Accessing HPC clusters from Windows

To log in you will need an SSH client. We recommend PuTTY SSH but others are also available. After using PuTTY to get to gw.hpc.nyu.edu you will use the program ssh from a terminal window. If you are unfamiliar with the command line interface this may seem daunting - relax, it's easy and vastly more powerful than point-and-click. We have a basic tutorial here.

If you wish to use any software with a graphical interface, your Windows workstation must have an X server installed and running. This is described further in Preparing your Windows workstation below.

For easier access and to transfer files between your workstation and the clusters, you will eventually want to set up SSH tunneling.

Preparing your Windows workstation for X

If you wish to use any software with a graphical interface, you will need an X server. This is a software package that draws on your local screen windows created on a remote computer (such as an NYU HPC cluster). There are a couple of options out there:

- One option is Xming. Installation instructions can be found on its web site. To use with PuTTY, we recommend Xming. Before starting PuTTY you will need to launch Xming by double-clicking the Xming icon on your desktop or start it from the Start Menu.

- Another option is Cygwin/X. Instructions for downloading and installing it can be found here. Before starting PuTTY you will need to have the X server running, by double-clicking the “XWin Server” shortcut under Cygwin-X on the Start Menu. You may wish to add this to your Windows Startup folder so it runs automatically after starting Windows.

Note: There are complications since X server 1.17. See this Cygwin/X FAQ, and the superuser page for how to populate the PuTTY field ‘X authority file for local display’ (somewhere in the middle to bottom of the page).

You will also need to download and install PuTTY SSH if you have not already.

Logging In - the easy, primitive way

This method is useful as a first-time login, to ensure you are able to connect. For ongoing use however, we recommend setting up and using SSH tunneling instead.

When you installed PuTTY you will have added to your Desktop and also the the Start Menu and icon labeled “putty”. Double-clicking this icon will launch PuTTY, with the dialog initially in the “Session” category as in the screenshot below:

If this is not your first time through here, and you already saved a setup previously, you can select the saved session and hit “Load”. This will do the following steps for you so you can just hit “Open”. Otherwise, read on...

Enter the as Host Name “gw.hpc.nyu.edu”, leave the Port at its default value of 22 and select the “SSH” Protocol. Don’t hit “Open” just yet!

Eventually, if not now, you will probably want to use some graphical applications. For the procedure described here, you don’t need to check the “Enable X11 forwarding”. You may disable it by un-selecting Connection -> SSH -> X11 from the Category menu on the left.
Again, **don't** hit "Open" just yet...

You can save these settings to use again next time. Return to the "Session" category and give this setup a name in the "Saved Sessions" box (perhaps NYU HPC*). Now click "Save".

Finally, hit "Open". You will get a command terminal for gw.hpc.nyu.edu. This is a deliberately restricted environment from which you can do little other than to log in to one of the HPC clusters.

After you click "Open", you will get a terminal window where you will be prompted to login using your NYU NetID and password. The window will display the following:

```
login as: ssb536
** NOTICE: NYU Authorized Use Only **
```

Access and use, or causing access and use, of this computer system by anyone other than as permitted by New York University (NYU) is strictly prohibited by NYU and by law. Such use might subject an unauthorized user, including unauthorized employees, to criminal and civil penalties as well as NYU-initiated disciplinary proceedings. The use of this system is routinely monitored and recorded, and anyone accessing this system consents to such monitoring and recording.

Now, you are on the NYU Network.
Therefore, log into a cluster using one of the following commands:

```
$ ssh NetID@prince.hpc.nyu.edu
$ ssh NetID@dumbo.hpc.nyu.edu
```

Suppose, I wish to login into the prince cluster, the window will display the following:

```
ssb536@hpc-bastion1~$ ssh ssb536@prince.hpc.nyu.edu
ssb536@prince.hpc.nyu.edu's password:
Last login: Wed Aug 30 17:10:26 2017 from psd01a-0046s.cfs.its.nyu.edu
[ssb536@log-1 ~]$ 
```

In the boxes below and elsewhere in this wiki, the symbol "$" at the beginning of a line represents the command prompt - don't type the "$", type only the remainder of the line following the "$". Also wherever NetID appears, replace it with your NYU NetID.

On Prince you may notice that you are now on a host named "log-0" or "log-1" or something similar. These clusters use multiple login nodes and which one you get depends how busy each is at the time. The login nodes are configured identically and see the same filesystems, so the specific node you are logged in to is not important.

**Setting up SSH Tunneling**
Step 1: Creating the tunnel

1. First open PuTTY and prepare to log in to gw.hpc.nyu.edu, as you did in Logging in from Windows - primitive way. If you saved your session during that process, you can load it by selecting from the "Saved Sessions" box and hitting "Load". Don't hit "Open" yet!
2. Under "Connection" -> "SSH", just below "X11", select "Tunnels"

![PuTTY Configuration](image)

3. Write "8026" (the port number) in the "Source port" box, and "prince.hpc.nyu.edu:22" (the machine you wish to tunnel to - 22 is the port that ssh listens on) in the "Destination" box.
4. Click "Add". You can repeat step 3 with a different port number and a different destination. If you do this you will create multiple tunnels, one to each destination.
5. Before hitting "Open", go back to the "Sessions" page, give the session a name ("hcpgw_tunnel") and hit "Save". Then next time you need not do all this again, just load the saved session.
6. Hit "Open" to login in to gw.hpc.nyu.edu and create the tunnel. A terminal window will appear, asking for your login name (NYU NetID) and password (NYU password). Windows may also ask you to allow certain connections through its firewall - this is so you can ssh to port 8026 on your workstation - the entrance to the tunnel.

Using your SSH tunnel

To log in via the tunnel, first the tunnel must be open. If you've just completed Step 1, it will be open and you can jump down to "Step 2: Logging in via your SSH tunnel". If you completed Step 1 yesterday, and now want to re-use the tunnel you created, first start the tunnel:

You can add other NYU hosts to the tunnel by adding a new source port and destination and clicking "Add". For example, you could add "Source port = 8025" and "Destination = dumbo.hpc.nyu.edu:22", then press "Add". You would then perform Step 2 (below) twice - once for prince on port 8026 and once for dumbo on port 8025.
Starting the tunnel

During a session, you need only do this once - as long as the tunnel is open, new connections will go over it.

1. Start Putty.exe (again, if necessary), and load the session you saved in Setting up SSH Tunneling.
2. Hit “Open”, and log in to the bastion host with your NYU NetID and password. This will create the tunnel.

Step 2: Logging in via your SSH tunnel

1. Start the second Putty.exe. In the “Host Name” box, write “localhost” and in the “Port” box, write “8026” (or whichever port number you specified when you set up the tunnel in Setting up SSH Tunneling).
   We use “localhost” because the entrance of the tunnel is actually on this workstation, at port 8026.
2. Go to “Connections” -> “SSH” -> “X11” and check “Enable X11 forwarding”.

3. Optionally, give this session a name (in “Saved Sessions”) and hit “Save” to save it. Then next time instead of steps 1 and 2 you can simply load this saved session.

4. Hit “Open”. You will again get a terminal window asking for your login (NYU NetID) and password (NYU password). You are now logged in to the HPC cluster!