SSH and TigerVNC into GFDL

Note:
These instructions are for connecting to your own workstation if it is running RHEL7, and to the RHEL7 public servers (public3 & public4.)

Follow the RealVNC instructions instead if your own workstation is running RHEL6, or you wish to connect to the RHEL6 public servers (public1 (AKA "public") & public2.) The RealVNC instructions can be found under the link at the bottom of this page.

TigerVNC was chosen for RHEL7 because RealVNC is incompatible with GNOME on RHEL7.

QuickStart

For experienced SSH users, the steps are:

- If you have a CAC and are using Tectia SSH client, follow the instructions you received for it, and add port forwardings for:
    - 5905 -> <your workstation>:<VNC port number>
    - 5908 -> public3:<VNC port number>
    - 5909 -> public4:<VNC port number>
- If you only have an RSA token or have a Mac, use a standard SSH client (like PuTTY) to connect to First.Last@ssh.gfdl.noaa.gov . Your passcode requires your “PIN” and RSA fob number. **Add the port forwardings listed in the above sub-bullets.**
- Once logged in, run the command VNC and follow the menu
- Remember that you must use TigerVNC client, not RealVNC client.
    - Some 3rd-party VNC viewers will also work. RHEL7's "KRDC" works. RHEL7's "Vinagre" "Remote Desktop Viewer" does not.

SSH Configuration

Which SSH method to use?

There are two methods for connecting to the GFDL SSH bastions:

- Tectia, with a DoD CAC (Common Access Card)
    - You are supposed to use this method if you have a CAC, and your home/remote machine runs either Windows or Linux.
    - To download Tectia please submit a Service Desk Tectia Client Request. Make sure to fill out the request form completely so the staff can help you accurately.
    - As part of the Service Desk request, you will receive instructions. Follow those instructions, then proceed to the Tectia (CAC) Instructions in this document for additional setup.
- PuTTY (Windows) or command-line ssh (Linux/Mac OS X), with an RSA fob
    - Follow the PuTTY (Windows w/ RSA) Instructions or OpenSSH (Linux or Mac w/ RSA) Instructions in this document.

Tectia (CAC) Instructions

1. Follow the instructions for setting up Tectia that you were provided with as part of the Service Desk request.
   - Note that we will be expanding upon the VNC port instructions from that document in this document.
2. Determine your VNC port number
   - If you are already know your VNC port number (which is the same as with RHEL6 / RealVNC), you can skip this section.
   - Connect to the GFDL SSH bastion with Tectia.
     - Windows: Launch “Tectia - SSH Terminal” from your start menu, then select “Profiles” -> “GFDL”.
     - Linux: Open up a terminal and run: *`sshg3 GFDL`*
   - From the bastion, ssh into either your own workstation (if you have one), public3 or public4. For example:
     - ssh public3
   - Run: *`echo "`id -u` + 5900" | bc`*
     - This will return a 4 to 5 digit number. This is your VNC port number.
3. Add tunnels (port forwardings) for your workstation (if you have one), public3 & public4.
   - Go back to the session configuration’s tunnels page that you defined as part of the instructions provided with the ServiceDesk request.
     - Windows: Launch “Tectia - SSH Terminal” from your start menu, then select “Profiles” -> “Edit Profiles...”
     - Linux: Run: `ssh-tectia-configuration`
     - Then on either OS: Connection Profiles -> GFDL -> Tunneling -> Local Tunnels
   - Do you have an existing tunnel on listen port 5905?
     - If you have your own workstation and listen port 5905 is pointing to it, make sure the Dest port is correctly listing your VNC port number. You have nothing further to do for listen port 5905.
     - If you have your own workstation and there is no tunnel on listen port 5905, create one. Start by clicking “Add…”
       - Type: TCP
       - Listen port: 5905
       - Destination host: Name of your workstation (three letter initials/alias)
       - Destination port: Your VNC port number.
       - Check the box “Allow local connections only”
     - If you do not have your own workstation and listen port 5905 is pointing to public1 or public2 (or just “public”), you can leave it there.
   - Click “Add...” to add a tunnel for public3 on listen port 5908:
     - Type: TCP
     - Listen port: 5908

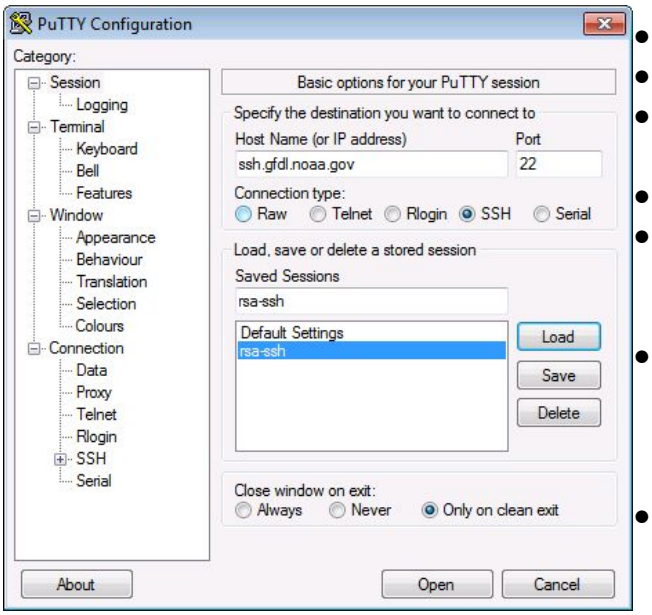
    - Destination host: public3
    - Destination port: Your VNC port number.
    - Check the box “Allow local connections only”
- Click “Add...” to add a tunnel for public4 on listen port 5909:
    - Type: TCP
    - Listen port: 5909
    - Destination host: public4
    - Destination port: Your VNC port number.
    - Check the box “Allow local connections only”
- Click “OK” to exit the Tectia configuration & save your settings.
- Once a connection has been established, continue to the TigerVNC Steps section.

4. Reminders:

- ssh-cac.gfdl.noaa.gov is only a bastion. It does not give you any tools to do work on it.
- From ssh-cac.gfdl.noaa.gov you can ssh to an internal Linux workstation or public server. You can work within your Tectia window or start VNC.

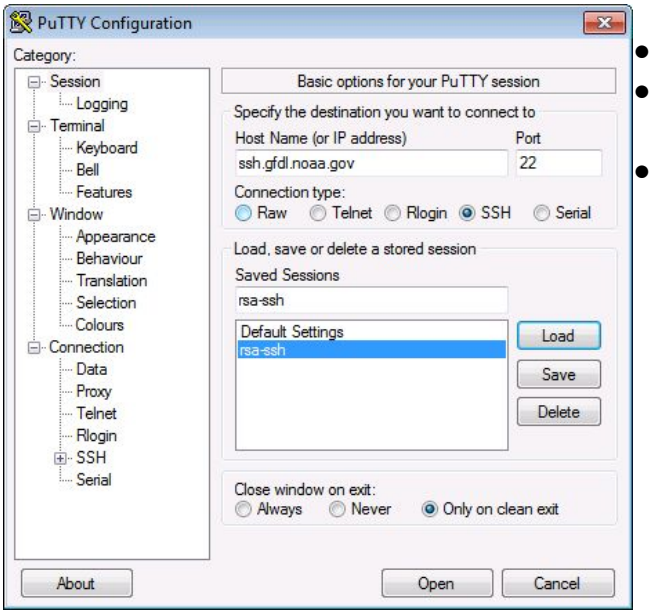
PuTTY (Windows w/ RSA) Instructions

1. Follow the instructions to configure PuTTY to connect to GFDL in the 1st place under: https://www.gfdl.noaa.gov/access/documentation/
2. Determine your VNC port number
   - If you are already know your VNC port number (which is the same as with RHEL6 / RealVNC), you can skip this section. Otherwise, follow this section to determine it.



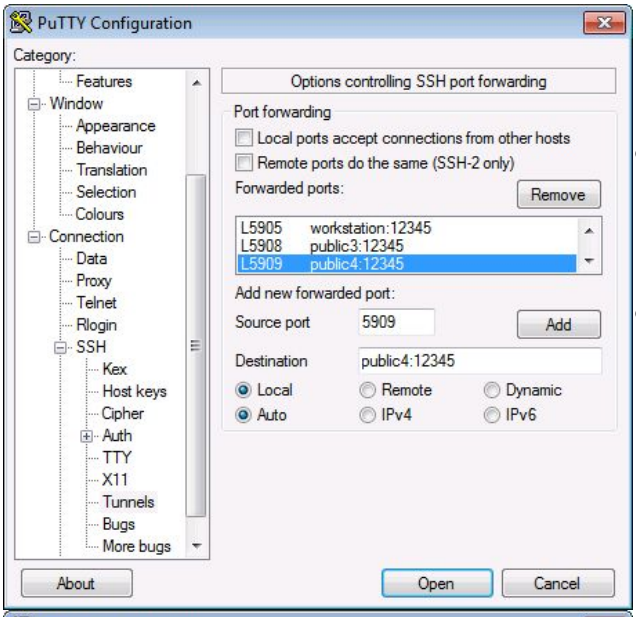
- Start *PuTTY*
- You can find *PuTTY* under “Start”, “All Programs”
- Click “rsa-ssh” under ”Saved Sessions”. You created this in the PuTTY Instructions document.
- **Click the “Load” button.**
- Click “Open". This will open an *ssh* session to “ssh.gfdl.noaa.gov”, GFDL’s *ssh* bastion for RSA tokens. (This is the same as “ssh-rsa.gfdl.noaa.gov”.)
- ssh into either your own workstation (if you have one), public3 or public4. For example:
  - `ssh public3`
  - Enter your GFDL (Active Directory) password.
- Run: `echo "`id -u` + 5900" | bc`
  - This will return a 4 to 5 digit number. This is your VNC port number.

3. Add tunnels (port forwardings) for your workstation (if you have one), public3 & public4.

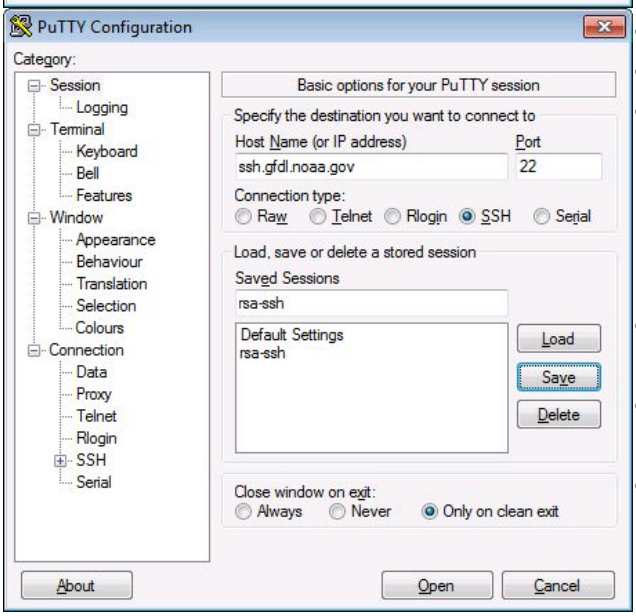


- Re-Open PuTTY
- Click “rsa-ssh” under ”Saved Sessions”. You created this in the PuTTY Instructions document.
- Click the “Load” button.

- Go to the Tunnels Category as shown below.
- Note that you may already have tunnels that append ".gfdl.noaa.gov" to the machine name. These are equivalent to just specifying the machine name.
- Do you have an existing tunnel on listen port 5905?
    - If you have your own workstation and L5905 (Source Port 5905) is pointing to it, make sure the Destination port (on the right) is correctly listing your VNC port number. You have nothing further to do for Source port 5905.
    - If you have your own workstation and there is no L5905, create one.
        - Source port: 5905
        - Destination: <workstation>:<VNC port number>
            - "<workstation>" is your workstation's alias / three letter initials.
        - Click "Add"
    - If you do not have your own workstation and listen port 5905 is pointing to public1 or public2 (or just "public"), you can leave it there.



- Create a tunnel for public3 on L5908
    - Source port: 5908
    - Destination: public3:<VNC port number>
    - Click "Add"
- Create a tunnel for public4 on L5909
    - Source port: 5909
    - Destination: public4:<VNC port number>
    - Click "Add"
- The image to the left shows all 3 tunnels, assuming the workstation alias (your initials) is "workstation" and the VNC port number is "12345". Your workstation alias & VNC port number will differ.



- Return to the "Session" category.
- Make sure the "rsa-ssh" "Saved Session" is selected.
- Click the "Save" button on the right to save your changes to the "rsa-ssh" session.

4. Reminders:

- In the future click on "rsa-ssh" in the "Saved Sessions" list to open the connection.
- ssh.gfdl.noaa.gov is only a bastion. It does not give you any tools to do work on it.
- From ssh.gfdl.noaa.gov you can ssh to an internal Linux workstation or public server. You can work within your PuTTY window or start VNC.

OpenSSH (Linux or Mac w/ RSA) Instructions

1. Determine your VNC port number

- If you are already know your VNC port number (which is the same as with RHEL6 / RealVNC), you can skip this section. Otherwise, follow this section to determine it.
- ssh into the GFDL SSH bastion:
  - ssh First.Last@ssh.gfdl.noaa.gov
  - Replace “First.Last” with your username.
  - After a warning banner, you will be prompted for a PASSCODE. Enter in your “PIN” and your PASSCODE from your RSA FOB.
  - Once connected, you should see a prompt like: [First.Last@ssh ~]$
- ssh public3
  - Enter your GFDL (Active Directory) password.
- echo "`id -u` + 5900" | bc
  - This will return a 4 to 5 digit number. This is your VNC port number.

2. Edit your OpenSSH config file

With any text editor, open up ~/.ssh/config . The config should like look the following:

```
Host GFDL
  HostName                ssh.gfdl.noaa.gov
  User                    First.Last
  LocalForward            5905 <workstation>:<VNC port number>
  LocalForward            5908 public3:<VNC port number>
  LocalForward            5909 public4:<VNC port number>
  GatewayPorts            no
```

- If you already have existing configuration for the GFDL, with “Host” set to anything, and with HostName set to either “ssh.gfdl.noaa.gov” or “ssh-rsa.gfdl.noaa.gov”, you can use it instead, but you need to add the lines listed below.
- Replace “First.Last” with your own username.
- Replace “<VNC port number>” with your actual number.
- For the line with “5905 <workstation>”
  - Replace “<workstation>” with your workstation alias (your initials) if you have your own workstation.
  - Remove this line altogether if you do not have your own workstation.
  - If you have port 5905 pointing to public1 or public2 (or just “public”), you can keep that line. You must not have 2 lines with “5905” specified. (or any other local port # for that matter.)
- Note: “GatewayPorts no” is a security precaution. It makes ssh listen only on localhost.

3. Connect with OpenSSH

- Run: `ssh GFDL`
  - After a warning banner, you will be prompted for a PASSCODE. Enter in your “PIN” and your PASSCODE from your RSA FOB.

    - Once connected, you should see a prompt like: [First.Last@ssh ~]$
- From there, you can connect to your own workstation or public3/public4 with a command like:
    - ssh public3
    - Enter your GFDL (Active Directory) password.

4. Reminders:

- ssh.gfdl.noaa.gov is only a bastion. It does not give you any tools to do work on it.
- From ssh.gfdl.noaa.gov you can ssh to an internal Linux workstation or public server. You can work within your OpenSSH window or start VNC.

TigerVNC Instructions

Starting the VNC session

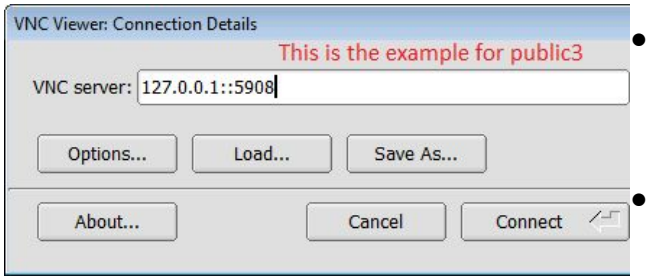
- Log into your internal GFDL linux workstation via SSH. If you do not have one, log into public3 or public4 instead.
    - Remember which of these you used.
- Enter the command “VNC” and follow the instructions.
- Leave the PuTTY, Tectia, or ssh terminal window open.
    - It does not need to be connected to your workstation afterwards, but the initial connection to the SSH bastion must remain open.

Install TigerVNC Viewer on your computer

- Download & install TigerVNC Viewer from: https://bintray.com/tigervnc/stable/tigervnc/
    - For Windows:
        - It is recommended that you download & use the portable viewer (vncviewer*.exe), which does not require admin rights.
        - You can download and run the full installer (tigervnc*.exe.) However, it requires admin rights, and defaults to installing the server. Many anti-virus programs consider the server to be a PUP (potentially unwanted program) and remove it almost the same as if they were removing a virus. It is best to avoid the hassle and just use the portable viewer.
        - If your computer is 64-bit, it is recommended that you use the 64-bit version, but it is not required.
    - For Mac, download TigerVNC*.dmg
        - This does not require admin rights.
    - For Linux
        - You can download the portable precompiled i386 or x86_64 tarball
        - You can also browse to "files" and download Ubuntu or RHEL/CentOS packages.
    - **Note: It is not possible to use RealVNC viewer to connect to a TigerVNC server.**
    - Note: Some 3rd-party VNC viewers will also work. RHEL7's "KRDC" works. RHEL7's "Vinagre" "Remote Desktop Viewer" does not.

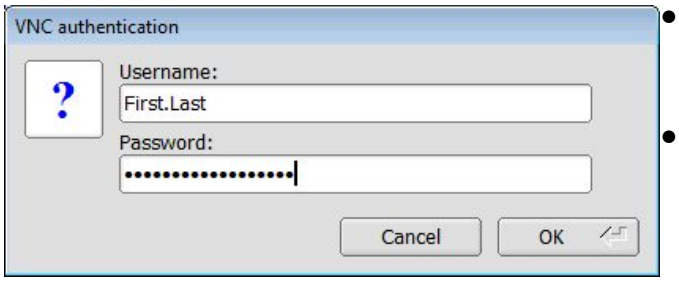
Connect with TigerVNC Viewer

- Launch TigerVNC Viewer.
    - On Windows: Start Menu → All Programs → TigerVNC (64-bit) → TigerVNC Viewer.
    - On Linux: Either search your applications for “TigerVNC Viewer”, or find it at the start menu path:Applications → Internet → TigerVNC Viewer.
    - On Mac: Find the “TigerVNC Viewer” application either in the applications folder or by using Finder or QuickSilver.



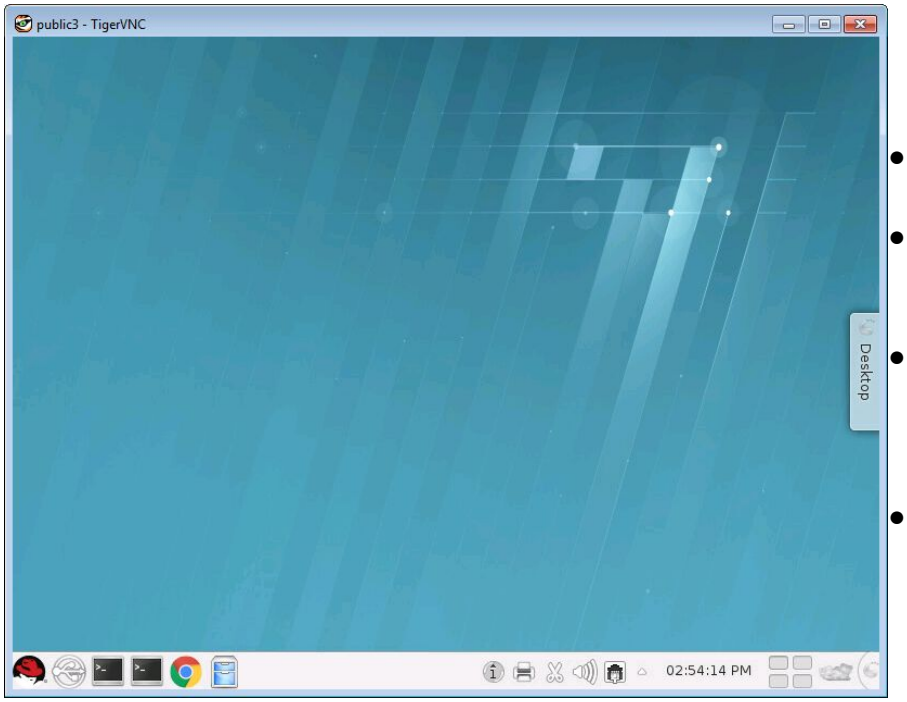
- Enter one of the following:
  - To connect to your own workstation: 127.0.0.1::5905
  - To connect to public3: 127.0.0.1::5908
  - To connect to public4: 127.0.0.1::5909
- Note: If you are on a computer within the GFDL or on a GFDL laptop using VPN, you would connect to: <machinename>:<VNC Port Number>

- Note: There is no need to customize your Options. See the VNC Options section in this document if you would like more info on them.
- Click “Connect”. The “VNC Authentication” window should appear.



- Enter your username with the exact capitalization listed in the output of the “VNC” command, or with no capitalization at all.
- Enter your GFDL (Active Directory) password.
  - It is possible to lock yourself out after 3 failed logins. If so, go to https://passwords.gfdl.noaa.gov

- Your desktop should appear



TigerVNC usage Reminders:

- The Session can be resized after connecting by resizing the window.
- To go full-screen, including using multiple monitors, press F8. To leave full-screen, press F8 again.
- To disconnect from your session and resume it later, click the X in the top-right window. Your session will continue to run for 1 week.
- Note: To end your session, you should select to logout within it. This is safer than running “VNC 0” from the terminal.

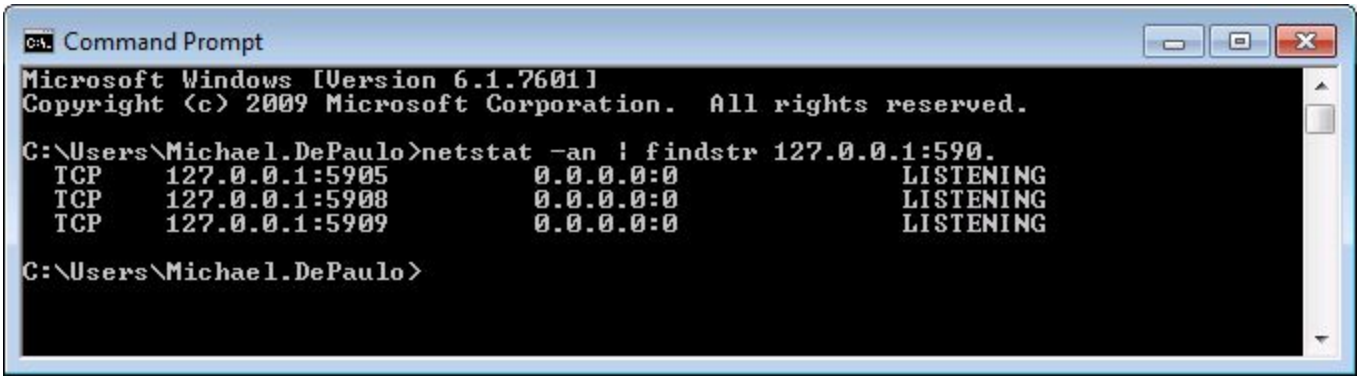
What to do if VNC doesn't work:

Verify your workstation is running RHEL7:

On your workstation, run: `cat /etc/redhat-release`
If the version is 6.x, you must use RealVNC viewer instead. Directions can be followed here.

Verify the tunnels exist (Windows):

- Make sure the PuTTY or Tectia session is running and connected to either the SSH bastion, or your workstation / public server after that.
- Launch "Command Prompt" via: Start Menu -> All Programs -> Accessories -> Command Prompt
- Run: `netstat -an | findstr 127.0.0.1:590.`
    - The period at the end is part of the command.



- The row with "127.0.0.1:5905" should exist if you have your own workstation. The other 2 rows should always exist.
- Any additional lines are OK.

Verify the tunnels exist (Linux):

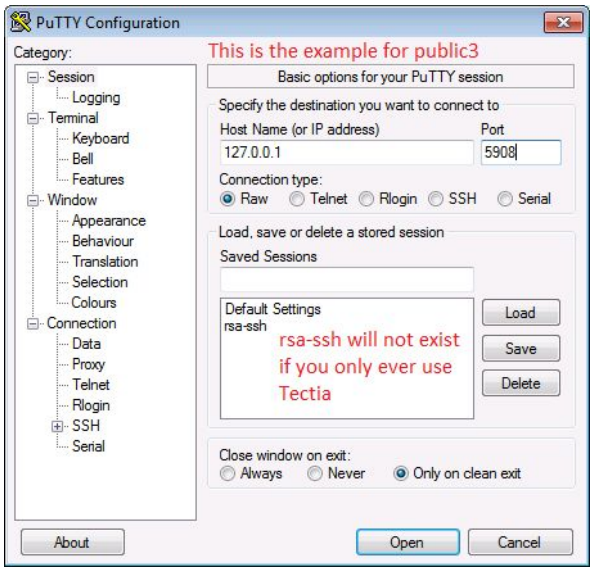
- Make sure the ssh terminal window or Tectia session is running and connected to either the SSH bastion, or your workstation / public server after that.
- Open up a terminal window and run: `netstat -lntp | grep 127.0.0.1:590.`
    - The period at the end is part of the command.
- The output should look like:

```
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 127.0.0.1:5905          0.0.0.0:*               LISTEN      15087/ssh
tcp        0      0 127.0.0.1:5908          0.0.0.0:*               LISTEN      15087/ssh
tcp        0      0 127.0.0.1:5909          0.0.0.0:*               LISTEN      15087/ssh
```

    - The 1st 2 lines of output may or may not exist.
    - The row with "127.0.0.1:5905" should exist if you have your own workstation. The other 2 rows should always exist.
    - The number at the end (15087 in this example, but it is random) should exist. If it doesn't, it means that some other user account is using that port.
    - The "ssh" at the end will be different if Tectia (or a different ssh client altogether) is in use.

Verify the tunnel is working (Windows):

- If you connected with PuTTY, leave the existing PuTTY session open, and open up PuTTY again, but do not connect yet.
- If you connected with Tectia:
    - Make sure the Tectia session is running and connected, and then connect to the workstation / public server after that.
    - Check if PuTTY is installed. If not, download & install it. Then open it.



- Connection Type: Raw
- Host Name (or IP address): 127.0.0.1
- Port:
    - For your own workstation: 5905
    - For public3: 5908
    - For public4: 5909
- Click “Open”

- You should see the output in this screenshot (but with a larger window by default):

    - (If you see “RFB 004.001”, that means you are connected to a RHEL6 RealVNC machine instead of a RHEL7 TigerVNC machine.
- Click the X.

Verify the tunnel is working (Linux):

- Make sure the ssh terminal window or Tectia session is running and connected to either the SSH bastion, or your workstation / public server after that.
- Run one of the following commands, depending on which machine you are using:
    - Your own workstation: `telnet 127.0.0.1 -p 5905`
    - public3: `telnet 127.0.0.1 -p 5908`
    - public4: `telnet 127.0.0.1 -p 5909`
- You should then see the following output:

```
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
RFB 003.008
```

    - (If you see “RFB 004.001”, that means you are connected to a RHEL6 RealVNC machine instead of a RHEL7 TigerVNC machine.
- You can then either click the X on your terminal window, or gracefully exit the telnet command by typing the following, hitting the Enter key after each step.
    - Ctrl +]
    - quit

If you need help:

Contact the helpdesk at https://helpdesk.gfdl.noaa.gov or oar.gfdl.help@noaa.gov

Frequently Asked Questions

Why I am I creating 2 or 3 tunnels when I only use 1 machine at a time?

You are creating them as a precaution, in case of downtime with your workstation or any 1 public server.

What machines may I connect to with TigerVNC? What tunnels (port forwardings) should exist?

It is a good idea to create all of the TigerVNC tunnels listed below. This ensures that you can connect to more than just 1 machine in case of downtime.

Any additional tunnels you may have been instructed to add can coexist safely. 2 tunnels cannot share the same Local Port (AKA “Source Port”) though.

The entire set of tunnels that the GFDL normally instructions you to create are as follows. **(Only the ones in bold are needed for TigerVNC though.)**

Target	**Local Port**	**Remote Port**	**Application**
Workstation alias	2905	22	SSH/SFTP (RHEL6 & RHEL7) and X2Go (RHEL7)
public1	2906	22	SSH/SFTP
public2	2907	22	SSH/SFTP
public3	2908	22	SSH/SFTP and X2Go
public4	2909	22	SSH/SFTP and X2Go
mayflower	3128	3128	Web Proxy
Workstation alias	**5905**	**VNC Port #**	**TigerVNC (RHEL7)** or RealVNC (RHEL6)
public1	5906	VNC Port #	RealVNC
public2	5907	VNC Port #	RealVNC
public3	**5908**	**VNC Port #**	**TigerVNC**
public4	**5909**	**VNC Port #**	**TigerVNC**

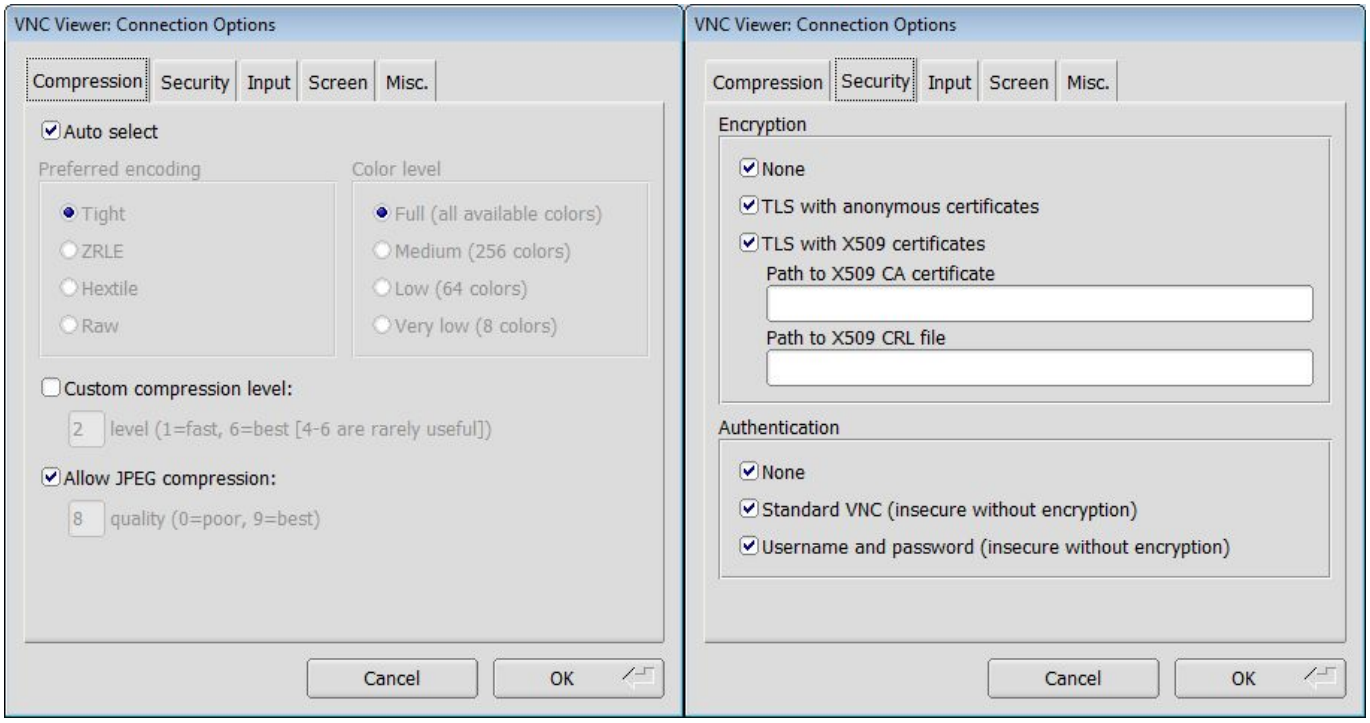
How do I get out of fullscreen mode?

Press F8 on the keyboard to access the menu.

Appendix A: Default TigerVNC Viewer Options

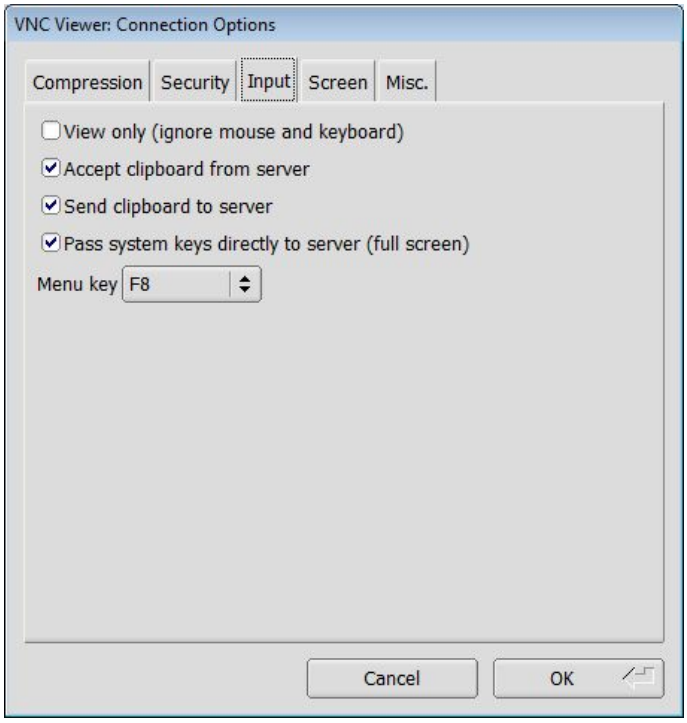
All of the default options in TigerVNC Viewer work successfully. Here is what they look like, in case you have changed them and wish to restore them back. These screenshots are from 1.8.0.

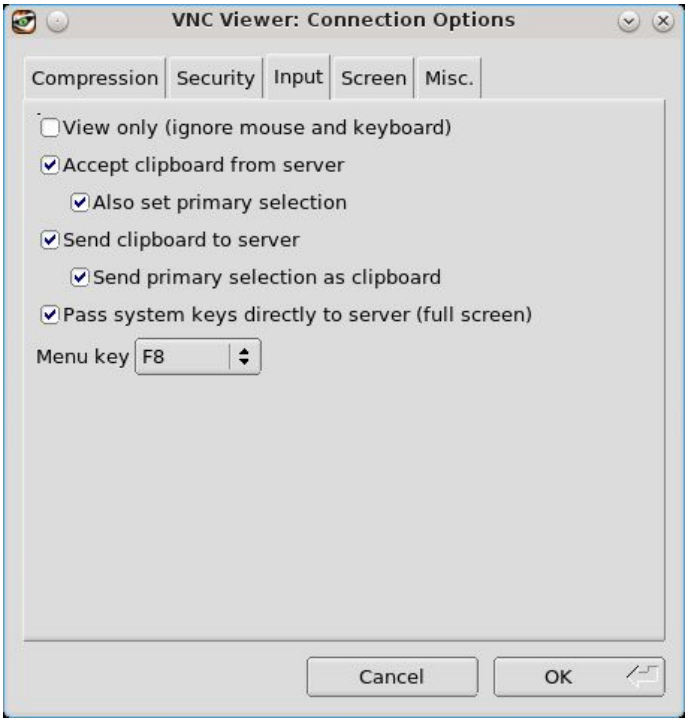
Compression & Security



Input

Only the Input tab differs between Windows & Linux.
Windows is on the left. Linux is on the right.





Screen & Misc