Remote Access to ECF Machines

This document describes several ways in which you may remotely connect to an ECF machine. It is largely based on the web page authored by ECF staff and that describes how to remotely connect to ECF[1]. Please feel free to also visit that page as well and go through it.

1 ECF Machines

The assignments in this course can only be done on ECF machines running the Linux operating system. You will most likely connect to the machine named `remote.ecf.utoronto.ca`, which is the main ECF remote access server.

You can also connect to other machines named `pX.ecf.utoronto.ca`, where `X` is a number that ranges between `1` and `185`. These are workstations that are located in the ECF labs. Thus, for example, you can connect to `p100.ecf.utoronto.ca` or to `p130.ecf.utoronto.ca`. However, if you connect to one of these machines from outside campus, you must use a VPN, which is not explained in this document; please refer to `https://isea.utoronto.ca/services/vpn/utorvpn/users/` for instructions on how to use the University's VPN service.

ECF machines must be accessed securely. This is often done using a secure shell or `ssh`. Thus, you must have an `ssh` *client* on your computer and use it to access one of the ECF machines. There are several `ssh` clients for Windows. This document describes only one: `PuTTY`. For macOS, `ssh` is built-in.

2 Connecting from a Windows Machine

The first step is to download `PuTTY` from `https://www.putty.org/` and install it on your machine. The first time you run `PuTTY` you will be prompted to configure it by providing a host name. Enter `remote.ecf.utoronto.ca`, as shown in the Figure 1 below. Click `Open` and you should be connected to `remote.ecg.utoronto.ca` with `ssh`, where you can provide your username and password.

3 Connecting from a Mac/Linux Machine

An `ssh` client is built into macOS/Linux. Thus, you can start the `Terminal` app on your Mac or a `xterm` on your Linux box to launch a terminal window. In this window, you can connect to an ECF machine using the command, replacing *<ecf-username>* with your actual ECF username.

```
% ssh  <ecf-username>@remote.ecf.utoronto.ca
```

You will be promoted for your password to login.

[1] `https://undergrad.engineering.utoronto.ca/undergrad-resources/engineering-computing-facility-ecf/remote-access/`

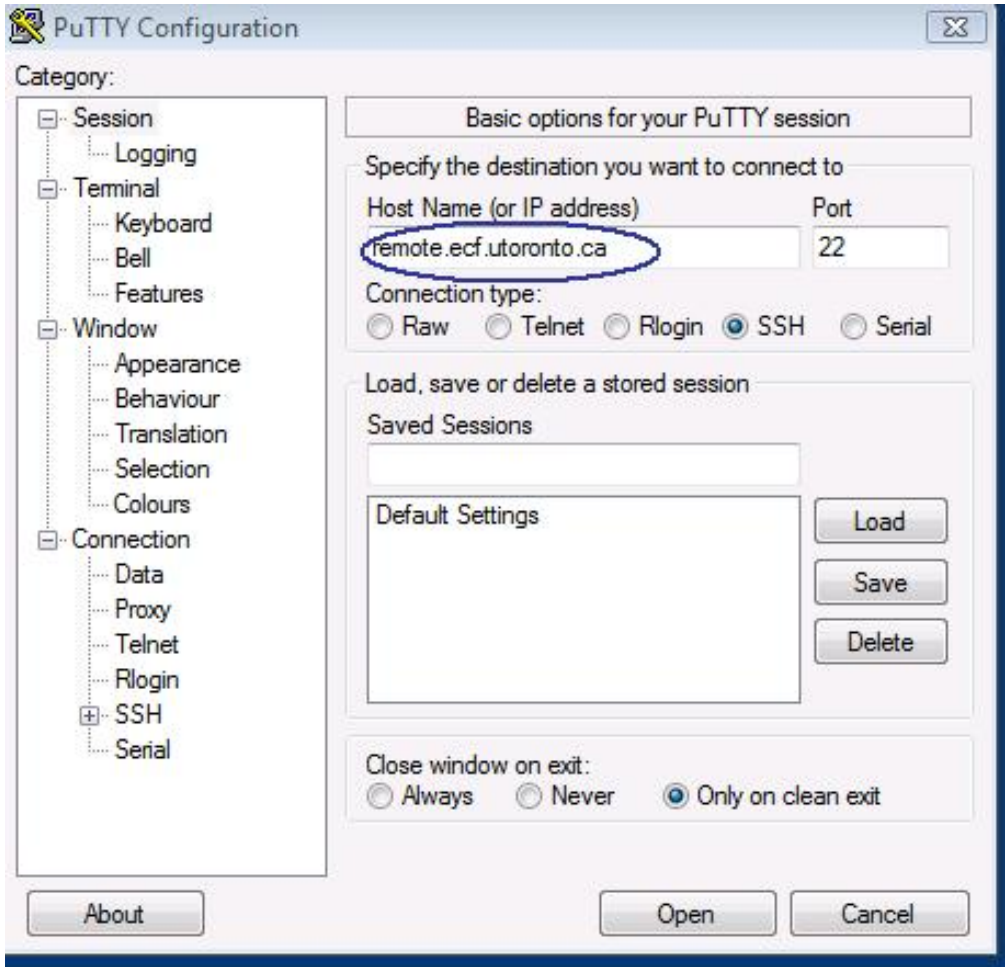

Figure 1: Providing a host name to `PuTTY`

4 Connecting using VNC

Virtual Network Computing (VNC) is a graphical desktop sharing system that allows a user on one computer to remotely control another computer. It does so by transmitting keyboard and mouse events from the user's computer to the remote one, and by relaying the graphical screen updates back in the opposite direction[2]. The communication between the two computers is often done over a secure network connection known as an *ssh tunnel*.

The use of VNC comes handy when working on graphics-based assignments. One can connect using VNC to ECF, run code there as if using one of the machines in the lab. Further, using VNC may result in faster response time compared to just forwarding an X11 connection and using a local X11 server.

4.1 Using VNC

In order to use VNC to connect your computer (referred to as the *client*) to an ECF machine (referred to as the *server*), two pieces of software must be running. The first is the VNC *server*, which runs on ECF. The second is the VNC *viewer*, which runs on the client (i.e., your com-

[2] `https://en.wikipedia.org/wiki/Virtual_Network_Computing`

puter). Further, and particularly if you are connecting from off-campus, there must exist a secure communication channel, i.e., the ssh tunnel, between the client and the server[3].

A VNC server is always running on `remote.ecf.utoronto.ca`. Thus, what remains for you to use VNC is: (1) download and run a VNC viewer on your computer, and (2) establish the secure channel, also known as an *ssh tunnel*. How you do this depends on what operating system you are running and which VNC viewer you will use. The remainder of this document details how to do so for Windows, macOS and Linux machines.

4.2 VNC Viewers

There are many VNC viewers available for various operating systems and target computers. They include `TightVNC`, `RealNVC` and `TigerVNC` just to name a few. Some viewers are free while others must be purchased. Regrettably, it is not possible to make any recommendation on a viewer. It is probably best that you try a couple of viewers and see for yourself which one you like to use.

4.3 Instructions for Windows

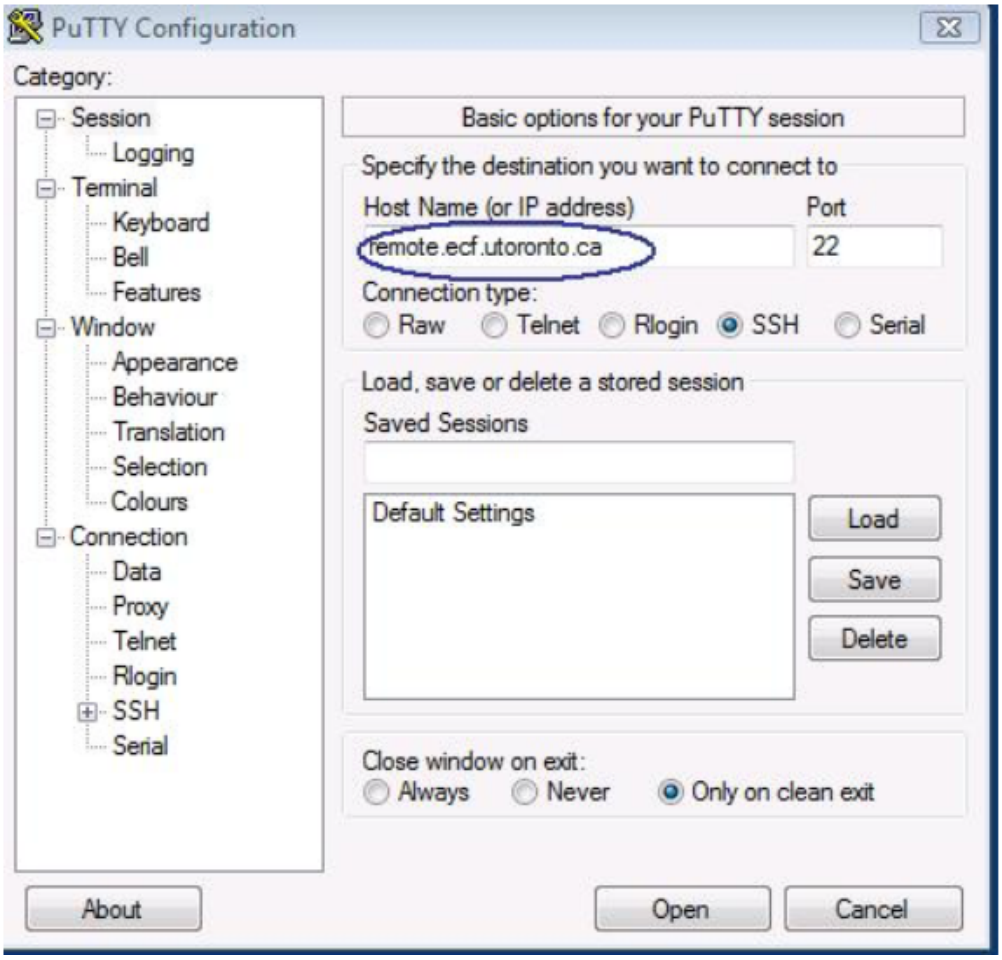

Figure 2: Connecting to ECF with `PuTTY`

[3]Establishing an ssh tunnel is only needed when connecting from off-campus. If you are connecting using any university network, including the wireless network, you can directly use your VNC client without a tunnel.

The first step to use VNC on your Windows machine is to use `PuTTY` to establish a secure tunnel between your machine and the ECF server. You can do this by running `PuTTY`. If this is the first time for you to use `PuTTY`, you will be prompted to enter your ECF user name and password. Please see Figure 2 and enter `remote.ecf.utoronto.ca`. To establish the tunnel, select `Connection -> SSH -> Tunnels`. Enter 2000 for the source port and `remote.ecf.utoronto.ca:1000` for the destination, as shown in Figure 3. Click on "Add" then click on "Open".

Once the tunnel has been established, you can run the VNC client you downloaded to your machine and enter `localhost:2000` as the server. You will be connected to ECF, where you can login with your user name and password.

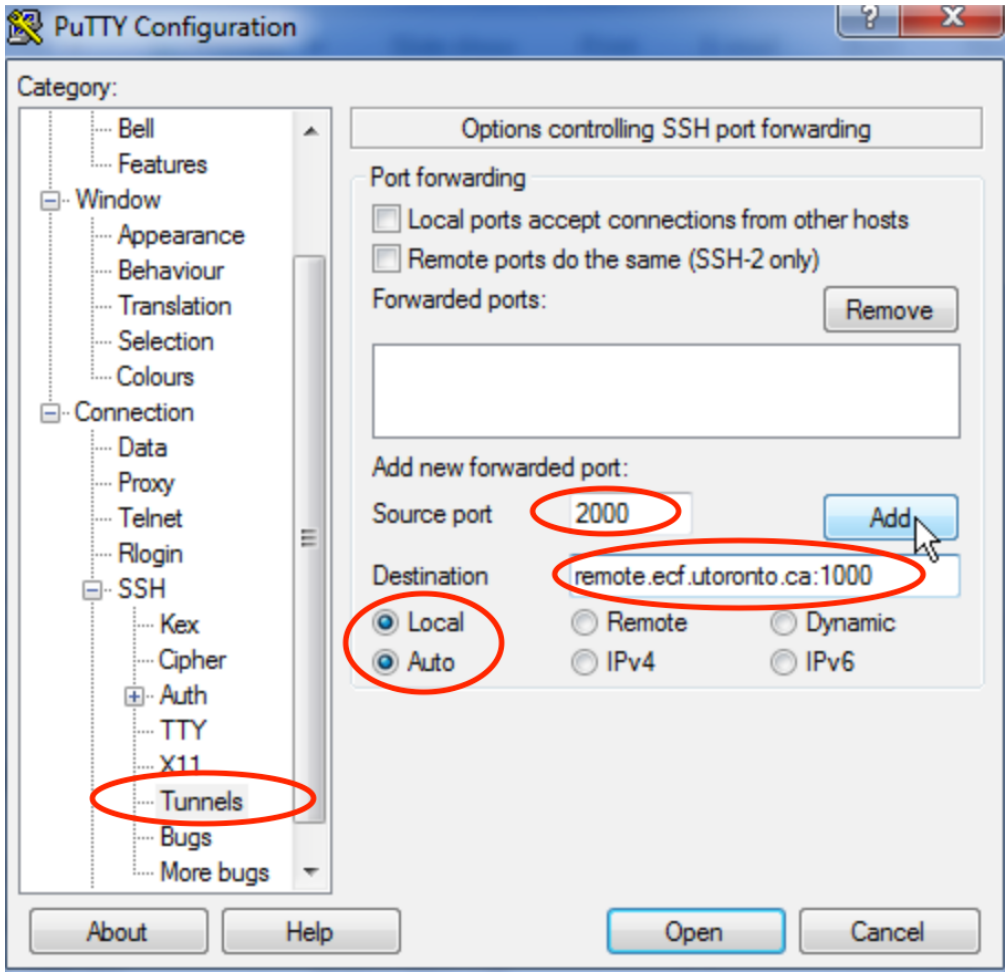

Figure 3: Configuring `PuTTY` to establish a secure ssh tunnel

4.4 Instructions for macOS

Start a terminal window through "`Applications -> Utilities -> Terminal`". Once the terminal window is open, type the following command in it, replacing *<ecf-username>* with your actual user name on ECF. Provide your ECF password.

```
% ssh -f -N -L 2000:localhost:1000  <ecf-username>@remote.ecf.utoronto.ca
```

The above command establishes a tunnel that listens to traffic on port 2000 of your local machine and forwards it to port 1000 on `remote.ecf`, where the VNC server is. if you get a message that looks like:

```
The authenticity of host 'remote.ecf.utoronto.ca (x.x.x.x)' can't be established.
RSA key fingerprint is xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.
Are you sure you want to continue connecting (yes/no)?
```

Make sure that you entered `remote.ecf.utoronto.ca` correctly and then type `yes`. This should happen only the first time you connect.

Now start your VNC viewer for macOS and specify a connection to `localhost:2000`. For example, if you are using `realVNC` for macOS, start it and type in `localhost:2000` followed by enter to connect, as shown in Figure 4. Click on `Continue` to proceed. You will be connected to ECF, where you can login with your user name and password.

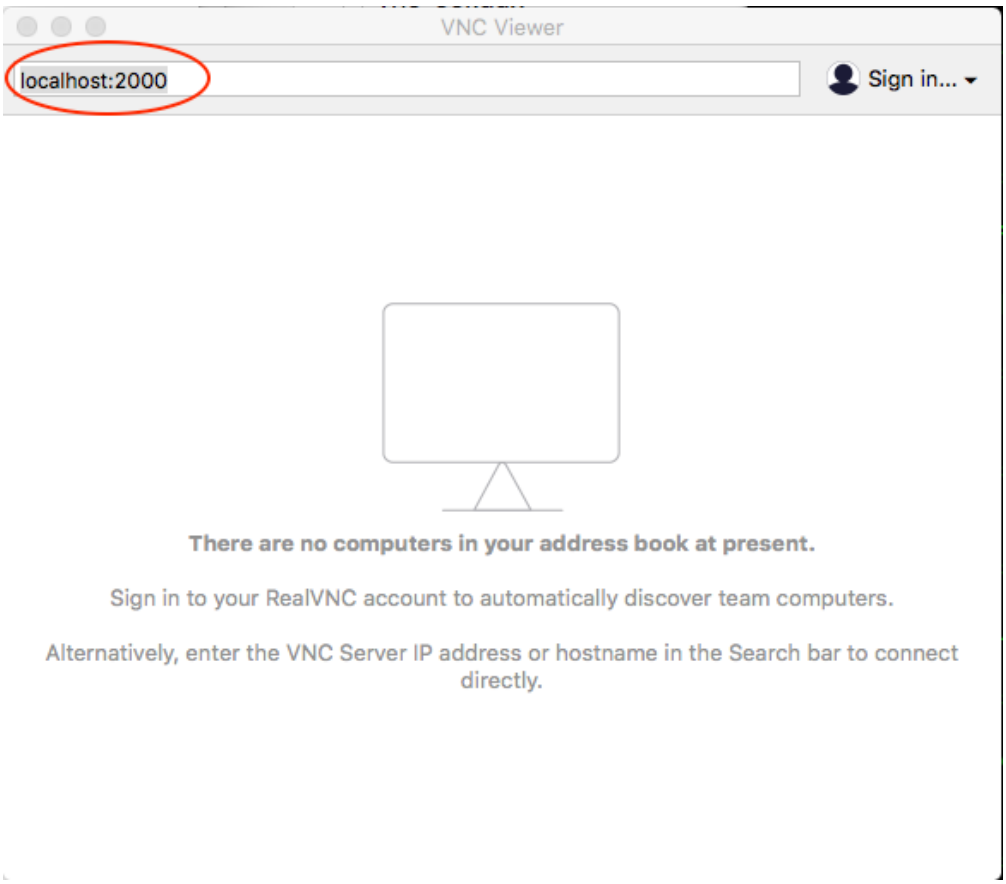

Figure 4: Specifying VNC connection on `RealVNC` on macOS

4.5 Instructions for Linux

The instructions for Linux are very similar to those for macOS. Start a terminal window (xterm) and type the following commands, replacing *<ecf-username>* with your actual user name on ECF.

```
% ssh -f -N -L 2000:localhost:1000  <ecf-username>@remote.ecf.utoronto.ca
% vncviewer localhost::2000
```

The first command establishes the tunnel that listens to traffic on port 2000 of your local machine and forwards it to port 1000 on `remote.ecf`, where the VNC server is. The second runs the VNC viewer (here, the `TightVNC` one is used), asking it to direct traffic to port 2000 on the local machine. When the viewer starts, follow the instructions to login to ECF.