA type, you may find optional item at the position specified by "2". Please choose/input value there.

3. Start Generation of Key

Once you click the "Generate" button, the key generation will begin. You need to move mouse cursor around to proceed the key generation after clicking the button.

Key Generation (2) - set passphrase and save keys



Once the key generation completed, the appearance of the window will change like above.

1. OpenSSH type public key

The public key shown as a string in this field is what we need. Extract all the contents in this filed into notepad or others, and then save it! (Do not miss ssh-/ecdsa- part in the beginning!) Note: you don't need public key from "Save public key" button; we need only OpenSSH format one.

You can rebuild public keys via "Load" button or "Conversion" menu if you still have private key. (If you lost the private key, you need to generate a new key.)

2. Set passphrase for private key

You can set passphrase for private key here. We, RCCS, recommend passphrase of 10 or more characters containing 4 types of characters - "lower-case", "upper-case", "number", and "symbol".

3. Save the private key

After setting passphrase, click "Save private key" button to save the key. Easy-to-understand name such as "rccs.ppk" or "ccfep.ppk" may be a good choice. (NOTE: THE PRIVATE KEY FILE MUST BE KEPT SECRET!)

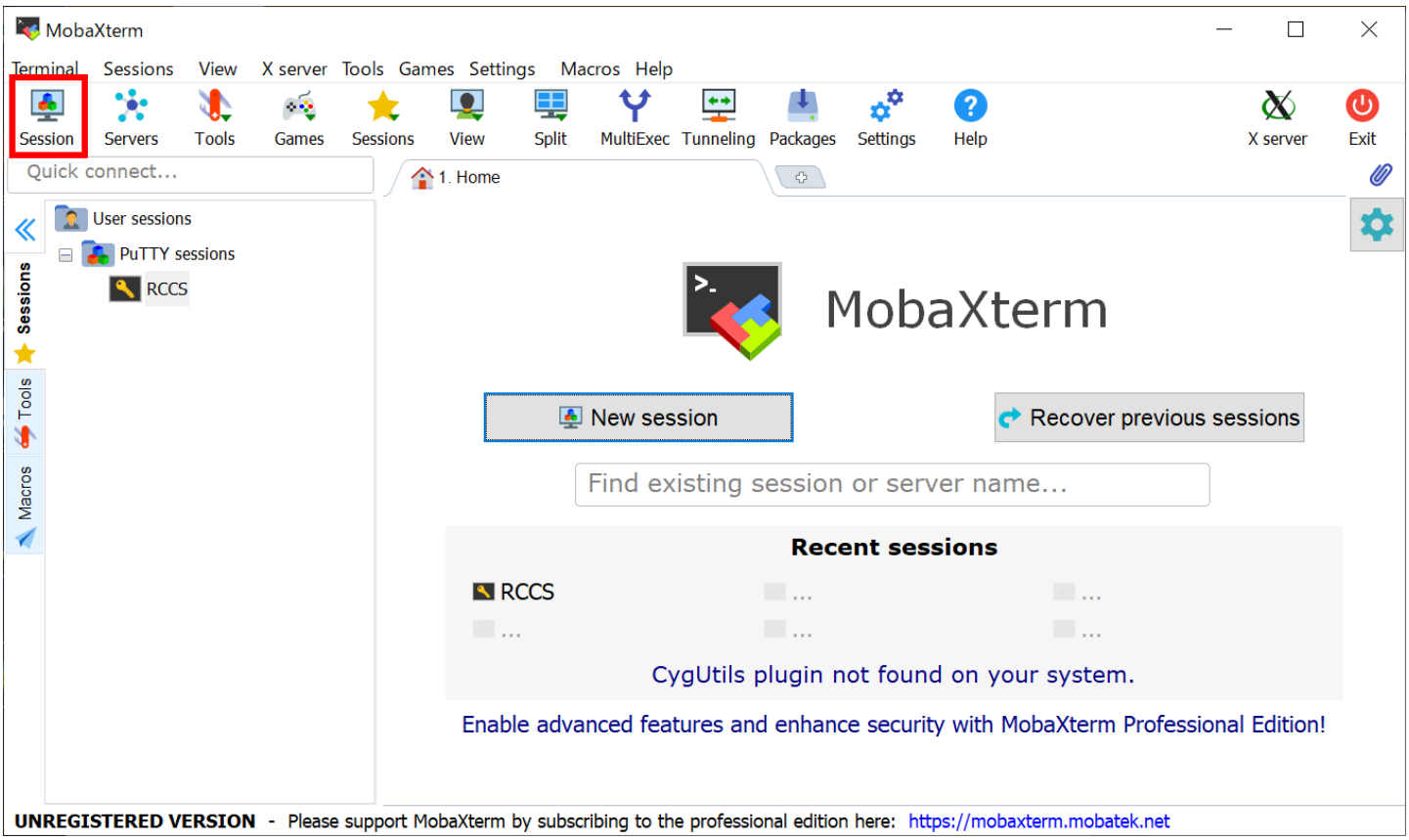
Register Public Key (Common)

You need to register the public key before login. Please register your public key according to the instructions in https://ccportal.ims.ac.jp/en/account.

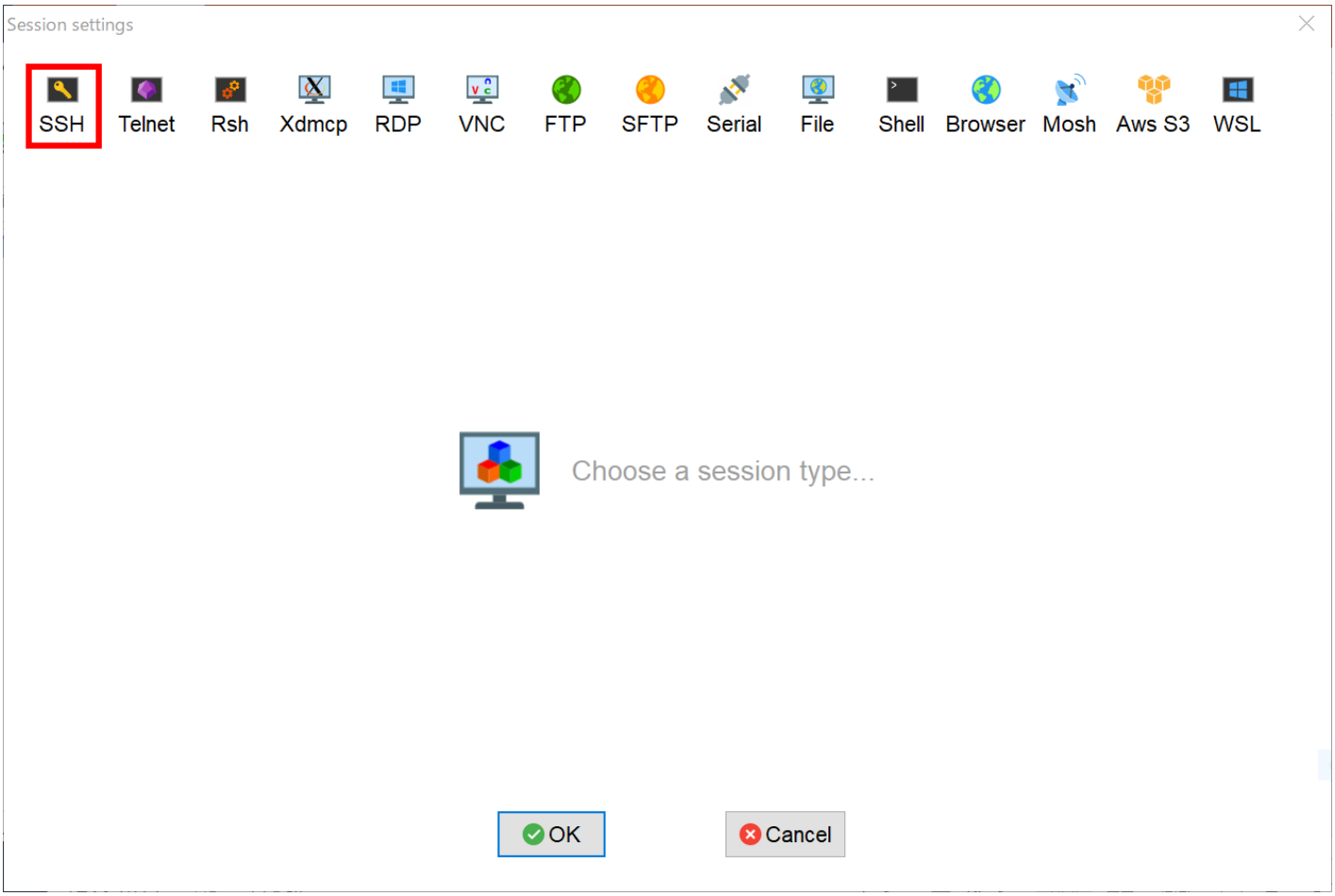
Please note that the public key here is an OpenSSH type one , not the one from "Save public key" button.

Login

Create a new session

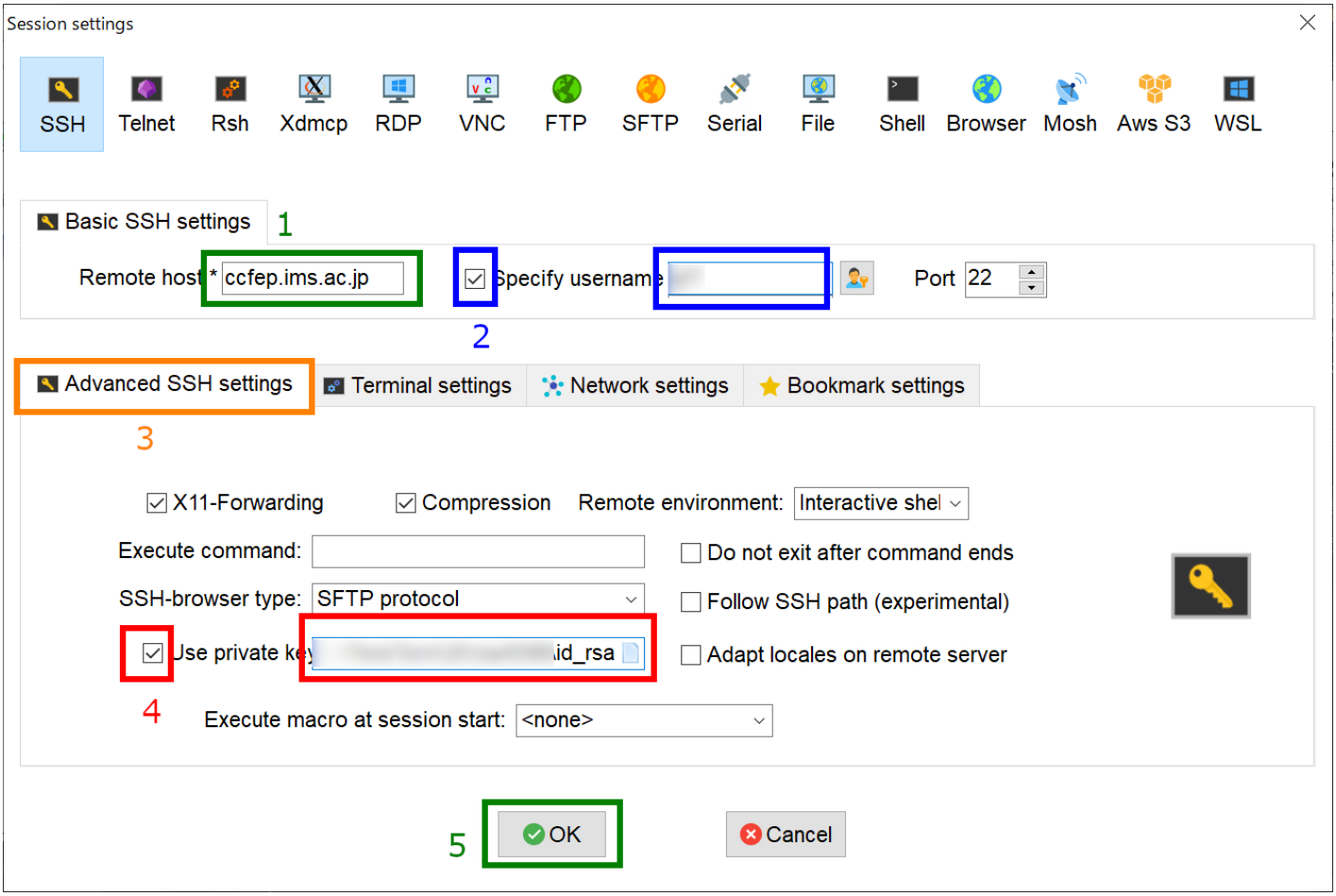


Quit MobaKeyGen (or restart MobaXterm) to go back to the MobaXterm window. Click "Session" button on top-left part of the window to create a new session.



Theh, Click "SSH" to create a new SSH session.

SSH Session Configuration

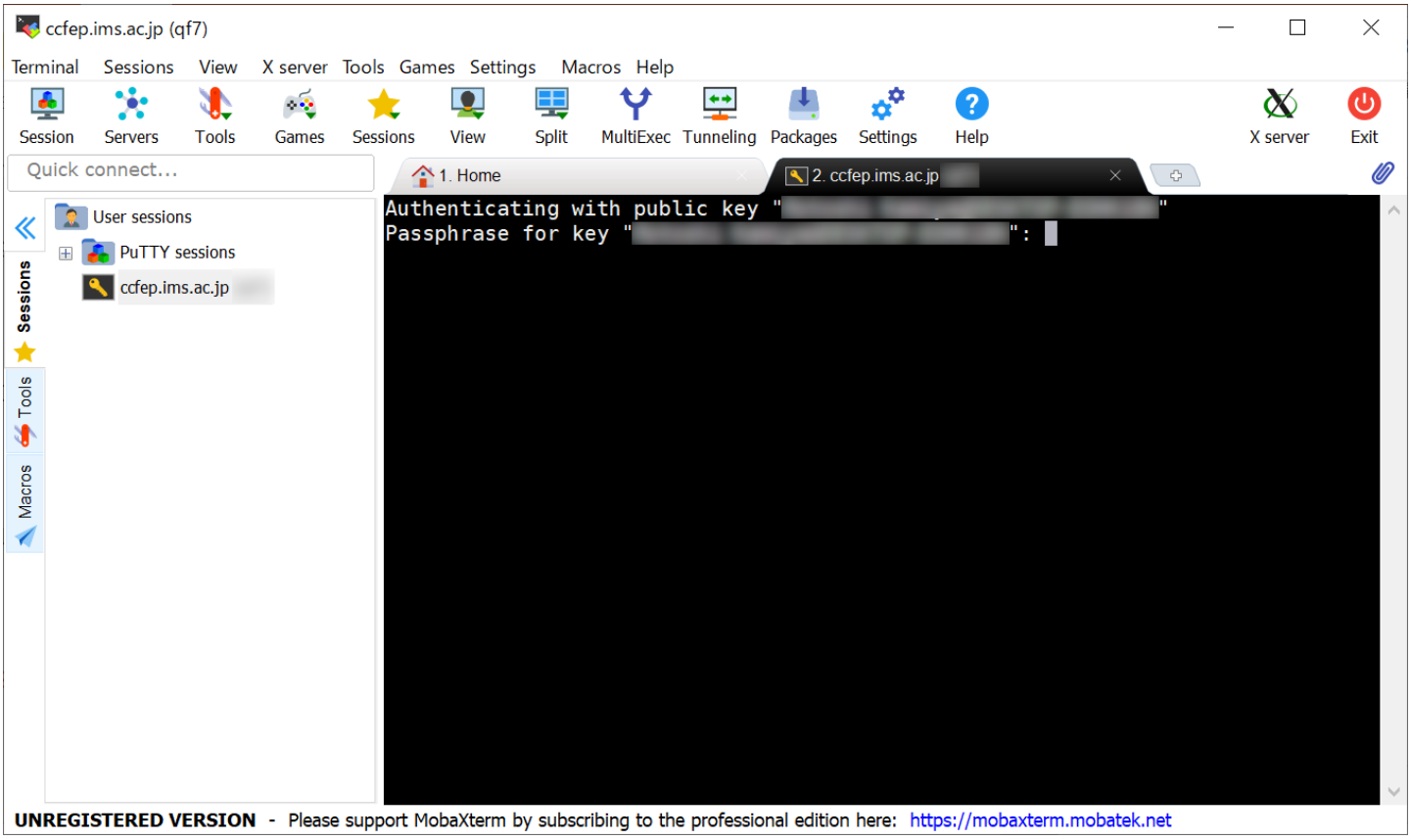


You need to complete following settings in this page.

1. input frontend hostname ccfep.ims.ac.jp into the box.
2. check "Specify username", then input RCCS user ID (three-letters ID) in the textbox.
3. click "Advanced SSH settings" tab to expand this.
4. check "Use private key" and specify private key file location (both of OpenSSH style and PuTTY style private keys are accepted).

5. click OK to proceed.

Input Passphrase

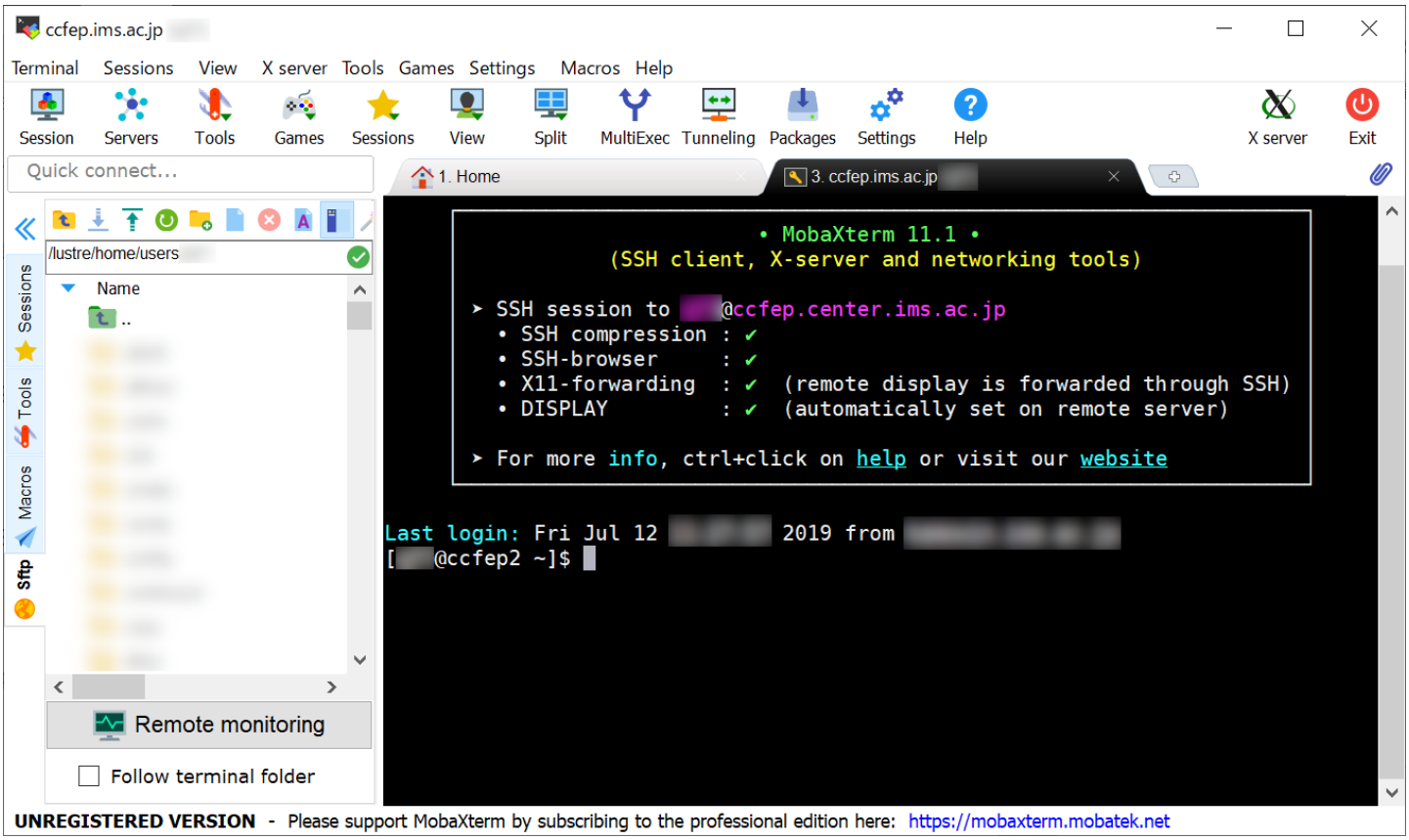


After the connection, you need to input passphrase of private key.

Note: MobaXterm skips verification of the connecting host in default. This verification can be enabled by checking "Validate host identity at first connection" item in SSH tab of "Settings" -> "Configuration" menu. Valid fingerprints of the frontend node are listed below.

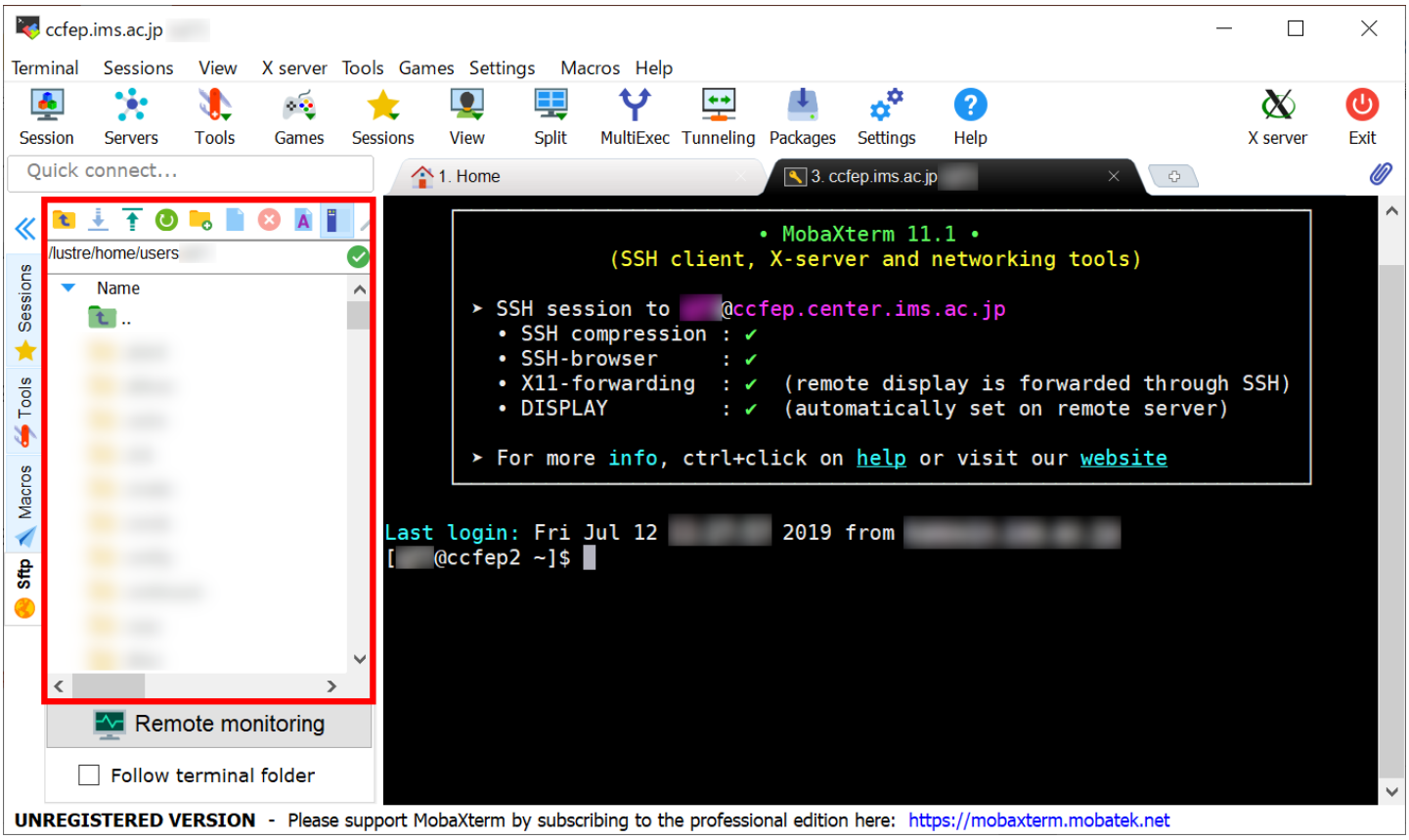
- ad:de:79:30:81:b0:b1:6a:17:f5:6f:ea:f4:b4:3b:de (MD5)
- e3:a9:bb:6f:e4:a9:37:fd:98:14:54:16:3c:81:2d:aa (MD5)
- 07:7e:df:7b:16:47:a8:f5:7c:48:b0:a3:d3:86:71:6a (MD5)
- wnEM30z4AxyDJ9XI/DdGr2PlNeoivFRR8v5krXHEmdU (SHA256)
- 0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZElolfVqXvbI (SHA256)
- Nhg+9Lgj3XeuW//A/j7jqgUJlIxWehryCtStIp1Dir (SHA256)

Login Completed



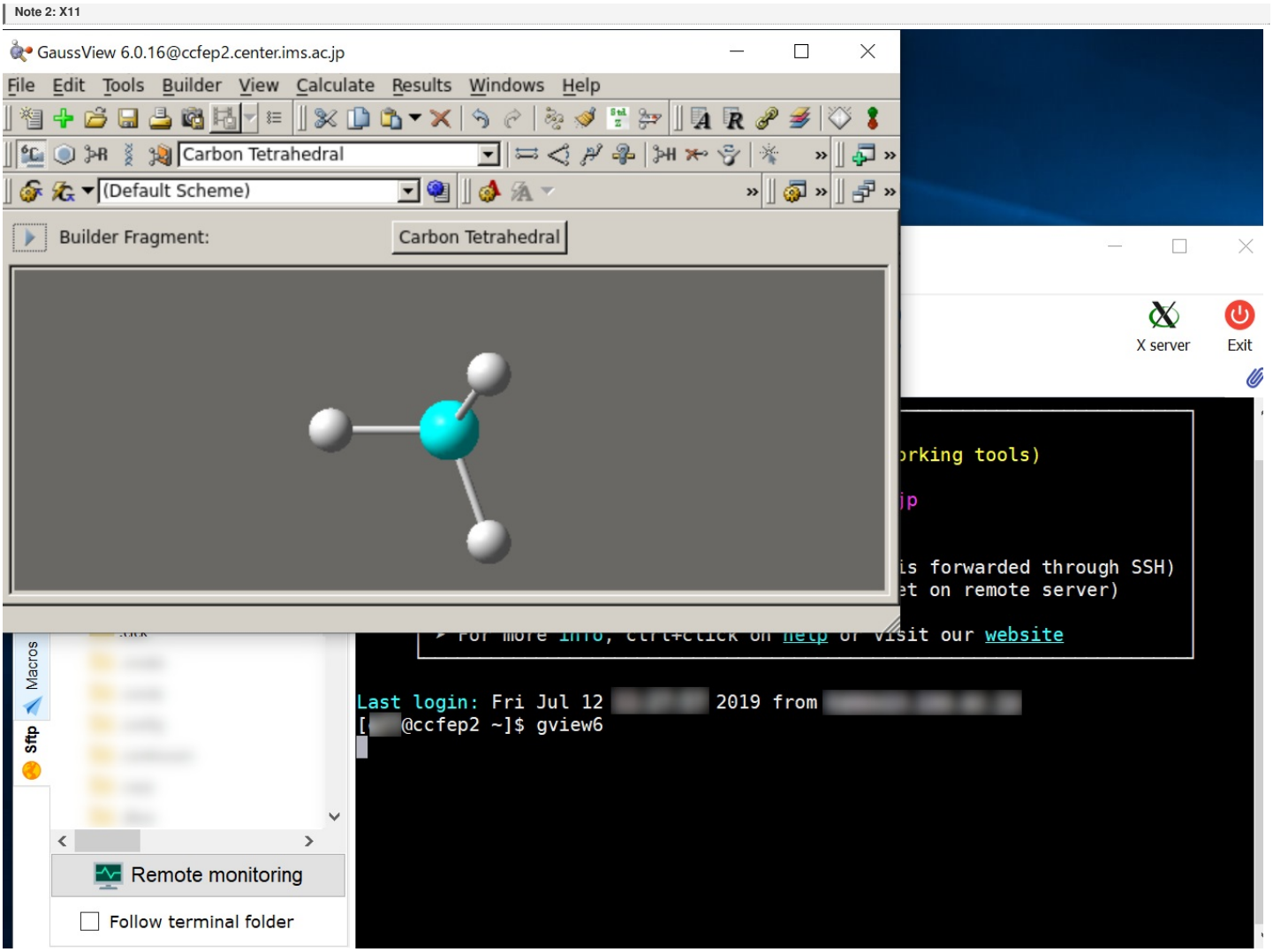
You may see window like above if you successfully logged in.

Note 1: SFTP



MobaXterm has SFTP functionality. In the left pane of the window (marked with red square), you can download/upload files via SFTP.

Note 2: X11



MobaXterm has internal X server. Therefore, you can use X window application without special settings. ("X11-forwarding" item must be checked in the message displayed upon successful login.)