


# Remote login via SSH

 **ssh**, the secure shell, is a way to establish a connection between two computers. In fact, you use it to login on a remote computer system, e.g. when you connect to our local computer system from home. Typically, you will have to provide a user name and a password to establish the connection. In our case, the authentication is done via a certificate that we provide you with at the beginning of the course<sup>1)</sup>. We differentiate between two scenarios:

- ssh from within our network
- ssh from outside of our network

## ssh connections within the network

You do this if you want to access a computer that

- has more computer power
- has more RAM
- is less busy

than the one you are sitting one.




You need

- your username
- your password
- the name or the IP address of the computer you want to connect to

- username: ingo
- password: 1234secret
- pool20

```
ssh -u ingo pool20
```

You will then be prompted to provide the password for the user *ingo*. The cursor will not move when you type your password, so don't worry. If the authentication was successful, you will be granted

access to the remote computer.  If you do an ssh within the network, you can omit the option `-u ingo`. This information is only required if your user name on the computer you establish the information from is different from your user name on the remote computer

## ssh connection from outside of the network

For security reason, you can access our computers via ssh from outside of our network only when you have a VPN<sup>2)</sup> connection established. This requires a ovpn certificate provided by us. Please follow the steps below to set up the VPN.

we have provided you with a OVPN certificate, that allows you to connect your local computer with our private network.

1. Download the certificate to your local computer
2. gunzip the certificate

```
gunzip *.ovpn.gz
```



3. Install an open VPN client on your local machine
  1. Windows users: install [OpenVPN connect client](#)
  2. Mac users
    1. install [Tunnelblick](#)
    2. on an iPad, you can install the OpenVPN Connect App
4. load the certificate
5. activate the VPN connection
  1. for this, you will need the username and the password provided by us<sup>3)</sup>
6. an [open terminal/shell](#)
7. The IP address of our gateway: **141.2.46.150**

## How the login via ssh works

If you have all the information specified above at hand, proceed to the next steps

- SSH from a [Windows](#) machine
- SSH from Mac OS or Linux: Take a look at the [following clip](#)

### Example

Type the following example command in the terminal window, where openssh22 is your certificate, and pbioc01 is your account. You will be prompted to introduce your password.

```
# To connect to the server
ssh -i pbioc_course/openssh22 pbioc01@141.2.46.150

# Select a working station
ssh pool01

# Copy files from your personal computer to our computer system.
# Syntax: scp <ssh key> <target file> <where to paste it>
scp -i pbioc_course/openssh22 file.fasta pbioc01@141.2.46.150:/home/pbioc06
scp -i pbioc_course/openssh22 pbioc01@141.2.46.150:/home/pbioc06/file.png
~/Desktop
```

If you encounter the message “WARNING: UNPROTECTED PRIVATE KEY FILE”. You will need to change

the permissions in your ssh certificate.

```
chmod 400 openssh22
```

- [computerenvironment](#)

1)

We do this only when it will be an online course

2)

virtual private network

3)

If you are unsure that you got the right username, ask the tutors. Using the wrong name will give you quite some headaches further down.

From:

<https://applbio.biologie.uni-frankfurt.de/teaching/wiki/> - **Teaching**

Permanent link:

<https://applbio.biologie.uni-frankfurt.de/teaching/wiki/doku.php?id=general:computerenvironment:ssh>

Last update: **2024/06/18 09:26**

