



High Performance
Computing &
Big Data Services



hpc.uni.lu



hpc@uni.lu



[@ULHPC](https://twitter.com/ULHPC)

HPC School - Beginner

S1-1 - Connection to ULHPC



Overview

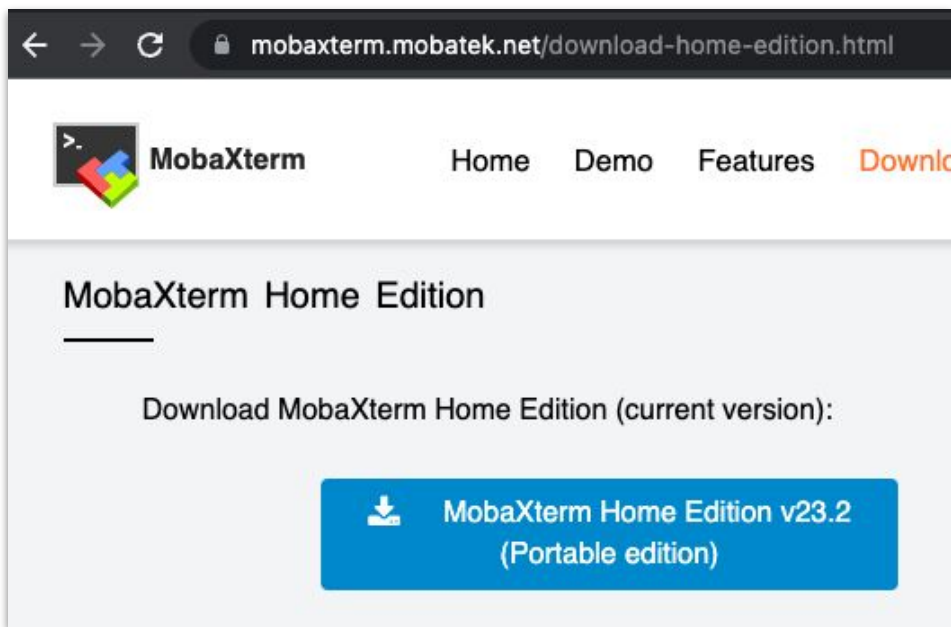


The main steps are:

1. Install the necessary software to connect to the ULHPC
2. Create a pair of SSH keys to authenticate yourself on the ULHPC
3. Set your public key in our authentication system
4. Establish a first connection

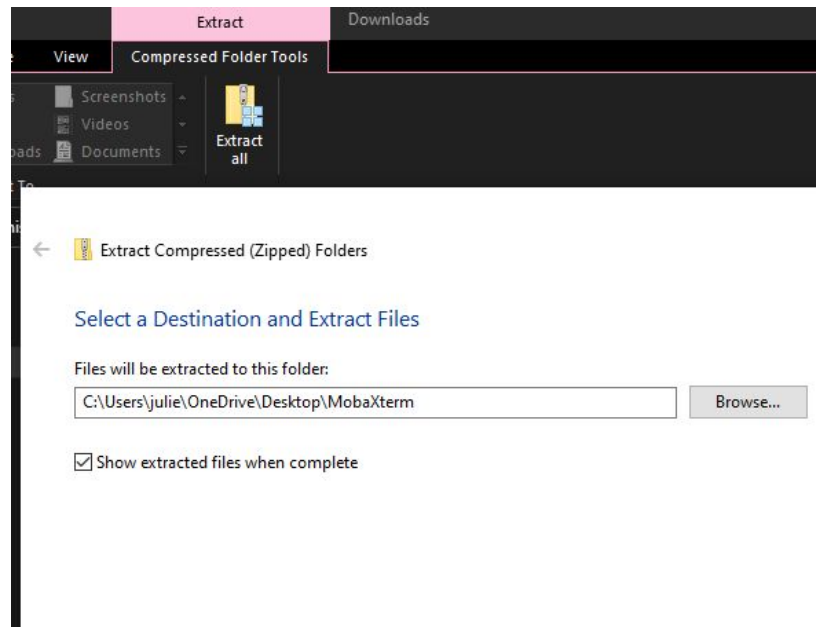
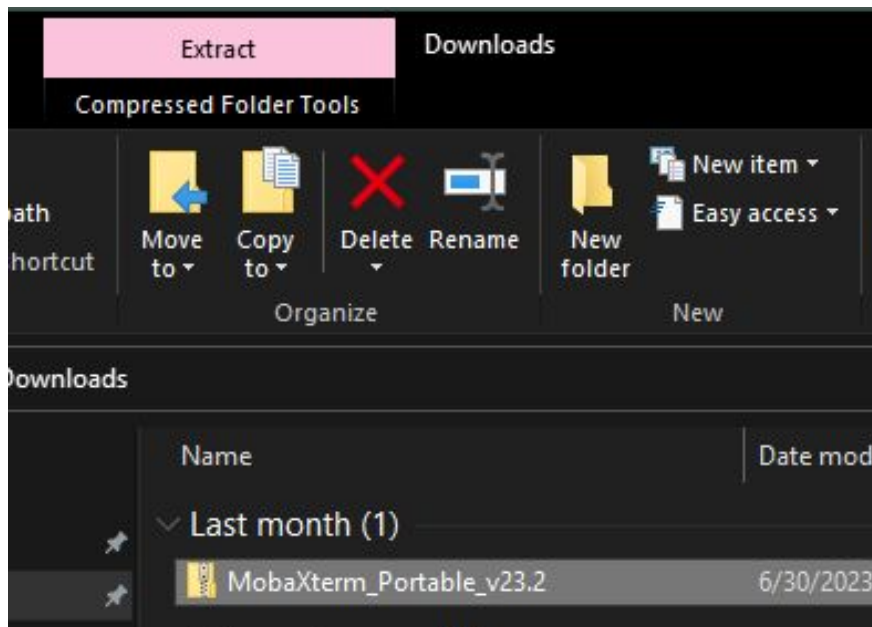
Step 1 - necessary software

Download MobaXterm Home Edition (portable), [use this link](https://mobaxterm.mobatek.net/download-home-edition.html)



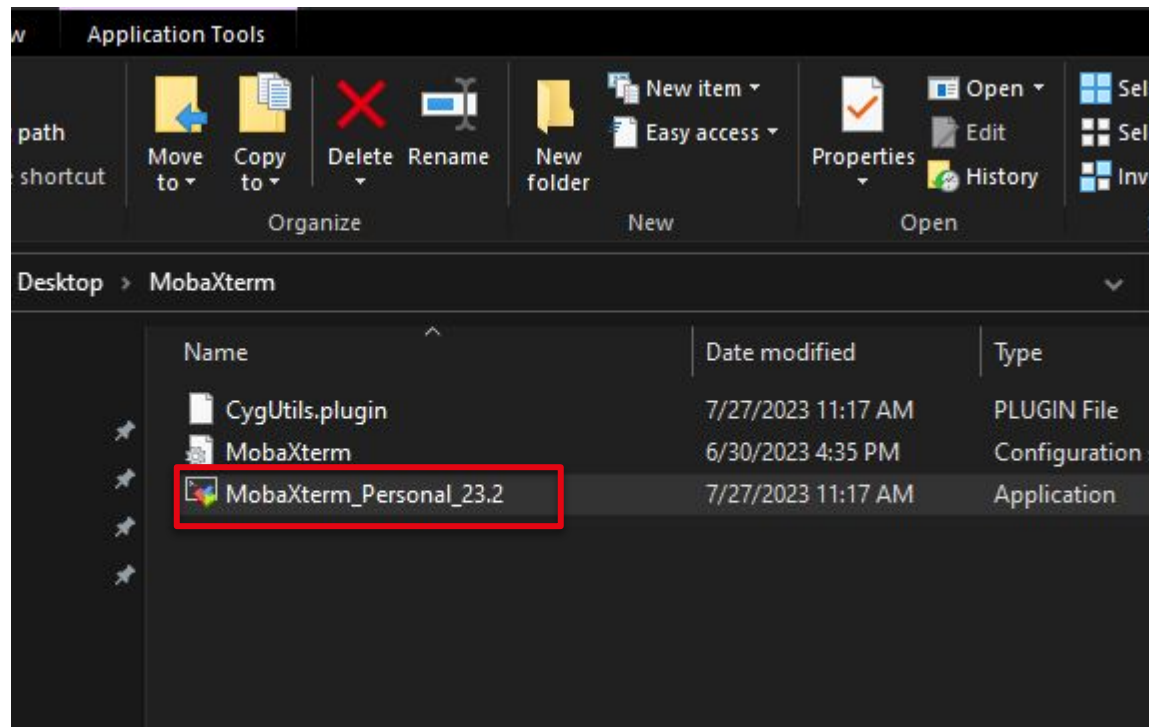
Step 1 - necessary software

Extract the archive containing the application in a folder of your choice



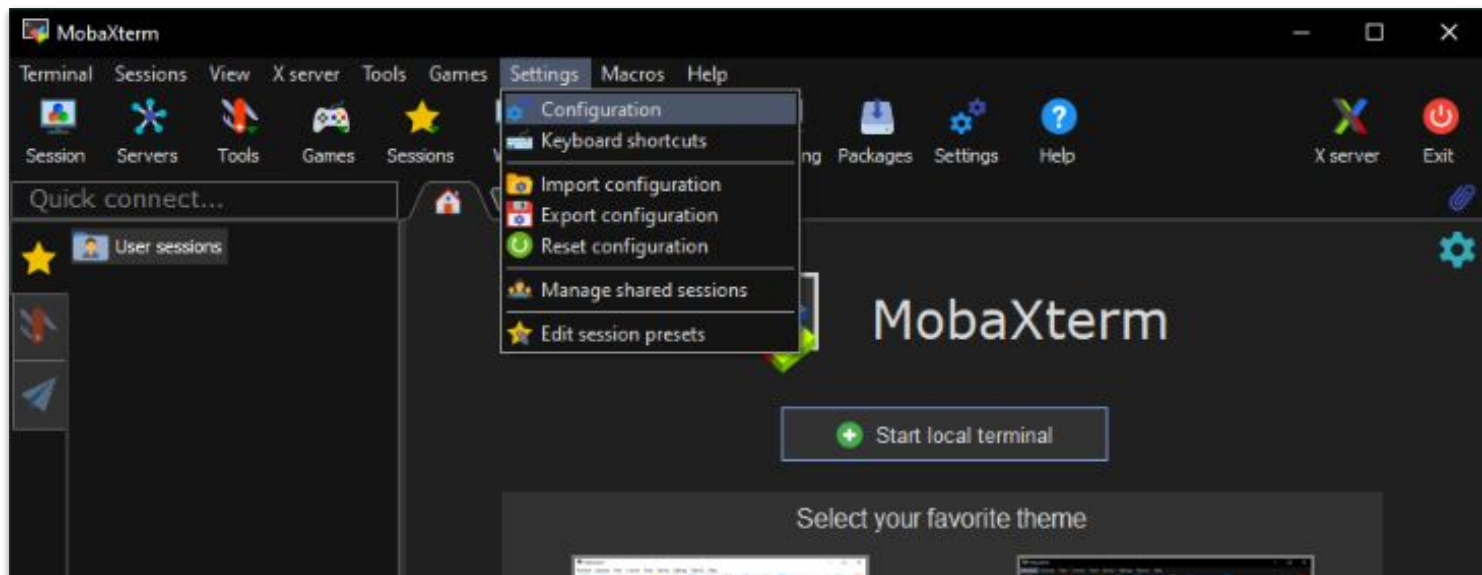
Step 1 - necessary software

Open MobaXterm



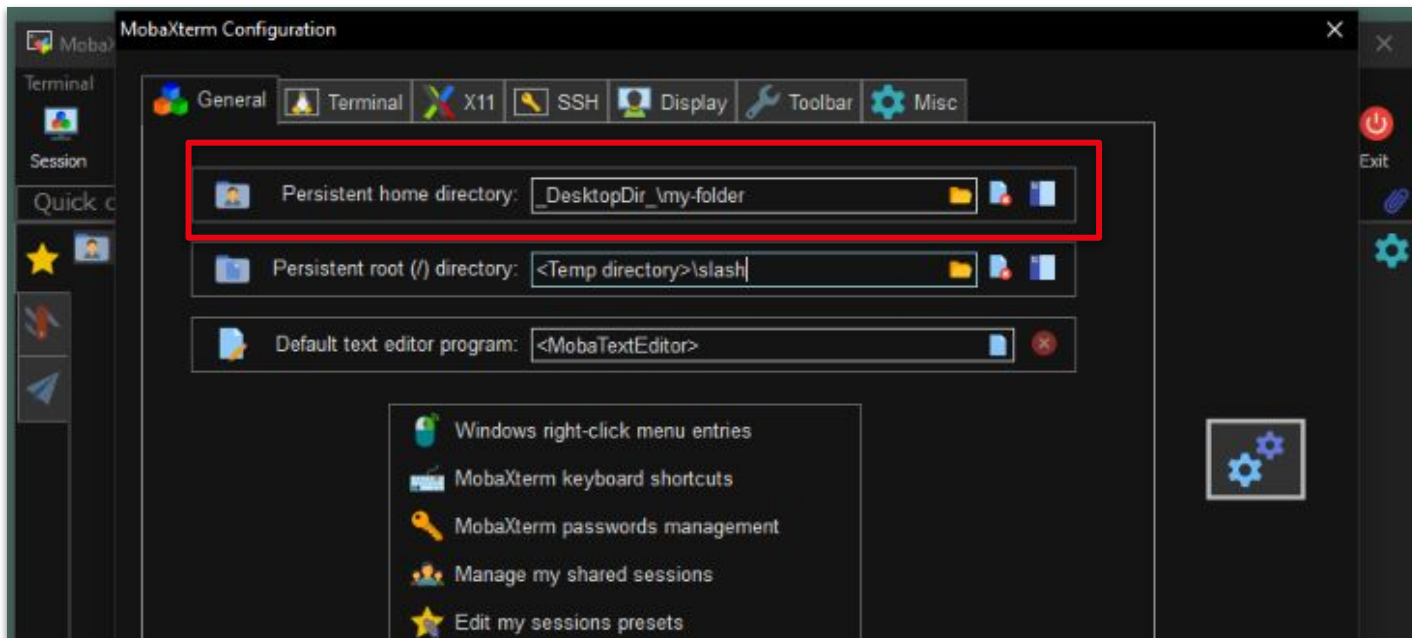
Step 1 - necessary software

Go to the configuration screen



Step 1 - necessary software

Change the persistent home directory to a folder of your choice on your machine



Step 2 - Creation of the SSH key pair



What is it?

SSH key pairs are a couple of files used to authenticate a user on a server without exchanging password

A pair of keys?

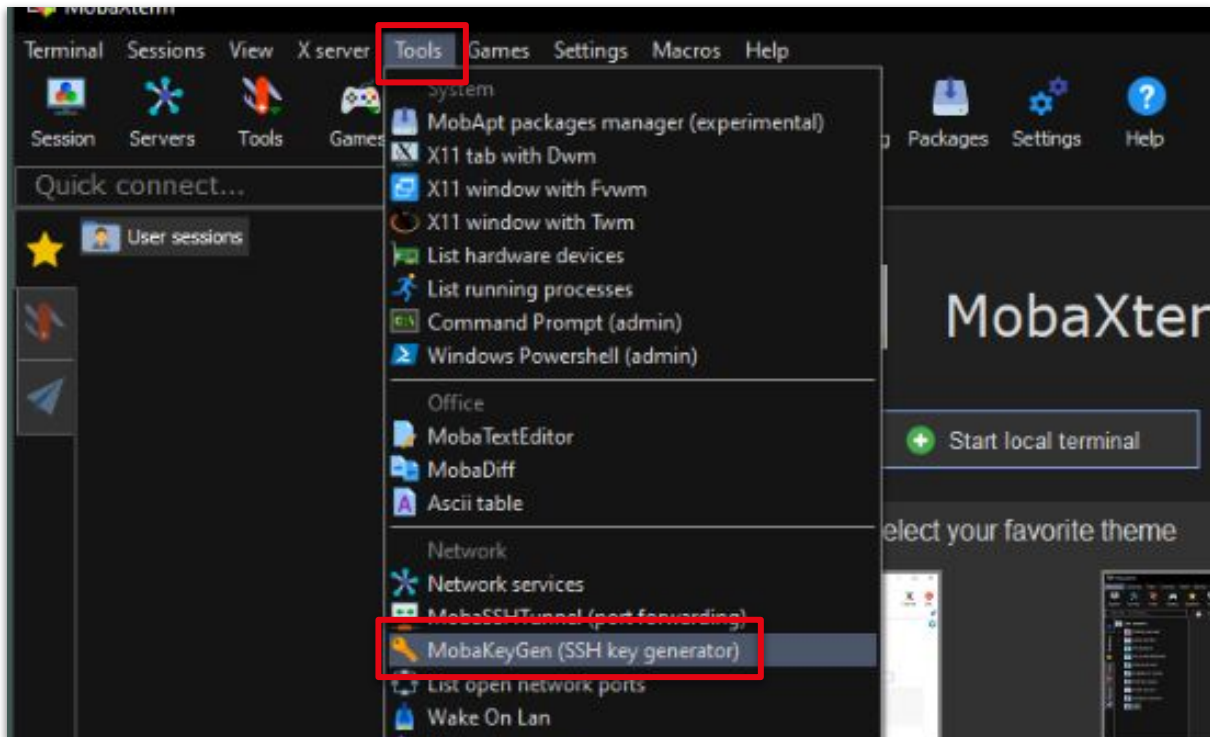
- the public key can (and should) be shared
- the private key should never be shared

Why not passwords?

Servers allowing access via password exchange are prone to be attacked

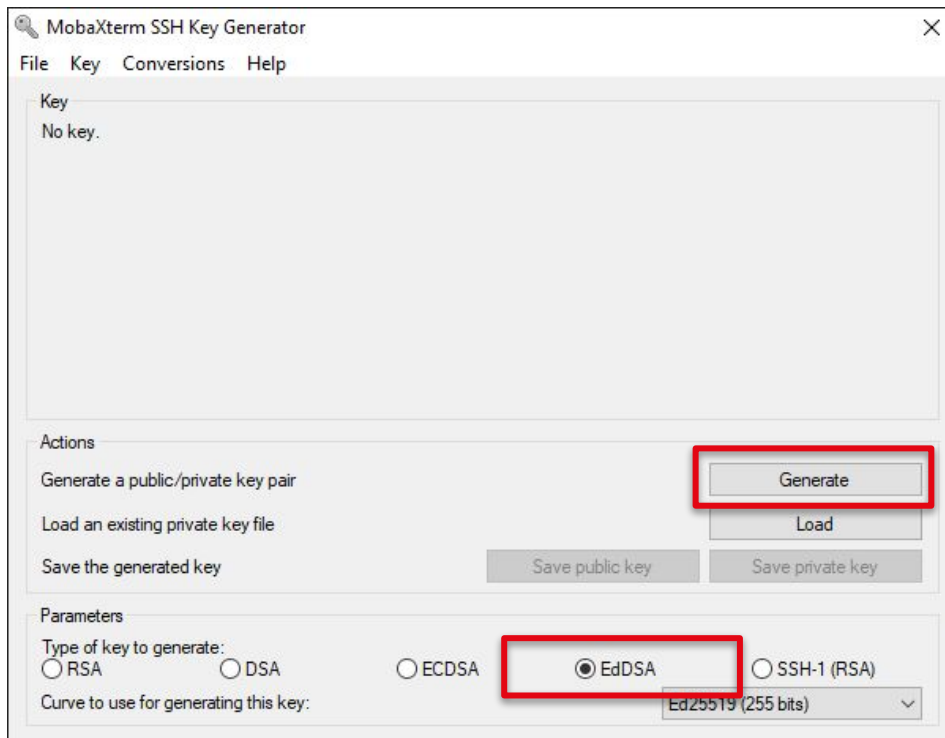
Step 2 - Creation of the SSH key pair

Go to the Tools menu and select MobaKeyGen (SSH key generator)



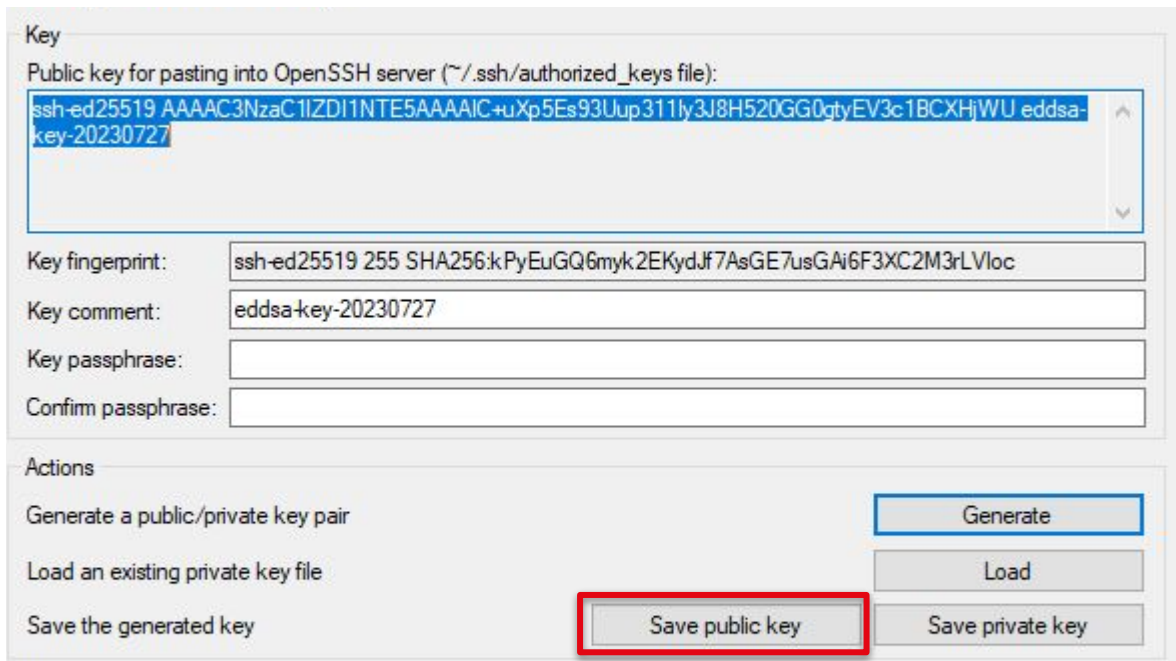
Step 2 - Creation of the SSH key pair

Select EdDSA and click on Generate and move your mouse to speed up the generation process



Step 2 - Creation of the SSH key pair

After a moment you should see a similar screen, click on Save public key



The screenshot shows a window titled "Key" with a text area containing the public key: `ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC+uXp5Es93Uup311ly3J8H520GG0qyEV3c1BCXHjWU eddsa-key-20230727`. Below the text area are fields for "Key fingerprint" (displaying `ssh-ed25519 255 SHA256:kPyEuGQ6myk2EKydJf7AsGE7usGAi6F3XC2M3rLVloc`), "Key comment" (displaying `eddsa-key-20230727`), "Key passphrase", and "Confirm passphrase". At the bottom, under the "Actions" section, there are three buttons: "Generate", "Load", and "Save public key". The "Save public key" button is highlighted with a red rectangle.

Key

Public key for pasting into OpenSSH server (`~/.ssh/authorized_keys` file):

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC+uXp5Es93Uup311ly3J8H520GG0qyEV3c1BCXHjWU eddsa-key-20230727
```

Key fingerprint: `ssh-ed25519 255 SHA256:kPyEuGQ6myk2EKydJf7AsGE7usGAi6F3XC2M3rLVloc`

Key comment: `eddsa-key-20230727`

Key passphrase:

Confirm passphrase:

Actions

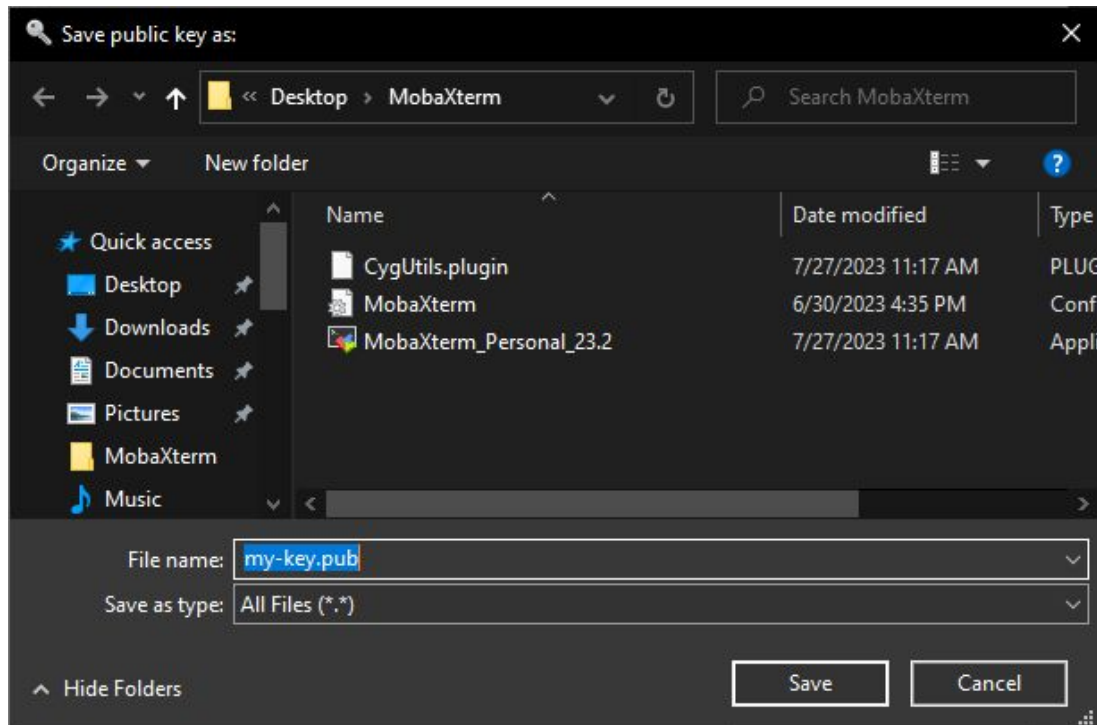
Generate a public/private key pair

Load an existing private key file

Save the generated key

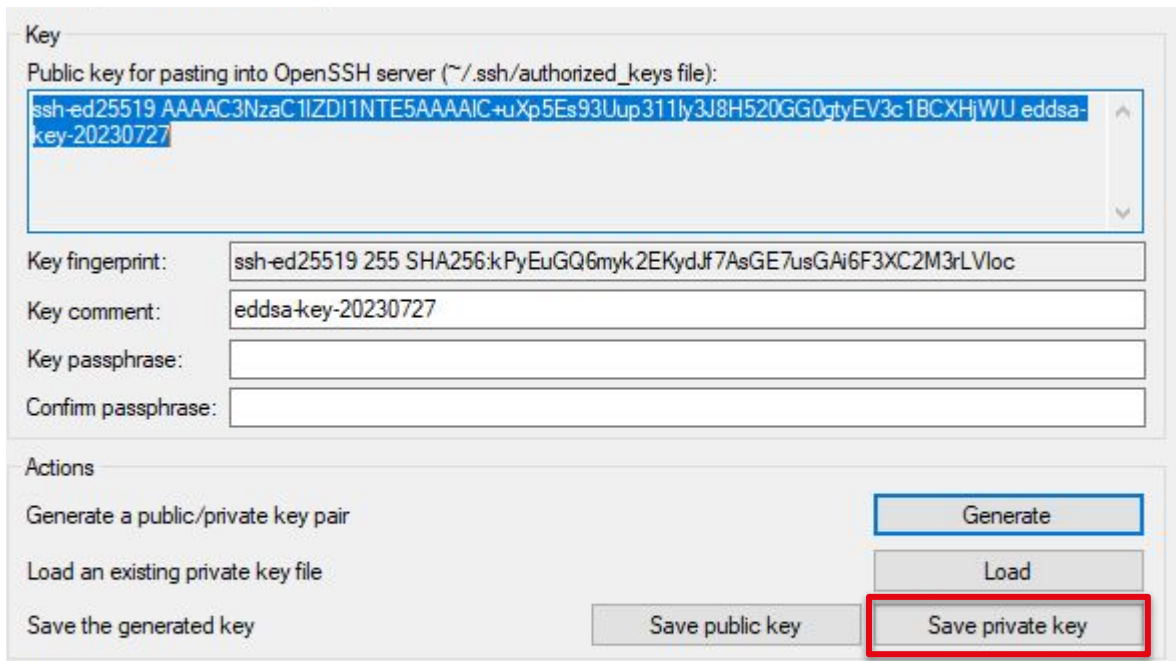
Step 2 - Creation of the SSH key pair

Select a folder and pick up a name, e.g. my-key.pub for your public key



Step 2 - Creation of the SSH key pair

Then click on Save private key



The image shows a 'Key' dialog box for generating an SSH key pair. It contains a text area for the public key, fields for the key fingerprint, comment, passphrase, and confirmation passphrase, and a section for actions with buttons for 'Generate', 'Load', 'Save public key', and 'Save private key'.

Key

Public key for pasting into OpenSSH server (~/ssh/authorized_keys file):

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC+uXp5Es93Uup311ly3J8H520GG0qtyEV3c1BCXHjWU eddsa-key-20230727
```

Key fingerprint: ssh-ed25519 255 SHA256:kPyEuGQ6myk2EKydJf7AsGE7usGAi6F3XC2M3rLVloc

Key comment: eddsa-key-20230727

Key passphrase:

Confirm passphrase:

Actions

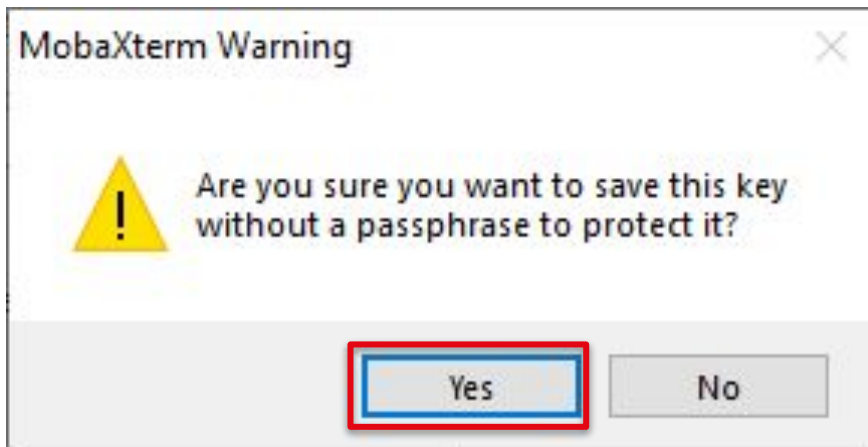
Generate a public/private key pair

Load an existing private key file

Save the generated key

Step 2 - Creation of the SSH key pair

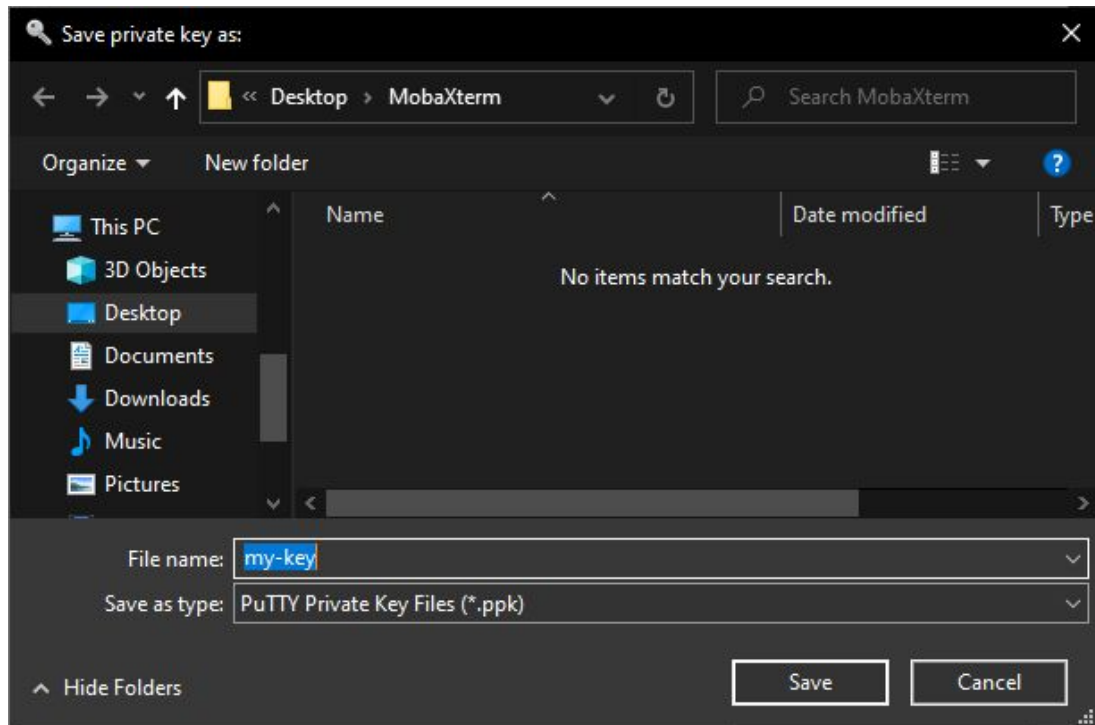
Choose Yes



Unlike what is shown, you can add a passphrase to add an extra layer of security. In this presentation we do not use it for the sake of simplicity.

Step 2 - Creation of the SSH key pair

Find the folder in which you stored your public key pick up a name, e.g. my-key for your private key



Step 3 - Give us your public key



IPA is the name of our authentication server: <https://hpc-ipa.uni.lu>

When your account has been created, you should have received an email with a link to IPA in order to set your account password.

Before being able to connect to the cluster, you need to add your public key to your account.

 Full documentation available here: <https://hpc-docs.uni.lu/connect/ipa/#upload-your-ssh-key-on-the-ulhpc-identity-management-portal>

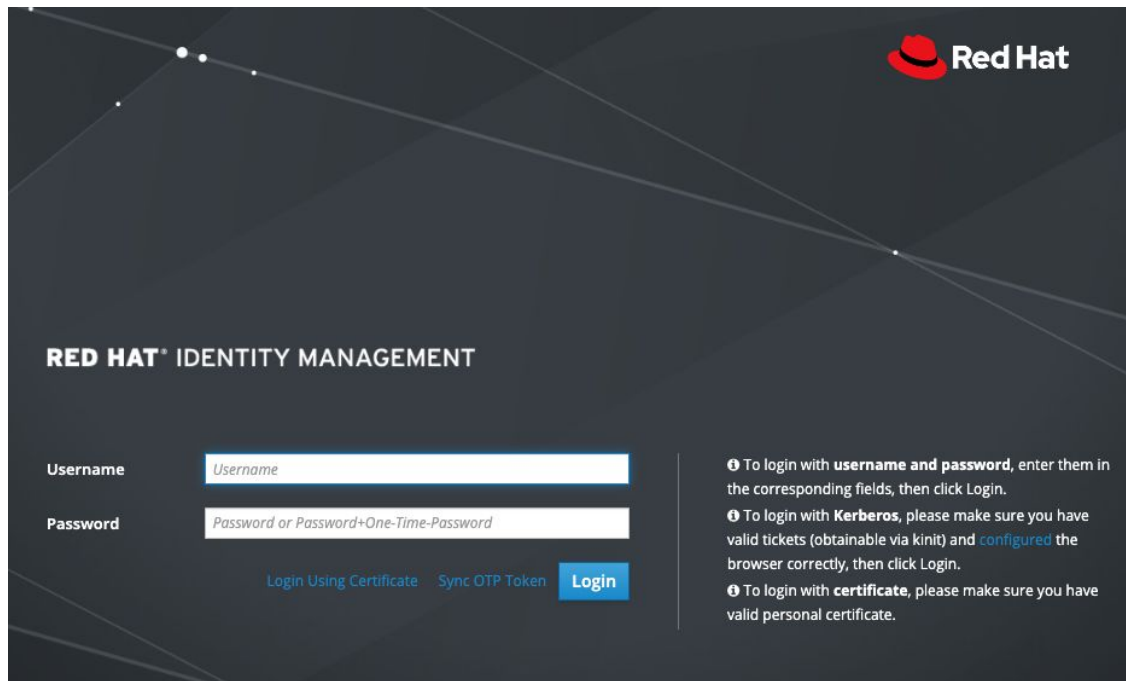
Step 3 - Give us your public key

- Log in on IPA with your password
- Select Identity / Users.
- Select your login (**this is not your UL account**, check your account creation email if you don't remember)
 - e.g., for me, it is `jschleich` and not `julien.schleich@uni.lu` or `julien.schleich`

 Full documentation available here: <https://hpc-docs.uni.lu/connect/ipa/#upload-your-ssh-key-on-the-ulhpc-identity-management-portal>

Step 3 - Give us your public key

Go to the following URL: <https://hpc-ipa.uni.lu> and enters your ULHPC username and password



The image shows the Red Hat Identity Management login page. The page has a dark background with the Red Hat logo in the top right corner. The main heading is "RED HAT® IDENTITY MANAGEMENT". Below this, there are two input fields: "Username" and "Password". The "Username" field has a placeholder text "Username" and the "Password" field has a placeholder text "Password or Password+One-Time-Password". Below the password field, there are three links: "Login Using Certificate", "Sync OTP Token", and a blue "Login" button. To the right of the input fields, there are three instructions for login methods, each preceded by a red hat icon: "To login with **username and password**, enter them in the corresponding fields, then click Login.", "To login with **Kerberos**, please make sure you have valid tickets (obtainable via kinit) and **configured** the browser correctly, then click Login.", and "To login with **certificate**, please make sure you have valid personal certificate."

Red Hat

RED HAT® IDENTITY MANAGEMENT

Username

Password

[Login Using Certificate](#) [Sync OTP Token](#) [Login](#)

❗ To login with **username and password**, enter them in the corresponding fields, then click Login.

❗ To login with **Kerberos**, please make sure you have valid tickets (obtainable via kinit) and **configured** the browser correctly, then click Login.

❗ To login with **certificate**, please make sure you have valid personal certificate.

Step 3 - Give us your public key

Click on your username and a similar page should open:

Identity	Policy	Authentication	Network Services	IPA Server
Users	Hosts	Services	Groups	ID Views
Automember ▾				

Active users » jschleich

✓ User: jschleich

jschleich is a member of:

Settings	User Groups	Netgroups	Roles	HBAC Rules	Sudo Rules
Refresh	Revert	Save	Actions ▾		

Identity Settings

Job Title	<input type="text" value="Research scientist"/>
First name *	<input type="text" value="Julien"/>
Last name *	<input type="text" value="Schleich"/>
Full name *	<input type="text" value="Julien Schleich"/>
Display name	<input type="text"/>
Initials	<input type="text"/>
GECOS	<input type="text" value="Julien Schleich <Julien.Schleich@uni.lu>, Belval - MNO/E02/0225100, +352 46 66 44 5337"/>

Account Settings

User login	<input type="text" value="jschleich"/>
Password	<input type="password" value="*****"/>
Password expiration	<input type="text" value="2024-02-21 07:57:44Z"/>
UID	<input type="text" value="5026"/>
GID	<input type="text" value="666"/>
Principal alias	<input type="text" value="jschleich@HPC.UNI.LUX"/> Delete
	Add

Step 3 - Give us your public key

On the right side, find SSH public keys and click on the Add button



The screenshot shows a configuration interface with the following elements:

- Login shell:** A text input field containing `/bin/sh`.
- Home directory:** A text input field containing `/home/user`, followed by an **Undo** button.
- SSH public keys:** A section highlighted with a red rectangle, containing an **Add** button.
- Certificate:** A section showing a warning icon and the text **No Valid Certificate**.

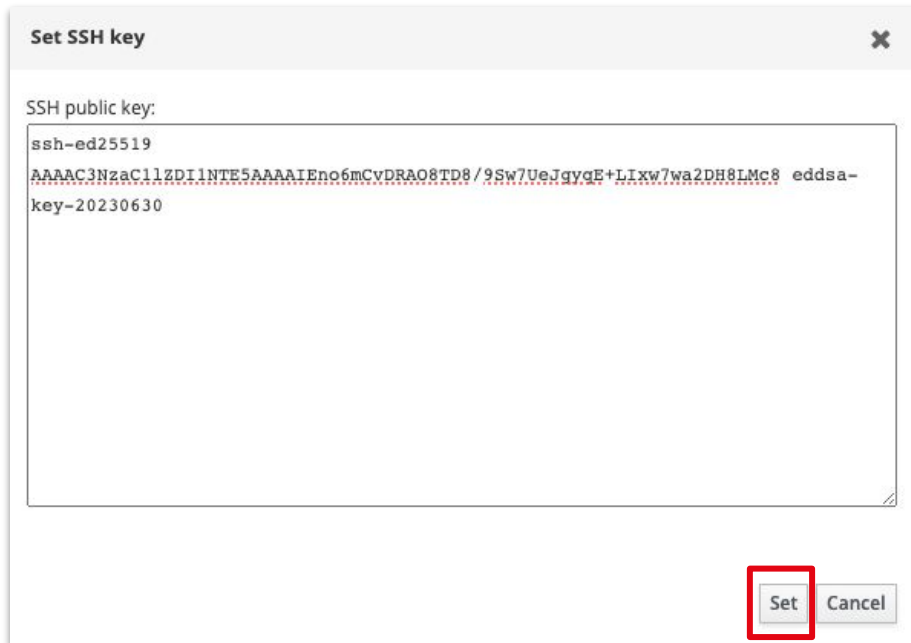


Full documentation available here:

<https://hpc-docs.uni.lu/connect/ipa/#upload-your-ssh-key-on-the-ulhpc-identity-management-portal>

Step 3 - Give us your public key

Paste the content of your public key
and click on Set



Set SSH key

SSH public key:

```
ssh-ed25519  
AAAAC3NzaC1lZDI1NTE5AAAAIEno6mCvDRAO8TD8/9Sw7UeJqygE+Lixw7wa2DH8LMc8 eddsa-  
key-20230630
```

Set Cancel



Full documentation available here:

<https://hpc-docs.uni.lu/connect/ipa/#upload-your-ssh-key-on-the-ulhpc-identity-management-portal>

Step 3 - Give us your public key

Ensure that you clicked on **Save** before leaving IPA otherwise your key will not be taken into account.

✓ User: jschleich

jschleich is a member of:

Settings	User Groups	Netgroups	Roles	HBAC Rules
----------	-------------	-----------	-------	------------

Refresh Revert **Save** Actions ▾

Identity Settings

Job Title

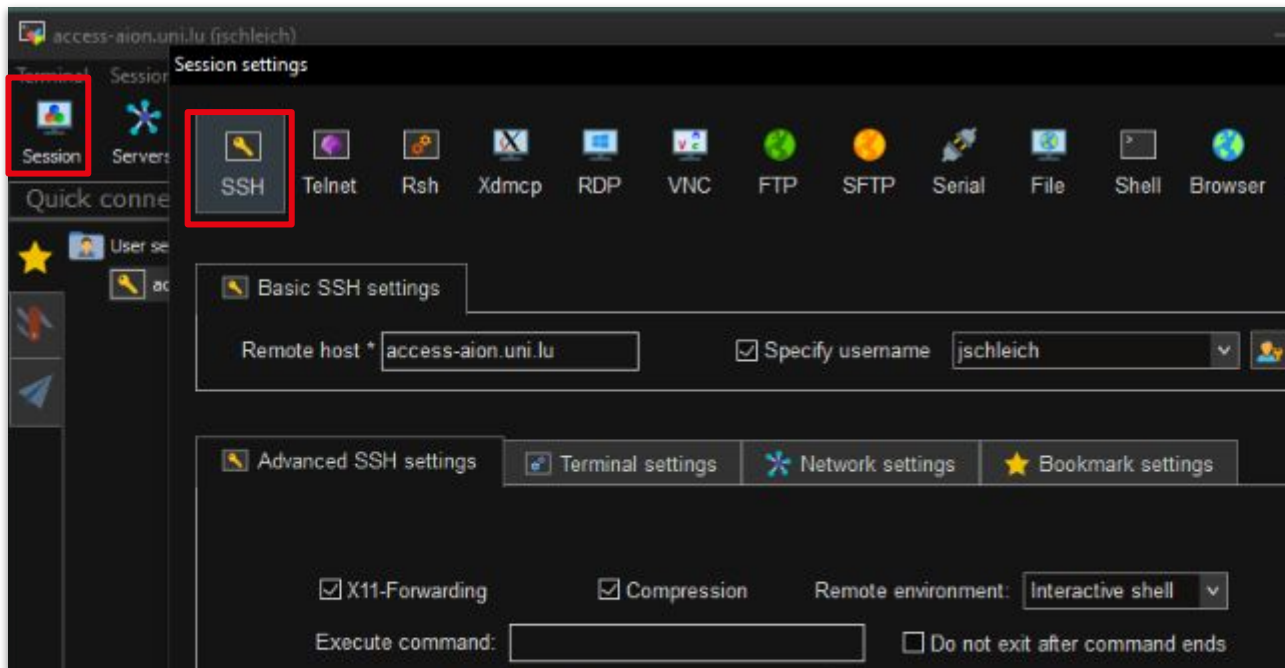


Full documentation available here:

<https://hpc-docs.uni.lu/connect/ipa/#upload-your-ssh-key-on-the-ulhpc-identity-management-portal>

Step 4 - First connection

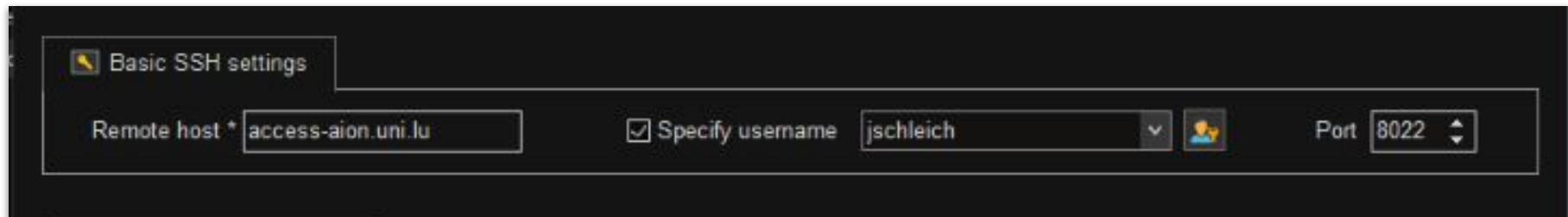
Click on Session and select SSH



Step 4 - First connection

In Basic SSH settings, fill in:

- Remote host (access-aion.uni.lu or access-iris.uni.lu)
- Specify your ULHPC username
- Specify the port (8022)

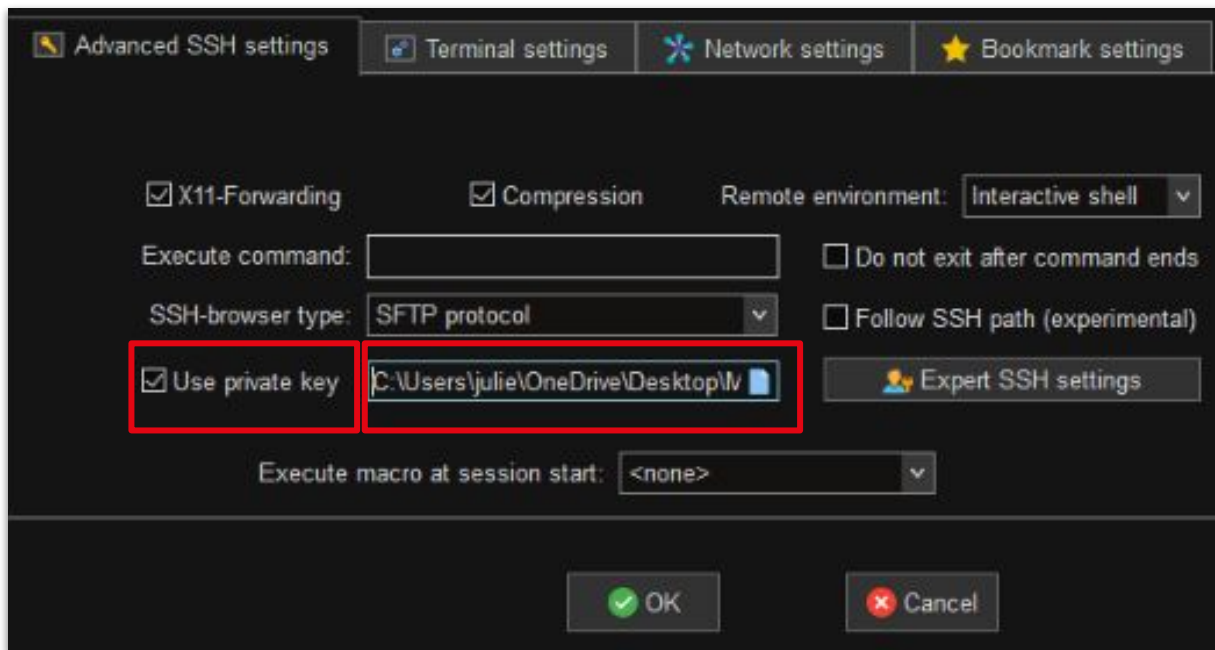


The screenshot shows a dark-themed dialog box titled "Basic SSH settings" with a yellow lightning bolt icon. It contains the following fields and controls:

- Remote host ***: A text input field containing "access-aion.uni.lu".
- Specify username**: A checked checkbox followed by a dropdown menu showing "jschleich" and a user icon.
- Port**: A numeric input field with "8022" and up/down arrow buttons.

Step 4 - First connection

In Advanced SSH settings, select Use private key and select your private key file



Advanced SSH settings | Terminal settings | Network settings | Bookmark settings

☒ X11-Forwarding ☒ Compression Remote environment: Interactive shell ▼

Execute command:

SSH-browser type: SFTP protocol ▼

☒ Use private key

☐ Do not exit after command ends

☐ Follow SSH path (experimental)

Execute macro at session start: <none> ▼

Step 4 - First connection



Upon your first connection, you will be prompted with the following message. Type yes to accept.

```
The authenticity of host '[access-aion.uni.lu]:8022 ([172.20.3.16]:8022)' can't be established.  
ED25519 key fingerprint is SHA256:jwbW8pkfCzXrh1Xhf9n0UI+7hd/YGi4Fly0E92yxxe0.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Step 4 - First connection

Click on the Ok button and you should be connected on the cluster!

```
=====
Welcome to access1.aion-cluster.uni.lux
=====

Access1
(Aion Cluster)

=====
Atos BullSequana XH2000 Direct Liquid Cooling (DLC) supercomputer
                                     https://hpc-docs.uni.lu/systems/aion/
=== Computing Nodes === #RAM/n === #Cores ==
aion-[0001-0354] 354 Atos X2410 AMD compute blade 256GB 40704
                 (2 AMD Epyc ROME 7H12 @ 2.6 GHz [64c/280W])
```

Troubleshooting



Connection timeout

You probably use an internet connection that filters out the 8022 port.

Try to use Eduroam or ethernet.

No route to host

Check that there is no typo in your configuration

Permission denied

- 1.You may have forgot to copy your public key in IPA
- 2.Check if you copy pasted correctly your key in IPA
- 3.If you already had other SSH keys, ensure you use the correct key to connect

Connection the cluster - Troubleshooting



A different situation? [Open a support ticket here](#)

Provide as many details as you can about the issue and what you tried to solve it.