

Remote access to Cadence

If you are working off campus:

First, connect to TAMU VPN using Cisco:

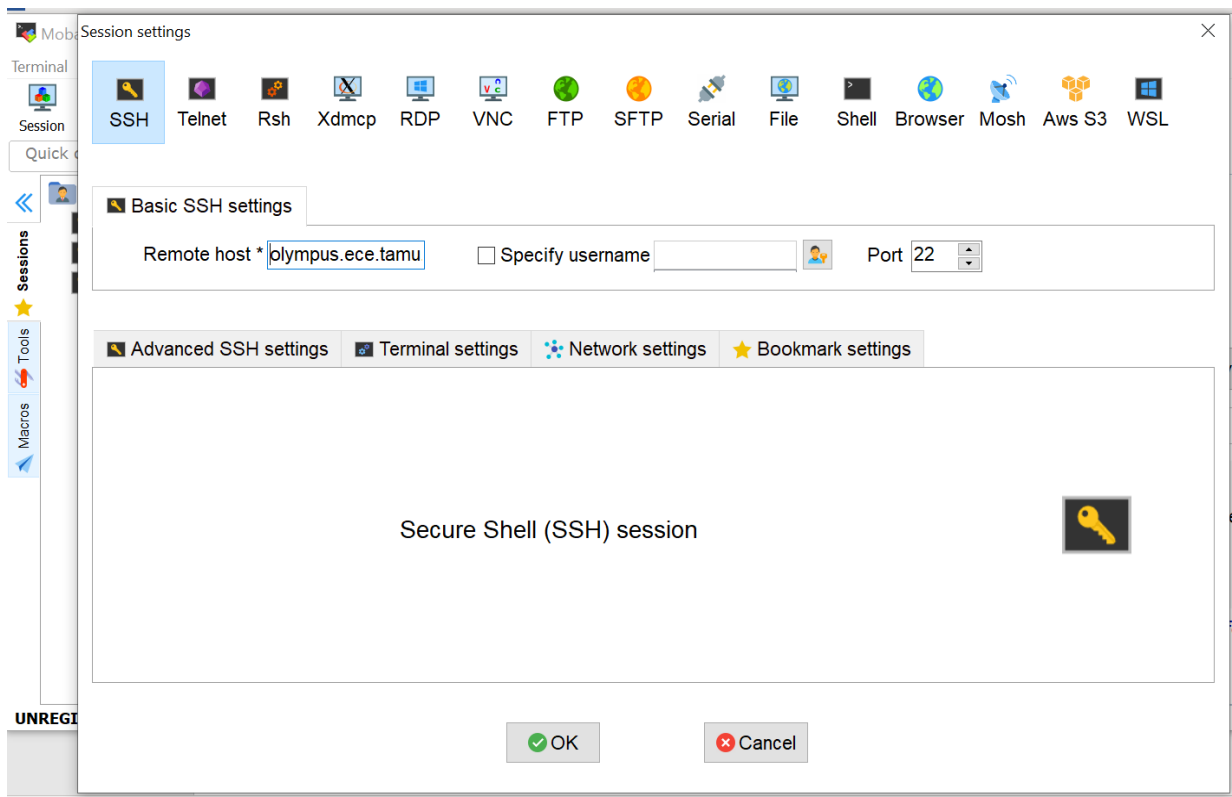
<https://tamuengr.atlassian.net/wiki/spaces/helpdesk/pages/1148059651/Installing+and+Using+Cisco+VPN>

If you got error message "failed to create home directory", please refer to:

<https://tamuengr.atlassian.net/wiki/spaces/helpdesk/pages/1986396173/Home-directory+Setup>

### For Window users:

1. Download and install [MobaXterm](#).
2. Run the program.
3. On the left side of the menu bar click on Session>>SSH.
4. In the remote host section type: olympus.ece.tamu.edu and click ok.



5. Now, under the user sessions panel, you can see the remote host name (Olympus). Double click on the session. A tab will open and ask for your username and password.

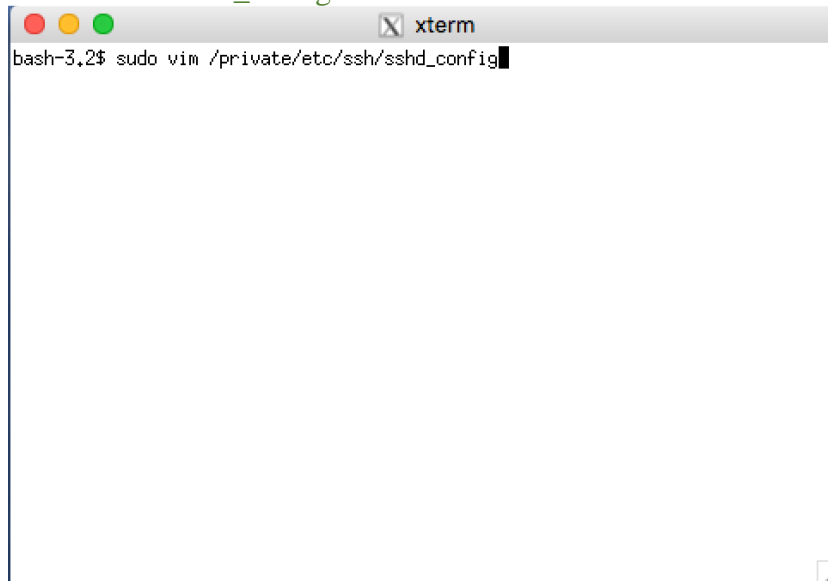
6. **Important step:** When working remotely, after getting logged in, you need to type the following command in the terminal: **load-ecen-454**

Without running the above command, other commands that are used during the labs may not work properly.

#### For Mac users:

1. Google **XQuartz**. Download and install it. The XQuartz project is an open-source effort to develop a version of the X.Org X Window System that runs on OS X.
2. Open XQuartz, edit the **sshd\_config** file. The **/etc/ssh/sshd\_config** file is the system-wide configuration file for OpenSSH which allows you to set options that modify the operation of the daemon. If you are not familiar with vim editor, select your preferred editor.

**\$ sudo vim /private/etc/ssh/sshd\_config**



**Notice:** Since this is a configuration file for OpenSSH server, you could make a backup of your sshd\_config file by copying it to your home directory

3. Find “**X11Forwarding no**” option and set it to **yes**

```
xterm
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
# Also, PAM will deny null passwords by default. If you need to allow
# null passwords, add the "nullok" option to the end of the
# securityserver,so line in /etc/pam.d/sshd.
#UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding yes
#XauthLocation xauth # Default is to search $PATH (set by launchd(8)). It is re
commended that a full path be provided.
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
```

4. Save the file by command “:w!”, then quit by command “:q!”  
You can run “\$ vim /private/etc/ssh/sshd\_config” to check if your setting works.
5. Under the bash root, using your NetID to launch hera.ece.tamu.edu SSH server  
\$ ssh -X [NetID@olympus.ece.tamu.edu](mailto:NetID@olympus.ece.tamu.edu)
6. Enter your password to log in. After getting logged in, you need to type the following command in the terminal: **load-ecen-454**

### Setting up Cadence Virtuoso

- 1) Log in to the systems using your NETID login and password (similar to logging in HOWDY portal).
- 2) Open a terminal, create a directory named "ecen454\_714" (or a name you prefer) under your home directory using mkdir command:  
mkdir ~/ecen454\_714
- 3) Change your working directory to the directory you created using cd command (cd ~/ecen454\_714)
- 4) Execute the following commands:
  - source /opt/coe/cadence/INCISIVE152/setup.INCISIVE152.linux.bash
  - source /opt/coe/ncsu/ncsu-cdk-1.6.0.beta/ncsu.sh