

Server Connection Instructions

2020 Bioinformatics Research Experience

Mac

1. Software needed:
 - a. XQuartz <https://www.xquartz.org/>
 - b. Cyberduck <https://cyberduck.io/>
 - c. Cisco AnyConnect VPN
2. Connecting to the server
 - a. Sign into Cisco AnyConnect VPN
 - i. Under VPN, in the box next to the Connect button, put in the vpn address, `vpn.coriell.org`
 - ii. Click **Connect**
 - iii. In the popup, enter your username and password. For the **Group** dropdown menu, you should select **Default**
 - iv. Click OK and you should be connected to the VPN. The VPN client also should have a green check mark over the lock and say "Connected to `vpn.coriell.org`"
 - b. Open terminal and type the command to connect to the server `ssh -Y yourusername@10.1.105.13`
 - i. Your username is your first initial, then last name, ex: Jane Doe's username would be `jdoe`
 - ii. Your password is "password"
 - c. Enter your password when prompted
3. Transferring files to and from the server
 - a. If you're not already, sign into Cisco AnyConnect VPN
 - b. Set up an SSH key in terminal
 - i. Type the command `ssh-keygen -t rsa -b 4096 -C "your_email@domain.com"` to generate an SSH key
 - ii. When you're prompted to "Enter a file in which to save the key," press Enter. This accepts the default file location.
 - iii. When you're asked to Enter passphrase either type a password you'll remember, or you can hit Enter to skip using a password. (On a secure personal machine I'd just hit Enter to make your life easier.)

- iv. Start the SSH agent in the background with the command
`eval "$(ssh-agent -s)"`
- v. Check to see if the file `~/.ssh/config` exists by entering the command `open ~/.ssh/config` If it doesn't exist create it with the command `touch ~/.ssh/config`
- vi. Last step, add your SSH private key to the ssh-agent with the command `ssh-add -K ~/.ssh/id_rsa`
- c. Launch Cyberduck
- d. Click on the + button in the lower left corner
 - i. On the drop down menu, select "SFTP (SSH File Transfer Protocol)"
 - ii. For the **Server** box enter `10.1.105.13`
 - iii. The **Port** box should say 22
 - iv. In the **Username** and **Password** boxes, put your username and password for the server
 - v. Click **Connect**
 - vi. When it asks about an **Unknown fingerprint** click the box next to **Always**, then click **Allow**

Windows

1. Software needed:
 - a. PuTTY <https://www.chiark.greenend.org.uk/~sgtatham/putty/>
 - b. Xming <https://sourceforge.net/projects/xming/>
 - c. WinSCP <https://winscp.net/eng/index.php>
 - d. Cisco AnyConnect VPN
2. Connecting to the server
 - a. Sign into Cisco AnyConnect VPN
 - b. Sign into the server using PuTTY
 - i. In the main screen under **HostName** type `10.1.105.13`
 - ii. Still on the main screen make sure the connection type is SSH
 - iii. On the left side panel expand the “**SSH**” section then click on **X11**. Make sure the box saying **Enable X11 forwarding** is checked.
 - iv. On the left side panel, click **Session** to go back to the main screen. Under **Saved Sessions**, type a name you want to save the settings under, then press **Save**.
 - v. Click **Open**.
 - vi. Enter your username and password when prompted.
 1. Your username is your first initial, then last name, ex: Jane Doe’s username would be `jdoe`
 2. Your password is “password”
3. Transferring files to and from the server
 - a. If you’re not already, sign into Cisco AnyConnect VPN
 - b. Launch WinSCP and on the **Login** screen that pops up when you launch it enter:
 - i. Under **HostName** put `cbix`
 - ii. Under **User name:** put your username for the server
 - iii. Under **Password:** put your password for the server
 - c. Click **Login**