The IPO Network & Security Engineering Group

GRAVITE VPN & RSA

Instructions Manual

Cisco VPN Client Installation & Profile Instructions

Cisco VPN Client for Windows

To install the VPN Client for Windows

1. Locate the setup.exe file for the Cisco VPN client for Windows that was sent to you via email or on a CD.
2. Double click the setup.exe file to begin the installation.
3. Once the installation completes you will need to reboot your computer
4. When your computer reboots launch the Cisco VPN client program to launch the VPN application
5. You now need to import the GRAVITE VPN profile (file has a .pcf extension) that was sent to you either via email or on a CD.
6. Copy the GRAVITE VPN profile locally on your computer to the folder location of your choice.
7. Click on the "import" icon on the VPN GUI application and browse to the location of the GRAVITE VPN profile to be imported.
8. You should now be able to see the GRAVITE VPN connection entry.
9. Double click the GRAVITE VPN entry to establish a VPN session to the GRAVITE VPN network.
10. You can now log on to the GRAVITE VPN service using your user name and for the passcode use your PIN code + the 6-digit code displayed on your token.

    Note: If you have not yet set up the PIN code on your GRAVITE RSA token please follow the instructions in this document to create your PIN code.
11. Use Putty or your favorite SSH client to access the GRAVITE SSH gateway as follows:
    a. For GRAVITE users accessing proc and Daq hosts you need to SSH to the IP address 192.168.9.208 (proc 8) and from there you need to SSH to the other GRAVITE hosts.
    b. For NSIPS users accessing NSIPS hosts you need to SSH to the IP address 192.168.9.221 and from there you need to SSH to the other NSIPS hosts.

Cisco VPN Client for Linux

To install the VPN Client for Linux

1. Copy the VPN Linux Client file that was sent to you via email or on a CD to a selected directory.
2. Unpack the file using the **zcat** and **tar** commands.

zcat vpnclient-linux-x86_64-4.8.02.0030-k9.tar.gz | tar xvf -

3. The command creates the vpnclient directory in the current directory
4. Obtain root privileges to run the install script
5. Enter the following commands:

cd vpnclient
./vpn_install

6. The default directories for the binaries, kernel, VPN modules, and profiles are listed during the installation process.
7. You receive the following prompts during the installation:
    a. Directory where binaries will be installed [/lib/modules/<kernel version>/build/]
    b. Automatically start the VPN service at boot time [yes]
    c. Directory containing linux kernel source code [/usr/src/linux]
    d. Is the above correct [y]

8. Press **Enter** to choose the default response. At the directory prompts, if you do not choose the default, you must enter another directory in your user's path.
9. If the installer cannot autodetect these settings, you might receive the following prompts:
    a. Directory containing init scripts:
        - The directory where scripts that are run at boot time are kept. Typically this is /etc/init.d or /etc/rc.d/init.d
    b. Directory containing run level directories (rcX.d):
        - The directory that contains init's run level directories. Typically this is /etc or /etc/rc.d
10. Enable the VPN service by using one of the following methods:
    a. Restart your computer.
    b. Enable the service without restarting. Enter the following command:

/etc/rc.d/init.d/vpnclient_init start

11. You now need to place the GRAVITE VPN profile (file has a .pcf extension) that was sent to you either via email or on a CD to the directory

/etc/CiscoSystemsVPNClient/Profiles/

12. User profile parameters include the remote server address, IPSec group name and password, use of a log file, and automatic connect upon startup. Each connection entry has its own user profile.
13. To establish a connection, enter the following command:

    vpnclient connect <profile>

    Note: The profile is the name of your GRAVITE VPN profile.

14. You will be prompted for the following:

    User name
    User password – This is your PIN code + the 6-digit code displayed on your token

    Note: If you have not yet set up the PIN code on your GRAVITE RSA token please follow the instructions in this document to create your PIN code.

15. Use your terminal to access the GRAVITE SSH gateway as follows:
    a. For GRAVITE users accessing proc and daq hosts you need to SSH to the IP address 192.168.9.208 (proc 8) and from there you need to SSH to the other GRAVITE hosts.
    b. For NSIPS users accessing NSIPS hosts you need to SSH to the IP address 192.168.9.221 (nsipsas1) and from there you need to SSH to the other NSIPS hosts.

Cisco VPN Client for Linux Install Scripts Notes

During the installation process:

1. The module is compiled, linked, and copied to either the directory /lib/modules/preferred/CiscoVPN, if it exists, or to /lib/modules/*system*/CiscoVPN, where *system* is the kernel version.
2. The application binaries are copied to the specified destination directory.
3. The startup file /etc/rc.d/init.d/vpnclient_init is created to enable and disable the VPN service.
4. The links /etc/rc3.d/s85vpnclient and /etc/rc5.d/s85vpnclient are added to run level 3 and level 5 if startup at boot time is requested.
5. These links allow the tunnel server to start at boot time and run in levels 3 and 5

GRAVITE RSA Tokens – Set Up PIN Code

Set up PIN code using the GRAVITE Web VPN page

To set up your PIN code using the GRAVITE Web VPN page:

1. Point a web browser to https://140.90.75.162/
2. Select your GRAVITE VPN Group based on the first 3-digits of your RSA Token serial number which is shown on the back of your token (follow the instructions on the GRAVITE WEB VPN web page)
3. Proceed to log in using your user name and for the initial password type in the 6 digits displayed on the RSA token
4. The VPN server will prompt you to create a PIN. The PIN must be between 4 and 8 digits. Follow the on-screen prompts.
5. You should know be logged in to a GRAVITE VPN client session.
6. Disconnect and close your browser.
7. Log on again to test and verify then PIN code of your RSA token. Using your user name and for the passcode use your PIN code + the 6-digit code displayed on your token.

   Note: The RSA token 6-digit number changes every 60 seconds and the same code can not be used twice.

Set up PIN code using the GRAVITE Cisco VPN Client

To set up your PIN code using the VPN client:

1. Launch your VPN client and connect using the GRAVITE VPN profile.
2. Log in using your user name and for the initial password type in the 6 digits displayed on the RSA token.
3. The VPN server will prompt you to create a PIN. The PIN must be between 4 and 8 digits. Follow the on-screen prompts to create and verify your PIN code.
4. You should know be logged in to a GRAVITE VPN client session.
5. Log out by clicking on "disconnect" for your GRAVITE VPN client session.
6. Try to log in again to test and verify the PIN code of your RSA token. Using your user name and for the passcode use your PIN code + the 6-digit code displayed on your token.

GRAVITE Cisco Web VPN (Clientless) Service

The following instructions describe the requirements needed for GRAVITE users to access GRAVITE host proc 8 via the GRAVITE Web VPN Clientless service. Access is provided by Port Forwarding method that use AES-128 bit encryption.

For Windows Web VPN User

1. Using either Internet Explorer or Mozilla Firefox browser go to https://gravite-vpn.ipo.noaa.gov/ to use the GRAVITE Web VPN service. Make sure your choice of browser has Java J2RE version 1.4 or greater installed.
   i. Select your GRAVITE VPN Group based on the first 3-digits of your RSA Token serial number which is shown on the back of your token (follow the instruction on the GRAVITE Web VPN web page).
   ii. Proceed to login using your username and your 2-factor RSA Token

   Note: If you have not yet set up the PIN code on your GRAVITE RSA token please follow the instructions in this document to create your PIN code.

2. After logging in you will notice a new Window will open that will run a Java applet. It is important to allow pop-ups for this GRAVITE Web VPN site if your browser is blocking pop-up windows.

3. Open PUTTY or your choice of SSH client and SSH to the following address to access GRAVITE host proc 8

   IP Address: 127.0.0.1
   Port: 2222

   Note: The GRAVITE Web VPN service utilizes Port Forwarding to redirect the address and port shown above to the SSH service on proc 8.

For Linux Web VPN User

2. If you are using x86_64 OS, you must use **32 bit Firefox browser.**

   Note: For RHEL5, 32 bit Firefox is installed by default in /usr/lib/firefox-<version>/firefox)

   i. Install jre-plugin (greater than version 1.4) in firefox, if it is not already installed.

   ii. If you don't have JRE package installed, please visit the SUN Java website link, shown below, for instructions on downloading and installing it.

   http://www.java.com/en/download/help/5000010500.xml

   Note: By default, JRE is installed at this directory: **/usr/java/jre1.6.0**

3. Enable and Configure

   i. Go to the plugins sub-directory under the Firefox installation directory **cd <Firefox installation directory>/plugins** (if the directory, plugins, is not there, create it).

   ii. In the current directory, create a symbolic link to the Java ns7/libjavaplugin_oji.so file Type:

   ln -s <Java installation directory>/plugin/i386/ns7/libjavaplugin_oji.so

   Example:

   - If Firefox is installed at this directory: **/usr/lib/firefox-3.0.14/**
   - And if the Java is installed at this directory: **/usr/java/jre1.6.0**
   - Then type at the terminal to go to the browser plug-in directory: **cd /usr/lib/firefox-3.0.14/plugins**
   - Enter the following command to create a symbolic link to the Java Plug-in for the Mozilla browser. **ln -s /usr/java/jre1.6.0/plugin/i386/ns7/libjavaplugin_oji.so**

4. Go to https://gravite-vpn.ipo.noaa.gov/ to use the GRAVITE Web VPN service

   i. Select your GRAVITE VPN Group based on the first 3-digits of your RSA Token serial number which is shown on the back of your token (follow the instruction on the GRAVITE Web VPN web page).

   ii. Proceed to login using your username and your 2-factor RSA Token

   Note: If you have not yet set up the PIN code on your GRAVITE RSA token please follow the instructions in this document to create your PIN code.

5. After logging in you will notice a new Window will open that will run a Java applet. It is important to allow pop-ups for this GRAVITE Web VPN site if your browser is blocking pop-up windows.

6. Open a terminal window and SSH to the following address to access GRAVITE host proc 8

   ssh 127.0.0.1 – p 2222

   Note: The GRAVITE Web VPN service utilizes Port Forwarding to redirect the address and port shown above to the SSH service on proc 8.

Accessing GRAVITE Hosts

The following instructions describe how the GRAVITE user can log on to the GRAVITE SSH gateway (proc 8) if it is their first time logging on with their provided GRAVITE account, and it also describes how the GRAVITE user can access other GRAVITE hosts once connected to the GRAVITE SSH gateway proc8.

Login To GRAVITE Hosts

To log on to the GRAVITE hosts using remtoe access the following are assumed.

If the user is ready to log on to the GRAVITE SSH gateway using a Cisco VPN client, then this assumes the user has already:

- Installed the Cisco VPN client on their workstation
- Imported the GRAVITE VPN profile
- Established a VPN connection to the GRAVITE network
- Provided user name and passcode credentials
- Set up their RSA token PIN code (if not done already)
- Established an SSH connection to the GRAVITE SSH gateway as follows :
    - If using a Putty – **IP address : 192.168.9.208 Port :22**
    - If using Linux terminal – **ssh 192.168.9.208**

OR

If the user is ready to log on to the GRAVITE SSH gateway using the GRAVITE Clientless Web VPN service then this assumes the user has already:

- Established a Web VPN connection to the GRAVITE network
- Selected the appropriate Web VPN Group name
- Provided user name and passcode credentials
- Set up their RSA token PIN code (if not done already)
- Established an SSH connection to the GRAVITE SSH gateway using Port Forwarding as follows :
    - If using a Putty – **IP address : 127.0.0.1 Port :2222**
    - If using Linux terminal – **ssh 127.0.0.1 –p 2222**

For both scenarios the GRAVITE user is prompted to with the login as prompt. At this prompt provide the user name that was assigned to you and press enter. At the password prompt log on with the default password Commerce.8455

user name: <your GRAVITE user account>
password: Commerce.8455

If you are not prompted to change your GRAVITE password at first log in, please do so immediately. The password policy is:

- At least 8 characters in length
- At least one numeric character
- At least one upper-case character
- At least one special character (i.e. $%#@&, etc.)

The GRAVITE remote access gateway IP address is 192.168.9.208. This is the only host you can connect to from the VPN session. Once logged in to 192.168.9.208, you can ssh to all other GRAVITE hosts. A list of our current hosts, their IP addresses, host names and functions is shown below.

Host Name	**IP Address**	**Function**
proc1	192.168.9.201	Application server
proc2	192.168.9.202	Application server
proc3	192.168.9.203	Application server
proc4	192.168.9.204	Application server
proc5	192.168.9.205	Application server
proc6	192.168.9.206	Application server
proc7	192.168.9.207	Application server
proc8	192.168.9.208	Application server / remote access gateway
gdp1	140.90.208.20	GRAVITE Data Portal (public access)
daq2	192.168.9.231	File server
daq3	192.168.9.215	File server
arch1	192.168.9.216	Archivist Server
sdsrs	192.168.9.230	SDS RIP Server

Note: host gdp1 is publicly-accessible and resides in a DMZ. It is only accessible via ssh from host daq2.

Accessing GRAVITE-NSIPS Hosts

The following instructions describe how the GRAVITE-NSIPS user can log on to the GRAVITE-NSIPS SSH gateway (nsipsas1) if it is their first time logging on with their provided GRAVITE-NSIPS account, and it also describes how the GRAVITE-NSIPS user can access other GRAVITE-NSIPS hosts once connected to the GRAVITE-NSIPS SSH gateway 192.168.9.221.

Login To GRAVITE-NSIPS Hosts

To log on to the GRAVITE-NSIPS hosts using remtoe access the following are assumed.

If the user is ready to log on to the GRAVITE-NSIPS SSH gateway using a Cisco VPN client, then this assumes the user has already:

- Installed the Cisco VPN client on their workstation
- Imported the GRAVITE VPN profile
- Established a VPN connection to the GRAVITE network
- Provided user name and passcode credentials
- Set up their RSA token PIN code (if not done already)
- Established an SSH connection to the GRAVITE-NSIPS SSH gateway as follows :
    - If using a Putty – **IP address : 192.168.9.221 Port :22**
    - If using Linux terminal – **ssh 192.168.9.221**

At this stage the GRAVITE-NSIPS user is prompted to with the login as prompt. At this prompt provide the user name that was assigned to you and press enter. At the password prompt log on with the default password Commerce.8455

user name: <your GRAVITE-NSIPS user account>
password: Commerce.8455

If you are not prompted to change your GRAVITE-NSIPS password at first log in, please do so immediately. The password policy is:

- At least 8 characters in length
- At least one numeric character
- At least one upper-case character
- At least one special character (i.e. $%#@&, etc.)

The GRAVITE remote access gateway IP address is 192.168.9.221 (nsipsas1). This is the only host you can connect to from the VPN session. Once logged in to 192.168.9.221, you can ssh to all other GRAVITE-NSIPS hosts. A list of our current hosts, their IP addresses, host names and functions is shown below.

Host Name	IP Address	Function
nsipsas1	192.168.9.221	NSIPS server
nsipsxs1	192.168.9.222	NSIPS server
nsipsds1	192.168.9.223	NSIPS server
nsipsts	192.168.9.224	NSIPS server
nsipsxs	192.168.9.225	NSIPS server
nsipsas	192.168.9.226	NSIPS server
nsipsds	192.168.9.227	NSIPS server

Note: host nsipsps is publicly-accessible and resides in a DMZ. It is only accessible via ssh from host 192.168.9.221 (nsipsas1).