Tunnel VNC through SSH Tutorial Version 1

UltraVNC features a Data Stream Modification (DSM) plugin system which can provide an encrypted tunnel for the Virtual Network Computing (VNC) connection. This tutorial shows you how to use OpenSSH to tunnel VNC traffic as an alternative to using one of the plugins.

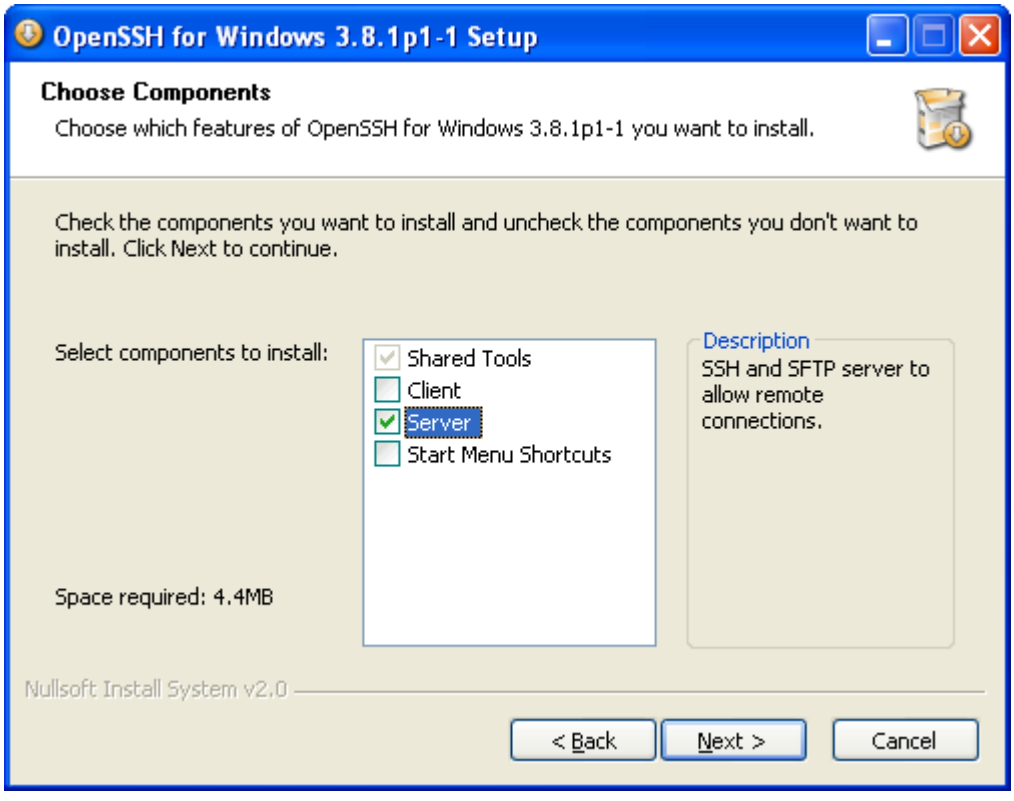
Note: if the PC you wish to access does not have a static IP address assigned by your internet service provider (which is typically the case for a home PC) you may want to sign up for a free DynDNS account so you can connect to your home network using a host name that will automatically track your dynamic public IP address.

PC You Wish to Access Remotely

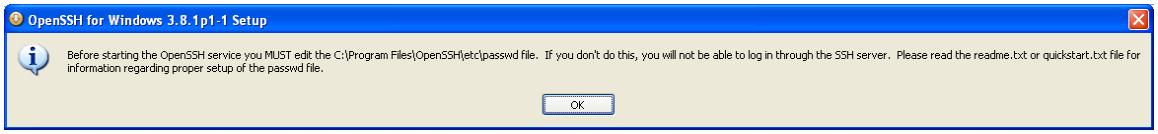
Secure Shell Setup

Download OpenSSH for Windows from http://sshwindows.sourceforge.net/ on the PC you wish to control from a remote location. OpenSSH supports 3DES, Blowfish, AES and arcfour as encryption algorithms. Refer to http://www.openssh.com/ for complete details.

Run the **setupssh.exe** executable program from the saved location. Select the defaults until you're prompted with the following. Only the Server is required for connecting from a remote PC, but the Client may be used to connect to other SSH servers if desired.



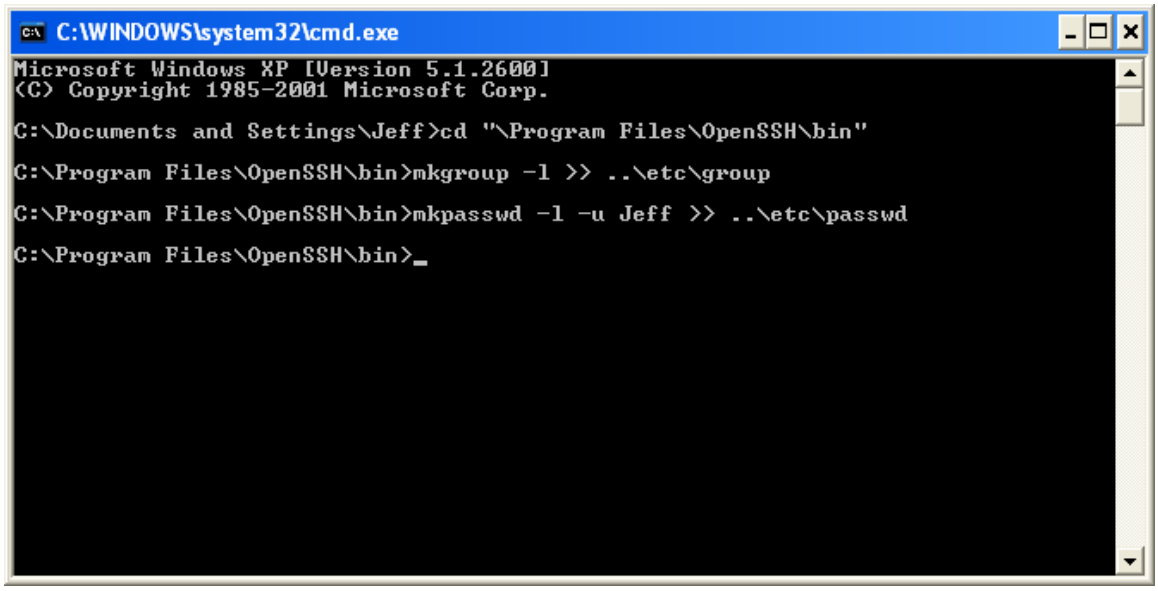
Use the defaults and you'll be prompted with the following message.



Note: In order to connect from a remote PC you'll be logging in using your Windows username and password so ensure that it's a secure one.

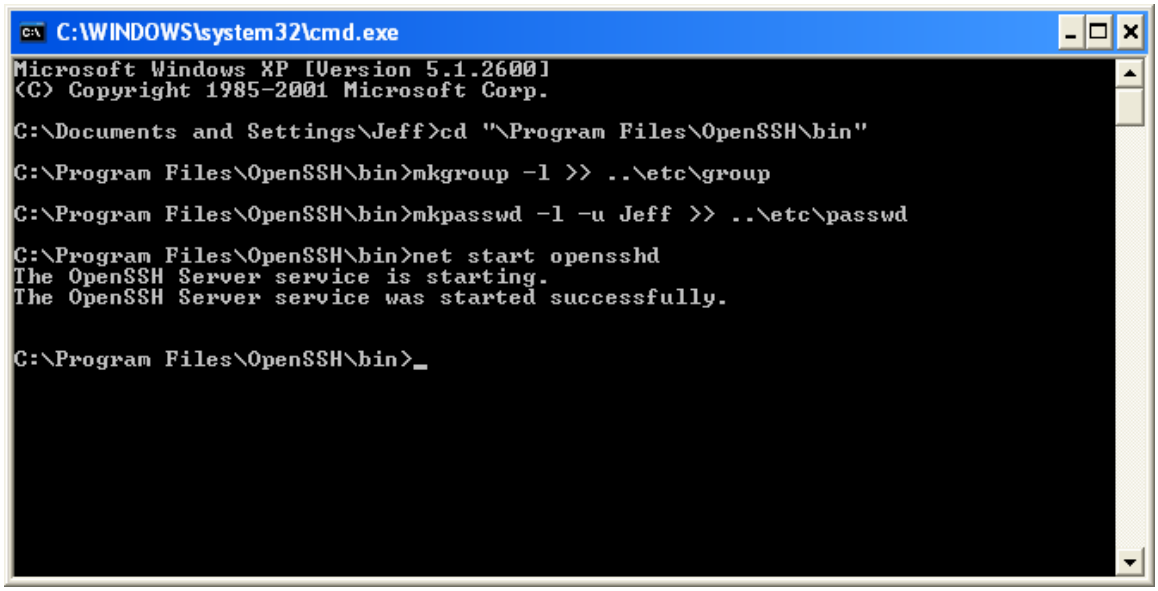
Open up a command prompt (click *Start* • *Run*, type **cmd**, and press **<Enter>**) and Change Directory (CD) to the OpenSSH installation directory (*Program Files\OpenSSH* is the default) and then *CD* into the *bin* directory by typing **cd "\Program Files\OpenSSH\bin"** and press **<Enter>**.

Use *mkgroup* to create a group permissions file for the local groups by typing **mkgroup –l >> ..\etc\group** and press **<Enter>**. Use *mkpasswd* to add authorized local users into the passwd file by typing **mkpasswd –l –u <username> >> ..\etc\passwd**. For example, the following creates a group permissions file and adds the local user Jeff.



The OpenSSH server listens for traffic on TCP port 22 by default. If your firewall setup does not allow connections on this port, it can be changed by editing the *OpenSSH\etc\sshd_config* file. In addition, some corporate firewalls do not allow outbound traffic on port 22 so it may be desired to change this to port 443 which typically is not blocked. In any event, the chosen port will need to be forwarded to the OpenSSH server PC on your router. See http://portforward.com/routers.htm for instruction on how to port forward using the router you have. Also, if you are running a software firewall you will need to open the selected port on it as well.

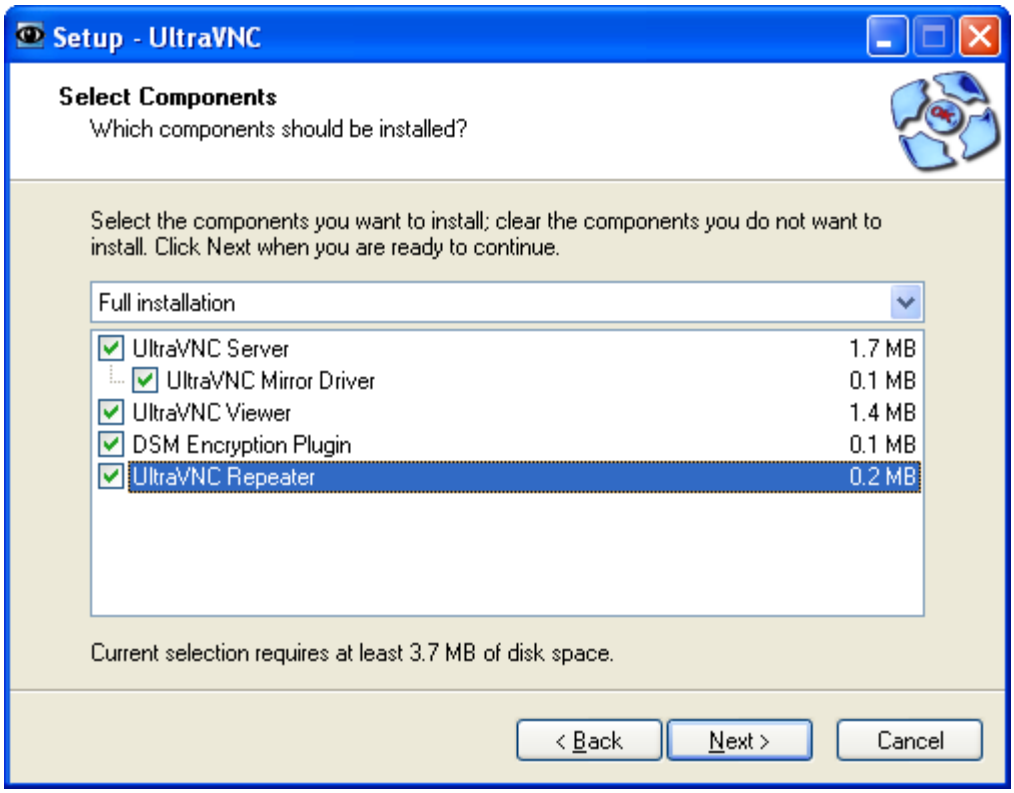
Once the firewall is configured, you can start the service as shown in the following screenshot. For further details of the OpenSSH server configuration refer to the readme.txt file located in the *OpenSSH\docs* directory.



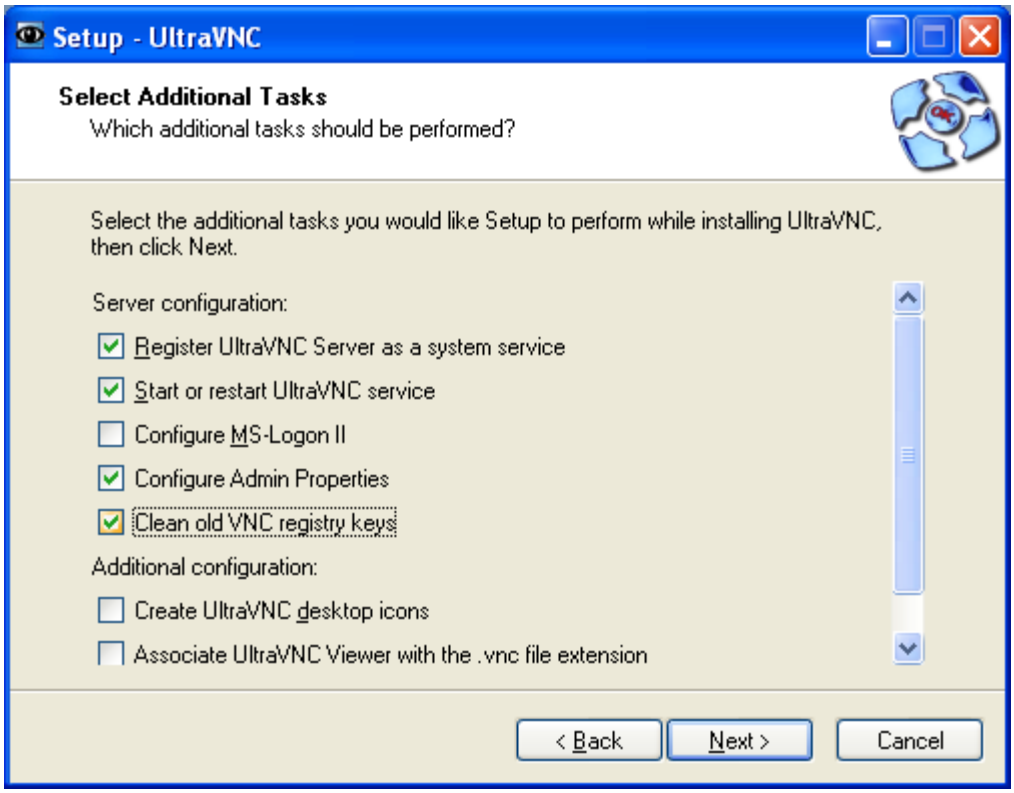
UltraVNC Setup

Download UltraVNC from http://www.uvnc.com/download/index.html on the PC you wish to control from a remote location. This tutorial covers a subset of the full installation options of UltraVNC that are covered at http://www.uvnc.com/install/installation.html. Refer there for explanation of all the configuration options.

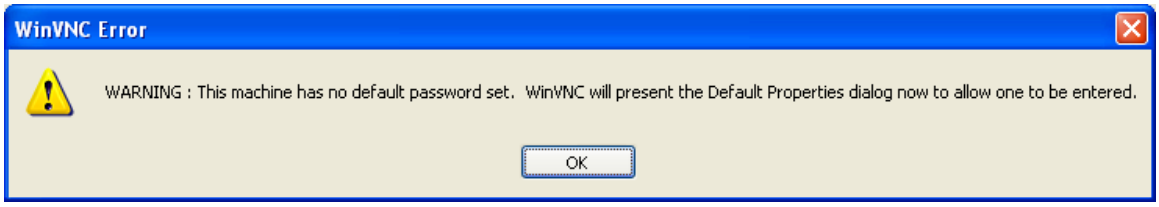
Run the **UltraVNC-102-Setup.exe** executable program from the saved location. Select the defaults until you're prompted with the following screenshot. Only the Server is required for connecting from a remote PC (and we'll be using the viewer to check the installation), but the other components may be desired. See http://www.uvnc.com/features/index.html for a description of the Mirror Driver and DSM Encryption Plugin and http://www.uvnc.com/addons/index.html for a description of the Repeater. The Viewer is used to connect to other UltraVNC Servers.



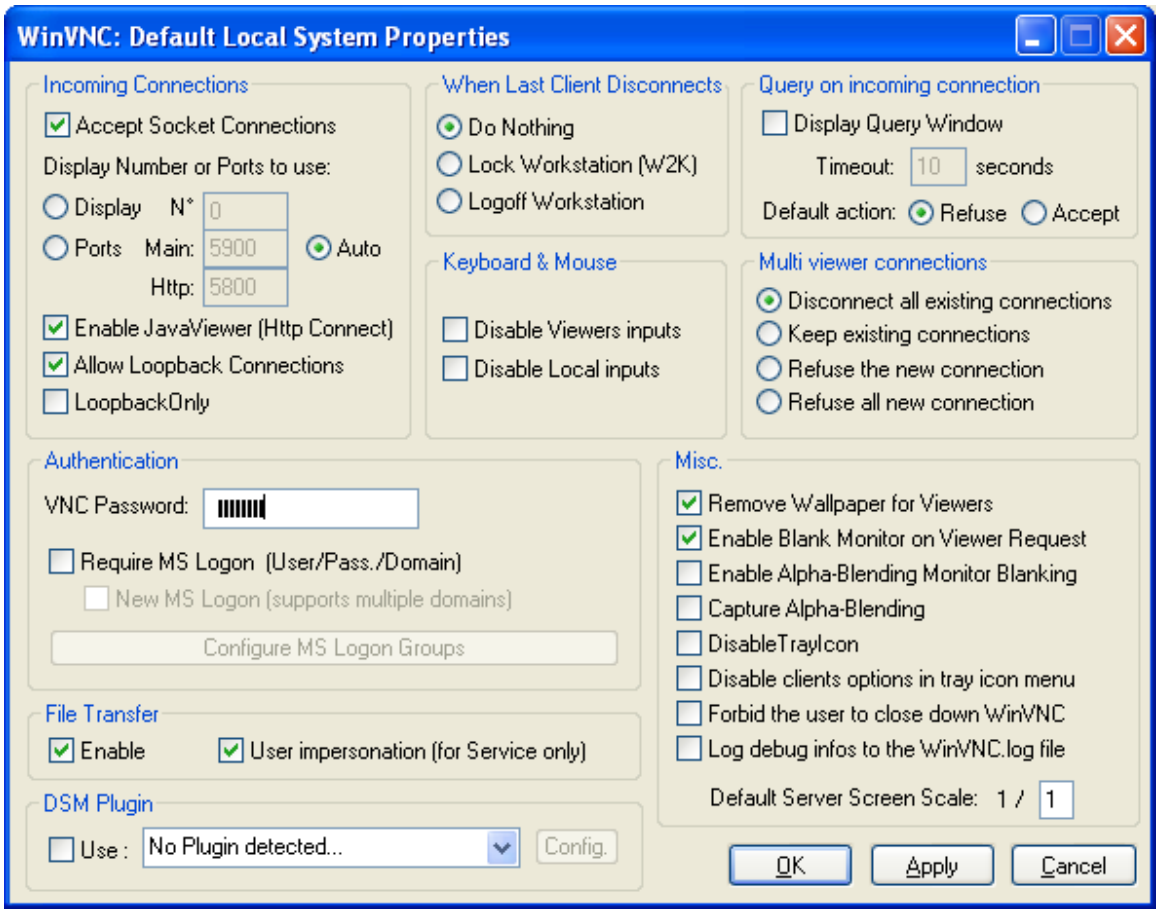
Select the defaults until you're prompted with the following screenshot. Select *Register UltraVNC Server as a system service*, *Start or restart UltraVNC service*, *Configure Admin Properties* and *Clean old VNC registry keys* (only need to clean keys if this isn't the first install of UltraVNC) then click *Next*.



Select the defaults and install. Since UltraVNC requires a password and one hasn't been set yet, the following error will occur.

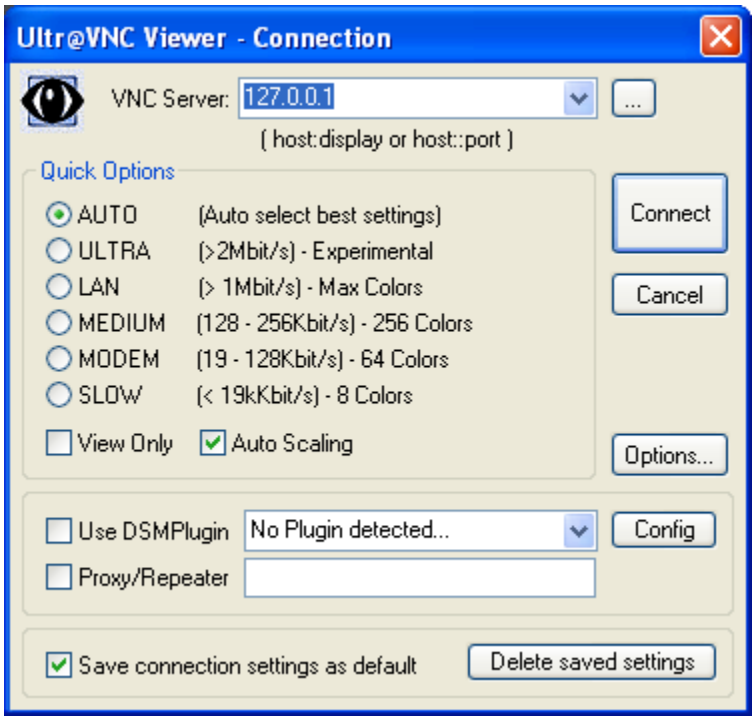


Acknowledge the error and configure the admin properties as follows. Ensure that you assign a *VNC Password* (up to 8 characters) at this point so you can connect later. Since the OpenSSH server is running on the same machine as the UltraVNC server, we need to *Allow Loopback Connections*. If this is the only method that you'll use to connect to this machine it may be a good idea to select the *LoopbackOnly* option. I typically connect to other machines on my private network without using the secure shell so I've left it blank. For an explanation of all the other options refer to http://www.uvnc.com/install/configuration.html.

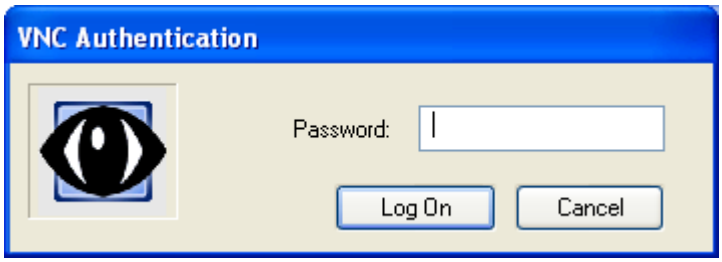


Select *OK* and use the defaults for the remaining dialogs.

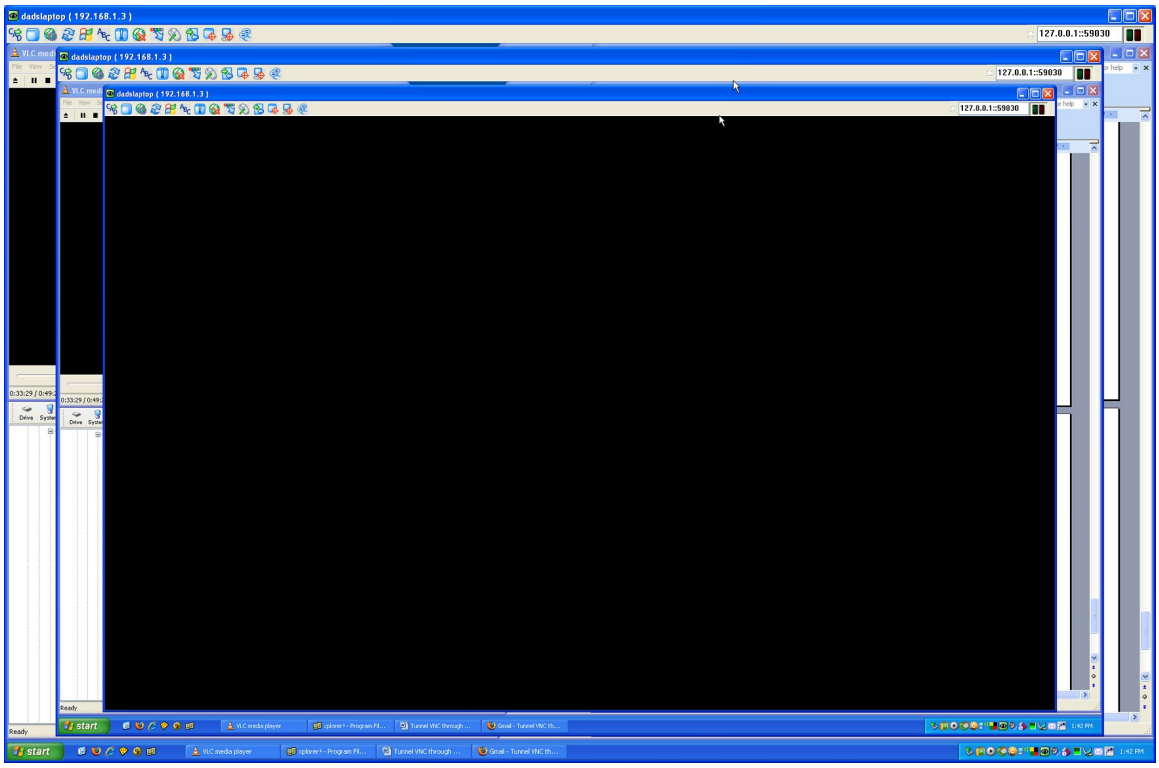
After completing the UltraVNC server installation, test the loopback configuration by connecting using the viewer on the same PC. To do this, click *Start* • *Run*, type **vncviewer**, and press **<Enter>** to open the viewer as shown in the following screenshot.



To attempt the connection, specify **127.0.0.1** or **localhost** as the *VNC Server* and select *Connect*. After selecting *Connect*, you will be prompted for the VNC password assigned in the administrative properties section above (not the windows user password).



After entering the correct password, you will see the standard UltraVNC window of the local desktop which, in turn, shows the same UltraVNC window and so on as shown in the following screenshot. We just want to ensure that we connect without interference from any security software so disconnect using the *Close Connection* button (don't simply close the window).

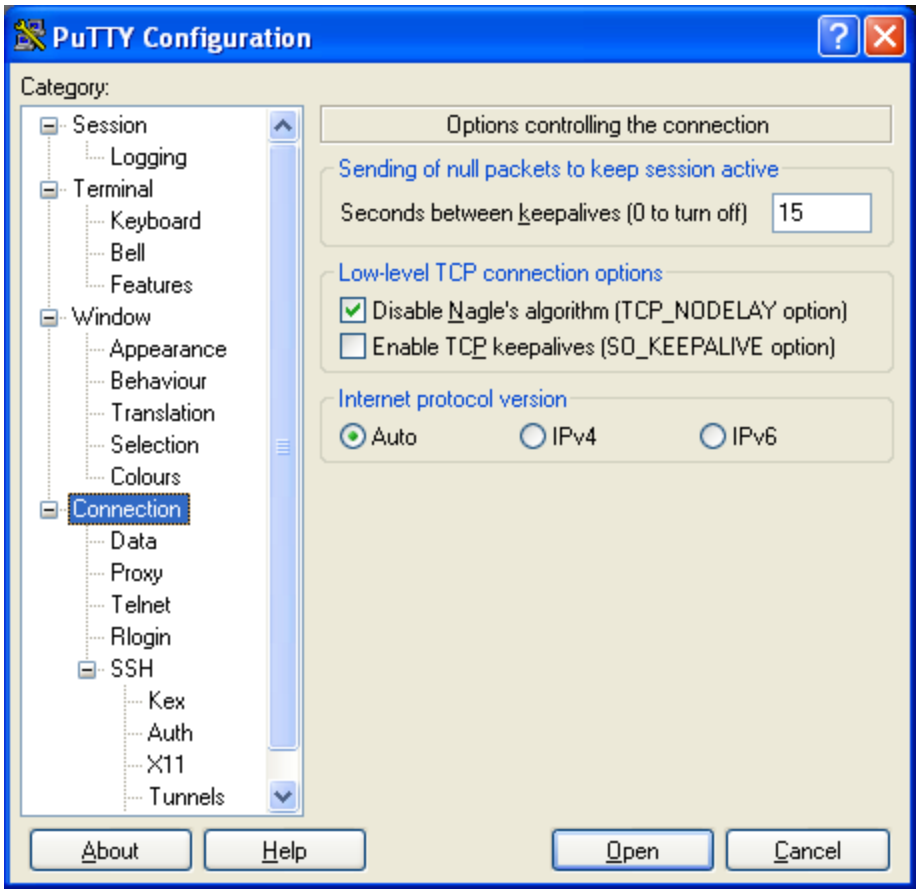


Remote PC

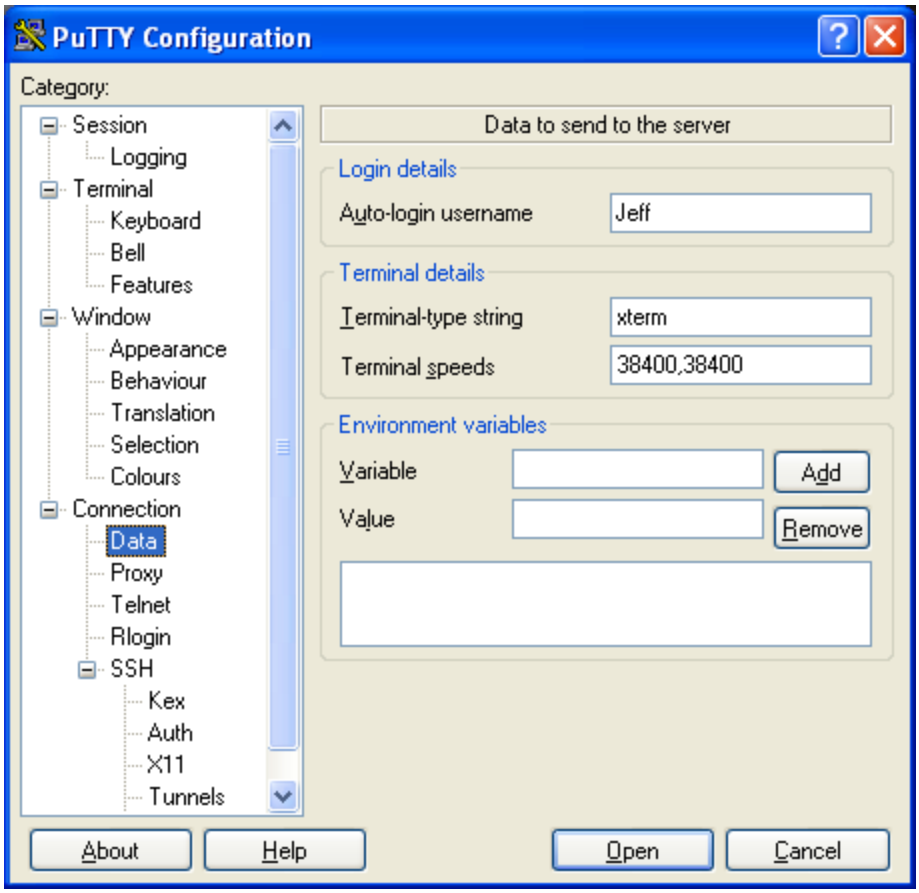
PuTTY Setup

As a prerequisite to configuring PuTTY to connect to the PC you wish to control from a remote location, OpenSSH needs to be configured as described in the Secure Shell Setup section above.

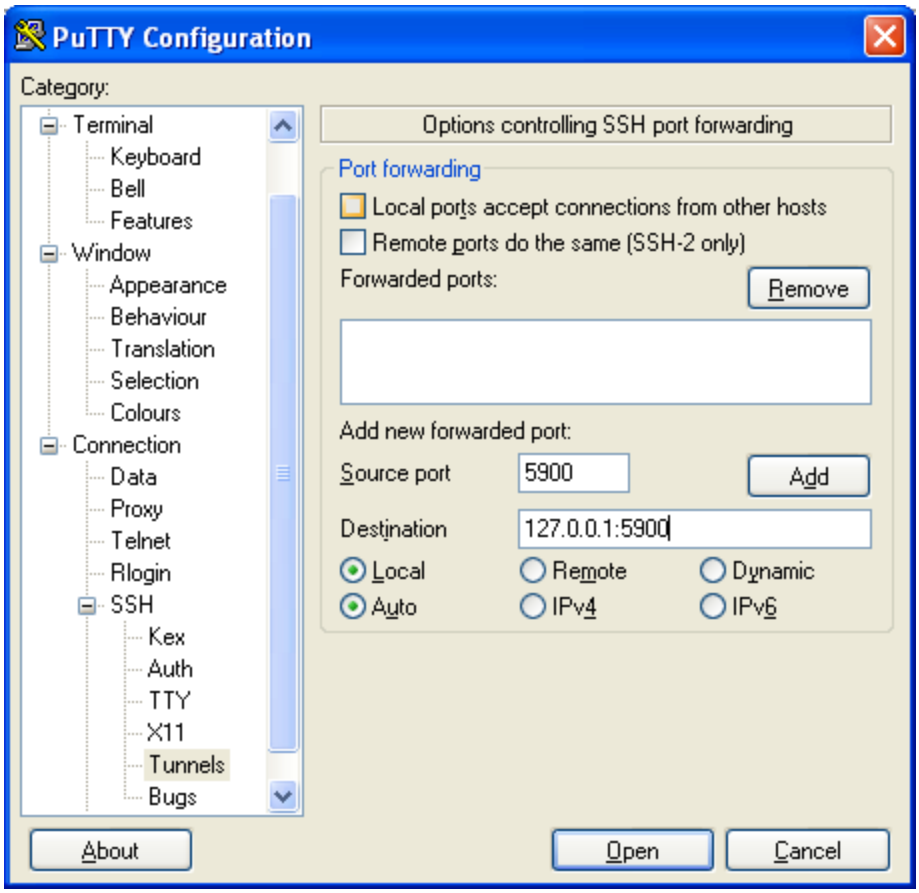
Download PuTTY on the remote PC. I use a portable version from http://socialistsushi.com/portaputty unzipped on a portable flash drive so I always have it handy, but you can download the standalone executable from http://www.chiark.greenend.org.uk/%7Esgtatham/putty/download.html. I use mostly default settings with a few exceptions. I've found that I get a more reliable connection during file transfers by setting the *Seconds between keepalives* to **15** seconds.



I also set up PuTTY to *Auto-login* as myself.



Set up the SSH tunnel by setting the *Source port* to the UltraVNC server's listening port (**5900** is default) and a *Destination* of **127.0.0.1:5900** and select *Add*.

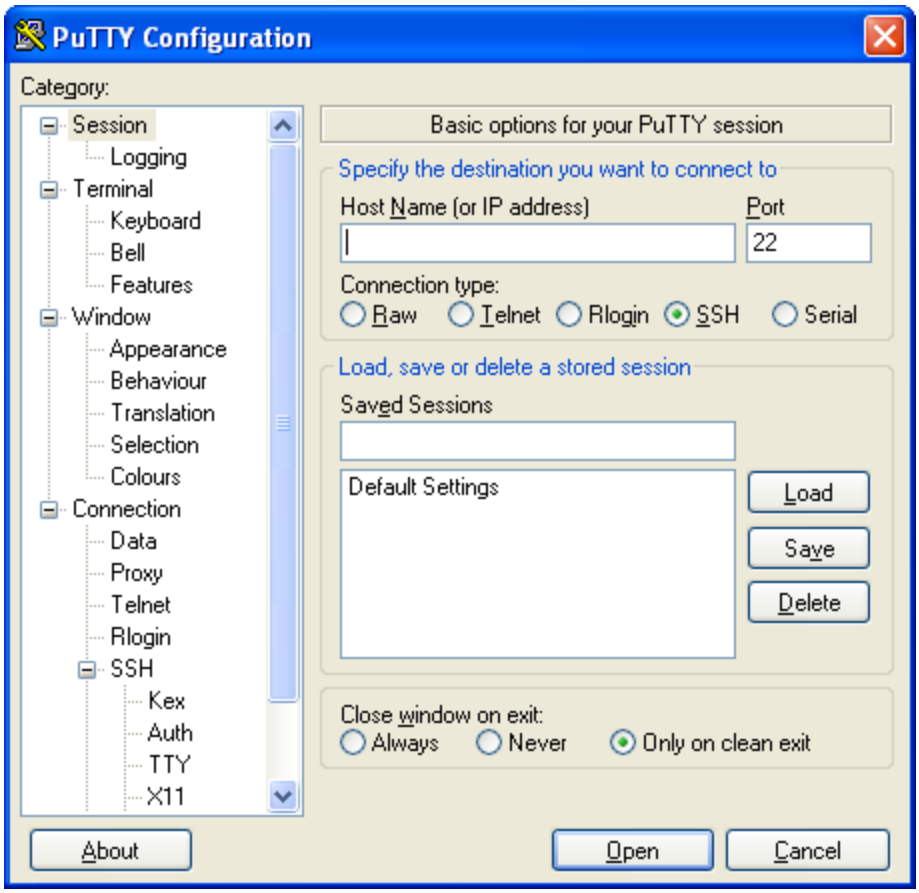


After selecting *Add* an item will be added to the *Forwarded ports* section as **L5900 127.0.0.1:5900**.

In addition, **127.0.0.1** may be replaced by **localhost**, the PC's private IP address, the PC's name or the name/IP address of any other PC on your home network. I have three PCs on my LAN that have UltraVNC installed, each listening on a different port, and use the single OpenSSH server. I then set up tunnels for each PC.

Define the remote PC's *Host Name (or IP address)*, change the *Port* number if the default port 22 was not used in the *OpenSSH\etc\sshd_config* file, give the *Saved Sessions* a name and *Save* it for future use in the Session dialog shown in the following screenshot.

Note: if the PC you wish to access does not have a static IP address assigned by your internet service provider (which is typically the case for a home PC) you may want to sign up for a free DynDNS account so you can connect to your home network using a host name that will automatically track your dynamic public IP address.



Refer to http://the.earth.li/~sgtatham/putty/0.59/htmldoc/Chapter4.html#config for a full explanation of the PuTTY configuration.

Once PuTTY has been configured to match your OpenSSH setup, select *Open* from the preceding dialog. The first time you try to connect you will receive the following warning.

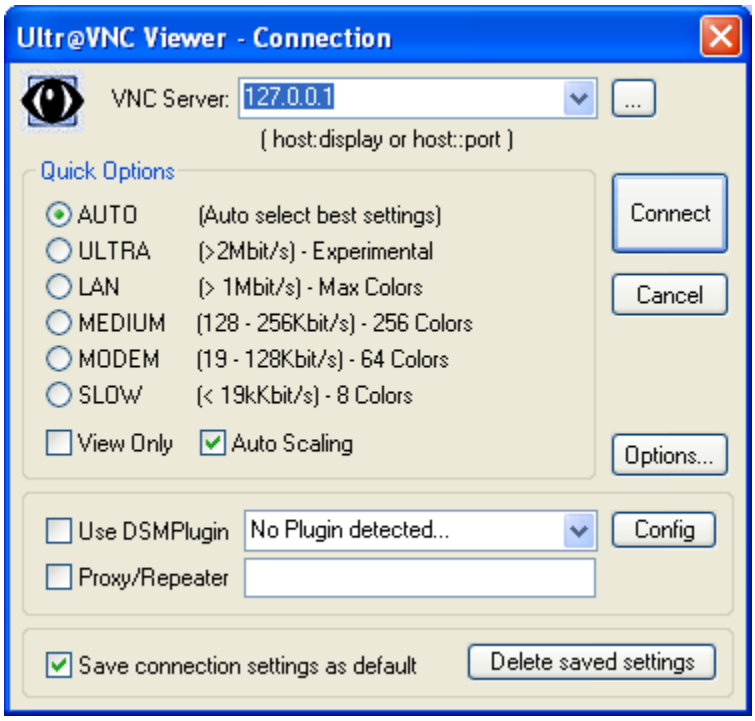
To add it to PuTTY's cache select *Yes*. If connection is successful, you will be prompted for your Windows password as shown below. After successfully entering the password you'll move to the user's home directory (\Documents and Settings\User).

UltraVNC Viewer Setup

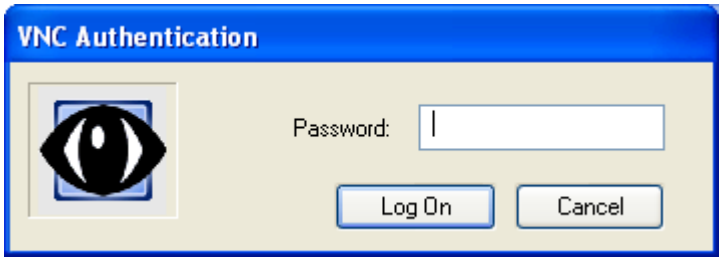
As a prerequisite to configuring the UltraVNC Viewer to connect to the PC you wish to control from a remote location, the UltraVNC Server needs to be configured as described in the UltraVNC Setup section above.

Download the UltraVNC Viewer from http://sourceforge.net/project/showfiles.php?group_id=63887 on the remote PC. I have the viewer installed on a portable flash drive so I always have it handy. It is also possible to copy the **vncviewer.exe**, **UnZip32.dll** and **Zip32.dll** files from the UltraVNC server PC if these were installed above. The DLL-files are required only for the file transfer capability.

There is no installation required to run the viewer so simply run the **vncviewer.exe** executable and connect to the local host VNC Server as shown in the following.



After selecting *Connect*, you will be prompted for the VNC password assigned in the administrative properties section above (not the windows user password).



After entering the correct password, you will see the standard UltraVNC view of the remote desktop. When you finish your session, ensure that you properly close the UltraVNC connection using the *Close Connection* button and type exit in the PuTTY window to close out the OpenSSH session (don't simply close the windows).