Common Access Card (CAC) Login

PLEASE CHECK BACK OFTEN FOR UPDATES DURING THE TRANSITION PERIOD.

Updated 11/15/16

Purpose / Scope

Starting 0Z on 11/01/16 all RDHPCS users with a CAC and logging in from Windows and Linux systems are required to use CAC bastion authentication. This section is for those users who are required to login via CAC. See: Logging in

Introduction

Background:

As part of HSPD-12 (Homeland Security Presidential Directive-12) and CITR-008 (Commerce Interim Technical Requirement-008) and NOAA's Cyber Sprint objectives, GSD is pushing CAC (Common Access Card) authentication and remote access compliance.

Presidential Directive (HSPD) -12, signed in 2004, is the basis for the federal government requiring the use of Personal Identity Verification (PIV) access cards. NOAA chose the Department of Defense (DoD) CAC Card as its specific PIV implementation, in part because CACs also satisfy NOAA/DOC policy, in place since 2009 (CITR-008, http://www.uspto.gov/about/vendor_info/current_acquisitions/qpb_ms_att4.pdf), which requires a 2-factor level of authentication for remote access. This mandate is the driving force behind CAC enforcement for accessing RDHPC Systems.

Tectia SSH Solution:

The Tectia SSH Client software has been selected to meet the remote CAC logon requirements for the RDHPCS program. One license has been purchased for each RDHPCS user (if you currently have a RDHPCS RSA token).

The following features are being supported:

* Port forwarding

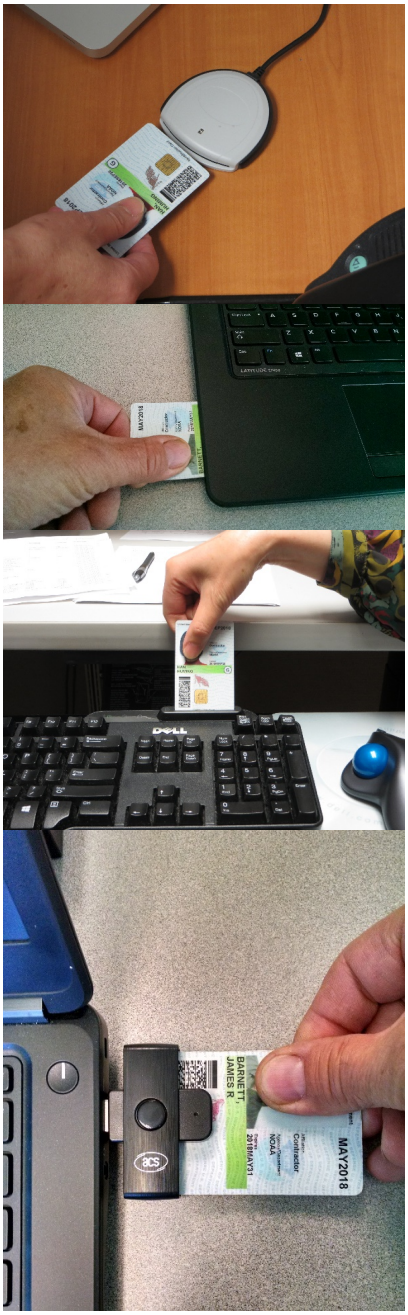
* X11 tunnelling

The following features are not being supported:

* Access to RDHPCS Systems from a system which does not have the ability to access a user's CAC card directly.

CAC Readers

Here are the four most common CAC readers. If you do not have a CAC reader for your Federal desktop/laptop, request one from your IT system administrator or NOAA sponsor.



CAC-Tectia Setup Procedures

Host names for the CAC bastion Server in Boulder, CO

```
bastion-jet.boulder.rdhpcs.noaa.gov
```

```
bastion-theia.boulder.rdhpcs.noaa.gov
bastion-gaea.boulder.rdhpcs.noaa.gov
```

Host names for the CAC Bastion Server in Princeton, NJ

```
bastion-jet.princeton.rdhpcs.noaa.gov
bastion-theia.princeton.rdhpcs.noaa.gov
bastion-gaea.princeton.rdhpcs.noaa.gov
```

The following OS specific sections (Windows, Linux, MAC) describe how to do the following:

```
* Download the Tectia software

* Install the Tectia software on your local laptop or workstation

* Install the license file on your local laptop or workstation

* Configure the Tectia software

* Use the client software to connect to R&D HPC Systems
```

Setting up Tectia SSH Client for Windows

Requirements

* Tectia SSH should install on the following Microsoft Windows versions, but only those versions supported by your NOAA IT department will be supported on your NOAA PC:

```
Microsoft Windows (x86)
XP, Server 2003, Server 2003 R2, Vista, Server 2008, 7, 8, 8.1

Microsoft Windows (x64)
Server 2003, Server 2003 R2, Vista, Server 2008, 7, Server 2008 R2, Server
2012, 8, 8.1, 10, Server 2012 R2
```

* In order to install the Tectia SSH Client, you must have the necessary administrator privileges on your system. If you do not have this access then please notify your IT system administrator for assistance.

* The Tectia Client installation requires about 140 megabytes of disk space.

* Your system needs to have a CAC reader.

Known Issues

* None at this time.

Installation

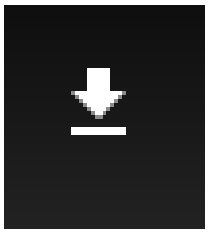
The Windows installation package is provided in the MSI (Microsoft Installer) format. The same package is compatible with the supported 32-bit (x86) and the 64-bit (x64) versions of Microsoft Windows.

1) Download the Tectia client

Copy and paste this link into a new tab on your browser:

https://drive.google.com/open?id=0B_s-UDArdhpMNnFDYWFqQ2ZIZDg

You will have to login with your NOAA email username and password in order to be able to reach the file. Once you have authenticated and the file is shown in your browser, click on the downloaded button, located in the upper right corner of your browser.



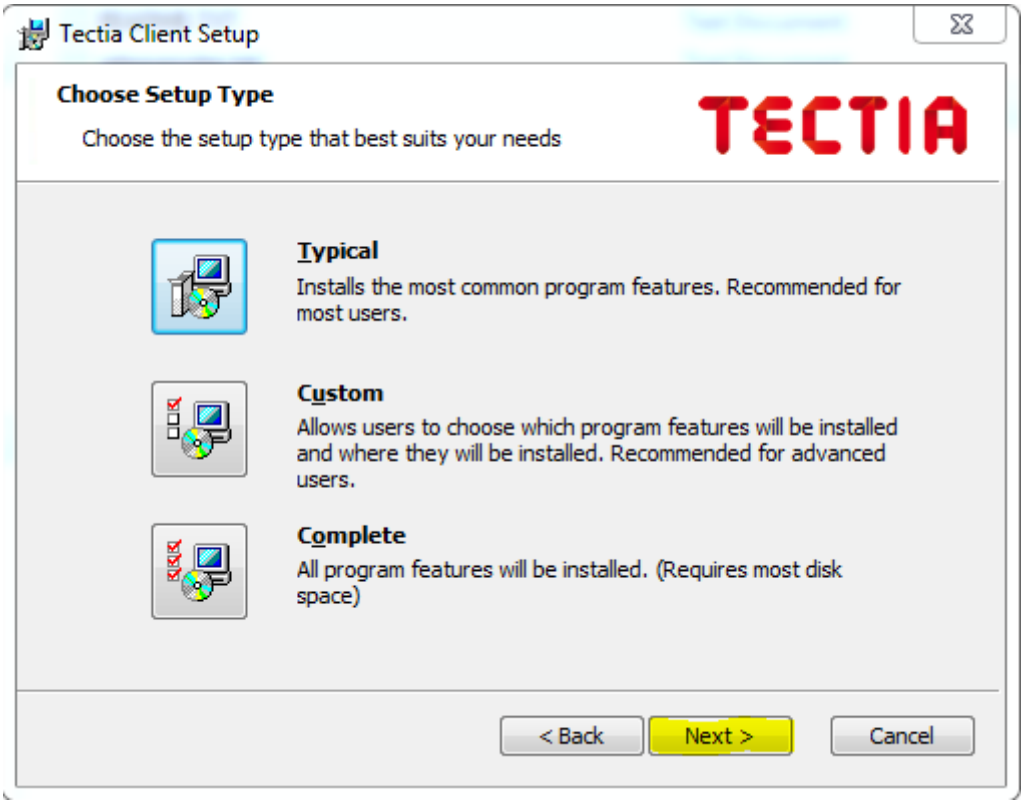
2) Extract the installation zip file contents to a temporary location.

NOTE: the download package includes Tectia documentation .pdf files that you can use after the basic install described here to learn more, customize, etc. Please review this documentation before requesting help beyond the scope of this basic setup procedure.

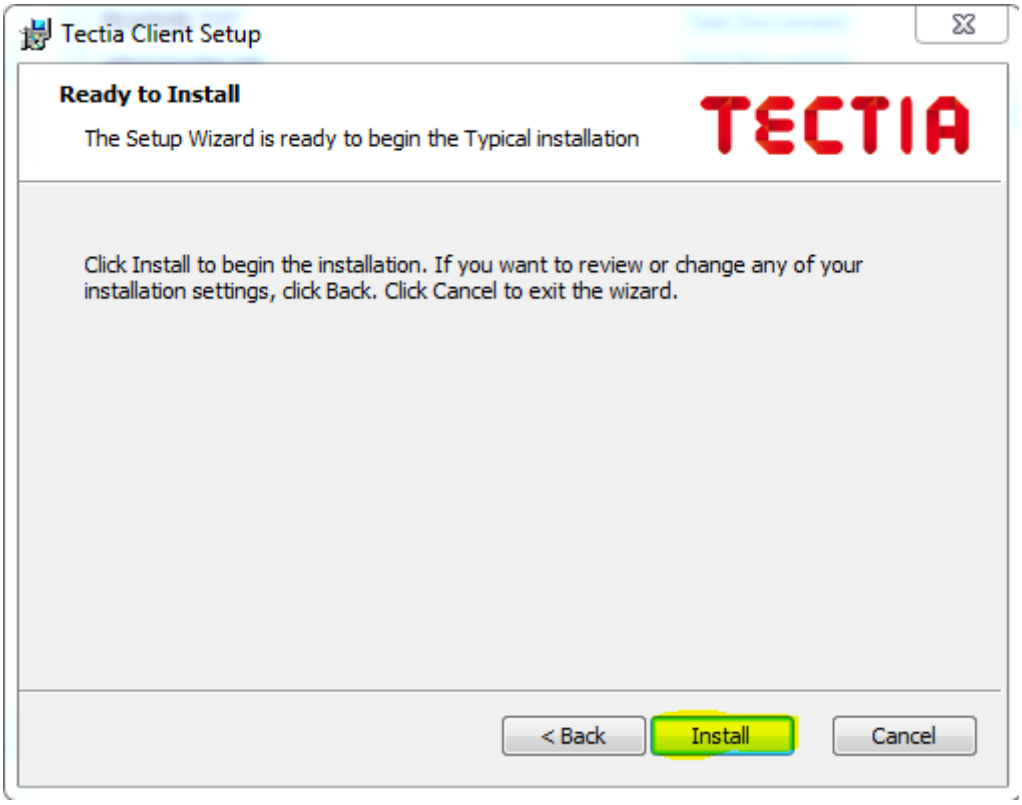
3) Locate the Windows Installer file ssh-tectia-client-<version>-windows.msi (where <version> corresponds to the version and build number, for example 6.4.10.123). On some Windows versions the .msi file type is not shown for the installer file.

4) Double-click the installation file, and the installation wizard will start.

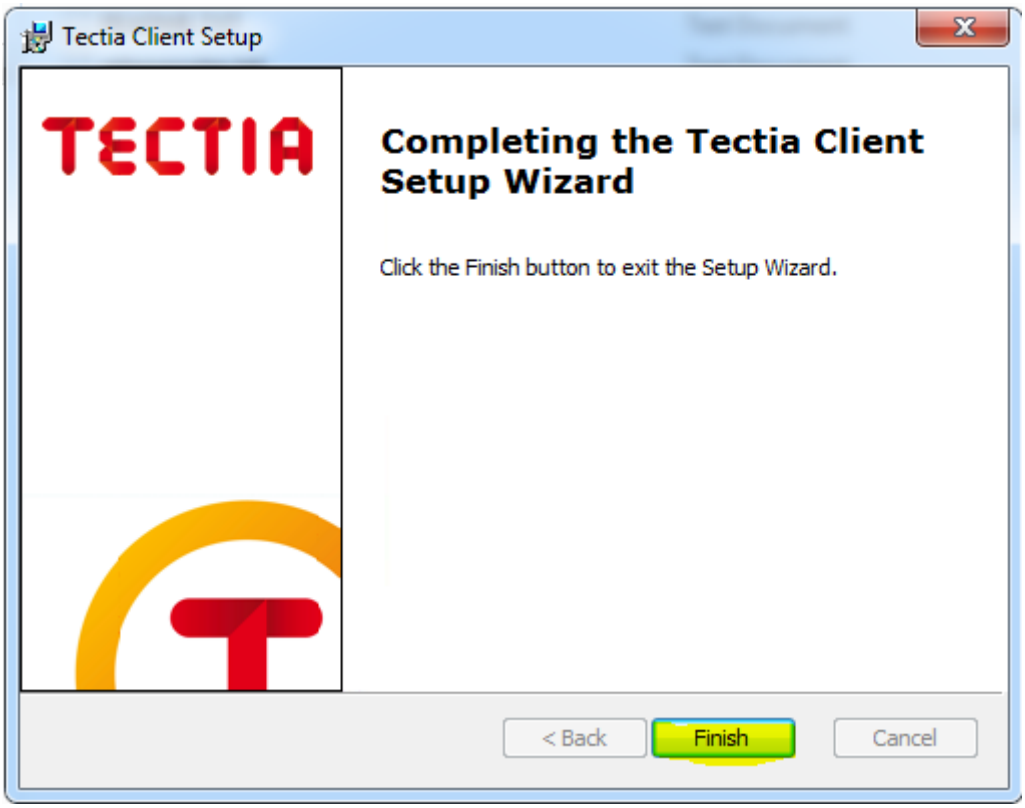
5) Click Next



6) Select Typical and click Next



7) Click Install



8) When the client is fully installed, click Finish.

9) You will now see 2 icons on your desktop. One is named “Tectia – SSH Terminal” and the second one is named “Tectia – Secure File Transfer”.

10) Reboot your computer

11) Request a Tectia license

The Tectia software you just installed only has a 45 day evaluation license, and works for all RDHPCS logons. To request an extended license, please email ONE help request to the help desk of the system you use the most. Please use the subject “Tectia license request”.

```
Theia Users: Email help tickets to:    rdhpcs.theia.help@noaa.gov

Jet Users: Email help tickets to:      rdhpcs.jet.help@noaa.gov

Gaea Users: Email help tickets to:     oar.gfdl.help@noaa.gov
```

12) Install the Tectia license. This step should be completed before your 45 day evaluation license expires.

Once you have received your “stc64.data” Tectia license file via the help system, move the file to the following location.

64-bit Windows versions

```
"C:\Program Files (x86)\SSH Communications Security\SSH Tectia\SSH Tectia
AUX\licenses"
```

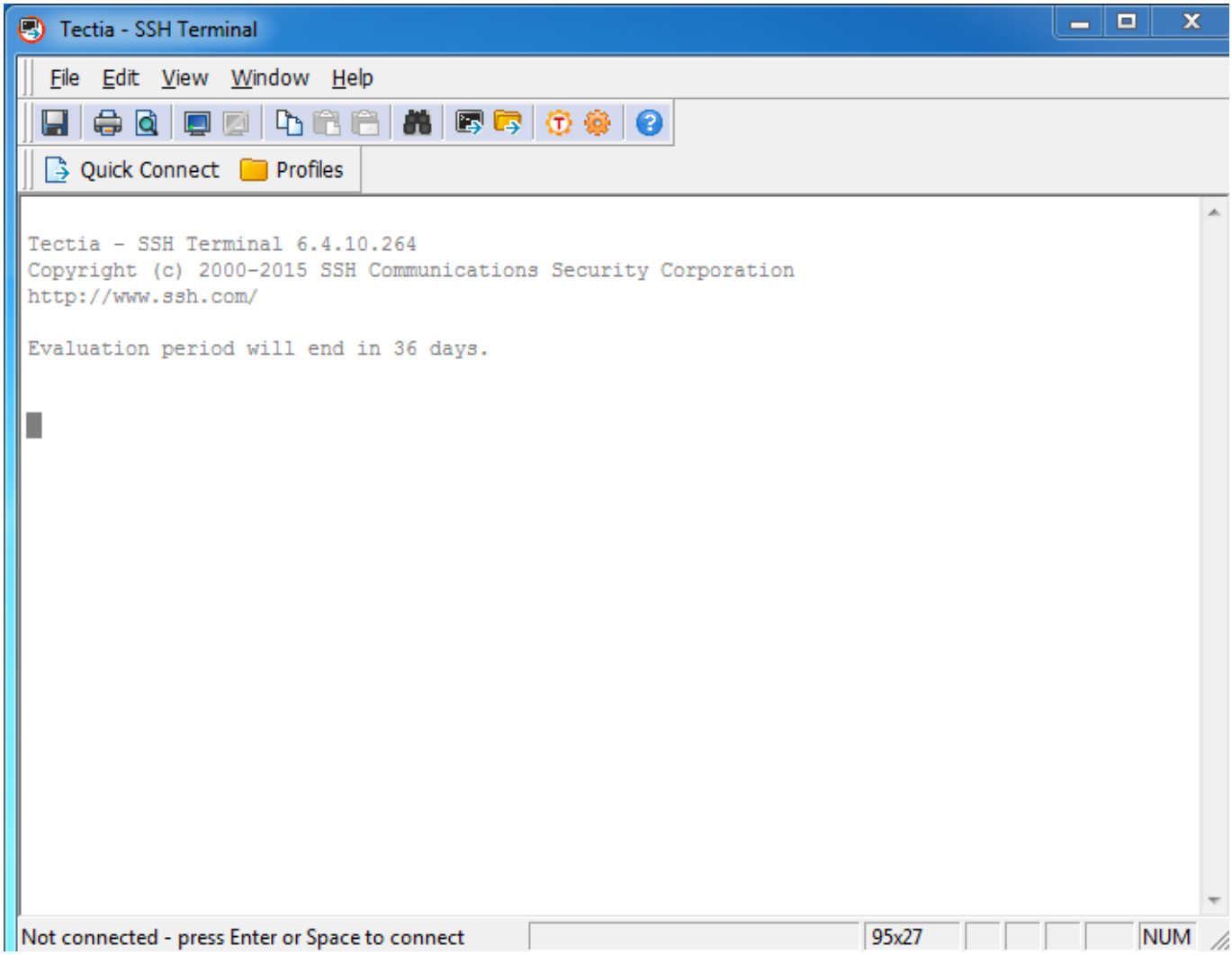
32-bit Windows versions

```
"C:\Program Files\SSH Communications Security\SSH Tectia\SSH Tectia
AUX\licenses"
```

Configuration

1) Double-click the “Tectia – SSH Terminal” icon on your desktop.

2) The following screen will appear.



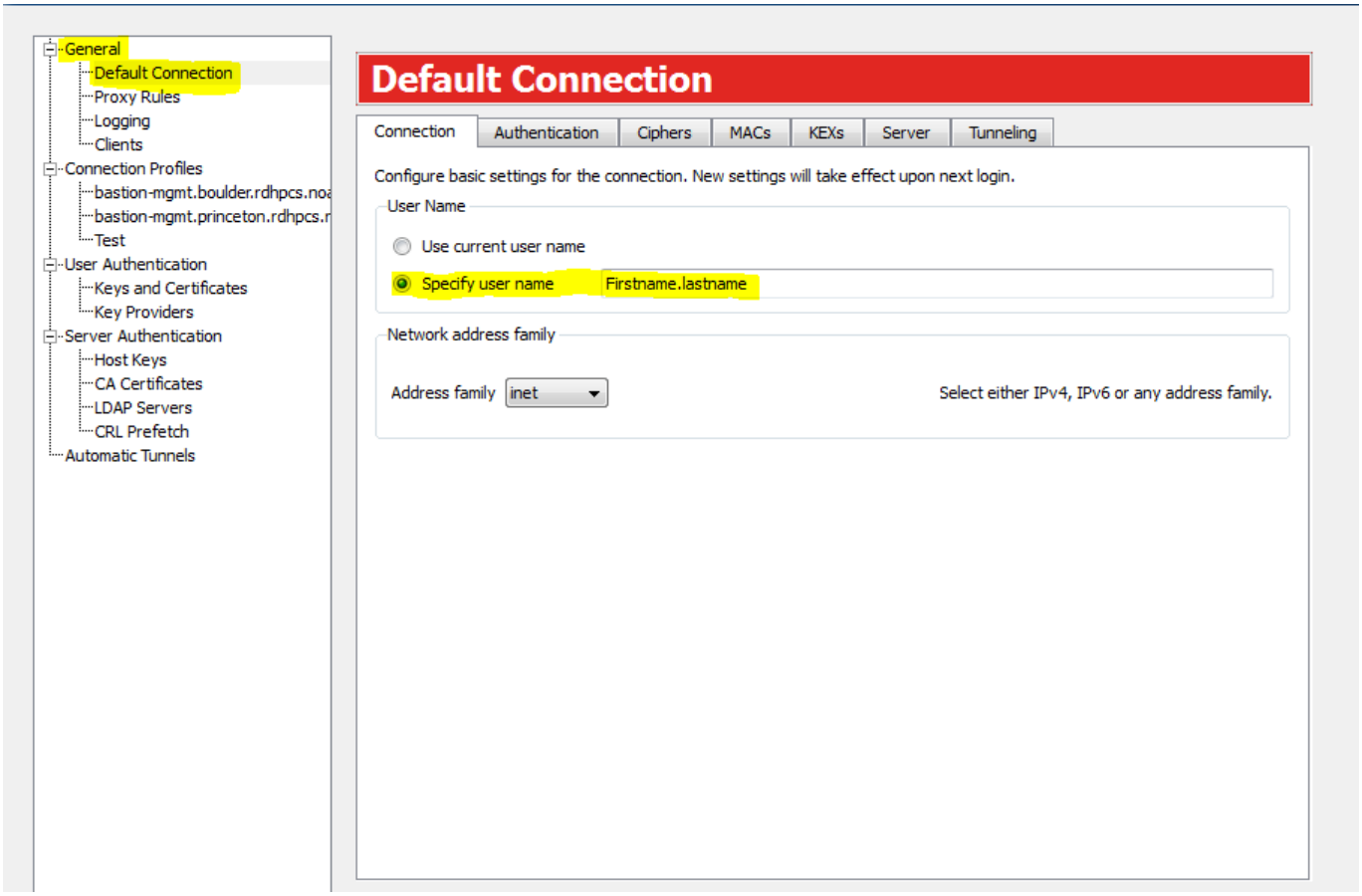
3) In the menu bar, select “Edit” > “Tectia Connections”.

4) Set your default username

In the sidebar menu select “General” > “Default Connection”

In the default “Connection” tab select “Specify user name”, and enter your user name. (your NOAA nems email Firstname.Lastname, ex: John.Smith, see: https://ai.nems.noaa.gov/). **Note:** Your user name is case sensitive. It MUST be exactly as it is in NEMS.

Select “Apply”



4a Optional: Set X windows forwarding

Select the “Tunneling” tab and check the two boxes shown below and click “Apply”

5) In the sidebar menu select “User Authentication” > “Key Providers” . Then select the “Enable Microsoft Crypto API” check box. This is needed so you can view your CAC card certificates.

Select “Apply”

6) Set up a connection profile for each host name that you want to use. There are two bastions, one in Boulder, CO and one in Princetion, NJ. It is highly recommended that you set up a profile from each bastion for each RDHPCS system you need to use, as bastions are typically down during maintenance periods.

Host names for the CAC bastion Server in Boulder, CO

```
bastion-jet.boulder.rdhpcs.noaa.gov
bastion-theia.boulder.rdhpcs.noaa.gov
bastion-gaea.boulder.rdhpcs.noaa.gov
```

Host names for the CAC Bastion Server in Princeton, NJ

```
bastion-jet.princeton.rdhpcs.noaa.gov
bastion-theia.princeton.rdhpcs.noaa.gov
bastion-gaea.princeton.rdhpcs.noaa.gov
```

In the sidebar menu select “Connection Profiles”.

Select “Add Profile” in the lower left

In the “Connection” tab: Fill out the information for the host name you are adding

Enter the “Profile Name” you want to assign to the host name you are adding (ex: Jet-BLDR bastion). Leave “Port number” =22.

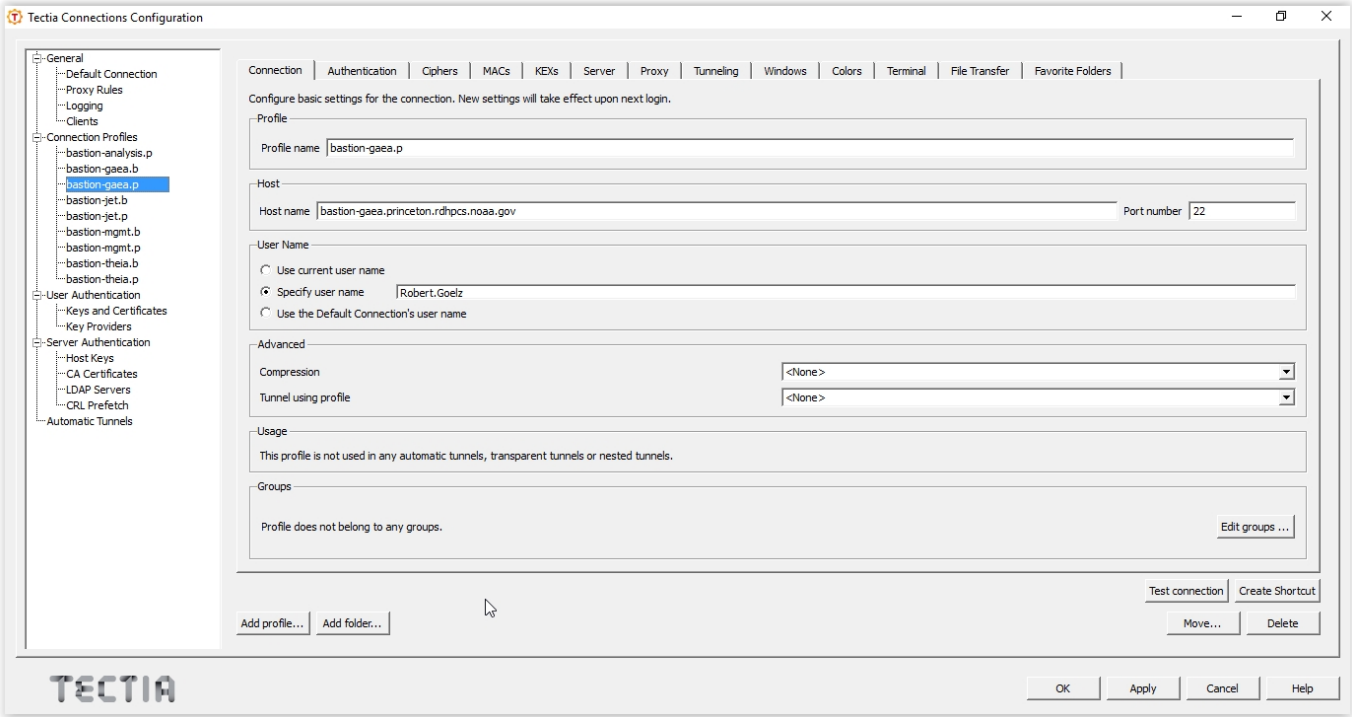
Enter the Host Name from the list above.

Select “Apply”

To add another profile select “Add Profile” in the lower left, and repeat the above steps.

Select “OK” when finished setting up all profiles

An example profile is shown below for the CAC gaea bastion in Princeton. The port used (22) is correct, as is the User Name selection (which can be set here, or just select the radio button next to “User the Default Connection’s user name”



Setting Port Forwarding for each of the profiles:

This will be necessary if you are planning to do files transfers from non-NOAA domains, or if you are planning to use Remode Desktop features such as FreeNX of X2go.

Please keep in mind the port numbers used for different bastions may be different, so be sure to get

your correct port number to use in this set up by logging in that specific host.

- Select the “Tunneling” Tab
- Select “Use Defaults” so that it will use the X11 forwarding setting that were set in Default Setting
- Select the “Add…” button
- In the steps below, replace “12345” with the unique **local port** number assigned to you when you login to Jet/Theia. Please note that port numbers are dependent on the host you are trying to connect
- “Type”= TCP
- “Listen Port”= 12345
- Select “Allow local connections only”
- “Destination host”=localhost
- “Destination port”= 12345

Click “OK”. This will populate the “Local Tunnels” tab in the configuration window as shown below:

Click “Apply” to save the profile

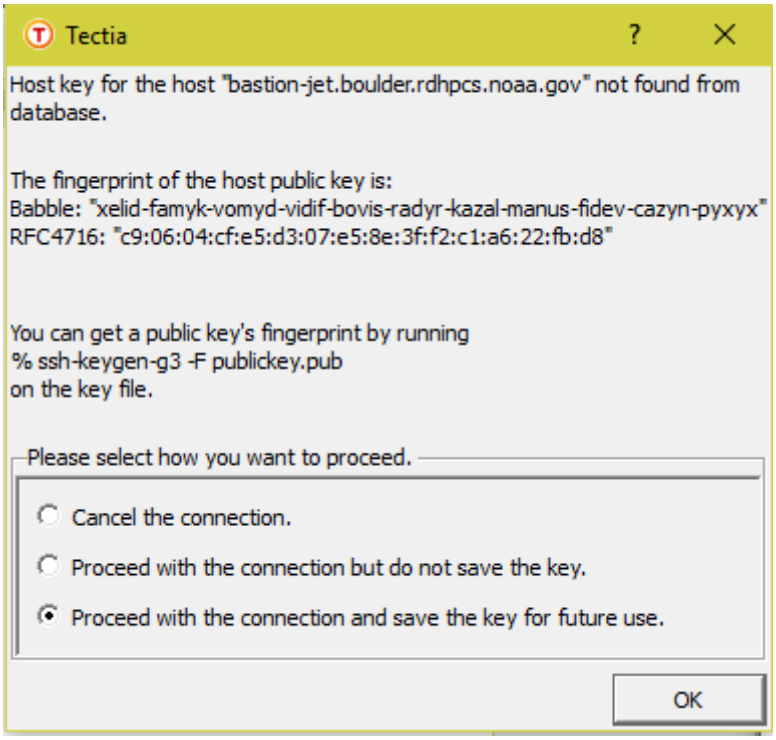
Repeat these steps for each of the profiles.

Using the Tectia SSH Client

1) Double-click the “Tectia – SSH Terminal” icon on the desktop.

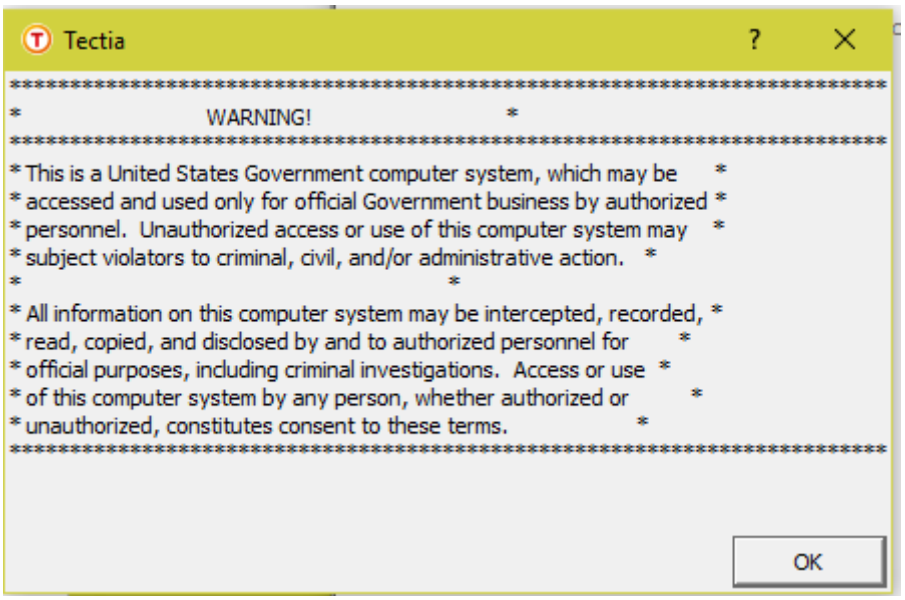
2) Click on the “Profiles” button, and select the Profile Name for the SSH connection you want to initiate

If this is your first time connecting from this local system the following screen will appear to accept the host key.

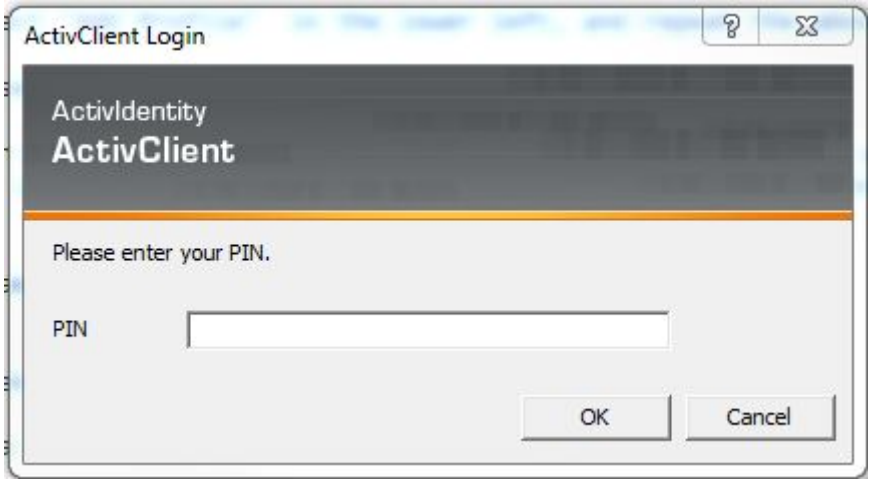


Select the 3rd option (“Proceed … and save the key for future use.”) to save the key and select “OK”.

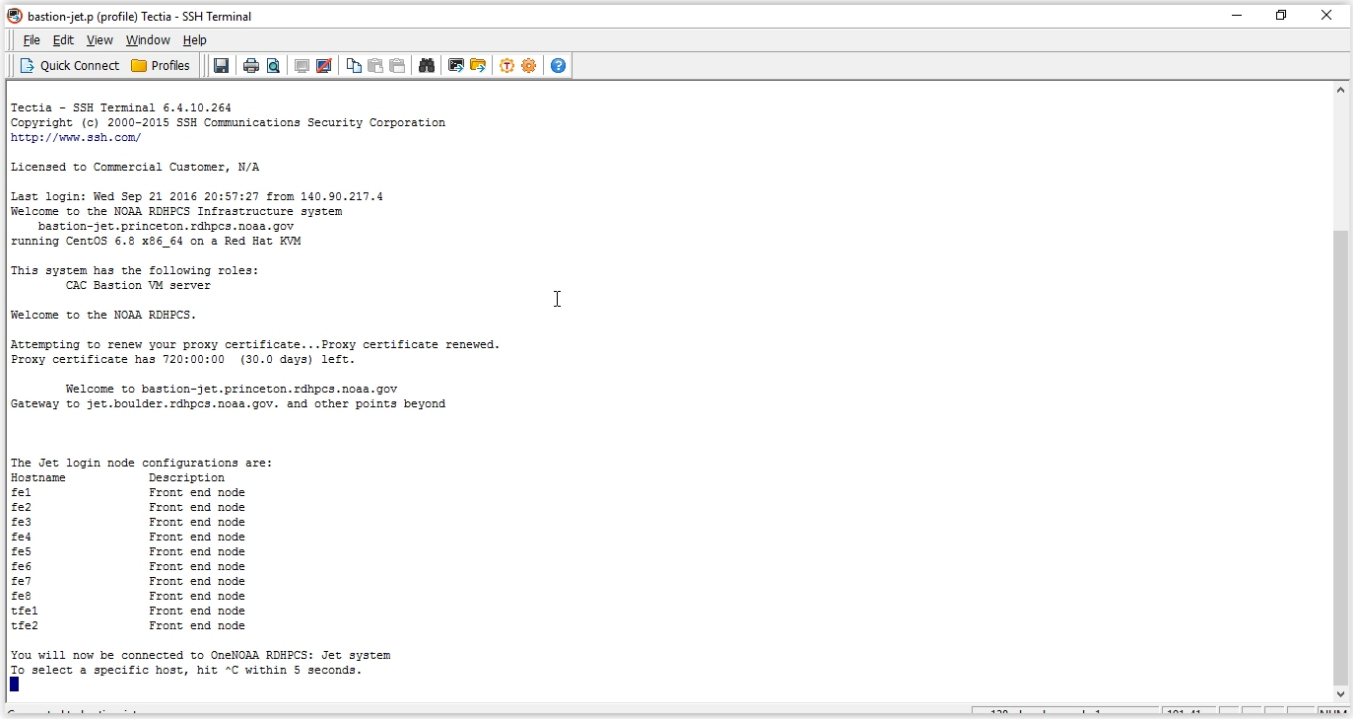
3) When you get the WARNING BANNER, select “OK”.



4) You will be prompted to enter your CAC pin.



5) You should now be authenticated through the bastion and see the Welcome Screen for the RDHPCS system. Example for Jet:



Setting up Tectia SSH Client for RHEL/CentOS

Requirements

* Tectia SSH will install on the following RHEL/CentOS version:

```
RHEL/CentOS (x86)
Version 6 and 7

RHEL/CentOS (x86_64)
Version 6 and 7
```

* In order to install the Tectia SSH Client, you must have the necessary administrator privileges. You will either need to login as the root account or be able to sudo to root using the command “sudo su -”. If you do not have this access then please notify your IT system administrator for assistance.

* The Tectia Client installation requires about 140 megabytes of disk space.

* Your system needs to have a CAC reader.

Prerequisites

* The Tetica client uses Coolkey to access the certificates on your CAC. Coolkey should be available in your distribution.

```
sudo yum install coolkey
```

Please Note: Once Coolkey is installed you will need to know the full path to the library, for example /usr/lib/pkcs11/libcoolkeypk11.so

Known Issues

* None at this time.

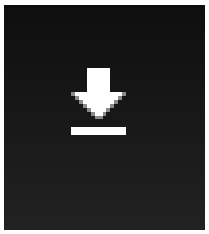
Installation

1) Download the Tectia client

Copy and paste this link into a new tab on your browser:

https://drive.google.com/open?id=0B_s-UDArdhpMMzlTQ0xLLTVEQzQ

You will have to login with your NOAA email username and password in order to be able to reach the file. Once you have authenticated and the file is shown in your browser, click on the downloaded button, located in the upper right corner of your browser.



2) Expand the archive

```
tar xf tectia-client-6.4.13.36-linux-x86_64-upgrd-eval.tar
```

NOTE: the download package includes Tectia documentation .pdf files that you can use after the basic install described here to learn more, customize, etc. Please review this documentation before requesting help beyond the scope of this basic setup procedure.

3) Change into the client directory

```
cd tectia-client-6.4.13.36-linux-x86_64-upgrd-eval/
```

4) Run the installer

```
rpm -i *.rpm
```

5) Modify your path

The Tetica client gets installed in /opt/tectia/. It is advisable to add the binary directory to your path.

If your default shell is bash then you need to edit your ~/.profile file.

```
vi ~/.profile

if [ -d "/opt/tectia/bin" ] ; then
  export PATH="$PATH:/opt/tectia/bin"
fi

if [ -d "/opt/tectia/man" ] ; then
  export MANPATH="$MANPATH:/opt/tectia/man"
fi
```

If your default shell is csh then you need to edit your ~/.cshrc file.

```
if ( -d "/opt/tectia/bin" ) ; then
  setenv PATH "$PATH:/opt/tectia/bin"
endif

if ( -d "/opt/tectia/man" ) ; then
  setenv MANPATH "$MANPATH:/opt/tectia/man"
endif
```

6) Request a Tectia license

The Tectia software you just installed only has a 45 day evaluation license, and works for all RDHPCS logons. To request an extended license, please email ONE help request to the help desk of the system you use the most. Please use the subject “Tectia license request”.

```
Theia Users: Email help tickets to rdhpcs.theia.help@noaa.gov

Jet Users: Email help tickets to rdhpcs.jet.help@noaa.gov

Gaea Users: Email help tickets to oar.gfdl.help@noaa.gov
```

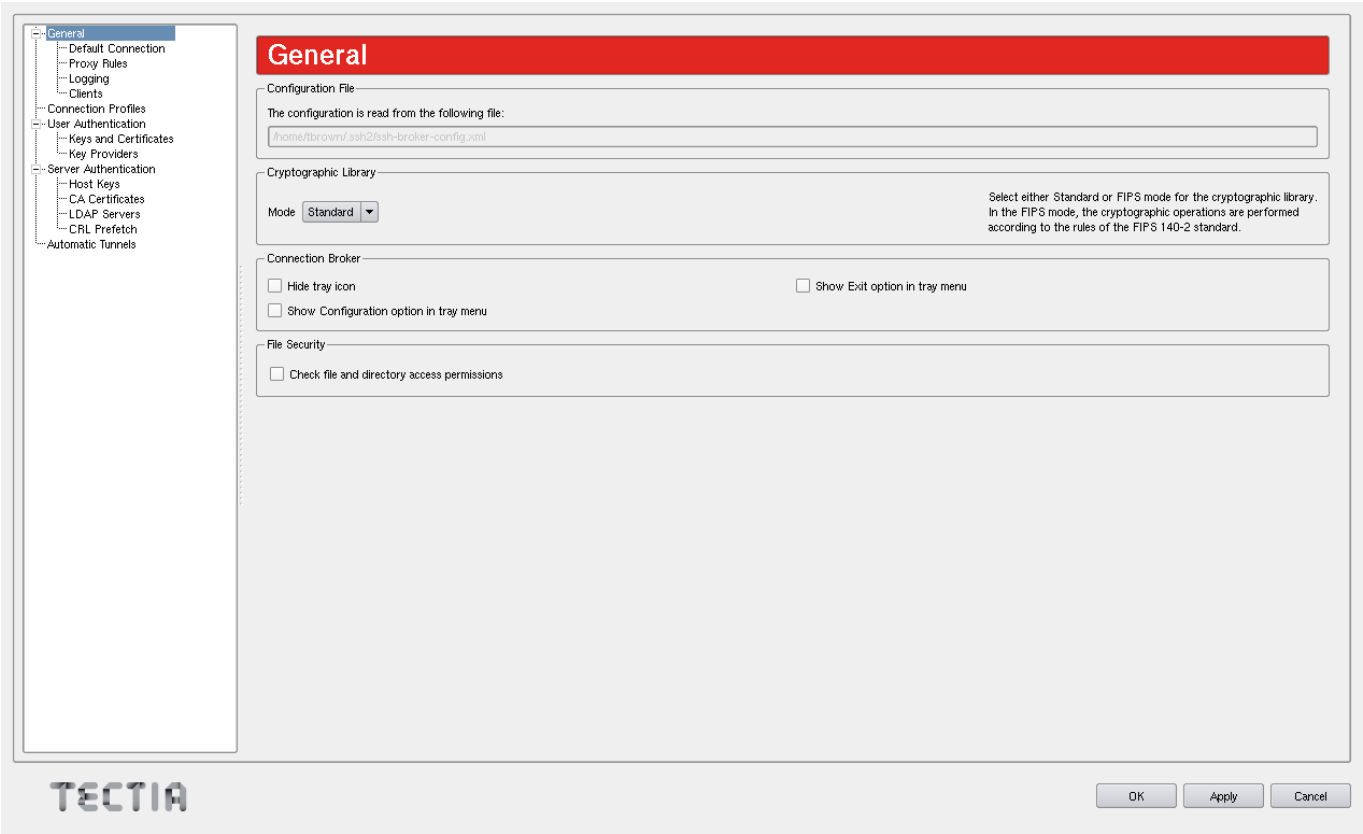
7) Install the Tectia license. This step should be completed before your 45 day evaluation license expires. Once you have received your Tectia “stc64.data” license file via the help system, create the proper directory for it and move the file to the directory.

```
cd <download directory>
mkdir /etc/ssh2/licenses/
mv stc64.dat /etc/ssh2/licenses/
```

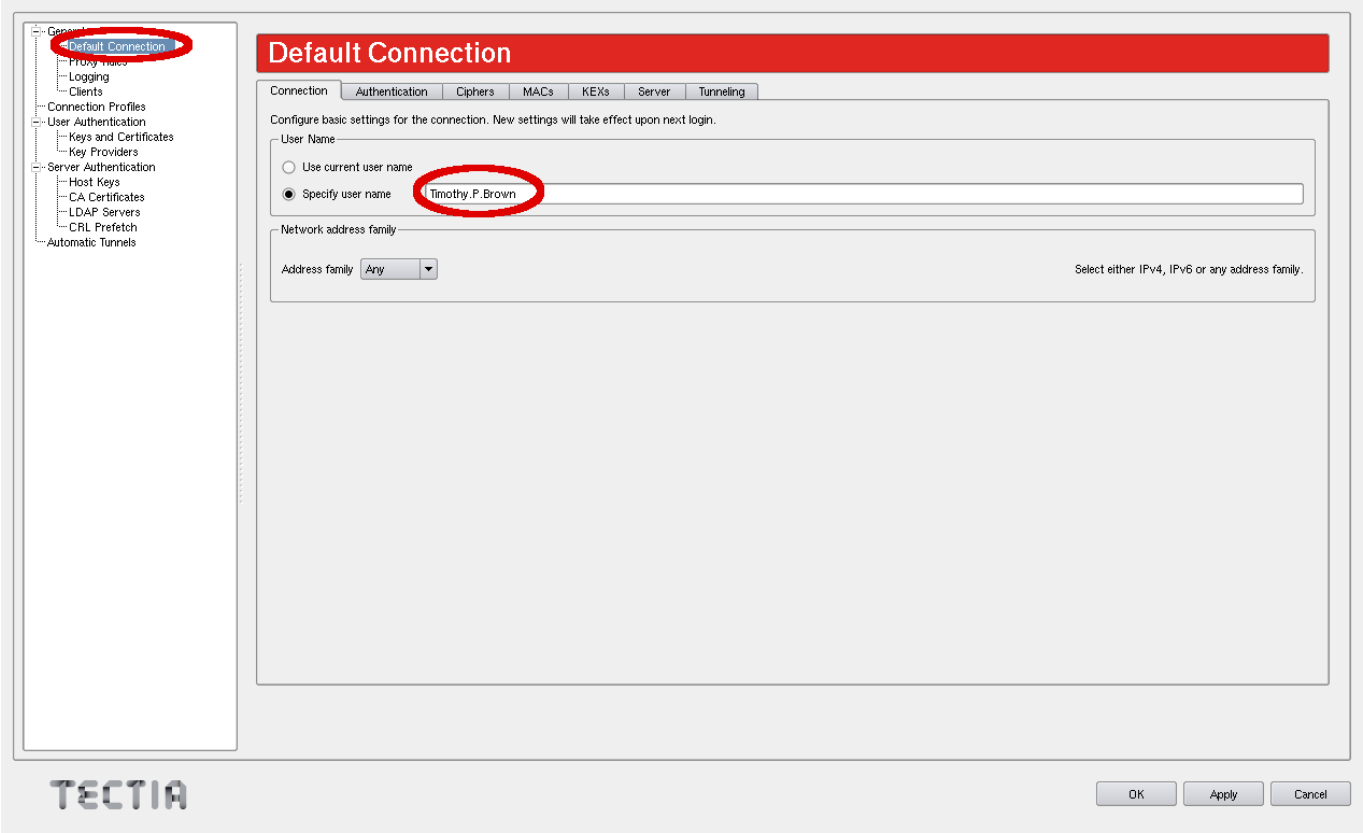
Configuration

Tetica stores it's configuration in ${HOME}/.ssh2 as an xml file called ssh-broker-config.xml. It is recommended to use the graphical configuration tool, ssh-tectia-configuration.

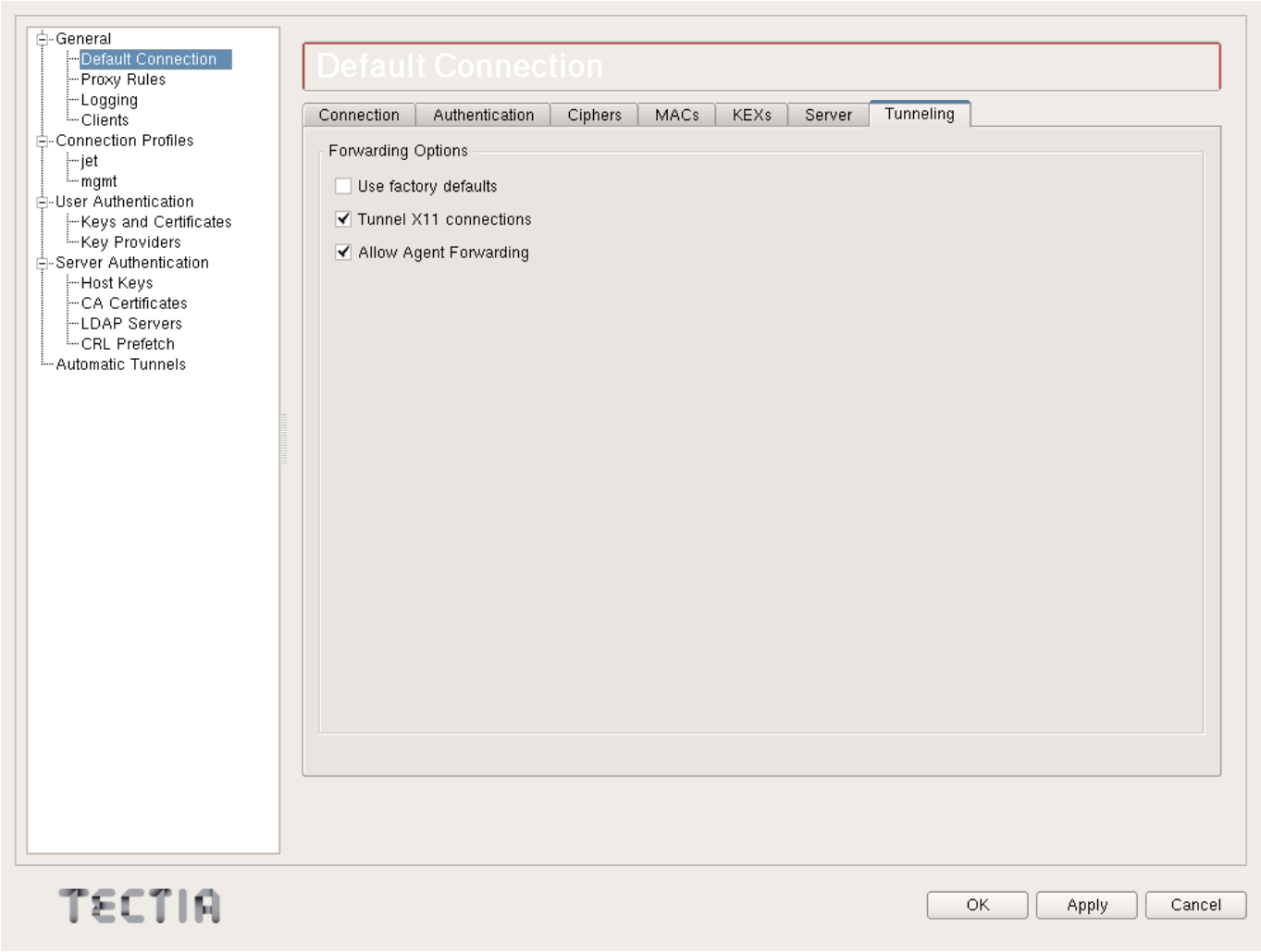
1) Launch the configuration client (ssh-tectia-configuration).



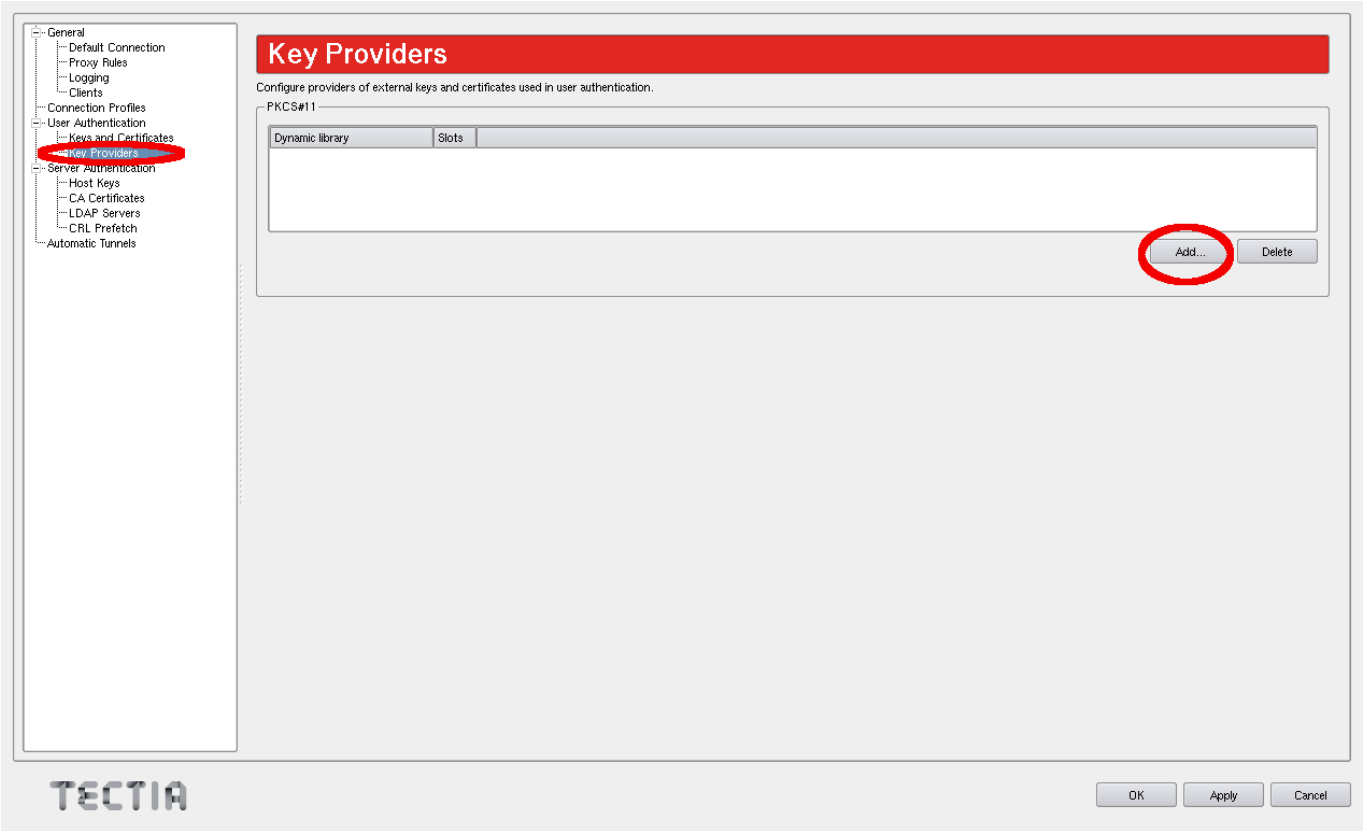
2) Set a default username under the "Default Connection" item.



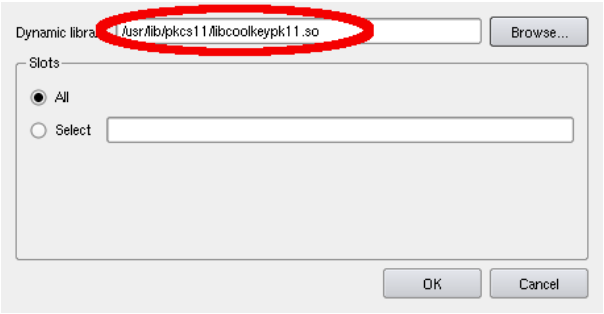
3) Enable X11 Forwarding



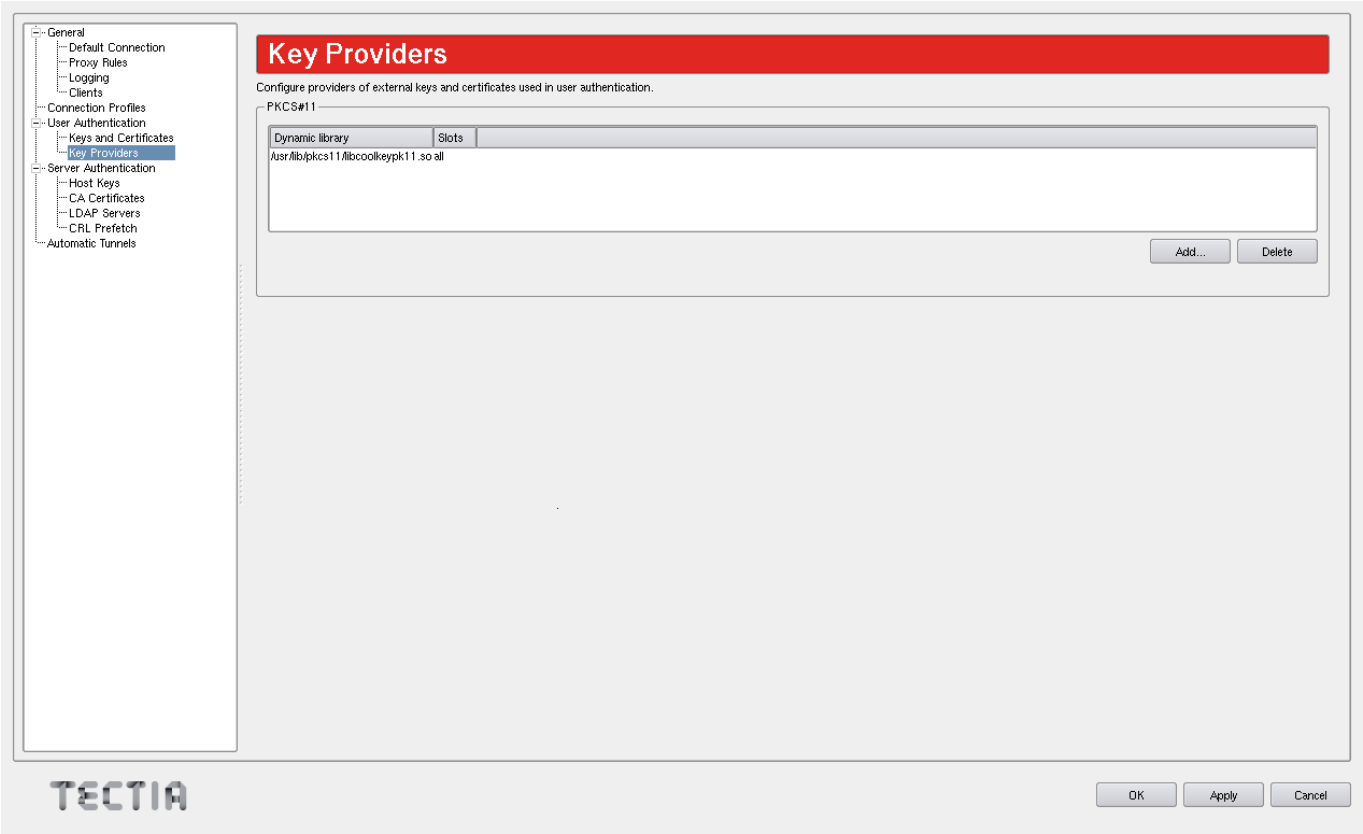
4) Add a PKCS 11 library under the “Key Providers” item.



* Click on the “Add” button.



* Add the full path to the Coolkey library. It should be “/usr/lib64/pkcs11/libcoolkeypk11.so”. Please check to make sure this is the correct location.



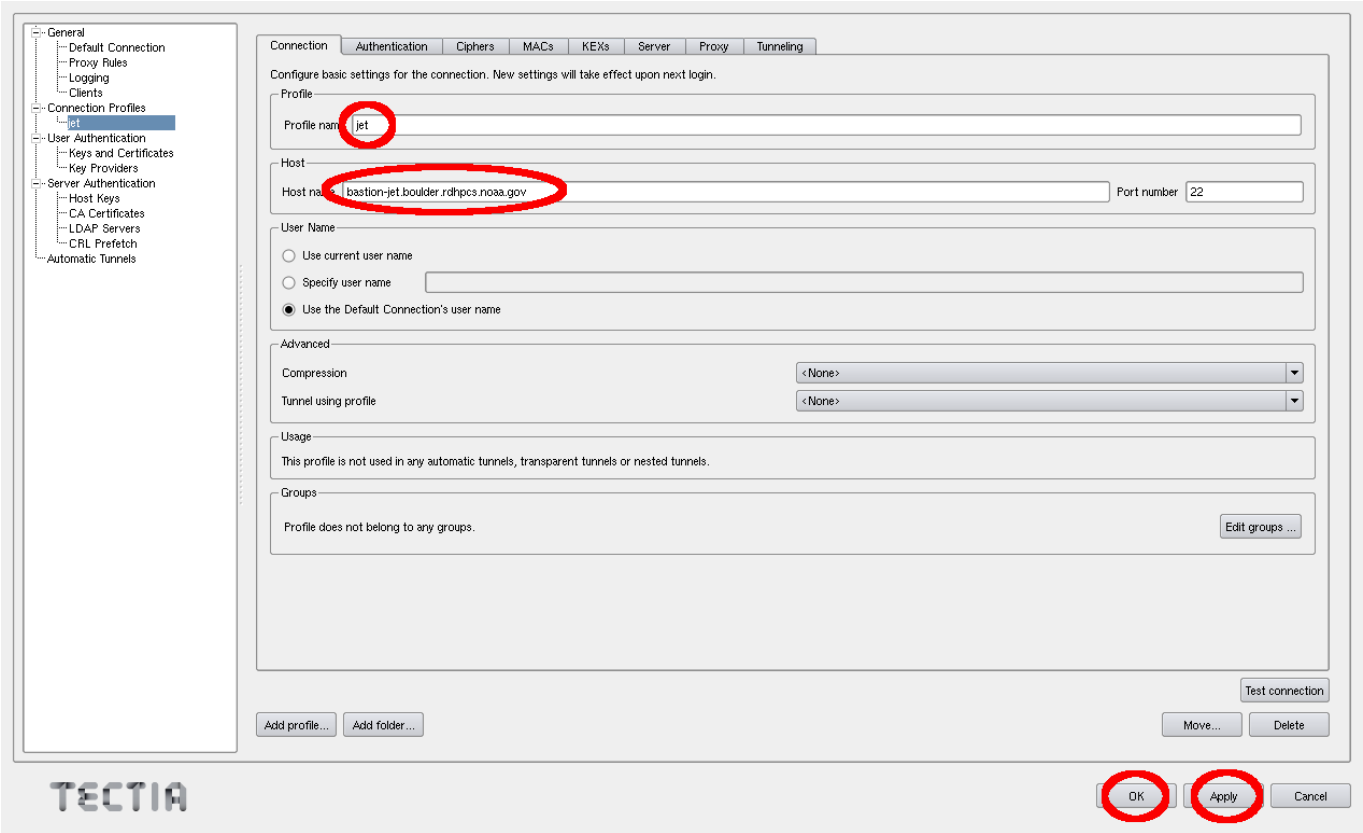
* Confirm that the PKCS 11 key providers contains the Coolkey library.

5) Add a new connection profile, under the “Connection Profiles” item.

* Set a profile name, for example “jet”.

* Set the full hostname, for exmaple “bastion-jet.boulder.rdhpcs.noaa.gov”.

* Apply the changes and then click OK.



* Once the Tetica Client has been configured, you can connect to any of the following CAC bastions.

Boulder, CO

```
bastion-jet.boulder.rdhpcs.noaa.gov
bastion-theia.boulder.rdhpcs.noaa.gov
bastion-gaea.boulder.rdhpcs.noaa.gov
```

Princeton, NJ

```
bastion-jet.princeton.rdhpcs.noaa.gov
bastion-theia.princeton.rdhpcs.noaa.gov
bastion-gaea.princeton.rdhpcs.noaa.gov
```

Using the Tectia SSH Client

Once Tetica has been configured and the binary directory has been added to your path. You can ssh into to Jet using your CAC. The Tetica ssh command is “sshg3”.

1) In a terminal window type “sshg3 jet” where “jet” is the name of the connection profile created under step 4a of the configuration.

2) You will be prompted to save and accept the key for this bastion. The RFC4716 fingerprint is “c9:06:04:cf:e5:d3:07:e5:8e:3f:f2:c1:a6:22:fb:d8” for bastion-jet.boulder.rdhpcs.noaa.gov. You need to type “save”.

3) Once the key is accepted you will be prompted for your CAC Pin (“Passphrase for the private key:”)

4) If successful you will see the message “Authentication successful.” and you will be forwarded to a

Jet front-end host.

Setting up Tectia SSH Client for Mac OS X

At this time, there is no officially supported Tectia client for Mac OS. A suitable client is currently undergoing testing. Once the testing has been completed and the the client deemed an acceptable solution, the full instructions will be defined. Until a solution is deployed, please continue to use your RSA SecureID token for remote access to R&D HPC Systems.

Requirements

Prerequisites

Installation

Configuration

Using the Tectia SSH Client

Known Issues

Testing the Port Tunneling Setup:

Once port tunneling has been setup, it will be good to test if the tunnel has been established correctly.

In order to do this, after the port tunnel has been established as described above, you should test it by trying to login using the local host and port combination. Please keep in mind you will have to use your RSA authentication for this testing.

You should try to connect using the following settings with your ssh client (with Windows you could use a client like putty, and with linux/Mac you should use ssh):

Host: localhost (This is literal string, that is, enter the word “localhost”)

Port: Your-assigned-local-port-on-thiea-jet (This is the number listed as Local Port when you login)

User: Your user name on Theia/Jet

When prompted, please enter your PIN + RSA Token as the password.

If you're able to login successfully and see your home directory, that confirms that your port tunneling is correct.

From:
https://rdhpcs-common-docs.rdhpcs.noaa.gov/wikis/rdhpcs-common-docs/ - **RDHPCS-Common-Docs**

Permanent link:
https://rdhpcs-common-docs.rdhpcs.noaa.gov/wikis/rdhpcs-common-docs/doku.php?id=cac_login&rev=1492543168

Last update: **2017/04/18 20:19**