Remote Access via CAC

From GFDL

There are several ways to access GFDL remotely. With our move to CAC, some of standard connection methods will be slightly different when compared to RSA. If you have any questions on the documentation or CAC in general, please open a help desk ticket or contact Operations.

Tectia Windows Quick Guide Installation

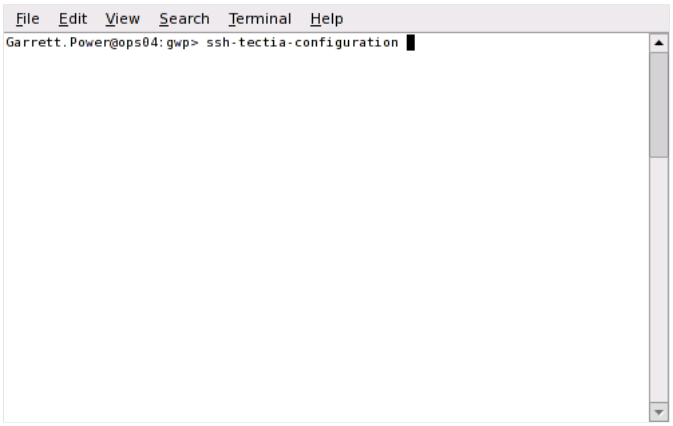
Contents

Linux

Tectia Linux Client Configuration (Goverment)

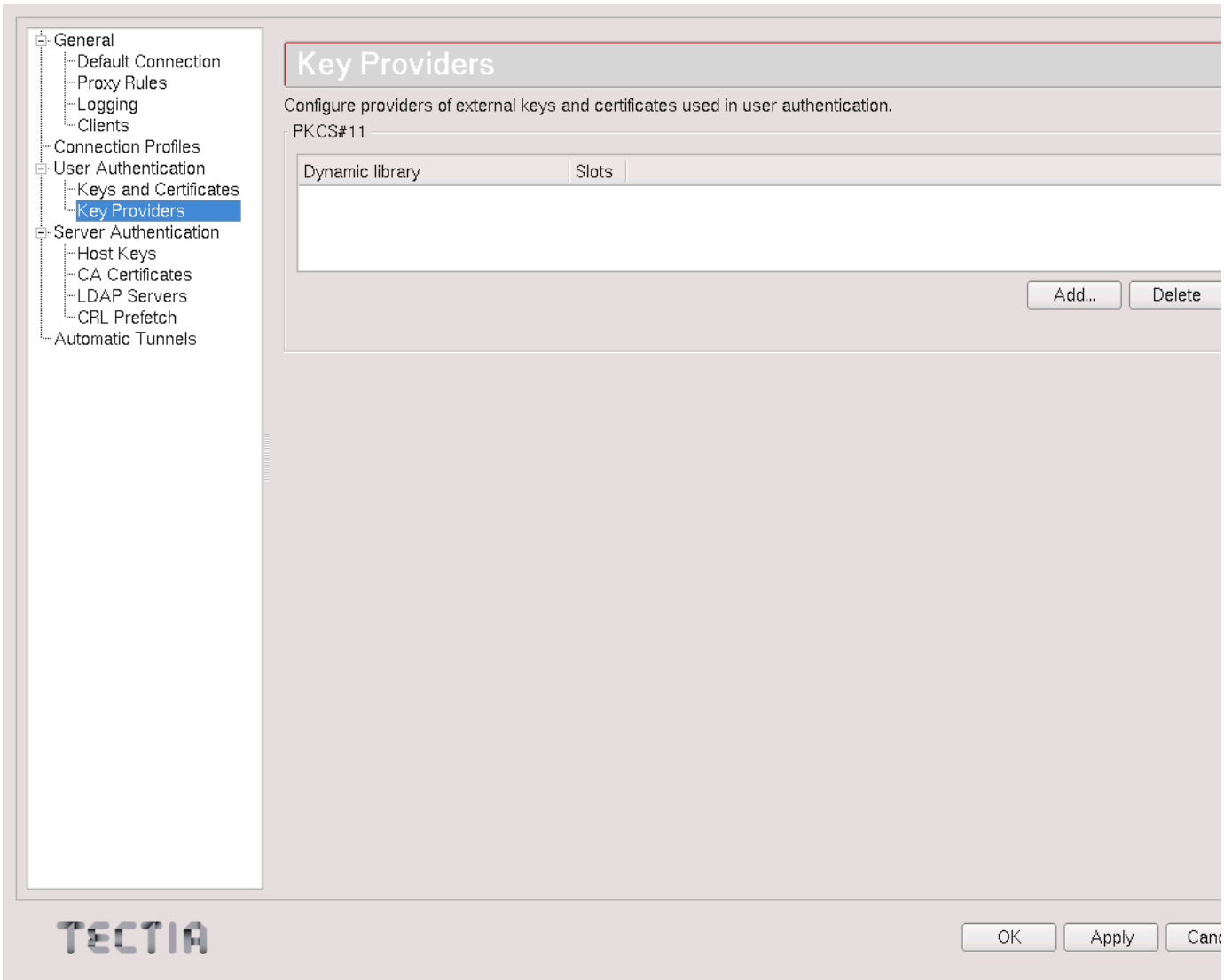
Tectia Configuration Tool

From a terminal window run the following command: ***ssh-tectia-configuration***



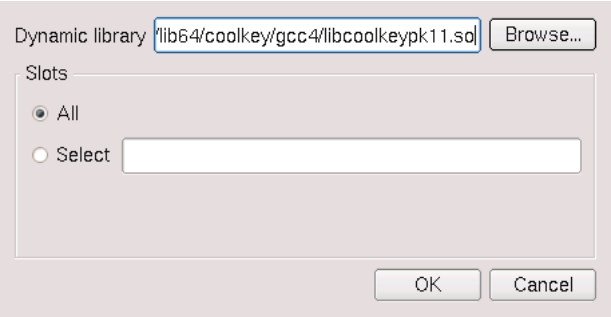
Configure Smart Card Reader

1. Click on ***Key Providers***

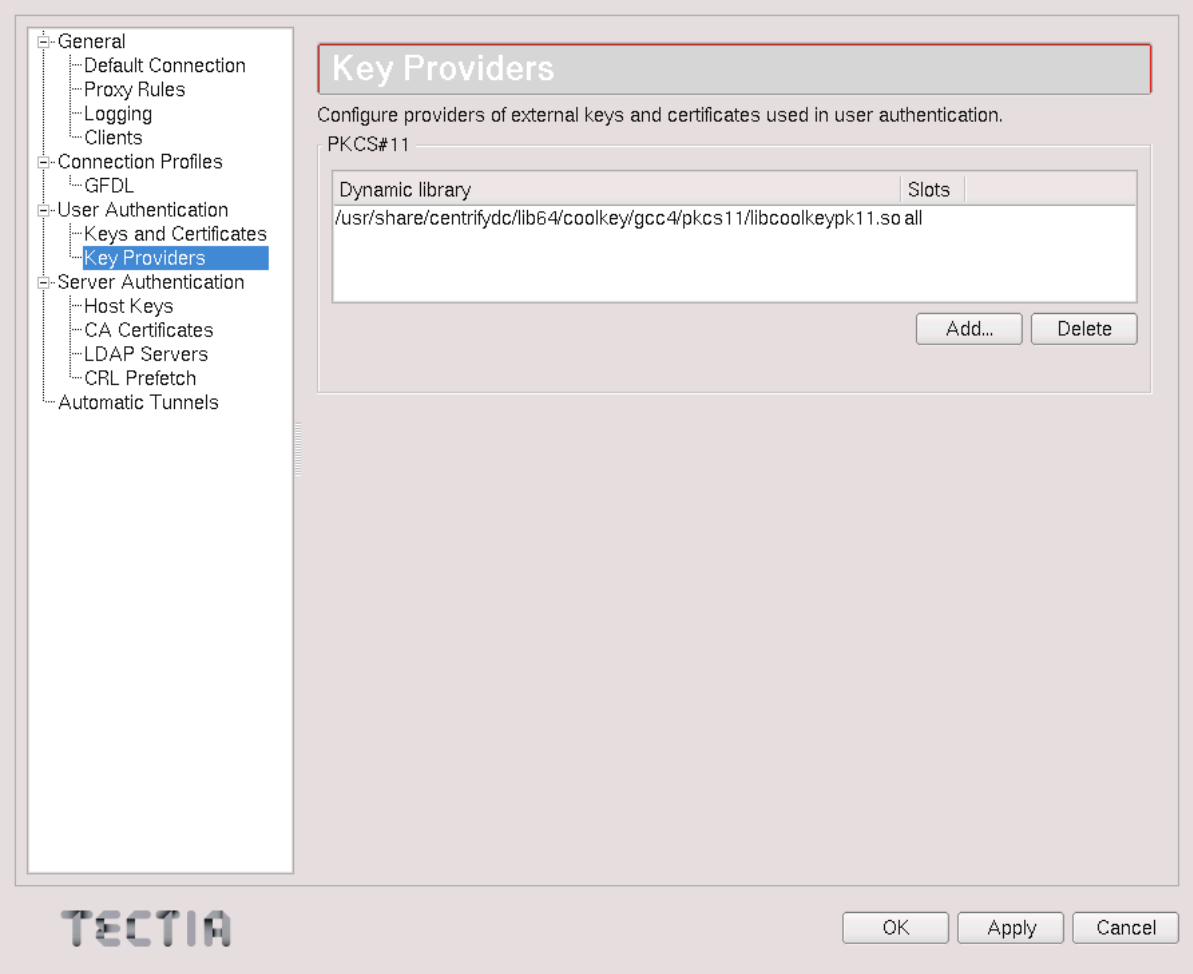


2. Click on ***Add*** and enter the following under ***Dynamic Library*** field:

   /usr/share/centrifydc/lib64/coolkey/gcc4/libcoolkeypk11.so

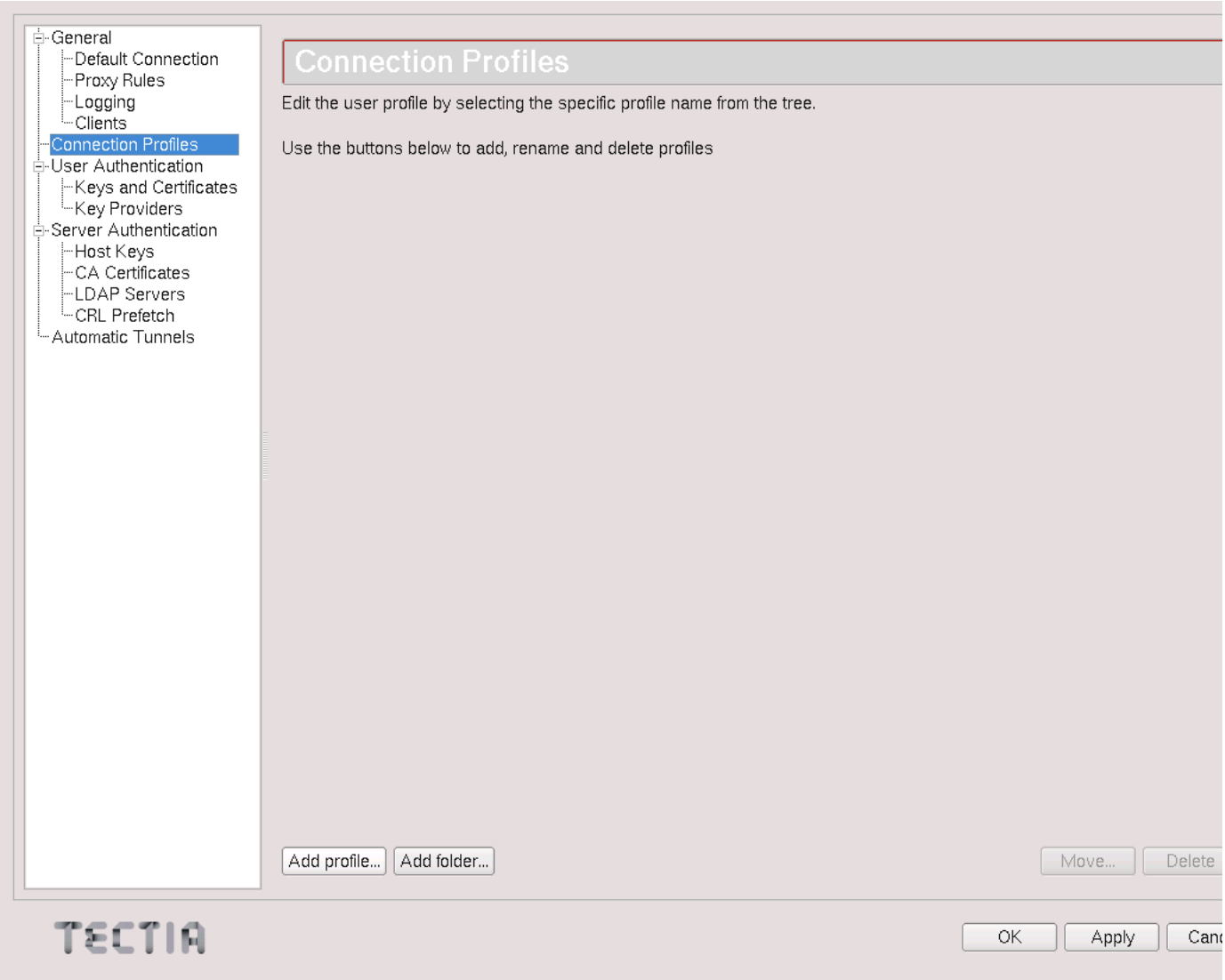


3. Click ***Apply***

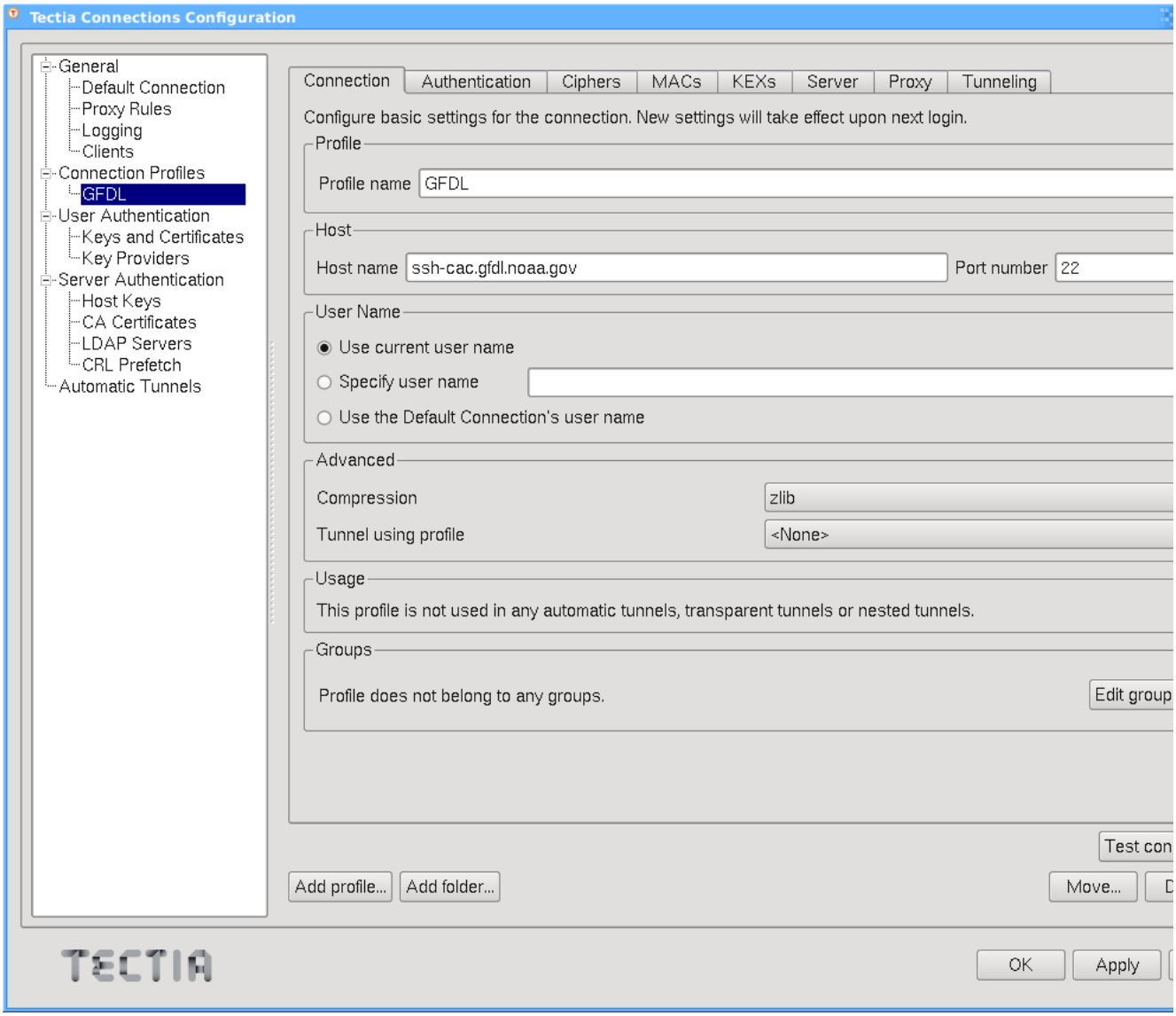


Create SSH Profile

1. Click on ***Connection Profiles***



2. Click on ***Add Profile***
3. Set the following settings on the **Connection** tab:
    1. Profile -> **Profile name: GFDL**
    2. Host -> **Host name: ssh-cac.gfdl.noaa.gov**
    3. Host -> **Port number: 22** (leave the default)
    4. Advanced -> **Compression: zlib**

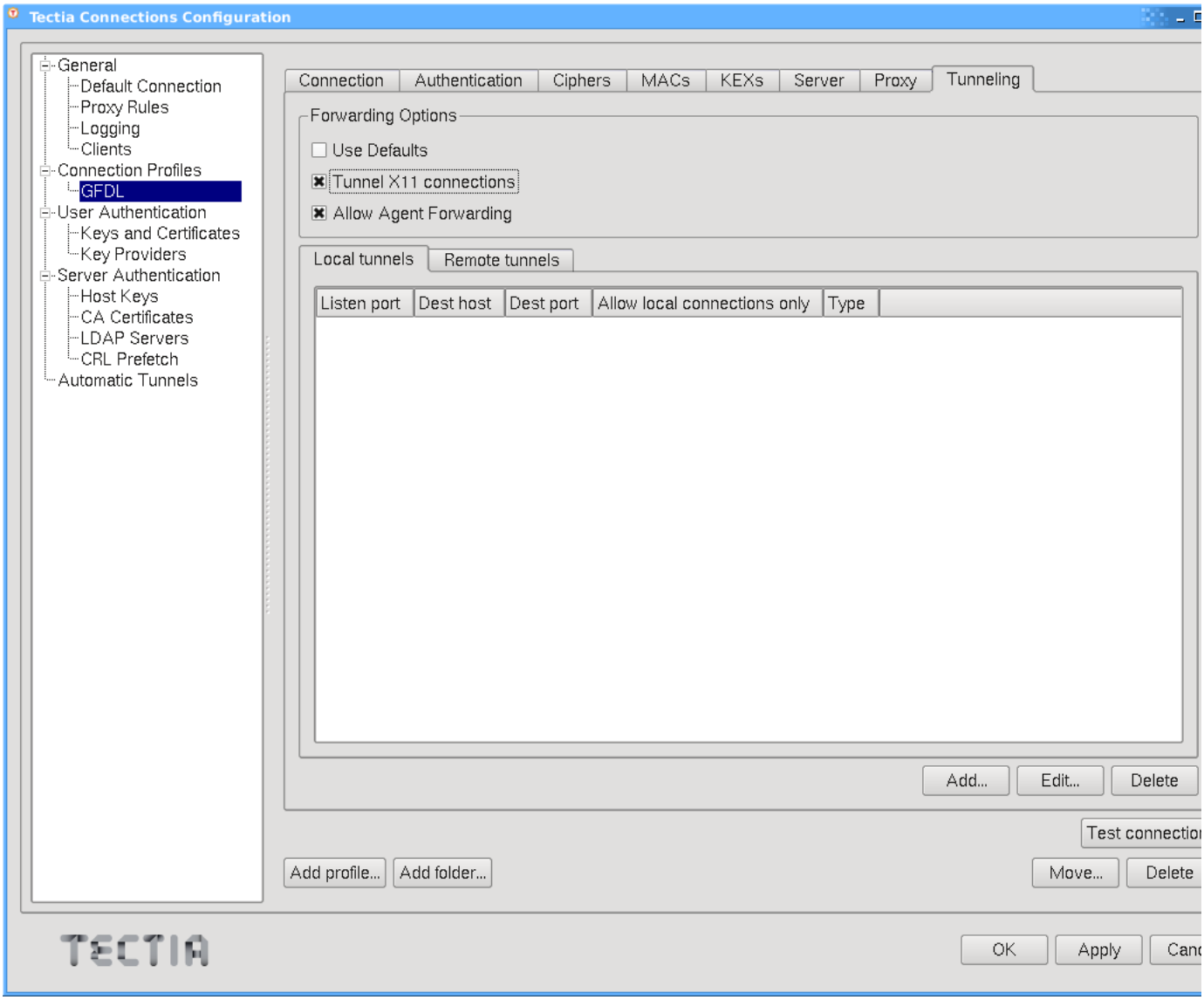


4. Click **Apply**

X11 Forwarding

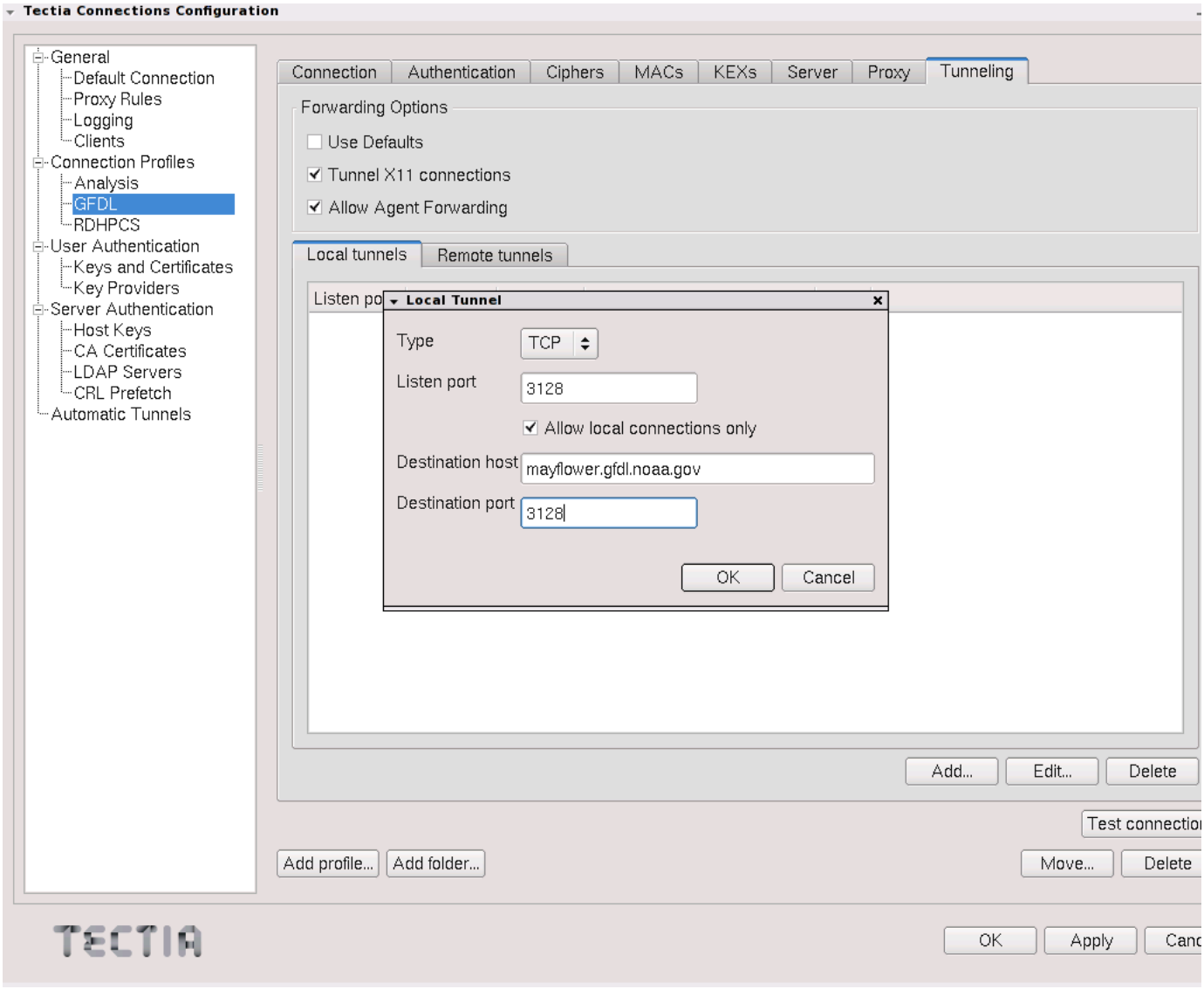
Set the following settings on the **Tunneling** tab:

1. Forwarding Options -> **Use Defaults: Deselect**
2. Forwarding Options -> **Tunnel X11 connections: Select**
3. Forwarding Options -> **Allow Agent Forwarding: Leave Selected**



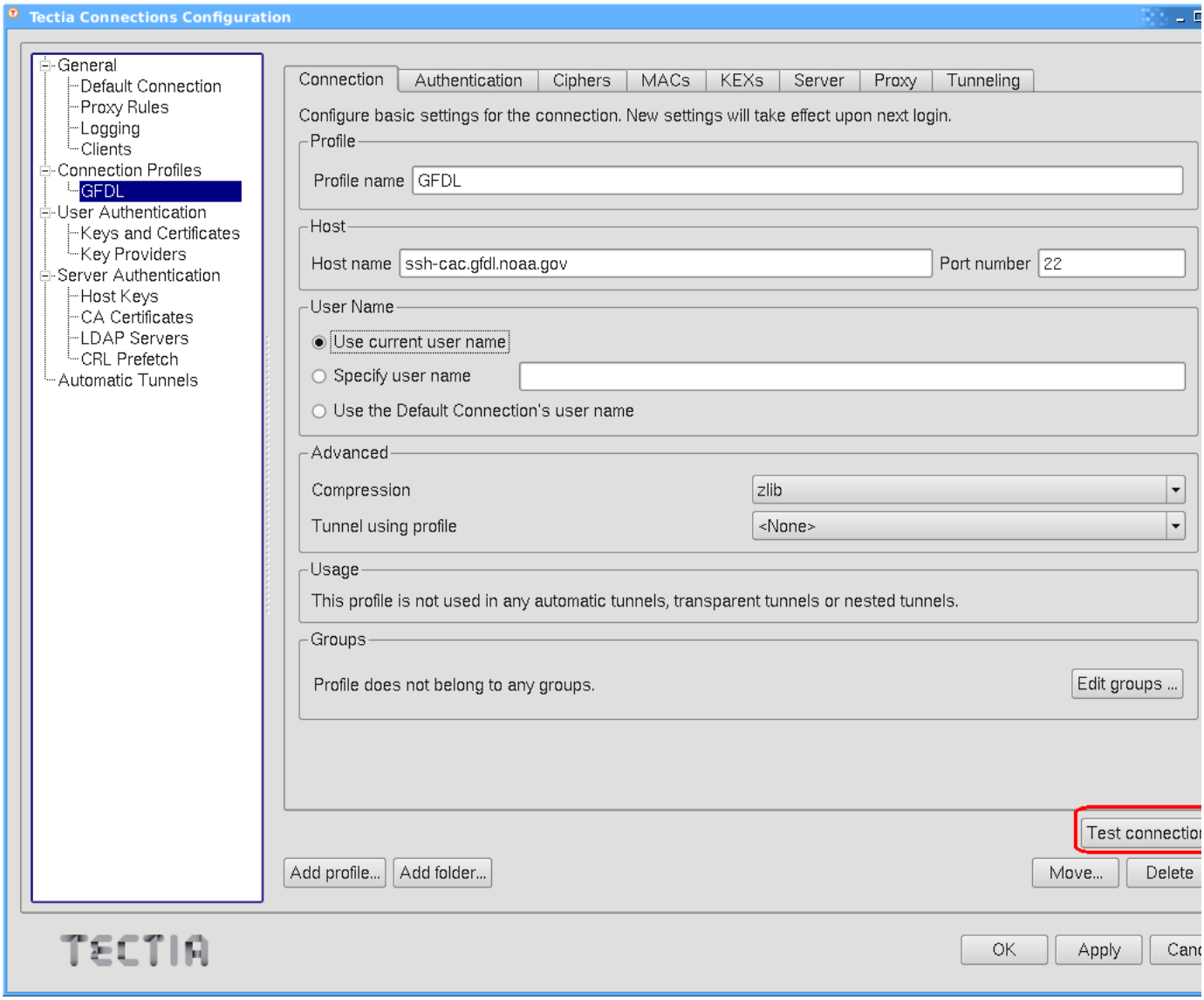
GFDL Proxy (Mayflower) Tunnel

1. Click on the **Tunneling** tab.
2. Click on **Add**
    1. Enter **3128** port in **Listen port** field.
    2. Enter **mayflower.gfdl.noaa.gov** in **Destination host** field.
    3. Enter **3128** port in **Destination port** field.
    4. Click on **OK**.
3. Click on **Apply**.

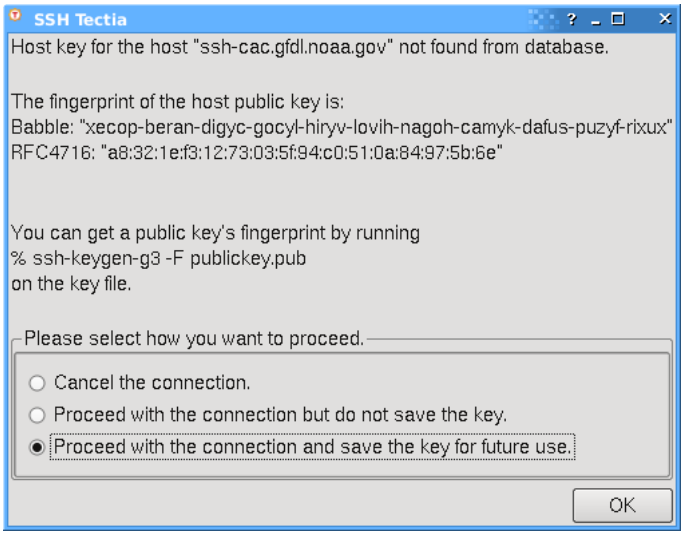


Test SSH Connection

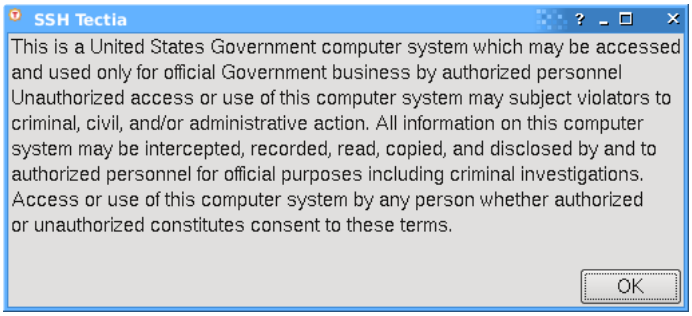
1. Switch back to the connection tab and click **Test connection**



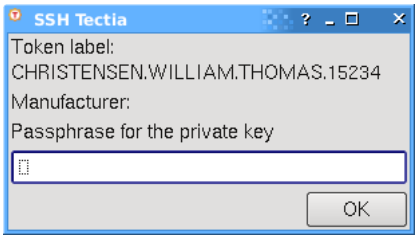
2. "**Proceed with the connection and save the key for future use.**"



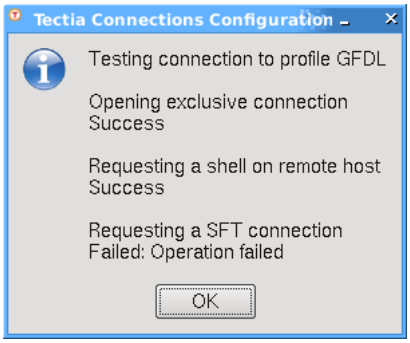
3. Accept the policy banner



4. Enter your CAC passphrase. **You may see a single rectangle for all the characters you type, or you may see asterisks.**



5. Hit OK once the connection is successfully tested



6. Exit the utility

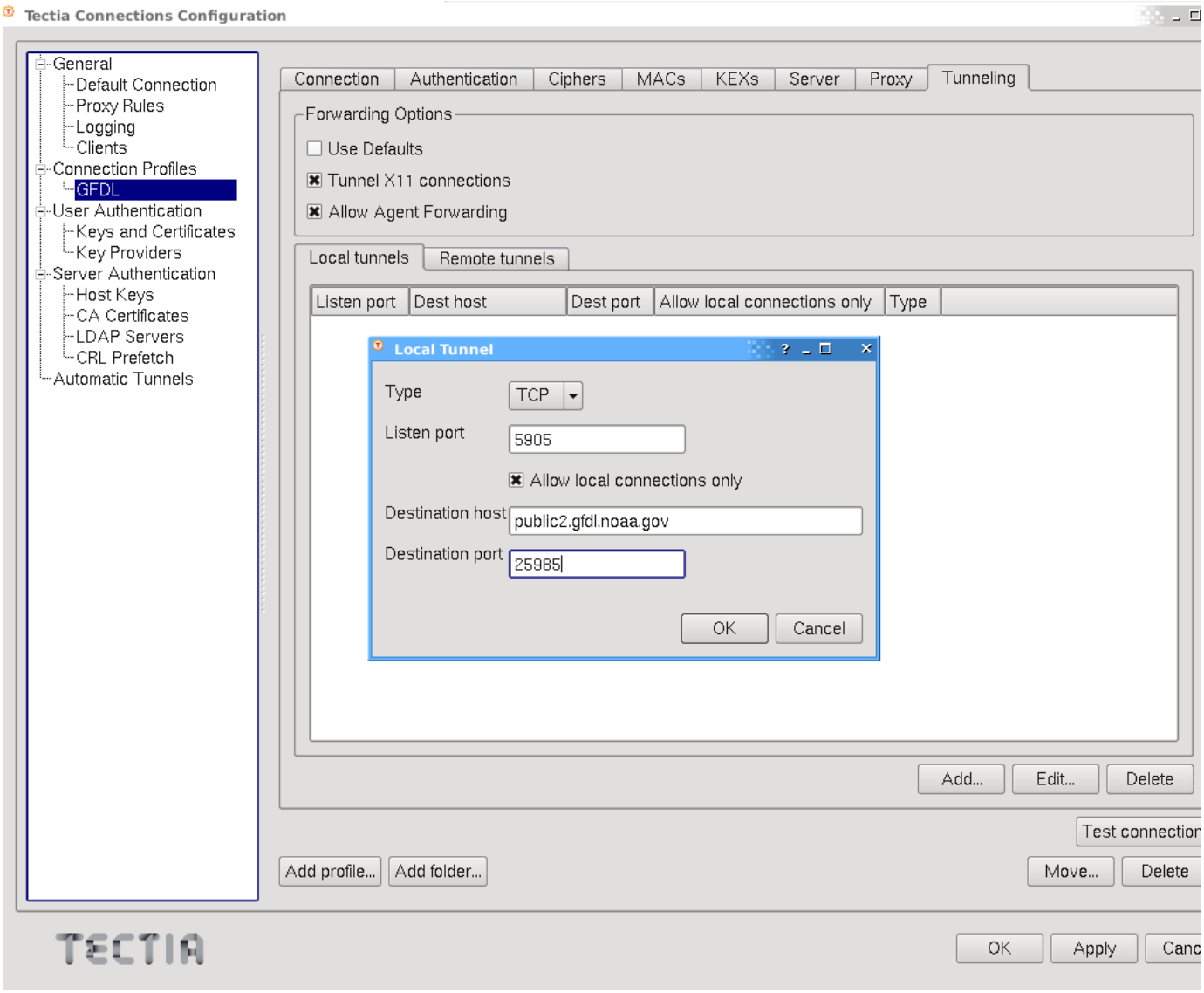
VNC Tunnel

Determine your VNC port

1. From a terminal window, connect to the SSH bastion by running the command: **sshg3 GFDL**
2. Connect to your workstation by running the commands, assuming your workstation is public2.gfdl.noaa.gov: **ssh public2.gfdl.noaa.gov**
3. Determine your port by running the command: **vncid**
4. Make note of the 4 or 5 digit number it outputted

Configure VNC Tunnel

1. Run the following command: **ssh-tectia-configuration**
2. In the left pane, switch to: **Connection Profiles -> GFDL**
3. Click on the **Tunneling** tab
4. Click on **Add**
    1. Enter **5905** in **Listen Port** field.
    2. Enter workstation where VNC is running in **Destination host** field. (e.g. public2.gfdl.noaa.gov)
    3. Enter your aforementioned VNC port in **Destination port** field. (e.g. **25985**)
    4. Click on **OK**
5. Click on **Apply**
6. Exit the utility



Tectia Linux Client Configuration (Personal)

Installation

Smart Card Reader Library

RedHat / CentOS

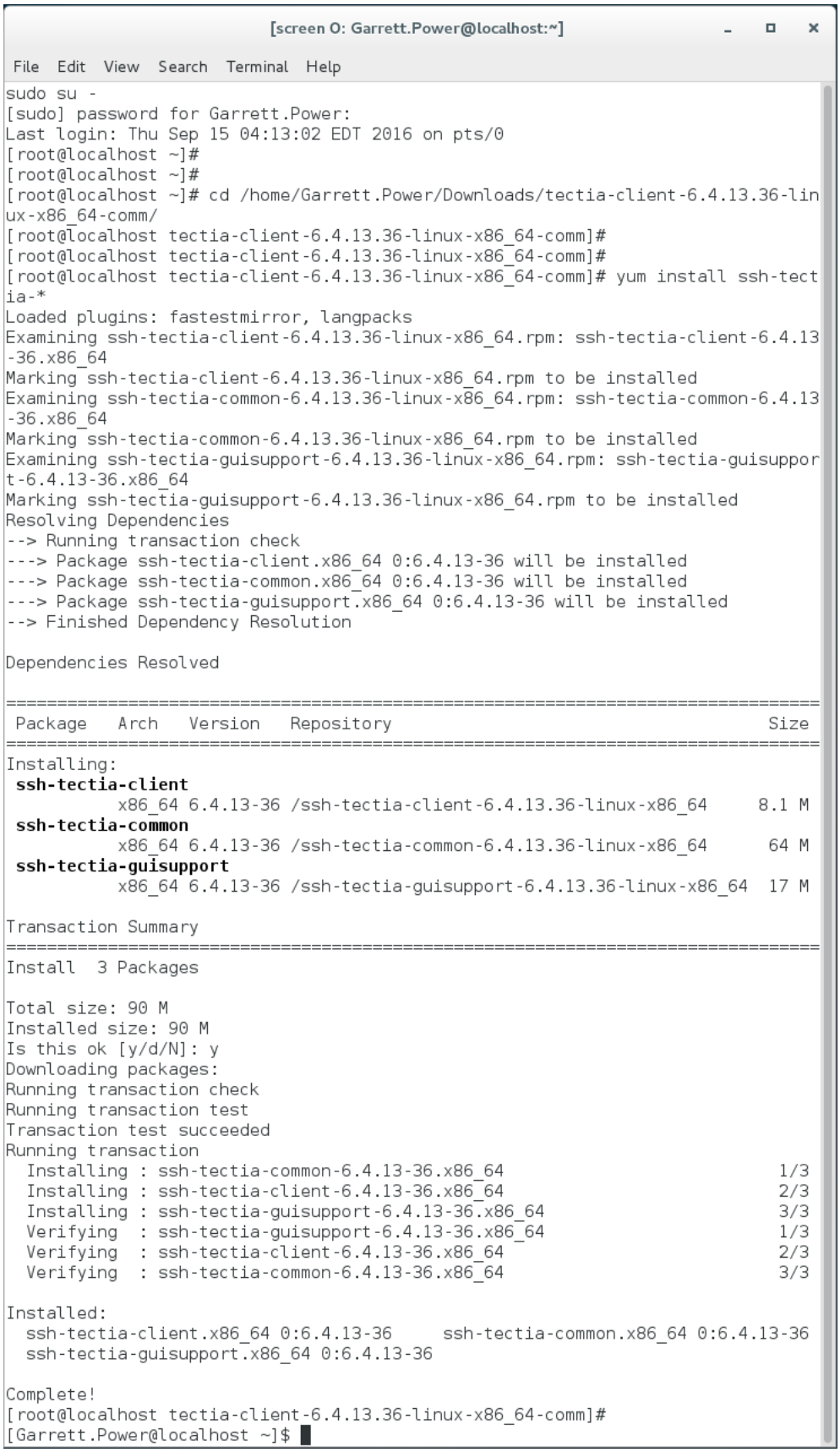
1. Open a terminal window
2. As **root**
    1. yum install coolkey

Tectia SSH Client

Install Software

1. Obtain the Tectia SSH Client
2. Extract the Tectia SSH Client zip
3. Open a terminal window
4. As **root**

1. cd /path/of/tectia_client_download
2. yum install ssh-tectia-*

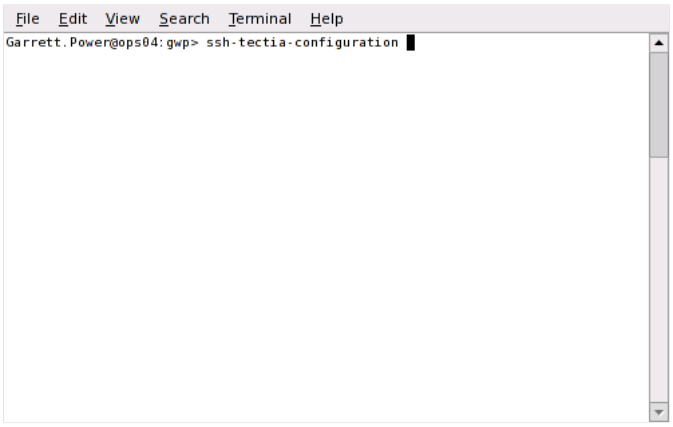


Install License

1. cd/path/to/tectia_client_download
2. cp stc64.dat/etc/ssh2/licenses/

Tectia Configuration Tool

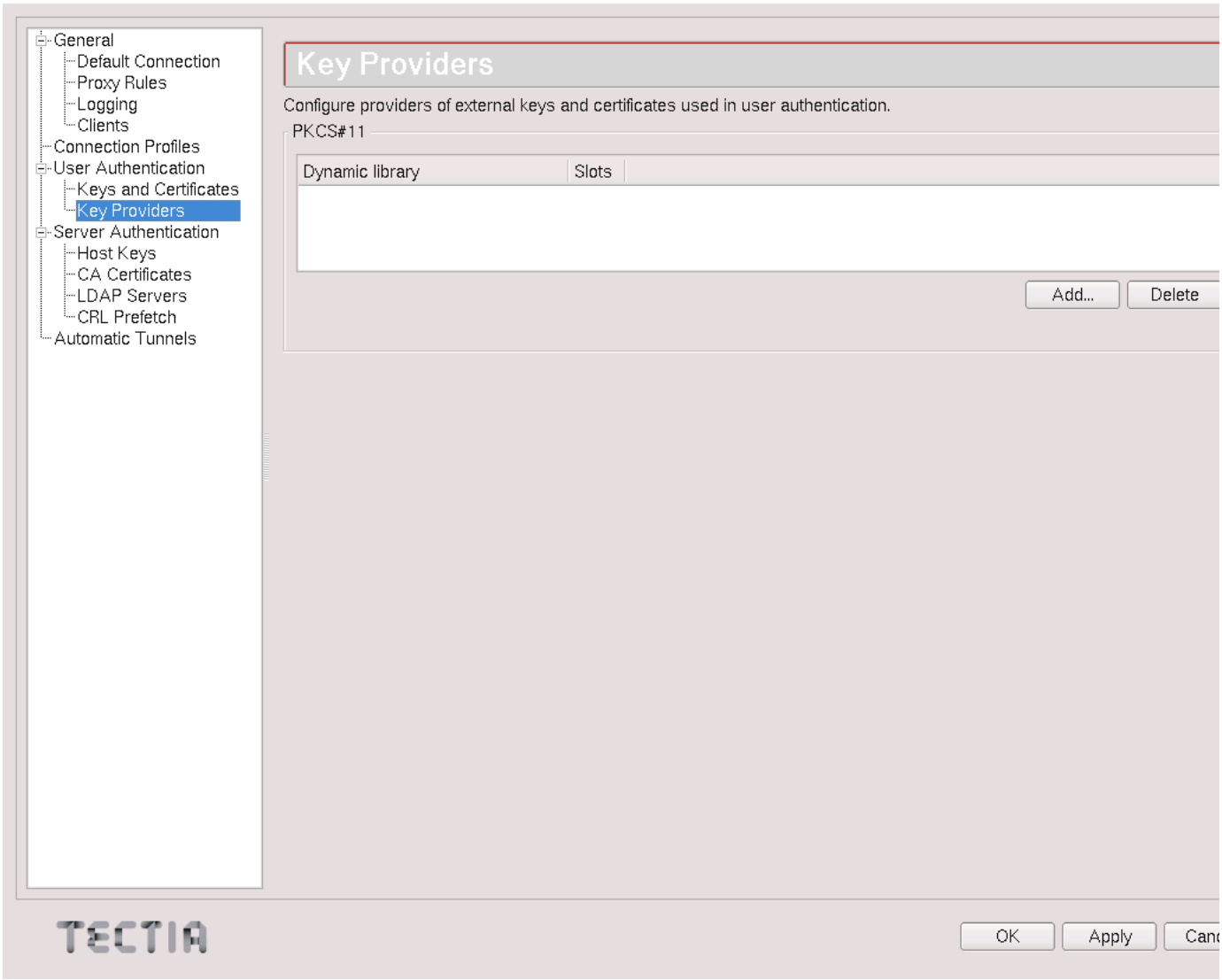
From a terminal window run the following command: ***ssh-tectia-configuration***



Configure Smart Card Reader

Before we can begin you need to have the libcoolkey package installed on your linux system.

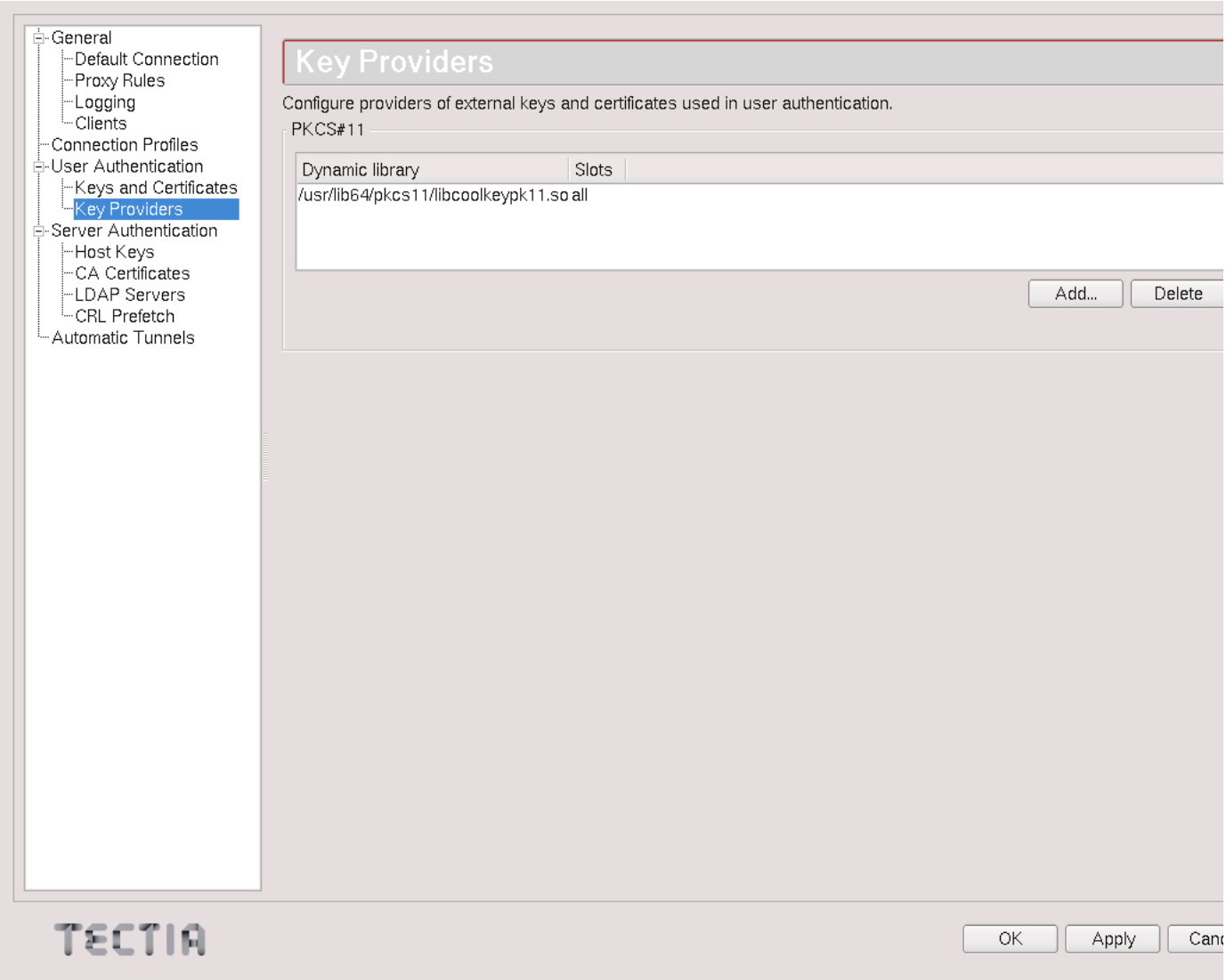
1. Click on ***Key Providers***



2. Click on ***Add*** and enter the following under ***Dynamic Library*** field:

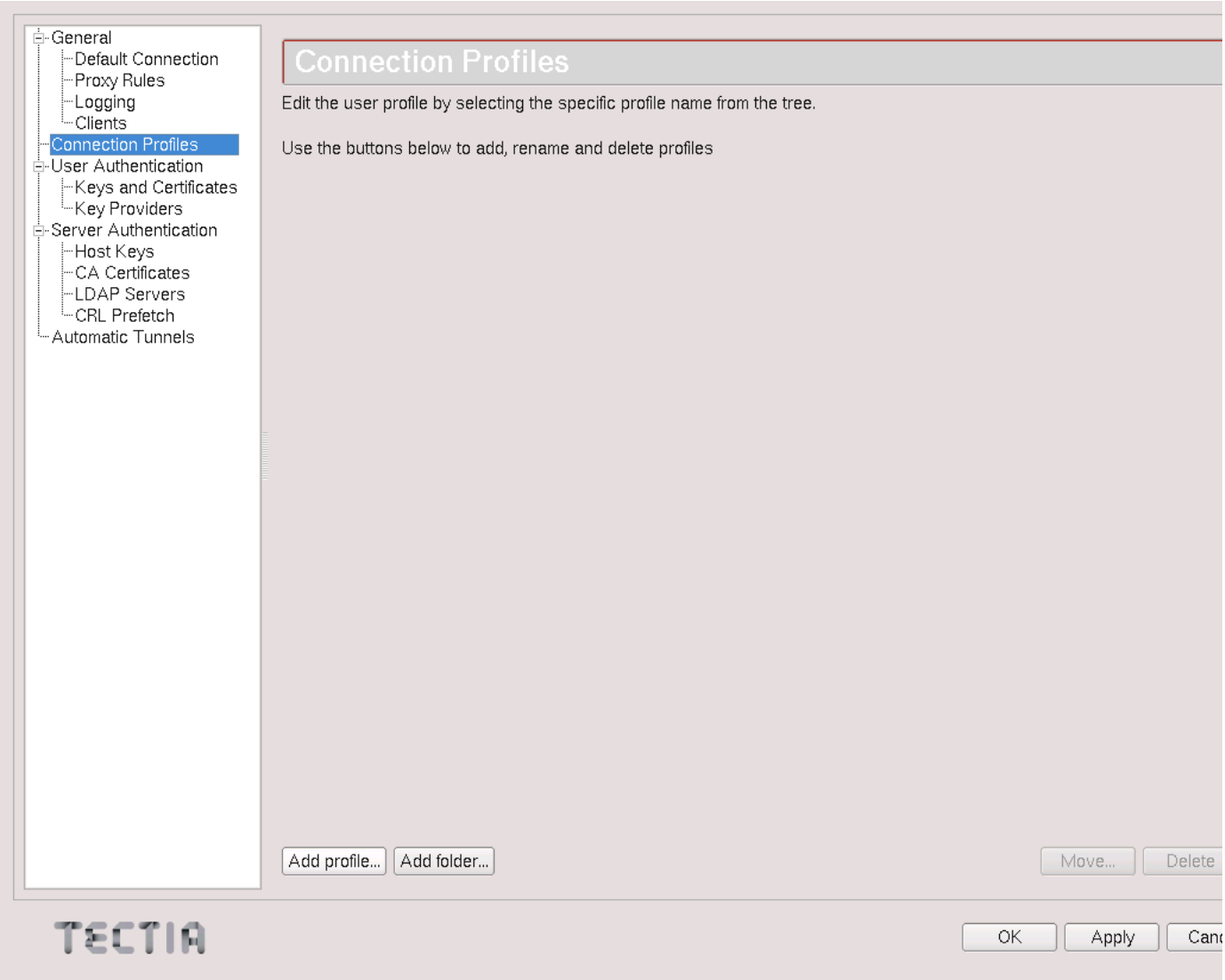
/usr/share/centrifydc/lib64/coolkey/gcc4/libcoolkeypk11.so

3. Click ***Apply***

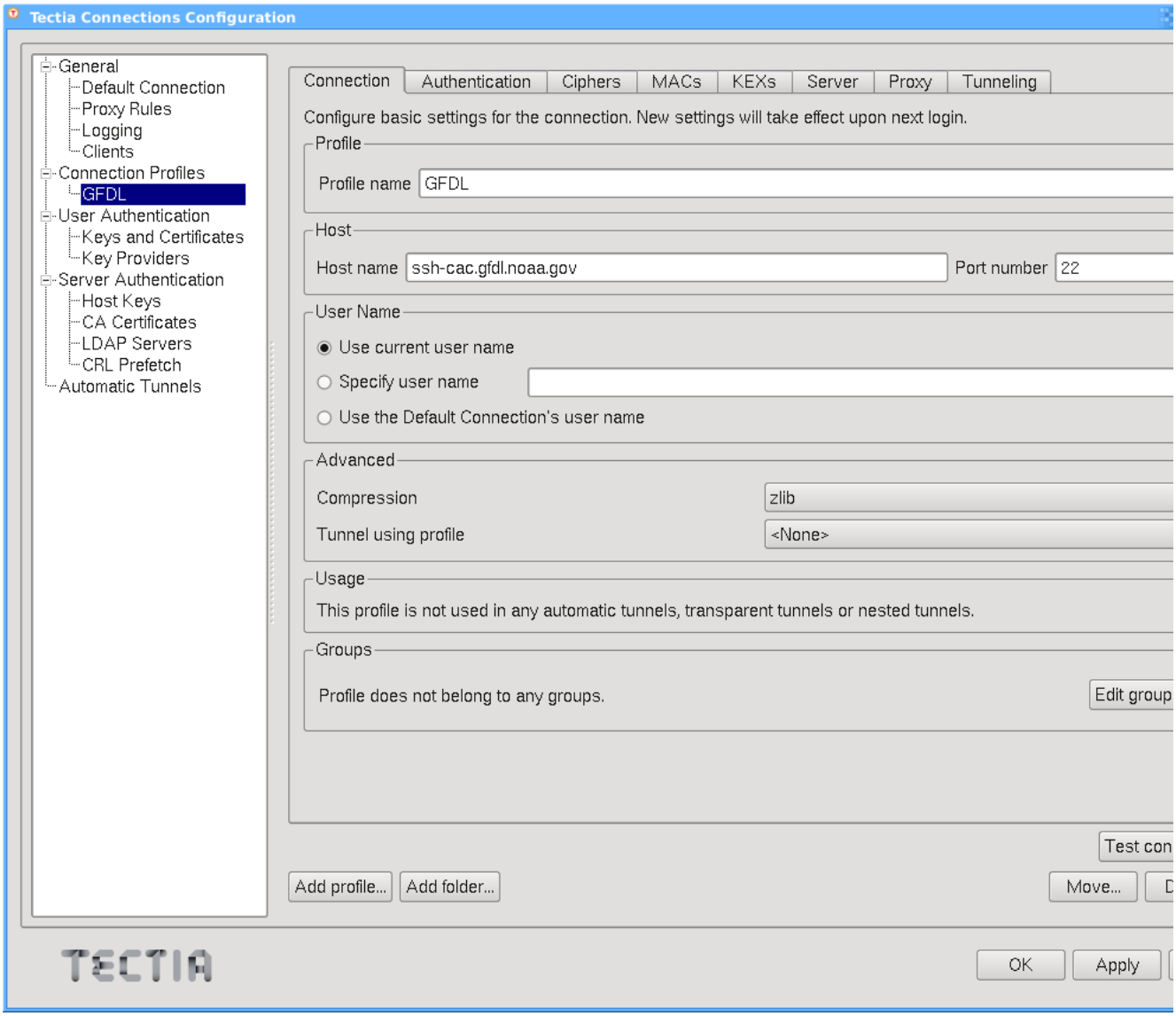


Create SSH Profile

1. Click on ***Connection Profiles***



2. Click on ***Add Profile***
3. Set the following settings on the **Connection** tab:
    1. Profile -> **Profile name: GFDL**
    2. Host -> **Host name: ssh-cac.gfdl.noaa.gov**
    3. Host -> **Port number: 22** (leave the default)
    4. Advanced -> **Compression: zlib**

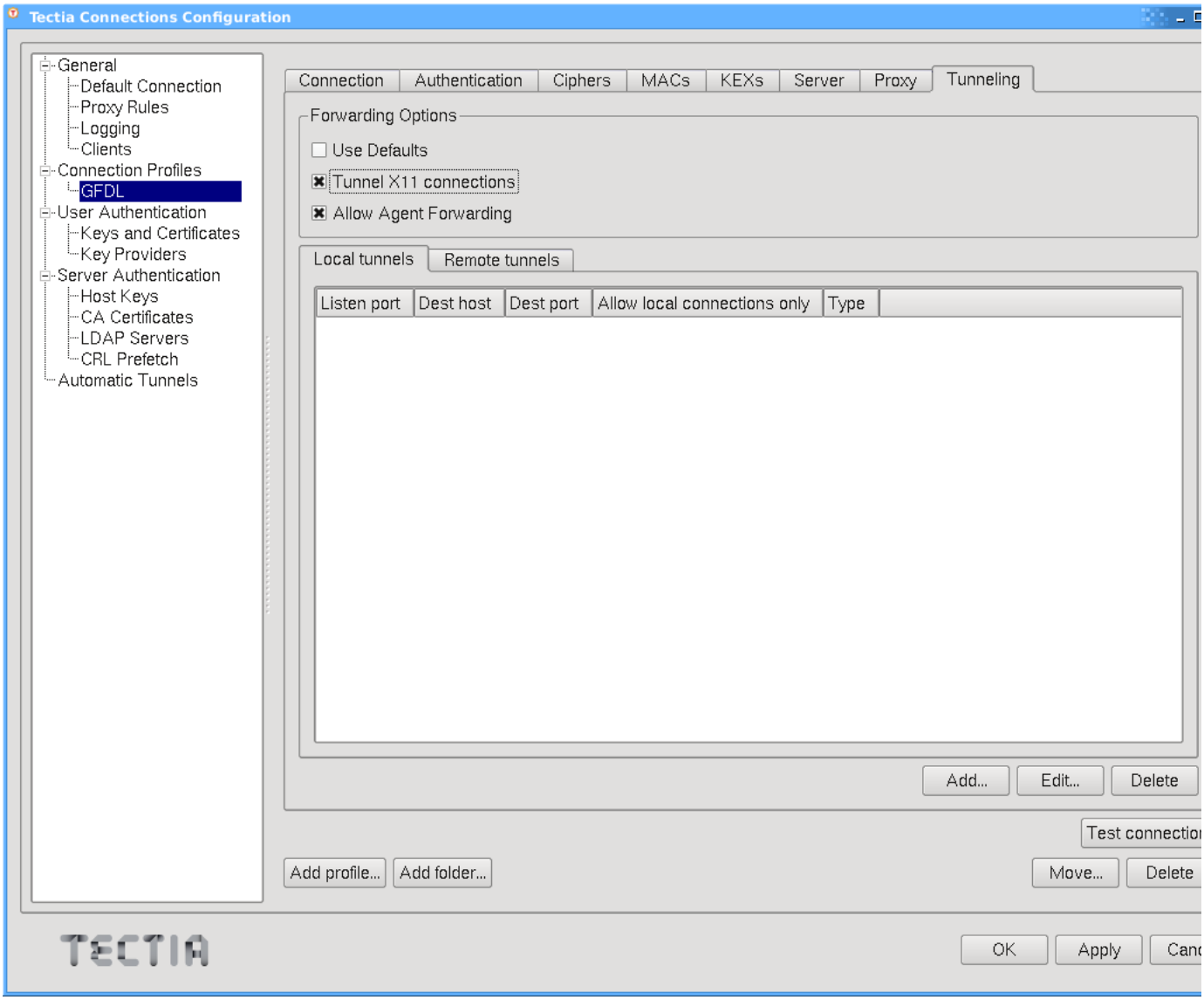


4. Click **Apply**

X11 Forwarding

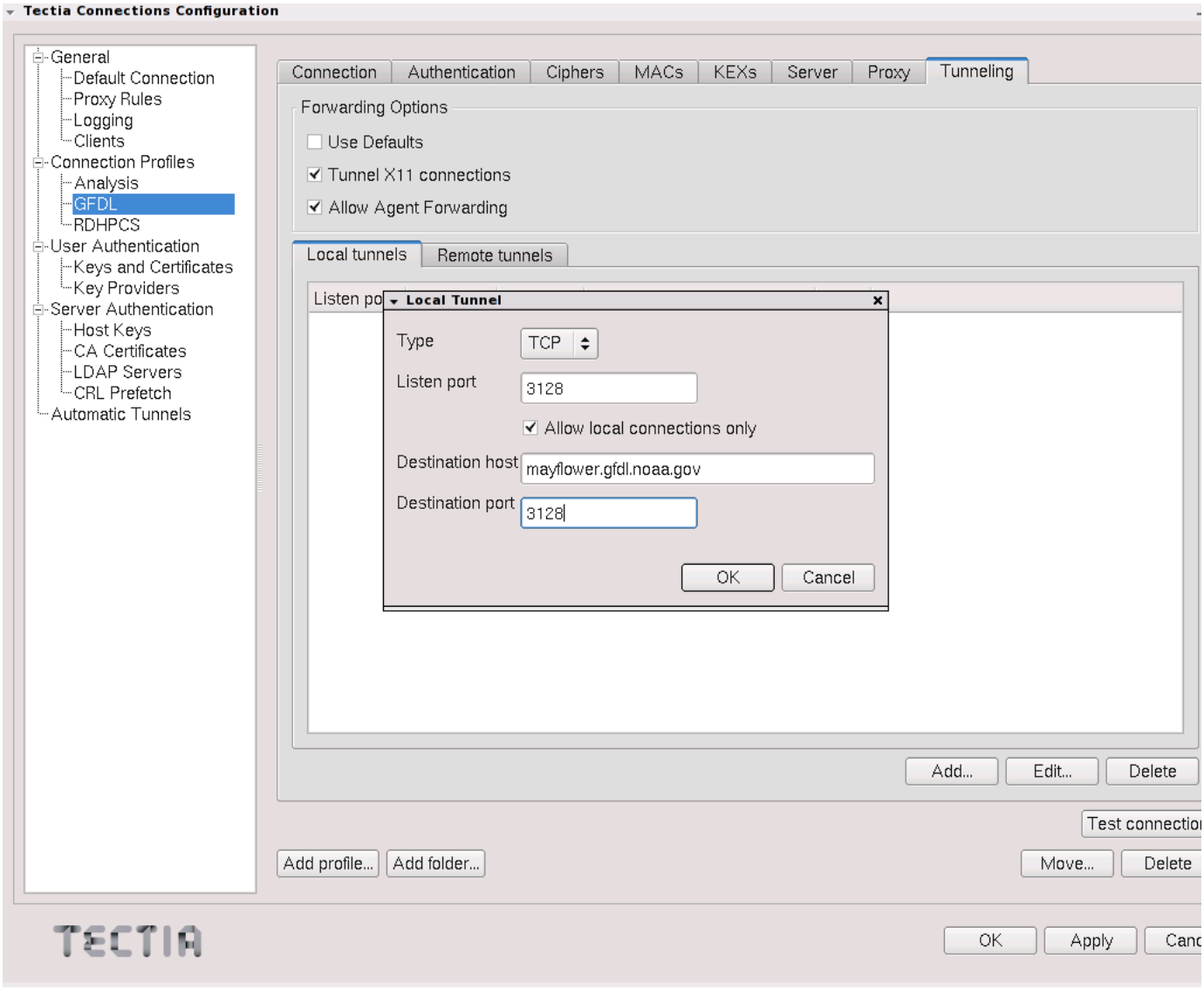
Set the following settings on the **Tunneling** tab:

1. Forwarding Options -> **Use Defaults: Deselect**
2. Forwarding Options -> **Tunnel X11 connections: Select**
3. Forwarding Options -> **Allow Agent Forwarding: Leave Selected**



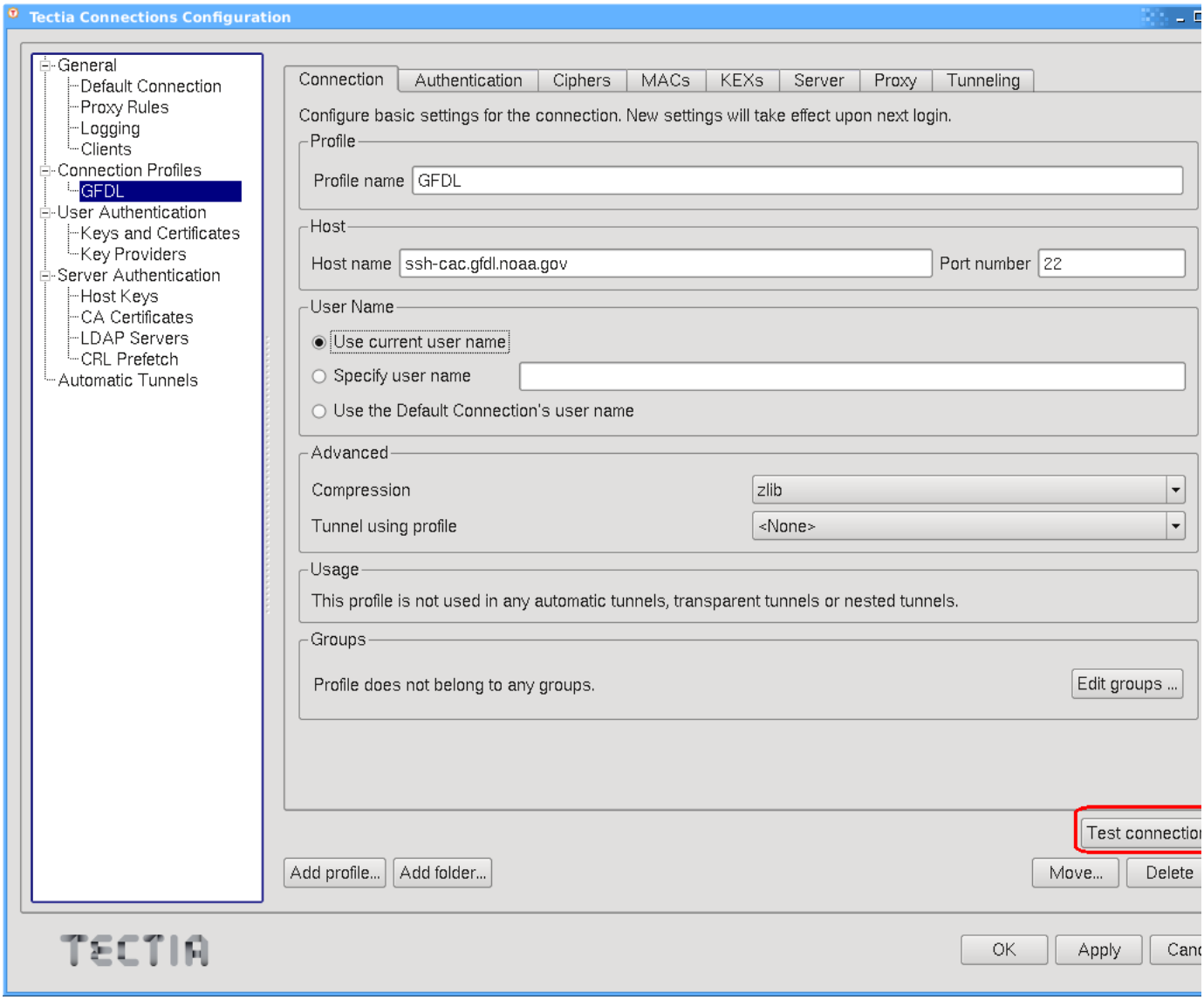
GFDL Proxy (Mayflower) Tunnel

1. Click on the **Tunneling** tab.
2. Click on **Add**
    1. Enter **3128** port in **Listen port** field.
    2. Enter m**ayflower.gfdl.noaa.gov** in **Destination host** field.
    3. Enter **3128** port in **Destination port** field.
    4. Click on **OK**.
3. Click on **Apply**.

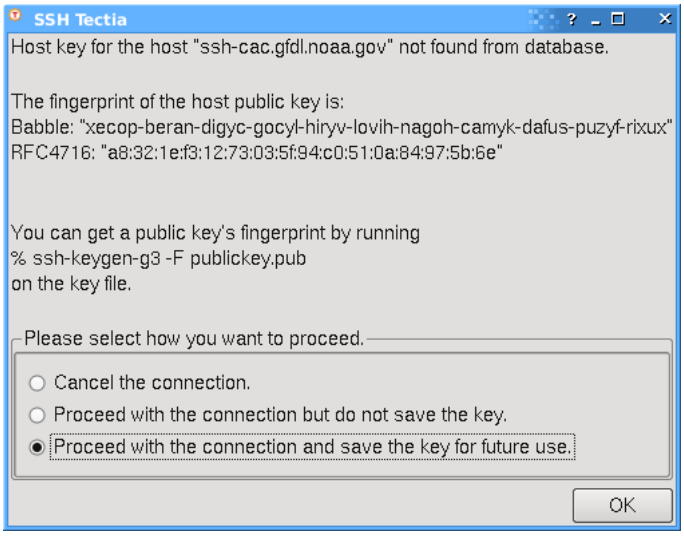


Test SSH Connection

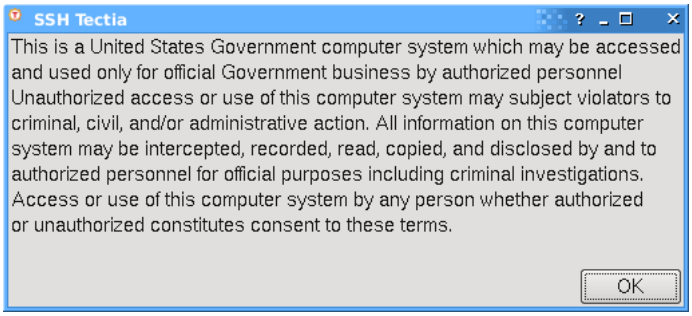
1. Switch back to the connection tab and click **Test connection**



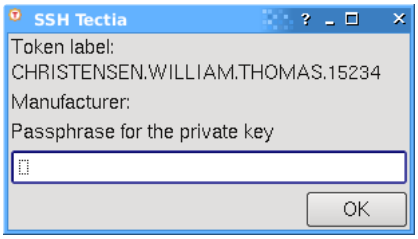
2. "**Proceed with the connection and save the key for future use.**"



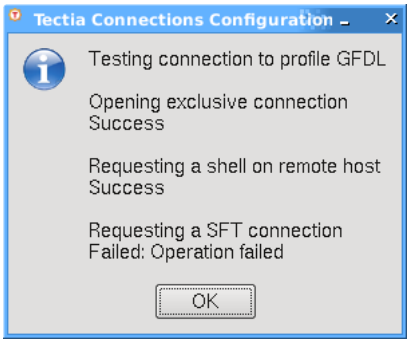
3. Accept the policy banner



4. Enter your CAC passphrase. **You may see a single rectangle for all the characters you type, or you may see asterisks.**



5. Hit OK once the connection is successfully tested



6. Exit the utility

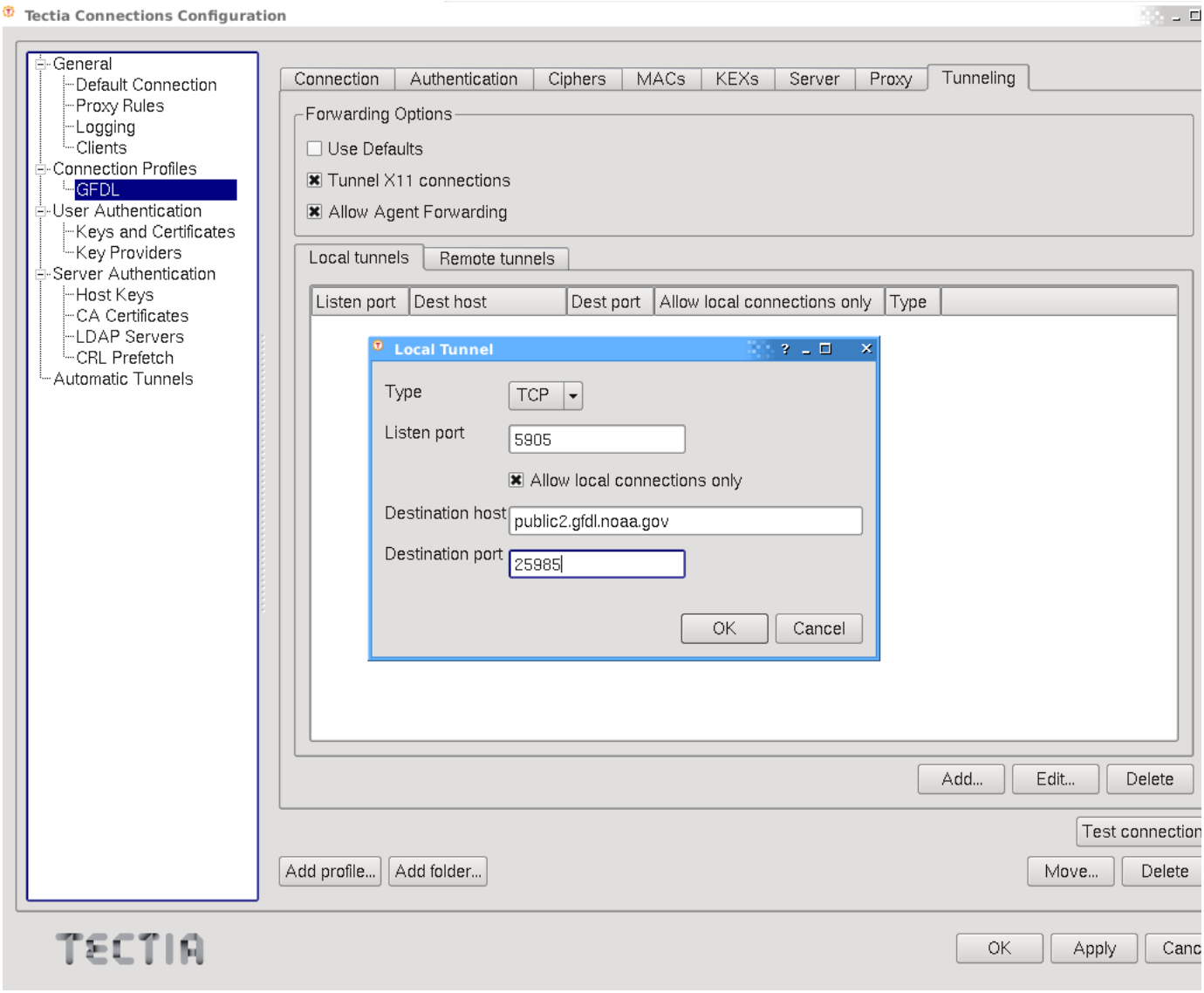
VNC Tunnel

Determine your VNC port

1. From a terminal window, connect to the SSH bastion by running the command: **sshg3 GFDL**
2. Connect to your workstation by running the commands, assuming your workstation is public2.gfdl.noaa.gov: **ssh public2.gfdl.noaa.gov**
3. Determine your port by running the command: **vncid**
4. Make note of the 4 or 5 digit number it outputted

Configure VNC Tunnel

1. Run the following command: **ssh-tectia-configuration**
2. In the left pane, switch to: **Connection Profiles -> GFDL**
3. Click on the **Tunneling** tab
4. Click on **Add**
    1. Enter **5905** in **Listen Port** field.
    2. Enter workstation where VNC is running in **Destination host** field. (e.g. public2.gfdl.noaa.gov)
    3. Enter your aforementioned VNC port in **Destination port** field. (e.g. **25985**)
    4. Click on **OK**
5. Click on **Apply**
6. Exit the utility



Windows

Tectia Windows Client Configuration

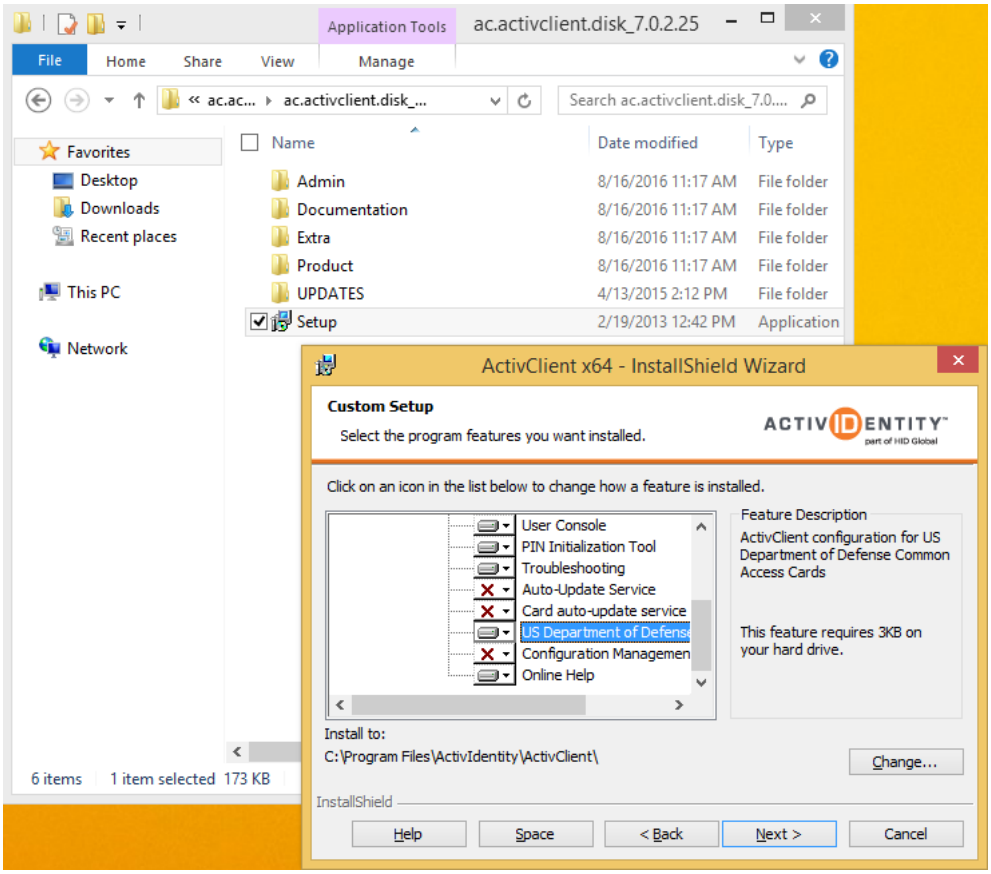
Installation

Tectia SSH Client

1. Given the “Client Installation Package” with Tectia Client 6.4.10.264, unzip the compressed folder
2. Locate the Windows Installer file ssh-tectia-client-6.4.10.264-windows.msi
3. Double-click the installation file, and the installation wizard will start
4. Select Complete Installation
5. Complete all required configuration information through completing the Installation Wizard
6. Once installation is complete, you will be required to restart your system. If you are not prompted to restart, please restart anyway.

ActivClient

1. Locate the “Active Identity Active Client” installation file (Setup.exe)
2. Double-click the installation file, and the installation wizard will start
    1. Select Custom Installation, Next
    2. Select to install: US Department of Defense feature

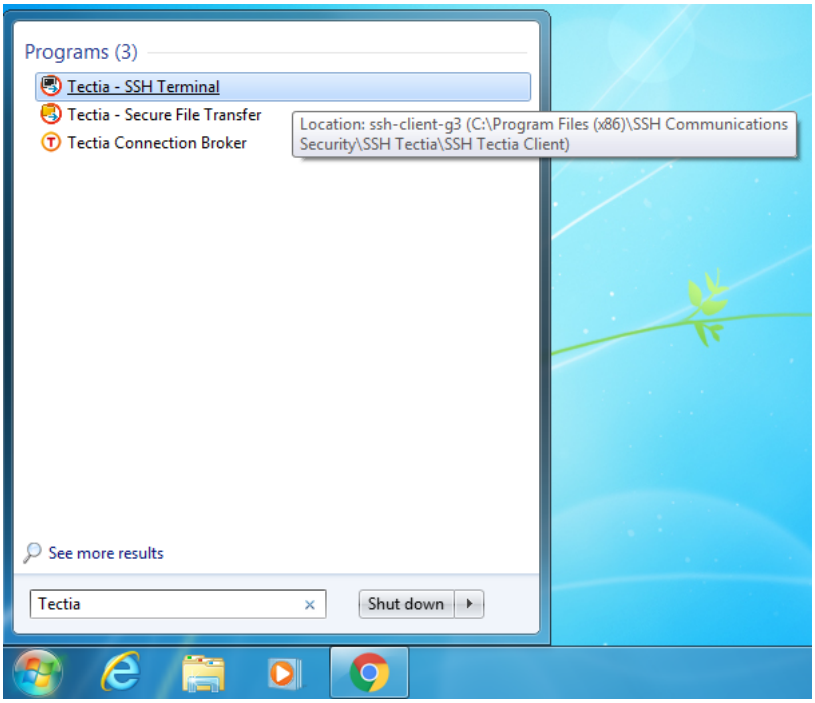


3. Continue with the rest of the installation steps

Configuration

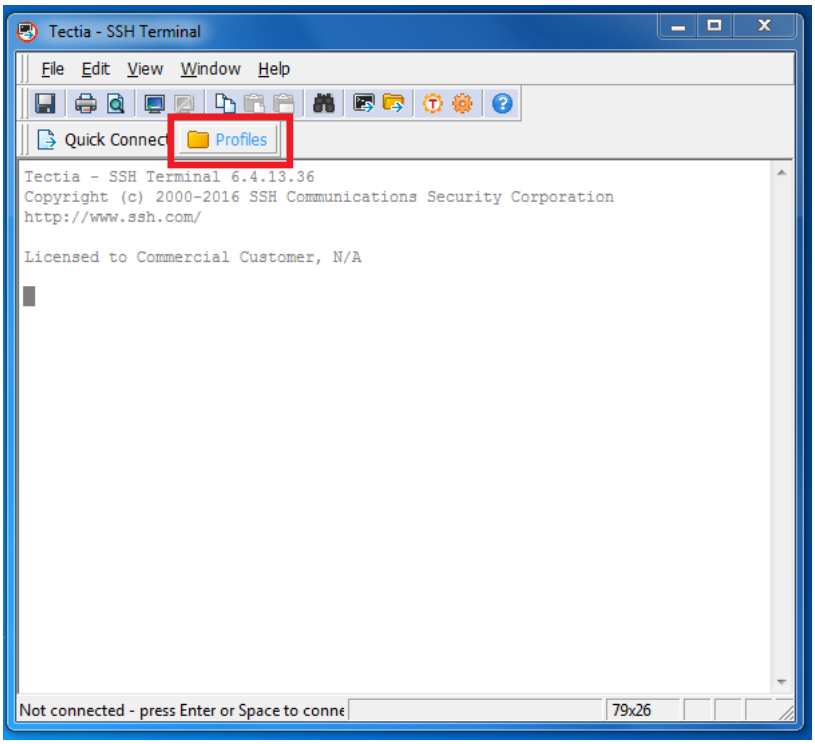
Run Tectia SSH Terminal

1. Click on **Start**
2. In the search type in **Tectia**
3. Click on **Tectia - SSH Terminal**

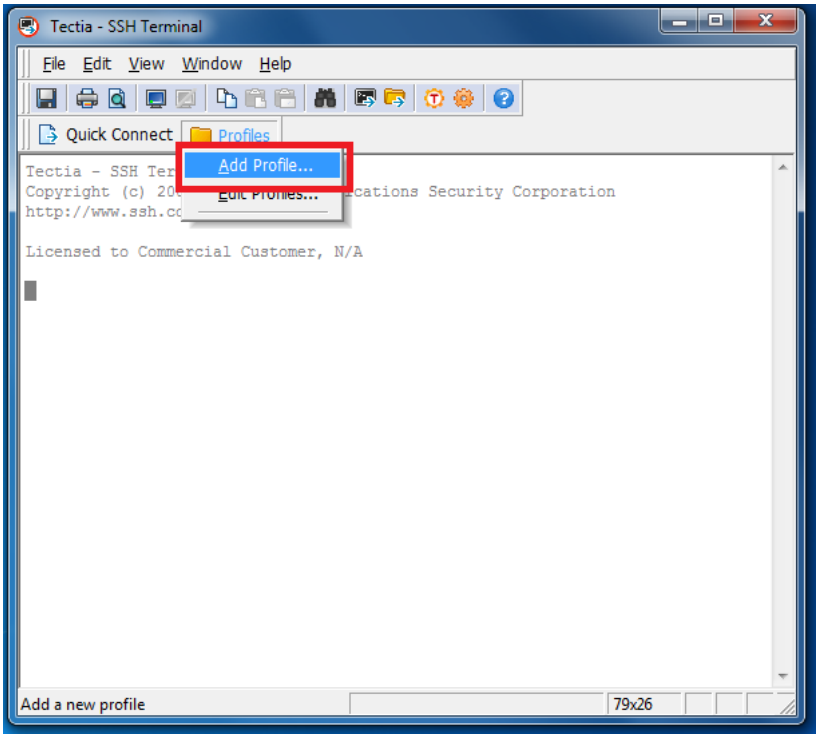


Create a Profile

1. In the Tectia - SSH Terminal window click on **Profiles**

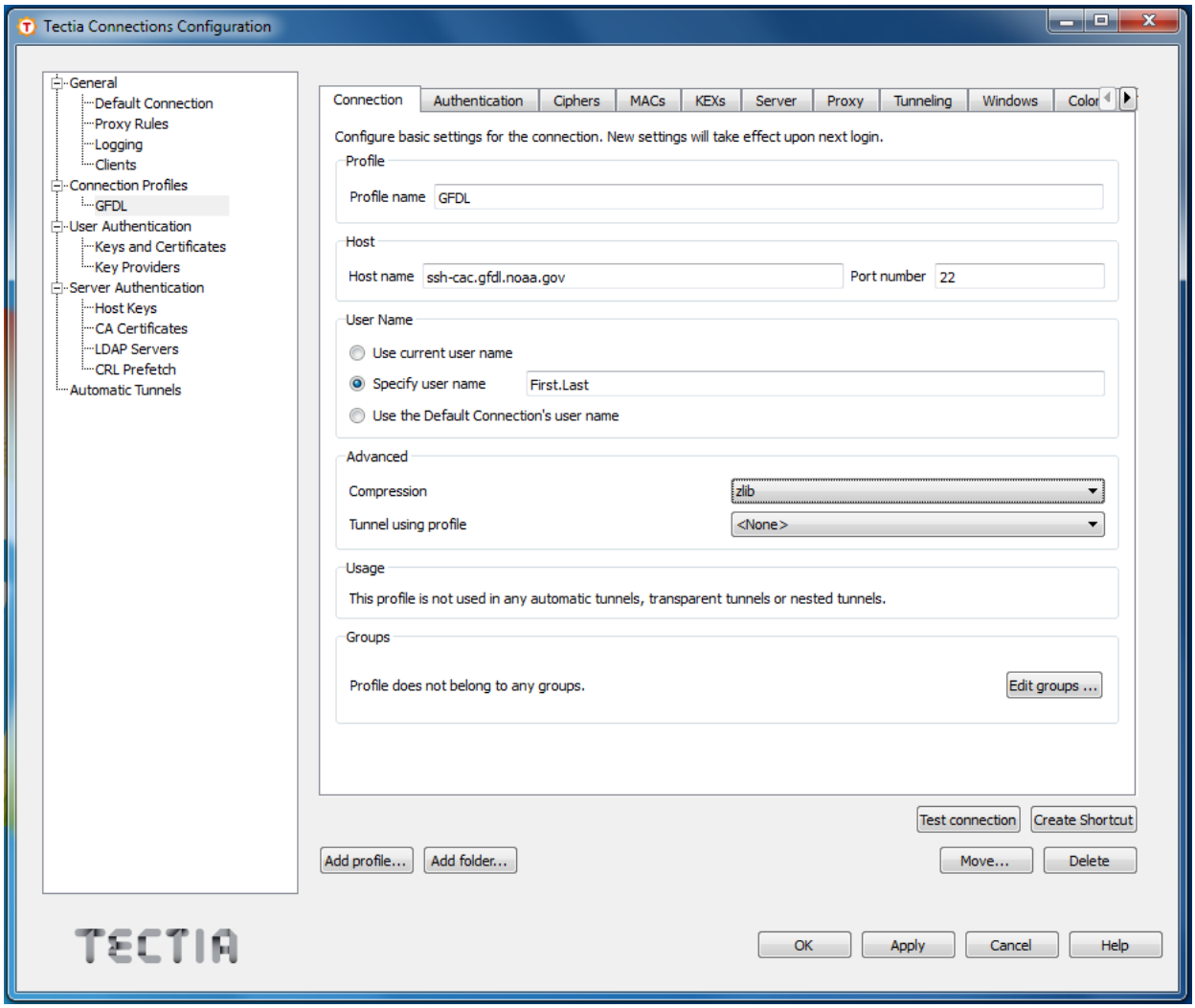


2. Click on **Add Profile**



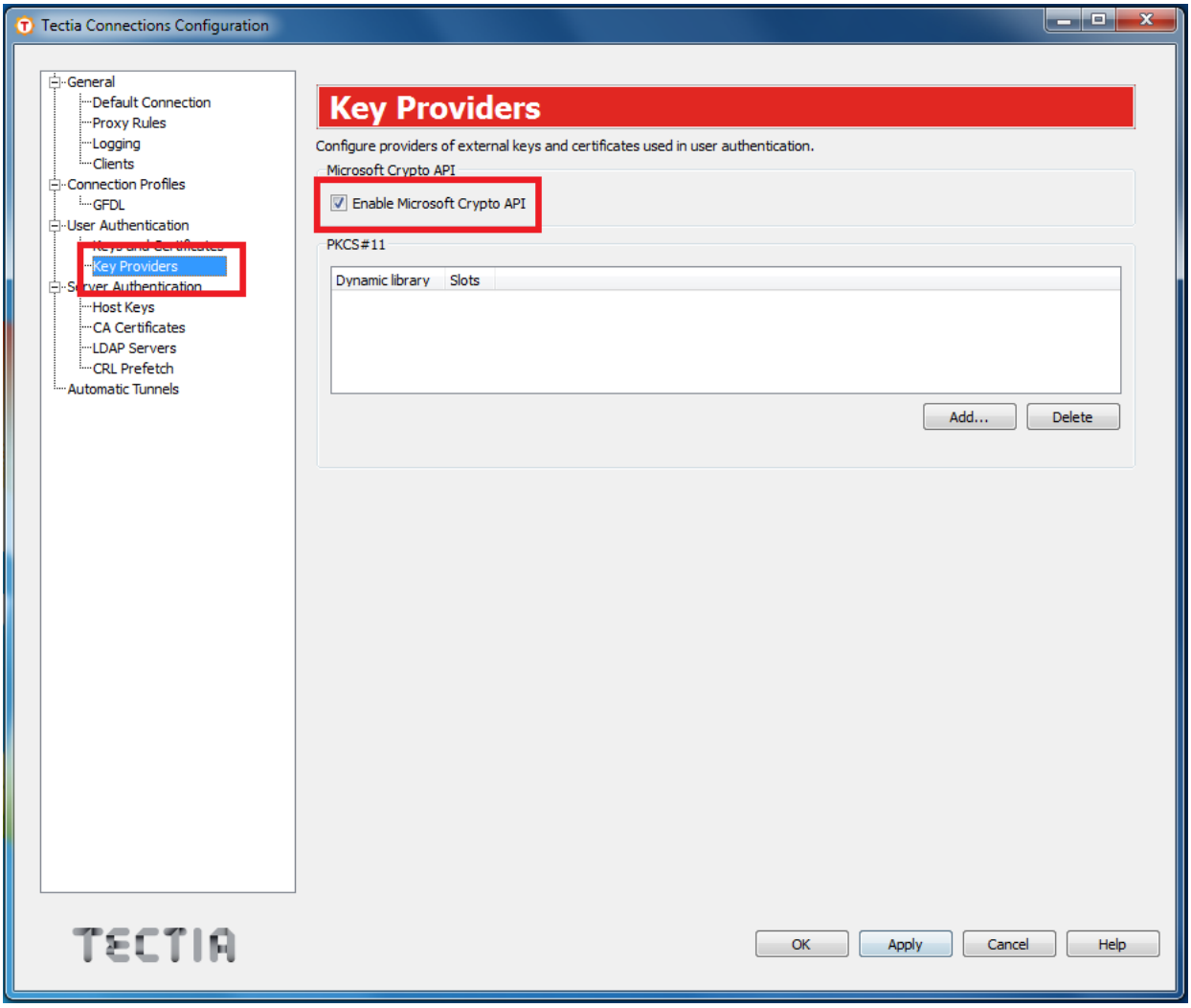
3. Fill in the following fields:
    1. Profile name: **GFDL**
    2. Host name: **ssh-cac.gfdl.noaa.gov**
    3. Port number: **22**
    4. User Name
        1. Check **Specify user name**
        2. Enter your **First.Last**

5. Compression: **zlib**
6. Click **Apply**



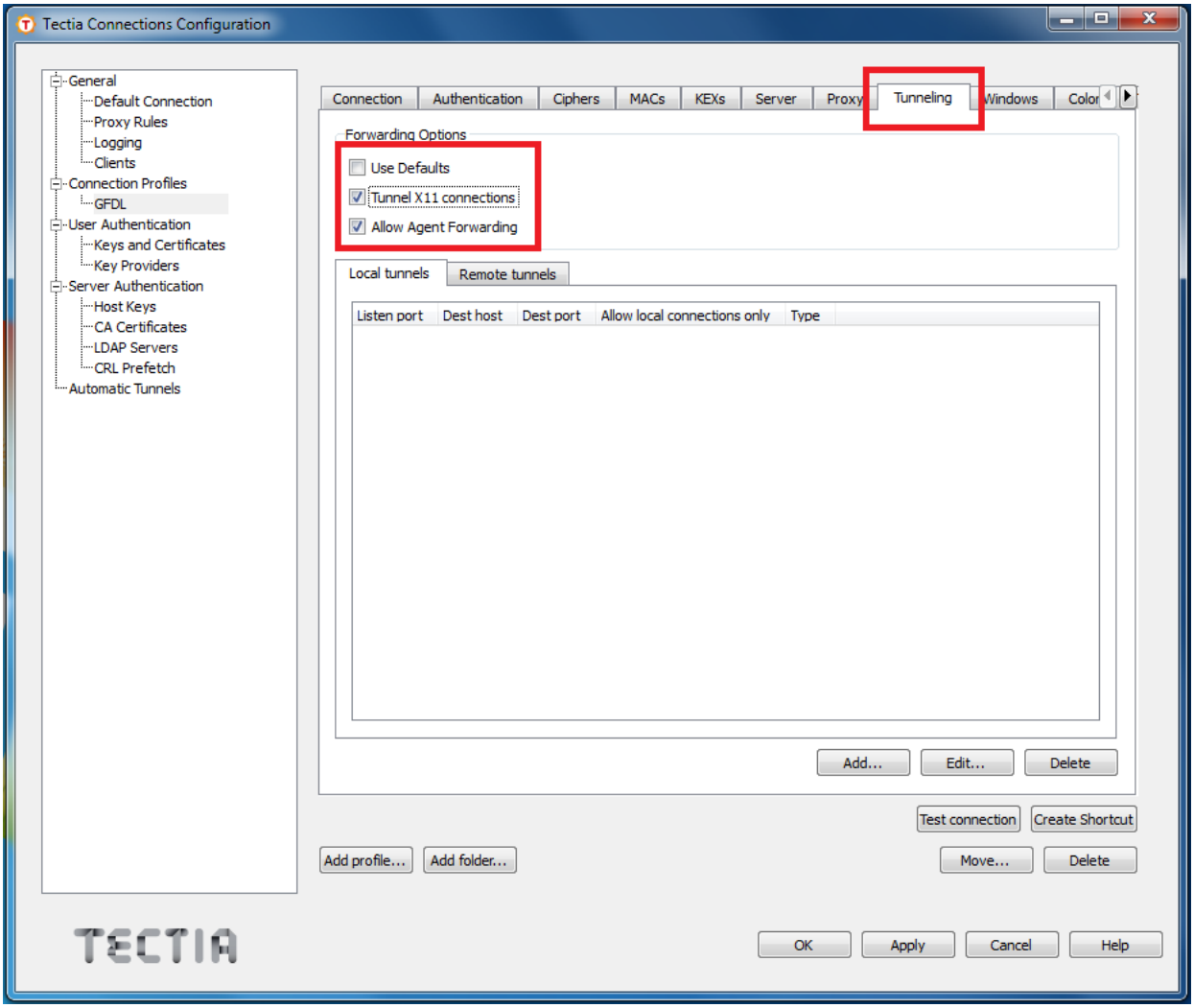
Configuring Smart Card Reader

1. Click on **Key Providers** on the left hand side.
2. Check **Enable Microsoft Crypto API**
3. Click **Apply**



X11 Forwarding

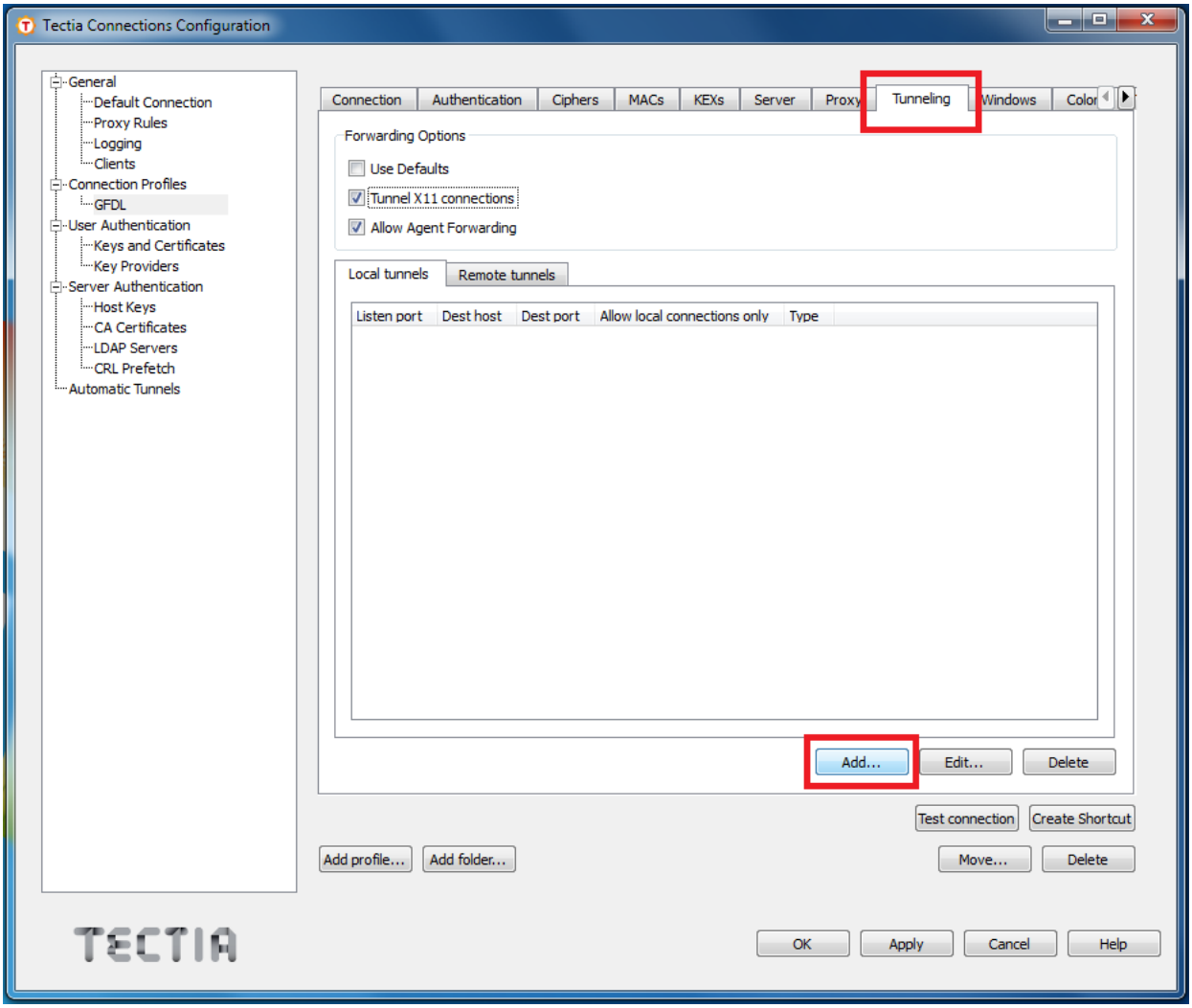
1. Click on the **Tunneling** tab
2. Uncheck **Use Defaults**
3. Check **Tunnel X11 connections**
4. Click **Apply**



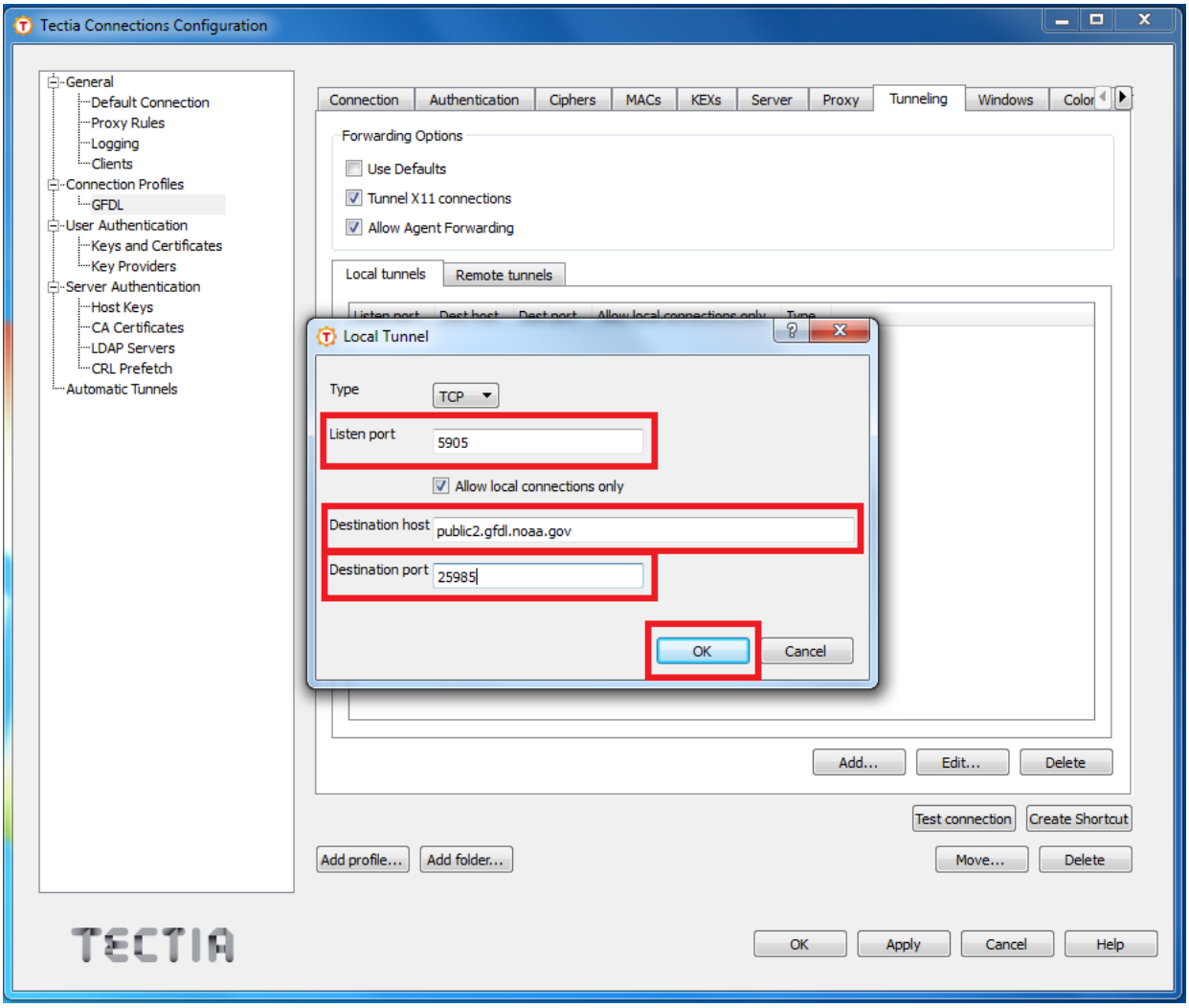
Tunnels

VNC

1. Click on the **Tunneling** tab
2. Click on **Add**

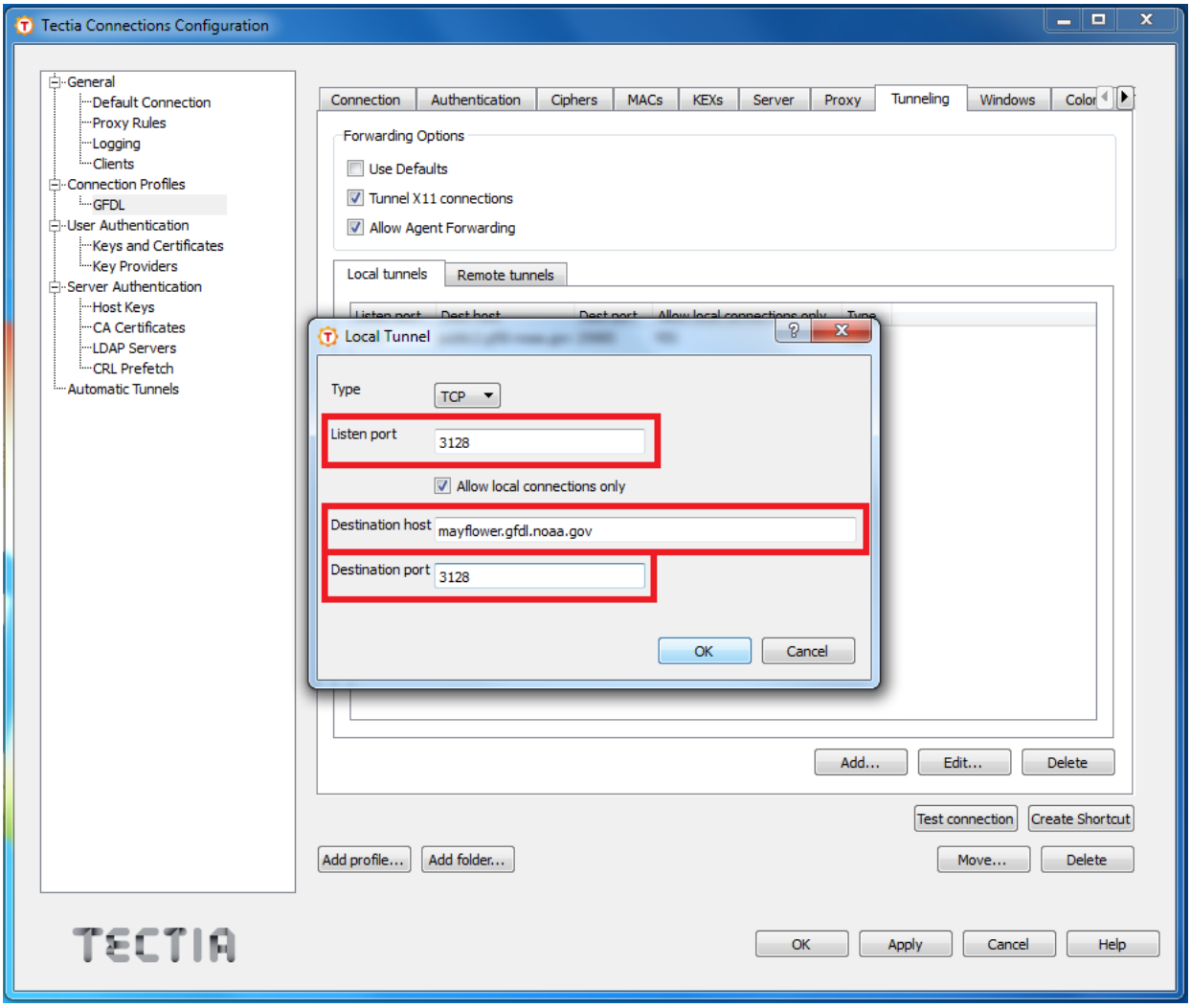


3. Enter VNC port in Listen Port field. (e.g. **5905**)
    1. Enter workstation where VNC is running in **Destination host** field. (e.g. **public2.gfdl.noaa.gov**)
    2. Enter VNC port in **Destination port** field. (e.g. **25985**)
    3. Click on **OK**
4. Click on **Apply**



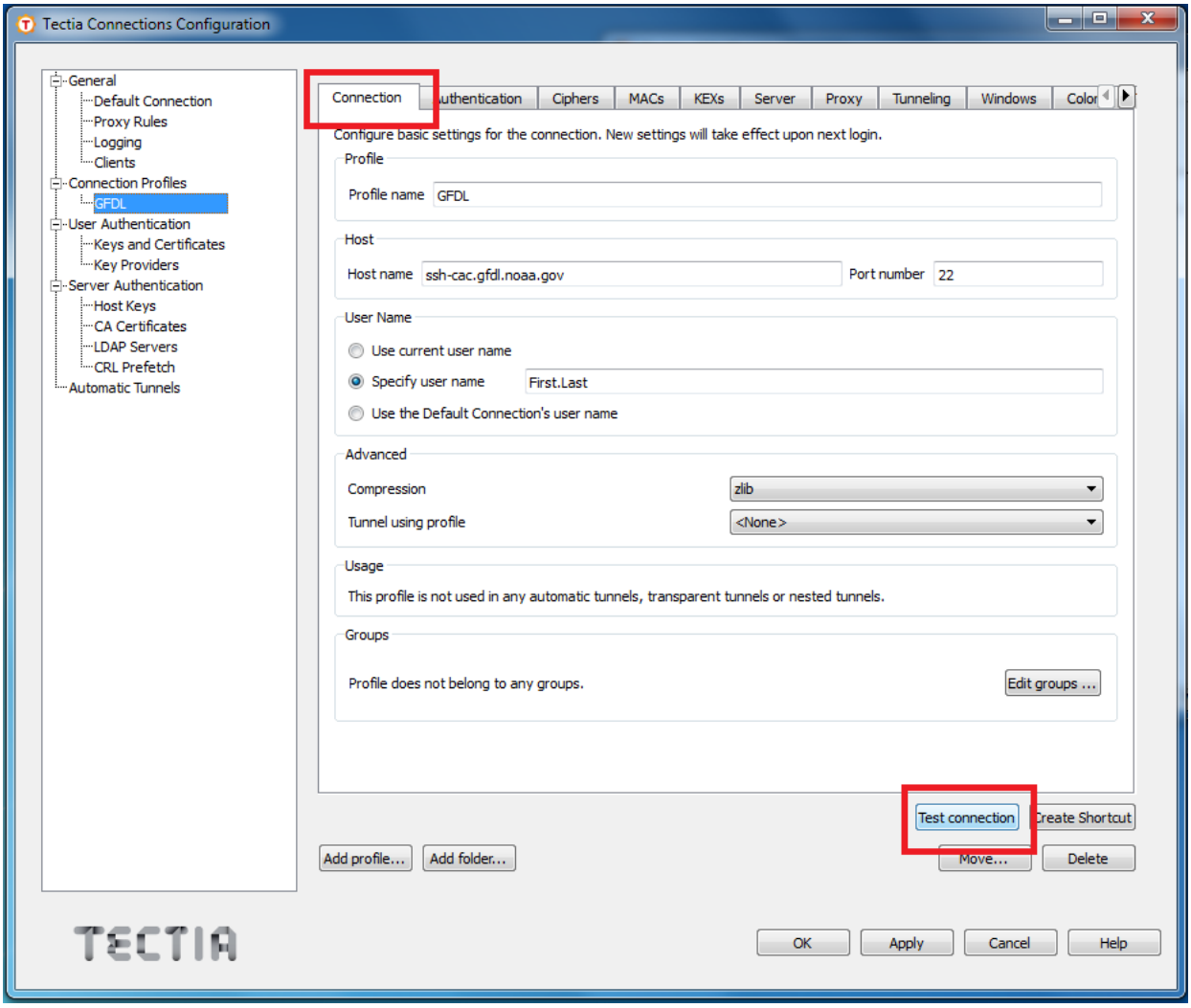
Mayflower

1. Click on the **Tunneling** tab.
2. Click on **Add**
    1. Enter **3128** port in **Listen port** field.
    2. Enter **mayflower.gfdl.noaa.gov** in **Destination host** field.
    3. Enter **3128** port in **Destination port** field.
    4. Click on **OK**.
3. Click on **Apply**.

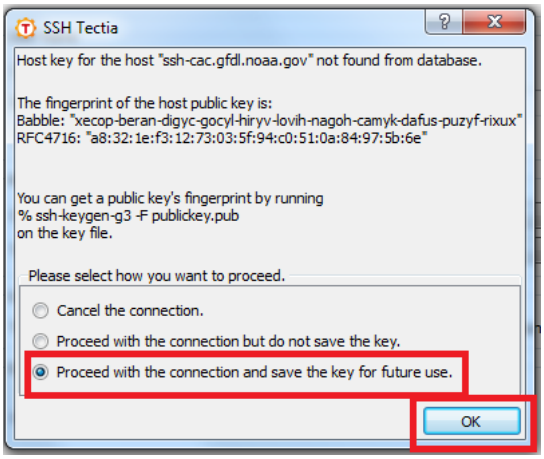


Test SSH Connection

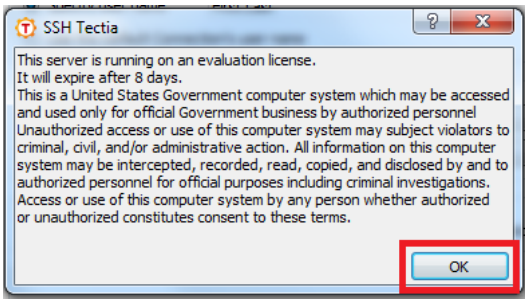
1. Switch back to th connection tab and click **Test connection**



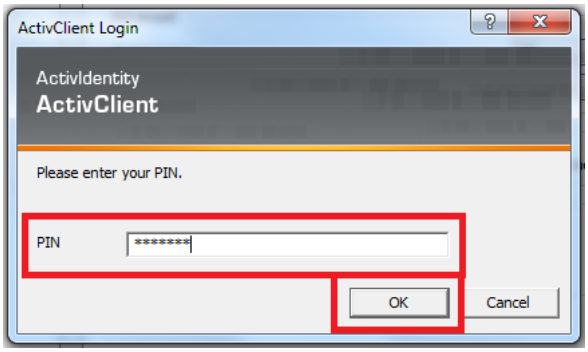
2. Select "**Proceed with the connection and save the key for future use.**"



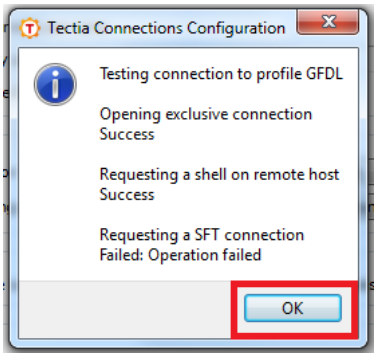
3. Accept the policy banner by pressing **OK**



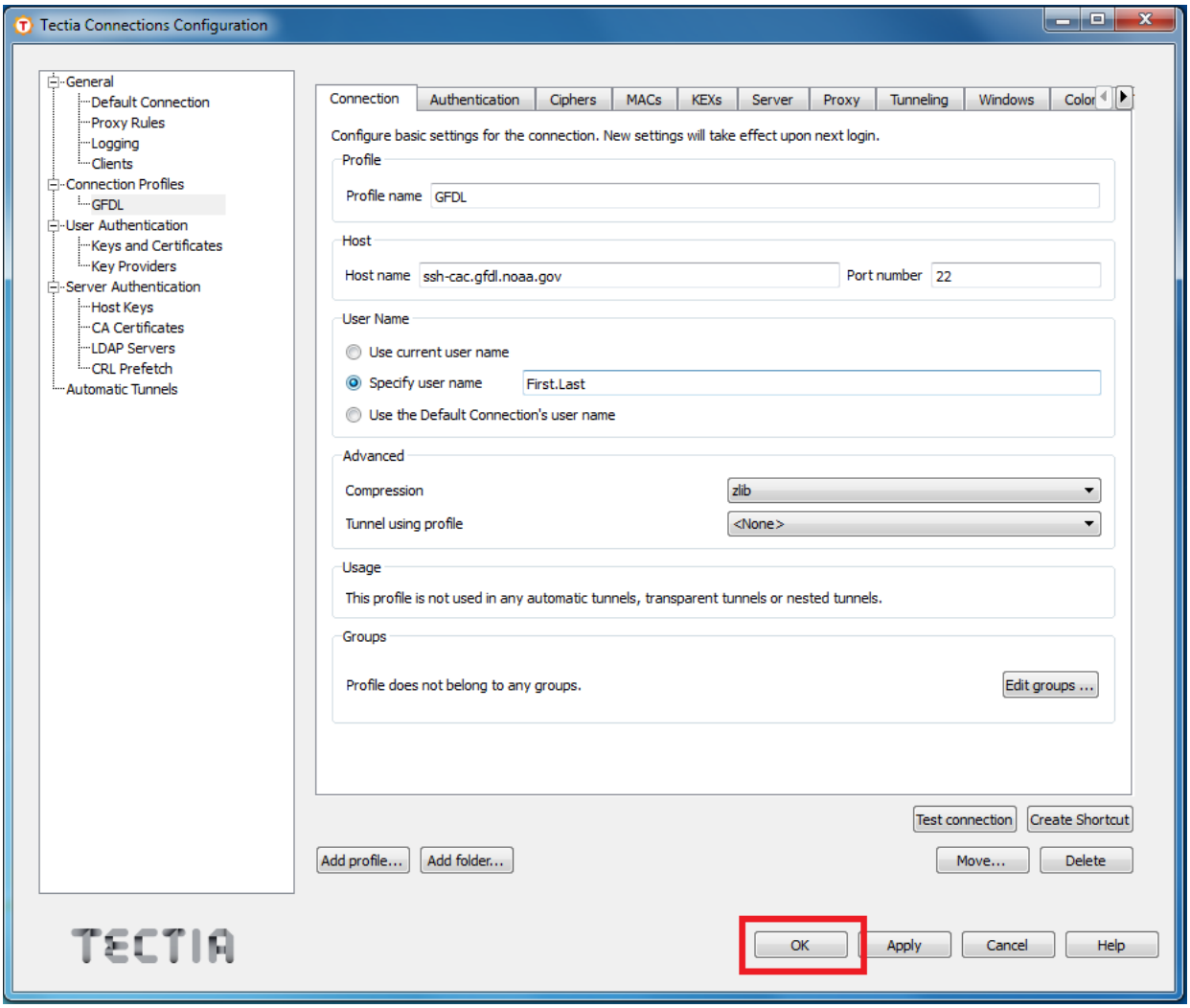
4. Enter your CAC passphrase and press **OK. (You maybe see a single rectangle for all the characters you type, or you may see asterisks.)**



5. Press **OK** once the connection is successfully tested.



6. Press **OK** to exit the utility.



Usage