# **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

• 2.1.3 Usage

# Linux

# **Tectia Linux Client Configuration (Goverment)**

# **Tectia Configuration Tool**

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

<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>S</u> earch	<u>T</u> erminal	<u>H</u> elp	
Garret	t.Pow	er@ops0	4:gwp> se	sh-tectia-c	onfiguration	-
						-

# **Configure Smart Card Reader**

# 1. Click on Key Providers

- General	]			
- Default Connection	Key Providers			
-Logging	Configure providers of exter	nal keys and certificates used in user	r authentication.	
Connection Profiles	PKCS#11			
User Authentication	Dynamic library	Slots		
-Keys and Certificates				
-Server Authentication				
Host Keys CA Certificates				
LDAP Servers				Add Delete
Automatic Tunnels				
200210				
ISCIIN			OK	Apply Cano

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

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

Dynamic library (lib64/coolkey/gcc4/lib	coolkeypk11.so  Browse
Slots	
<ul> <li>All</li> </ul>	
O Select	
	OK Cancel

## 3. Click Apply



#### **Create SSH Profile**

1. Click on Connection Profiles

- General	]	
-Default Connection	Connection Profiles	
-Proxy Rules		
Clients	Edit the user profile by selecting the specific profile name from the tree.	
Connection Profiles	Use the buttons below to add, rename and delete profiles	
🗄 User Authentication		
-Keys and Certificates		
E-Server Authentication		
-Host Keys		
CA Certificates		
Automatic Tunnels		
	Add profile	Move Delete
RITJET		OK Apply Can

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

on	
Connection       Authentication       Ciphers       MA         Configure basic settings for the connection. New it       Profile         Profile       Profile       Profile         Profile name       GFDL       It         Host       Host       It         Host name       ssh-cac.gfdl.noaa.gov       It         User Name       It       It         It Use current user name       Specify user name       It         Use the Default Connection's user name       Advanced       It         Compression       Tunnel using profile       It         Usage       This profile is not used in any automatic tunnels       Groups         Profile does not belong to any groups.       Profile does not belong to any groups.	VCs       KEXs       Server       Proxy       Tunneling         settings will take effect upon next login.
Add profile	Move
	OK Apply
	Connection       Authentication       Ciphers       MA         Configure basic settings for the connection. New       Profile       Profile         Profile name       GFDL       Host         Host name       ssh-cac.gfdl.noaa.gov       User Name         • User Name       Use current user name       Specify user name         • Use the Default Connection's user name       Advanced         Compression       Tunnel using profile         Usage       This profile is not used in any automatic tunnels         Groups       Profile does not belong to any groups.



# X11 Forwarding

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

- Forwarding Options -> Use Defaults: Deselect
   Forwarding Options -> Tunnel X11 connections: Select
   Forwarding Options -> Allow Agent Forwarding: Leave Selected

Tectia Connections Configura	tion _
<ul> <li>Tectia Connections Configura</li> <li>Fedault Connection         <ul> <li>Proxy Rules                 <ul> <li>Logging</li> <li>Clients</li> <li>Connection Profiles</li> <li>GFDL</li> <li>User Authentication                     <ul> <li>Keys and Certificates</li> <li>Key Providers</li> <li>Server Authentication</li></ul></li></ul></li></ul></li></ul>	Connection       Authentication       Ciphers       MACs       KEXs       Server       Proxy       Tunneling         Forwarding Options       Use Defaults       Image: Connections       Image: Connec
TECTIA	OK Apply Car

# GFDL Proxy (Mayflower) Tunnel

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

  - Enter 3128 port in Listen port field.
     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.

Tectia Connections Configuratio	n	
GeneralDefault ConnectionProxy RulesLoggingClientsConnection ProfilesAnalysisGFDLRDHPCSUser AuthenticationKeys and CertificatesKey ProvidersServer AuthenticationHost KeysCA CertificatesLDAP ServersCRL PrefetchAutomatic Tunnels	Connection       Authentication       Ciphers       MACs       KEXs       Server       Provember         Forwarding Options       Use Defaults       Use Defaults       Image: Connections       Image	xy Tunneling
	Destination host mayflower.gfdl.noaa.gov Destination port 3128 OK Cancel	
		Add Edit Delete
TECTIA	Add profile] Add folder	Move Delet

#### **Test SSH Connection**

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

	Tectia Connections Configurati	on				800 <b>-</b> 5	
٢							
	⊟-General —Default Connection	Connection Authentication	Ciphers MACs KEX	s Server Proxy	Tunneling		
	-Proxy Rules	Configure basic settings for the	connection. New settings will	take effect upon next login	1.		
	-Logging -Clients						
	Connection Profiles	Profile name GFDL					
	⊡-User Authentication     ⊡-Kevs and Certificates	-Host					
	Key Providers	Host name ssh-cac.gfdl.noa	a.gov	F	ort number 22		
	-Host Keys	User Name					
	-LDAP Servers	Use current user name					
	CRL Prefetch	O Specify user name					
		O Use the Default Connectio	n's user name				
		Advanced					
		Compression		zlib		•	
		Tunnel using profile		<none></none>			
		-Usage					
		This profile is not used in any automatic tunnels, transparent tunnels or nested tunnels.					
		Groups					
		Profile does not belong to any	y groups.			Edit groups	
						Test connectio	
		Add profile			Mo	ve Delete	
	TECTIA				ОК	Apply Can	

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

SSH Tectia	?_□ ×
Host key for the host "ssh-cac.gfdl.noaa.gov" not found from data	base.
The fingerprint of the host public key is: Babble: "xecop-beran-digyc-gocyl-hiryv-lovih-nagoh-camyk-dafus RFC4716: "a8:32:1e:f3:12:73:03:5f:94:c0:51:0a:84:97:5b:6e"	⊱puzyf-rixux"
You can get a public key's fingerprint by running % ssh-keygen-g3 -F publickey.pub on the key file.	
Please select how you want to proceed.	]
<ul> <li>Cancel the connection.</li> </ul>	
O Proceed with the connection but do not save the key.	
Proceed with the connection and save the key for future use	
	ОК

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.

SSH Tectia	3 _ 🗆	×
Token label:		
CHRISTENSEN.WILLIAM.T	HOMAS.15234	
Manufacturer:		
Passphrase for the private I	key	
	OK	

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  $\mathbf{OK}$
- 5. Click on Apply
- 6. Exit the utility



# **Tectia Linux Client Configuration (Personal)**

Installation

#### **Smart Card Reader Library**

#### RedHat / CentOS

Open a terminal window
 As root

 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

cd /path/of/tectia\_client\_download
 yum install ssh-tectia-\*

[screen 0: Garrett.Power@localhost:~] _ D
File Edit View Search Terminal Help
sudo su - [sudo] password for Garrett.Power: Last login: Thu Sep 15 04:13:02 EDT 2016 on pts/0 [root@localhost ~]# [root@localhost ~]#
<pre>[root@localhost ~]# cd /home/Garrett.Power/Downloads/tectia-client-6.4.13.36-lir ux-x86_64-comm/</pre>
[root@localhost tectia-client-6.4.13.36-linux-x86_64-comm]# [root@localhost tectia-client-6.4.13.36-linux-x86_64-comm]# [root@localhost tectia-client-6.4.13.36-linux-x86_64-comm]# yum install ssh-tect ia-*
Loaded plugins: fastestmirror, langpacks Examining ssh-tectia-client-6.4.13.36-linux-x86_64.rpm: ssh-tectia-client-6.4.13 -36.x86_64
Marking ssh-tectia-client-6.4.13.36-linux-x86_64.rpm to be installed Examining ssh-tectia-common-6.4.13.36-linux-x86_64.rpm: ssh-tectia-common-6.4.13 -36.x86_64
Marking ssh-tectia-common-6.4.13.36-linux-x86_64.rpm to be installed Examining ssh-tectia-guisupport-6.4.13.36-linux-x86_64.rpm: ssh-tectia-guisuppor t-6.4.13-36.x86_64
Marking ssh-tectia-guisupport-6.4.13.36-linux-x86_64.rpm to be installed Resolving Dependencies > Running transaction check
> Package ssh-tectia-Client.x86_64 0:6.4.13-36 will be installed > Package ssh-tectia-common.x86_64 0:6.4.13-36 will be installed > Package ssh-tectia-guisupport.x86_64 0:6.4.13-36 will be installed > Finished Dependency Resolution
Dependencies Resolved
Package Arch Version Repository Size
Installing:
x86_64 6.4.13-36 /ssh-tectia-client-6.4.13.36-linux-x86_64 8.1 M
x86_64 6.4.13-36 /ssh-tectia-common-6.4.13.36-linux-x86_64 64 M
x86_64 6.4.13-36 /ssh-tectia-guisupport-6.4.13.36-linux-x86_64 17 M
Transaction Summary
Install 3 Packages
Total size: 90 M Installed size: 90 M Is this ok [y/d/N]: y Downloading packages: Running transaction check Running transaction test Transaction test succeeded
Running transaction       1/3         Installing : ssh-tectia-common-6.4.13-36.x86_64       2/3         Installing : ssh-tectia-client-6.4.13-36.x86_64       2/3         Installing : ssh-tectia-guisupport-6.4.13-36.x86_64       3/3         Verifying : ssh-tectia-guisupport-6.4.13-36.x86_64       1/3         Verifying : ssh-tectia-client-6.4.13-36.x86_64       2/3         Verifying : ssh-tectia-client-6.4.13-36.x86_64       2/3         Verifying : ssh-tectia-client-6.4.13-36.x86_64       2/3         Verifying : ssh-tectia-client-6.4.13-36.x86_64       3/3
Installed: ssh-tectia-client.x86_64 0:6.4.13-36 ssh-tectia-guisupport.x86_64 0:6.4.13-36
Complete! [root@localhost tectia-client-6.4.13.36-linux-x86_64-comm]# [Garrett.Power@localhost ~]\$ ■

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

<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>S</u> earch	<u>T</u> erminal	<u>H</u> elp
Garret	t.Powe	er@ops0	4:gwp> ss	h-tectia-c	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

-General	Key Providers				
Proxy Rules Logging	Configure providers of extern	nal keys and certificates used in us	ser authentication.		
L. Clients	PKCS#11				
	Dynamic library	Slots			
-Keys and Certificates -Key Providers -Server Authentication -Host Keys - Coartificates					
-LDAP Servers				Add	Delete
CRL Prefetch					
922910					
1501H				OK Apply	Can

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

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

Dynamic library	/usr/lib64/pkcs11/libcoolkeypk11.so	Browse
Slots		
<ul><li>All</li></ul>		
O Select		
	OK	Cancel

# 3. Click Apply

- General	1			
Default Connection	Key Providers	;		
-Logging	Configure providers of exte	rnal keys and certificates used in user a	authentication.	
Clients	PKCS#11			
⊡-User Authentication	Dynamic library	Slots		
-Keys and Certificates Key Providers -Key Providers -Host Keys - Cot Cartificates	/usr/lib64/pkcs11/libcool	keypk11.so all		
-LDAP Servers				Add Delete
CRL Prefetch				
Automatic Tunnels				
-				
TECTIA			OI	Apply Can

# **Create SSH Profile**

1. Click on Connection Profiles

- General	]	
-Default Connection	Connection Profiles	
-Proxy Rules		
Clients	Edit the user profile by selecting the specific profile name from the tree.	
Connection Profiles	Use the buttons below to add, rename and delete profiles	
🗄 User Authentication		
Keys and Certificates		
E-Server Authentication		
-Host Keys		
CA Certificates		
Automatic Tunnels		
	Add profile	Move Delete
RITJET		OK Apply Can

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

on	
Connection       Authentication       Ciphers       MA         Configure basic settings for the connection. New set Profile       Profile       Profile         Profile name       GFDL       Image: GFDL       Image: GFDL         Host       Host name       ssh-cac.gfdl.noaa.gov       Image: GFDL         User Name       Image: GFDL       Image: GFDL       Image: GFDL         User Name       Image: GFDL       Image: GFDL       Image: GFDL         User Name       Image: GFDL       Image: GFDL       Image: GFDL         Use the Default Connection's user name       Image: GFDL       Image: GFDL         Usage       This profile       Image: GFDL       Image: GFDL         Usage       This profile is not used in any automatic tunnels       Groups         Profile does not belong to any groups.       Image: GFDL       Image: GFDL	VCs       KEXs       Server       Proxy       Tunneling         settings will take effect upon next login.
Add profile	Move
	OK Apply
	Connection       Authentication       Ciphers       MA         Configure basic settings for the connection. New       Profile       Profile         Profile name       GFDL       Host         Host name       ssh-cac.gfdl.noaa.gov       User Name         • User Name       Use current user name       Specify user name         • Use the Default Connection's user name       Advanced         Compression       Tunnel using profile         Usage       This profile is not used in any automatic tunnels         Groups       Profile does not belong to any groups.



# X11 Forwarding

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

- Forwarding Options -> Use Defaults: Deselect
   Forwarding Options -> Tunnel X11 connections: Select
   Forwarding Options -> Allow Agent Forwarding: Leave Selected

Tectia Connections Configura	tion _
<ul> <li>Tectia Connections Configura</li> <li>Fedault Connection         <ul> <li>Proxy Rules                 <ul> <li>Logging</li> <li>Clients</li> <li>Connection Profiles</li> <li>GFDL</li> <li>User Authentication                     <ul> <li>Keys and Certificates</li> <li>Key Providers</li> <li>Server Authentication</li></ul></li></ul></li></ul></li></ul>	Connection       Authentication       Ciphers       MACs       KEXs       Server       Proxy       Tunneling         Forwarding Options       Use Defaults       Image: Connections       Image: Connec
TECTIA	OK Apply Car

# GFDL Proxy (Mayflower) Tunnel

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

  - Enter 3128 port in Listen port field.
     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.

Tectia Connections Configuration	1	
GeneralDefault ConnectionProxy RulesLoggingClientsConnection ProfilesAnalysisGFDLRDHPCSUser AuthenticationKeys and CertificatesKey ProvidersServer AuthenticationHost KeysContributes	Connection       Authentication       Ciphers       MACs       KEXs       Server       Processor         Forwarding Options       Use Defaults       Use Defaults       Image: Connections       Image	xy Tunneling
-LDAP Servers -CRL Prefetch -Automatic Tunnels	Listen port 3128 Allow local connections only Destination host mayflower.gfdl.noaa.gov Destination port 3128 OK Cancel	
		Add Edit Delete
TECTIA	Add profile	OK Apply Ca

## **Test SSH Connection**

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

	Tectia Connections Configurati	on				800 <b>-</b> 5
٢						
	⊟-General —Default Connection	Connection Authentication	Ciphers MACs KEX	s Server Proxy	Tunneling	
	-Proxy Rules	Configure basic settings for the	connection. New settings will	take effect upon next login	1.	
	Clients	Profile				
	Connection Profiles	Profile name GFDL				
	⊡-User Authentication     ⊡-Kevs and Certificates	-Host				
	Key Providers	Host name ssh-cac.gfdl.noa	a.gov	F	ort number 22	
	-Host Keys	User Name				
	-LDAP Servers	Use current user name				
	CRL Prefetch	O Specify user name				
		O Use the Default Connectio	n's user name			
		Advanced				
		Compression		zlib		•
		Tunnel using profile		<none></none>		
		-Usage				
		This profile is not used in any	automatic tunnels, transparer	it tunnels or nested tunnel	S.	
		Groups				
		Profile does not belong to any	y groups.			Edit groups
						Test connectio
		Add profile			Mo	ve Delete
	TECTIA				ОК	Apply Can

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

SSH Tectia	?_□ ×
Host key for the host "ssh-cac.gfdl.noaa.gov" not found from data	base.
The fingerprint of the host public key is: Babble: "xecop-beran-digyc-gocyl-hiryv-lovih-nagoh-camyk-dafus RFC4716: "a8:32:1e:f3:12:73:03:5f:94:c0:51:0a:84:97:5b:6e"	⊱puzyf-rixux"
You can get a public key's fingerprint by running % ssh-keygen-g3 -F publickey.pub on the key file.	
Please select how you want to proceed.	]
<ul> <li>Cancel the connection.</li> </ul>	
O Proceed with the connection but do not save the key.	
Proceed with the connection and save the key for future use	
	ОК

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.

SSH Tectia	3 _ 🗆	×
Token label:		
CHRISTENSEN.WILLIAM.T	HOMAS.15234	
Manufacturer:		
Passphrase for the private I	key	
	OK	

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  $\mathbf{OK}$
- 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

General	
<ul> <li>General</li> <li>Default Connection</li> <li>Proxy Rules</li> <li>Clients</li> <li>Connection Profiles</li> <li>GFDL</li> <li>User Authentication</li> <li>Keys and Certificates</li> <li>Key Providers</li> <li>Server Authentication</li> <li>Host Keys</li> <li>CA Certificates</li> <li>LDAP Servers</li> <li>CRL Prefetch</li> <li>Automatic Tunnels</li> </ul>	Connection       Authentication       Ciphers       MACs       KEXs       Server       Proxy       Tunneling       Windows       Color       Image: Color
	This profile is not used in any automatic tunnels, transparent tunnels or nested tunnels.         Groups         Profile does not belong to any groups.         Edit groups         Test connection         Create Shorto         Add profile         Add folder
TECTIA	OK Apply Cancel He

# **Configuring Smart Card Reader**

Click on Key Providers on the left hand side.
 Check Enable Microsoft Crypto API
 Click Apply

🝸 Tectia Connections Configuration	
Context Configuration	Key Providers   Configure providers of external keys and certificates used in user authentication.   Microsoft Crypto API   PKCS#11   Unamic library     Slots     Add   Delete
TECTIA	OK Apply Cancel Help

# X11 Forwarding

- 1. Click on the **Tunneling** tab
- Check On the Funnening tab
   Uncheck Use Defaults
   Check Tunnel X11 connections
   Click Apply

#### Tunnels

VNC

Click on the **Tunneling** tab
 Click on **Add**

3. Enter VNC port in Listen Port field. (e.g. 5905)

- Enter workstation where VNC is running in Destination host field. (e.g. public2.gfdl.noaa.gov)
   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

  - Enter 3128 port in Listen port field.
     Enter mayflower.gfdl.noaa.gov in Destination host field.
  - Enter 3128 port in Destination port field.
     Click on OK.
- 3. Click on Apply.

Tectia Connections Configuration	
-General -Default Connection -Proxy Rules -Logging -Clients -GFDL -User Authentication -Keys and Certificates -Key Providers -Server Authentication -Host Keys -CA Certificates -UDAP Servers -CRL Prefetch -Automatic Tunnels	Connection       Authentication       Ciphers       MACS       KEXs       Server       Proxy       Turneling       Windows       Color         I uned X111       Connections       Iteration       Iteration </th
TECTIA	OK Apply Cancel Help

#### **Test SSH Connection**

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

<ol> <li>Tectia Connections Configuration</li> </ol>	
-General -Pofault Connection -Proxy Rules -Logging -Clients -General -Gene	Connection       uthentication       Ciphers       MACs       KEXs       Server       Proxy       Tunneling       Windows       Color       Image: Color
	Add profile     Add folder     Create Shortcut
TECTIA	OK Apply Cancel Help

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



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

(T) SSH Tectia	? X		
This server is running on an evaluation license. It will expire after 8 days. This is a United States Government computer system which may be accessed and used only for official Government business by authorized personnel Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action. All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes including criminal investigations. Access or use of this computer system by any person whether authorized or unauthorized constitutes consent to these terms.			
	ОК		

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.)

ActivClient Login	? X
ActivIdentity ActivClient	
Please enter your PIN.	_
PIN ******	
ОК	Cancel

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



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

Authentication       Ciphers       MACs       KE         ic settings for the connection. New settings will       Image: Connection is not used in any automatic tunnels, transparent       Image: Connection is not used in any groups.       Image: Connection is not used in any groups.	EXis Server Proxy Tunneling Windows Coloi   Itake effect upon next login.   Port number   22   Port number   22   It unnels or nested tunnels.   Edit groups
Add folder	Test connection     Create Shortcut       Move     Delete       OK     Apply     Cancel     Help
	Authentication       Ciphers       MACs       KE         sic settings for the connection. New settings will       e       GFDL       GFDL         ssh-cac.gfdl.noaa.gov       ssh-cac.gfdl.noaa.gov       GFDL       GFDL         rent user name       First.Last       GFDL       GFDL         n       g profile       GFDL       GFDL       GFDL         n       G profile       GFDL       GFDL       GFDL         n       G profile       GFDL       GFDL       GFDL         is not used in any automatic tunnels, transpare       GFDL       GFDL       GFDL         Add folder       GFDL       GFDL       GFDL       GFDL       GFDL

# Usage

Retrieved from "http://wiki.gfdl.noaa.gov/index.php/Remote\_Access\_via\_CAC"

- This page was last modified on 15 September 2016, at 17:13.Privacy policyAbout GFDL

- Disclaimer