

Network Connect Installation and Usage Guide

- I. Installing the Network Connect Client.....2**
- II. Launching Network Connect from the Desktop.....7**
- III. Launching Network Connect from the IVE Credential Provider.....9**
- IV. Installing Network Connect without stored domain credentials13**
- V. Troubleshooting Network Connect.....14**

Installing the Network Connect Client

NOTE

- *The computer must be connected to an external (off-state network) Internet connection.*
- *If you **do not** have a user profile on the computer **AND** you **do not** have access to a LAN connection to create a user profile, skip the steps below and go directly to page 13 to install Network Connect. If Network Connect is already installed (you can verify this if the IVE credential provider is visible as shown on page 10-12), then go to page 13 and start with step 8.*

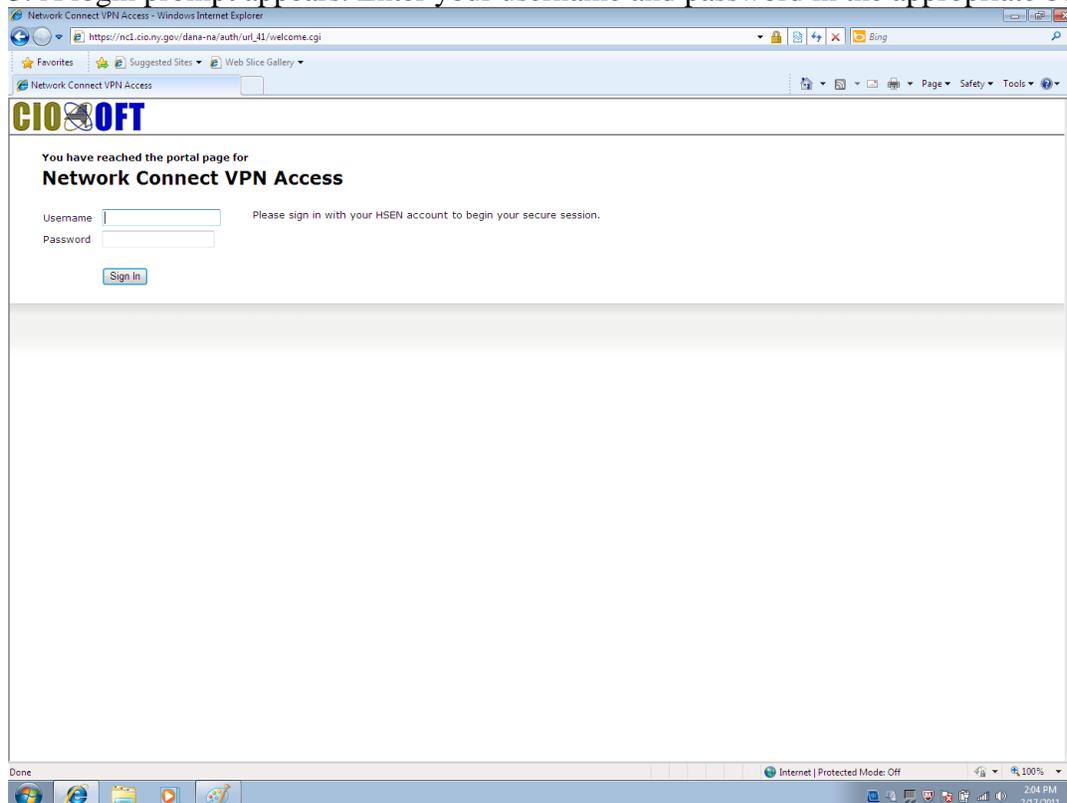
1. Sign into the computer using your domain account.

2. Launch a browser.

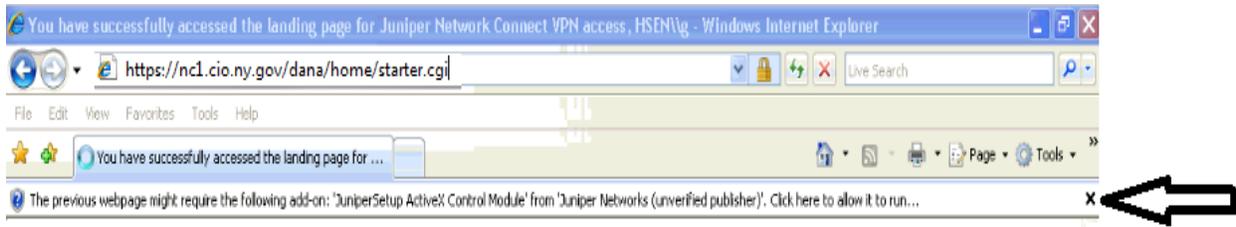
a. If you will be using an HSEN domain account to access the network, type <https://nc1.cio.ny.gov/hsen> into the address bar and select *Enter*.

b. If you will be using an NYS domain account to access the network, type <https://nc1.cio.ny.gov/nys> into the address bar and select *Enter*.

3. A login prompt appears. Enter your username and password in the appropriate boxes.



4. The Host Checker module will load and verify your computer meets CIO/OFT security requirements. If you receive a request to allow the ActiveX control to run, click the information bar to allow it to run.



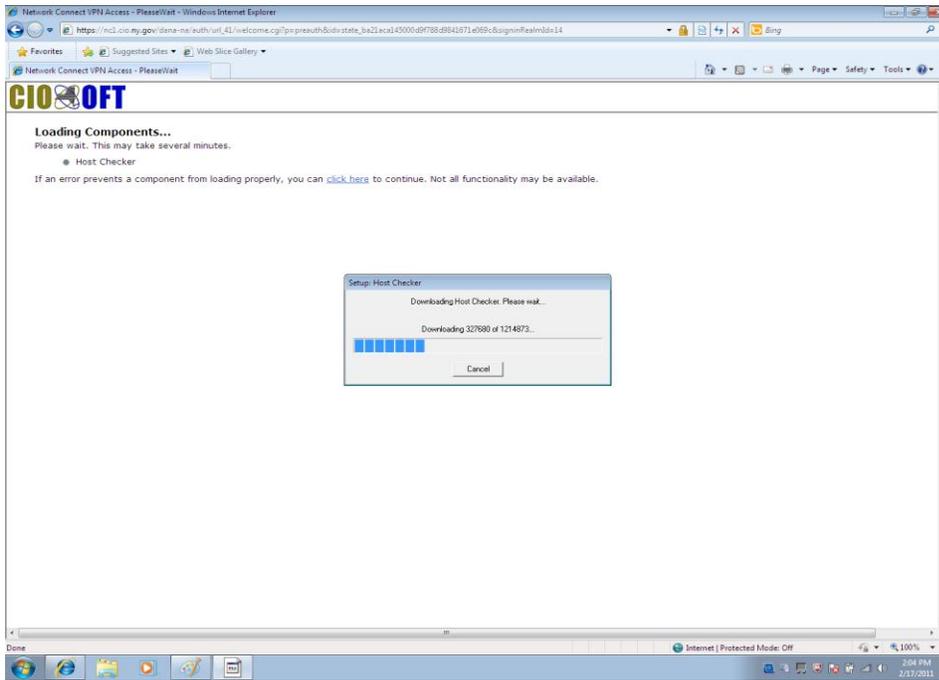
5. Select *Run* to allow the Juniper ActiveX component to load.



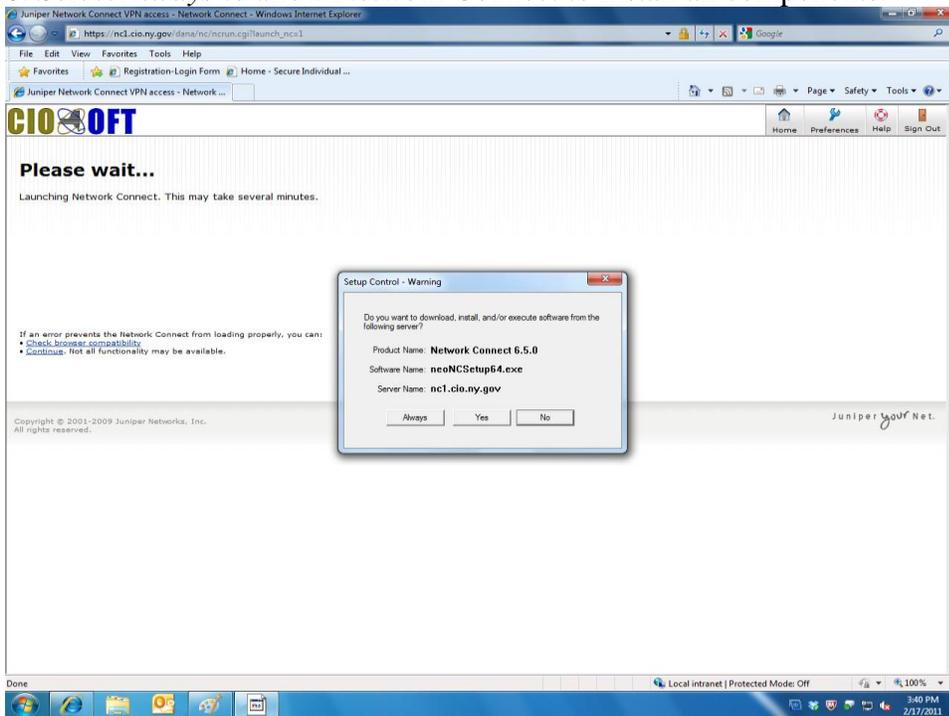
6. If you receive a request to install the JuniperSetupSP1.cab file, click *Install*.



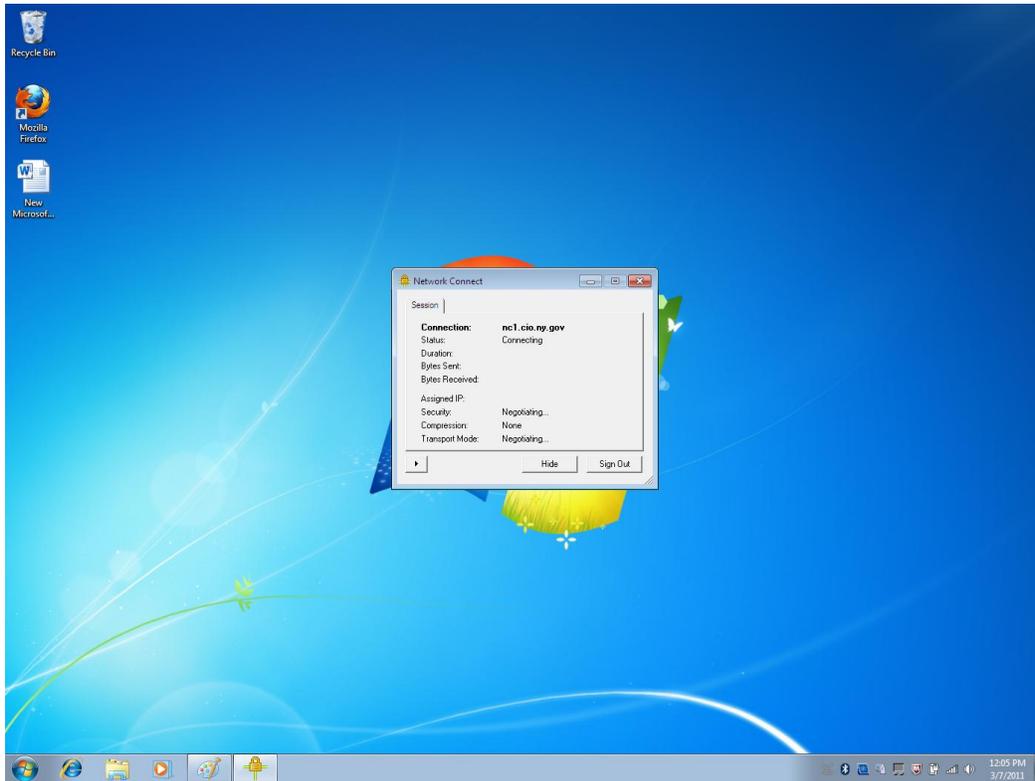
7. The Juniper Network Connect installation will begin. A progress bar appears, indicating that the Host Checker application is downloading.



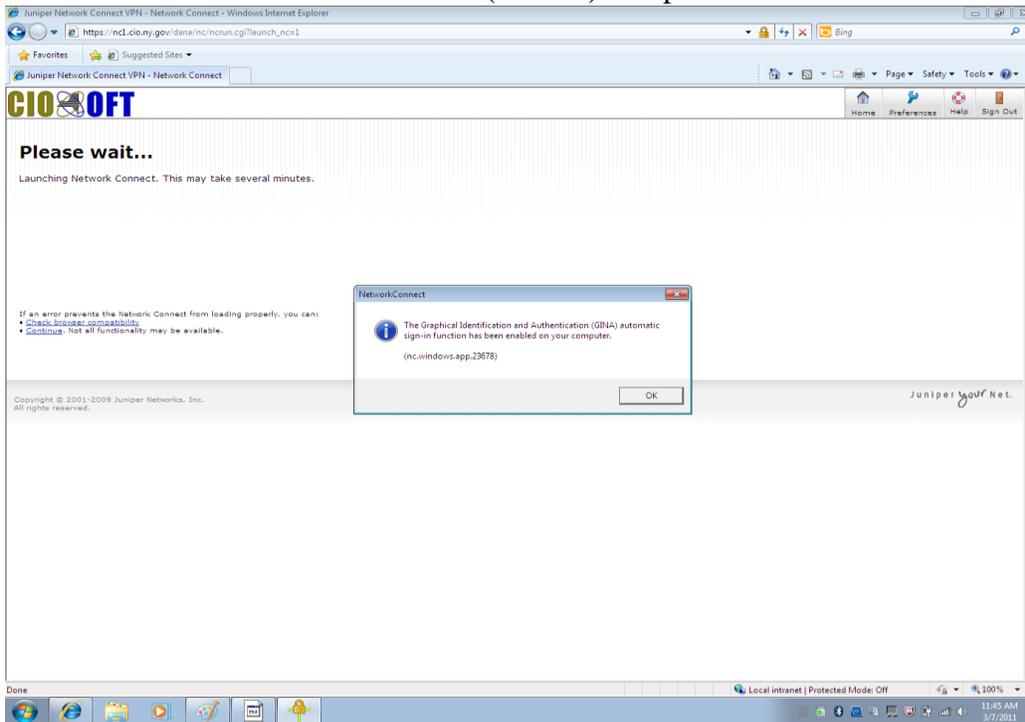
8. Select *Always* to allow Network Connect to install all components.



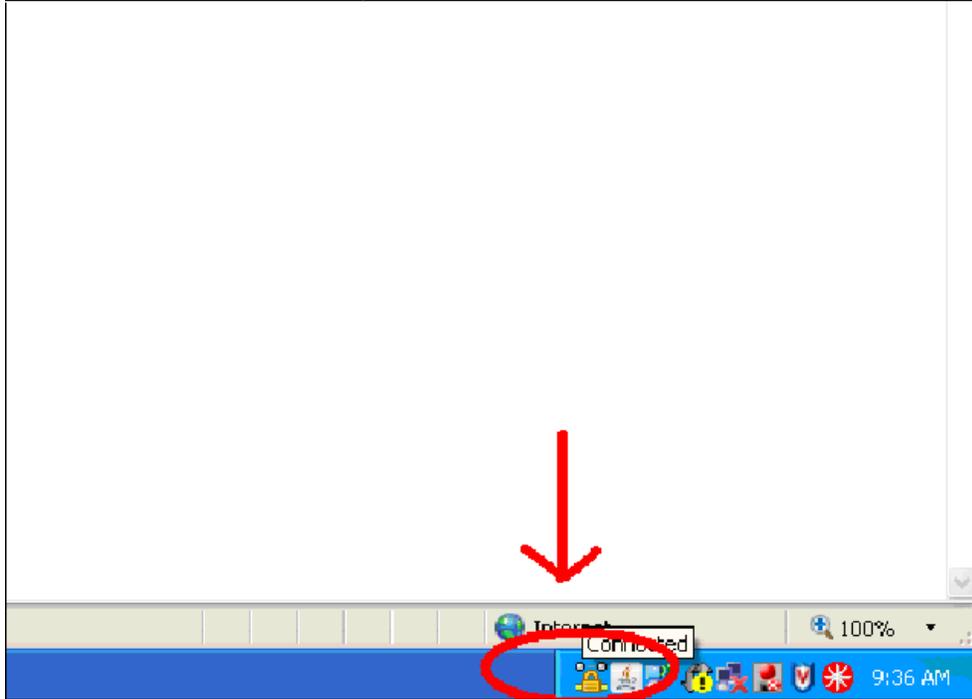
9. The Network Connect client will install and a VPN session will be initialized.



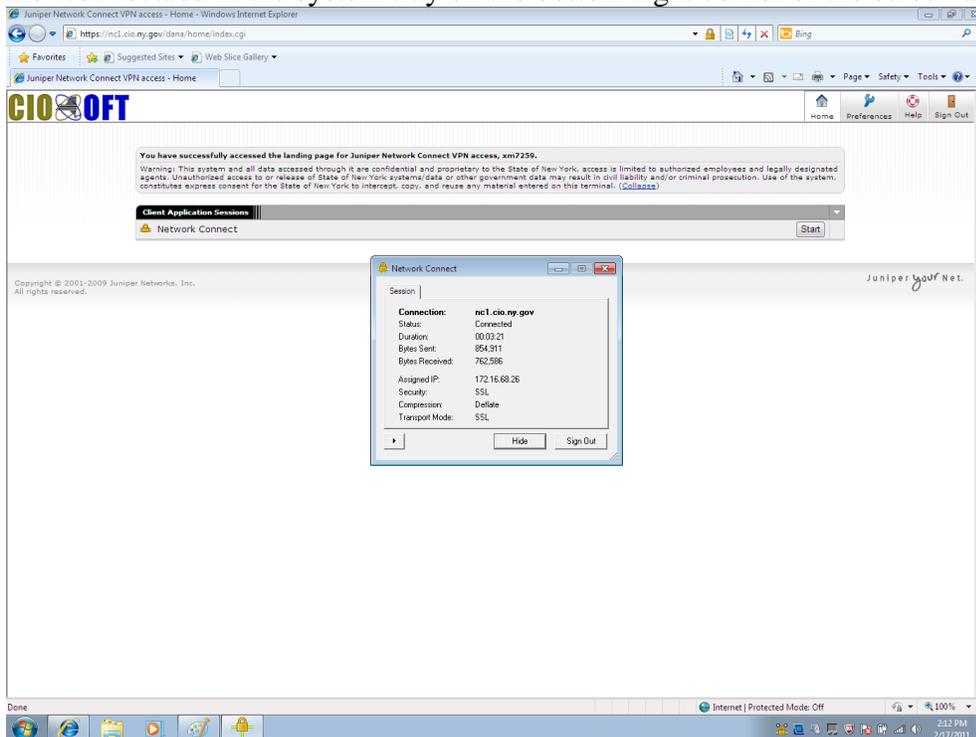
10. The IVE Credential Provider (GINA) component is enabled. Click OK.



11. Upon a successful connection, the Network Connect window will minimize to the system tray on the bottom right hand corner of the screen. You may minimize or close your browser window. This will not close your VPN session.

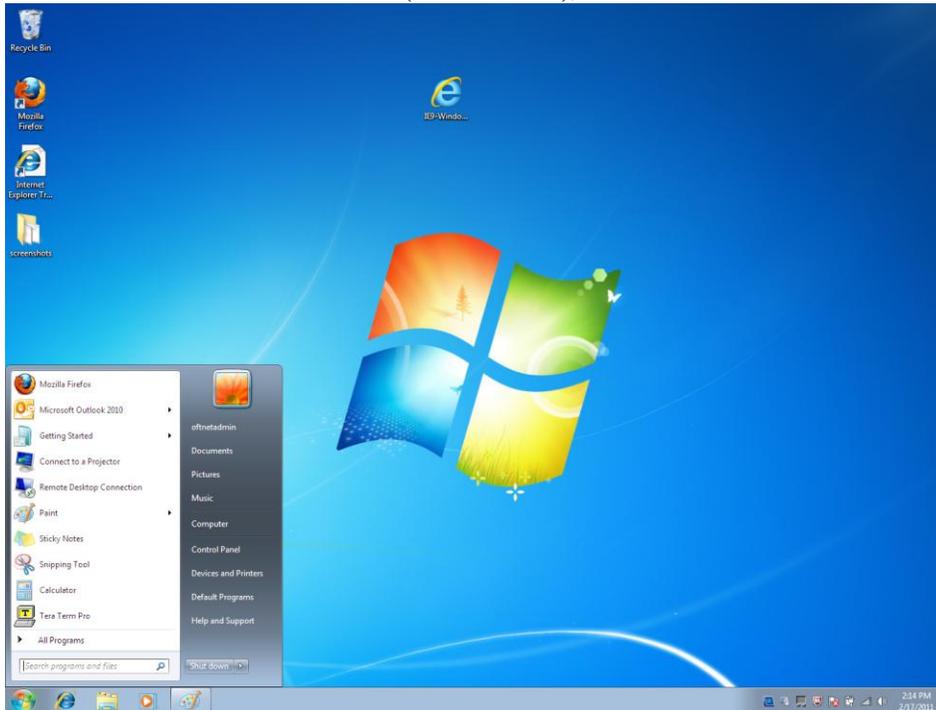


12. When finished with your VPN session, close the Network Connect client by double clicking the icon located in the system tray on the bottom right corner of the screen and select *Sign Out*.

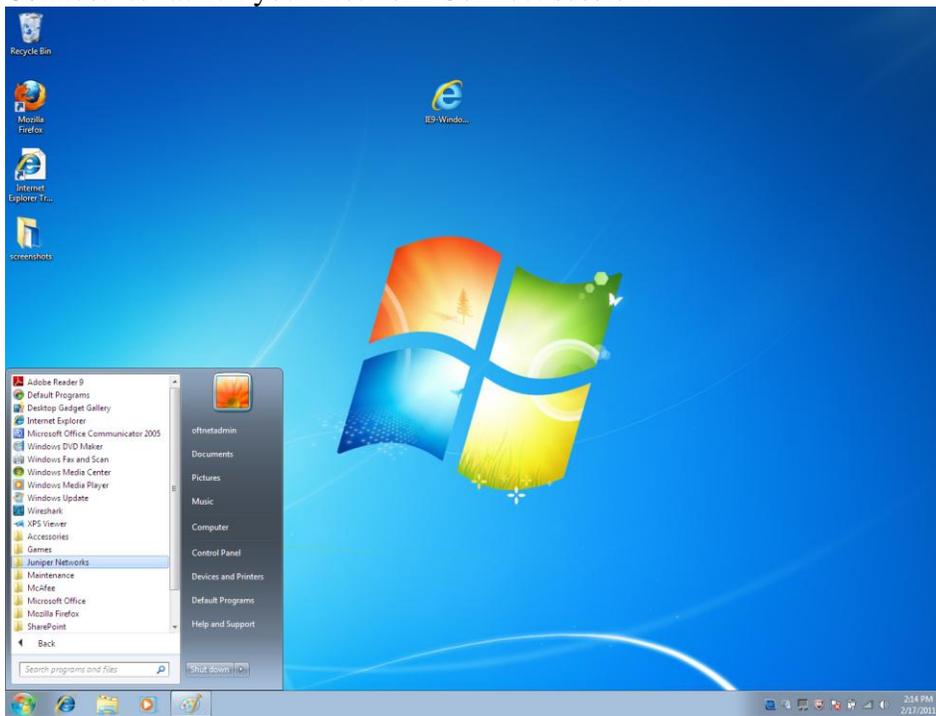


Launching Network Connect from the Desktop

1. Select the Windows Ribbon (Start button), located at the bottom left corner of the screen.

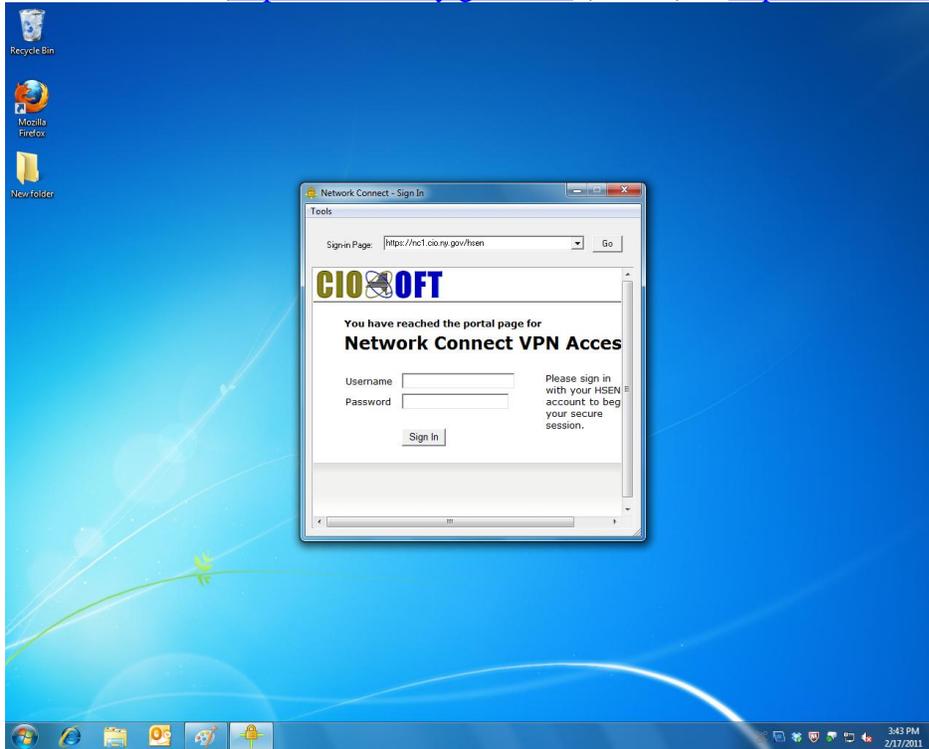


2. From the *All Programs* menu, select *Juniper Networks / Network Connect 6.5.0 / Network Connect* to launch your Network Connect session.

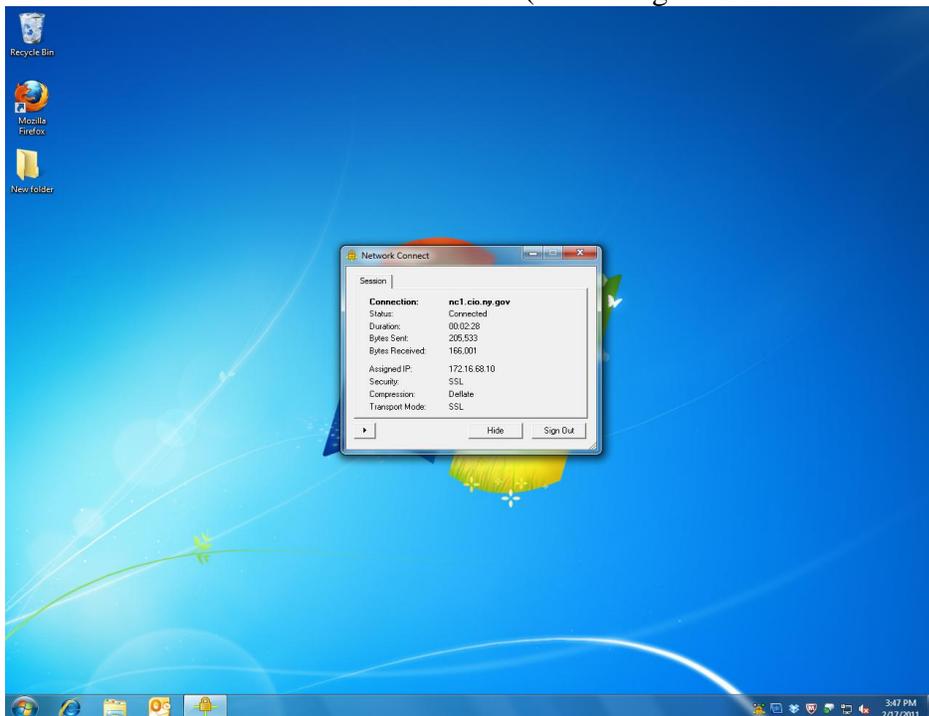


3. The Network Connect Sign In page appears.

* If you experience an issue connecting to Network Connect, verify that the address in the sign-in box is correct (<https://nc1.cio.ny.gov/hsen> (HSEN) or <https://nc1.cio.ny.gov/nys> (NYS)).



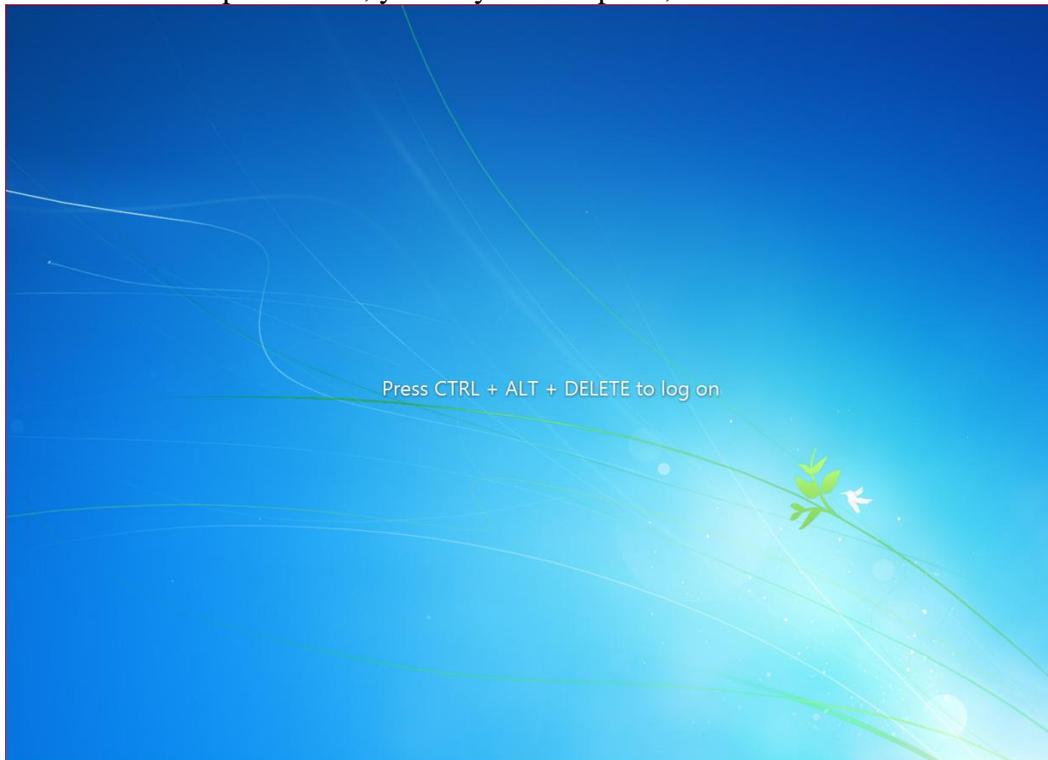
4. Upon a successful connection, the Network Connect window will minimize to the taskbar in the bottom right hand corner of the screen. To close the Network Connect client, double click the icon located in the Windows taskbar (bottom right corner of the screen) and select *Sign Out*.



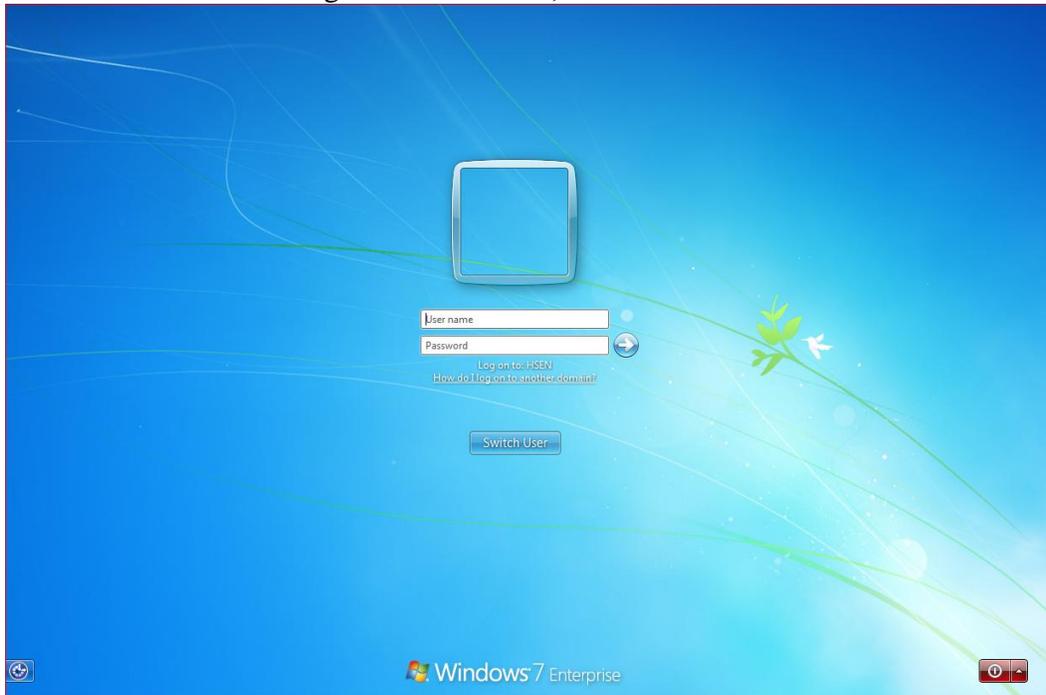
Launching Network Connect from the IVE Credential Provider

Juniper permits the Windows credential provider, formerly known as GINA, to establish a Network Connect session using the IVE Credential Provider prior to Windows login. To use the IVE credential Provider module you must sign out of Network Connect VPN (See page 6, step 12). After the initial download of Network Connect, you must restart the computer. If the machine is simply logged out of, the credential provider component will not appear.

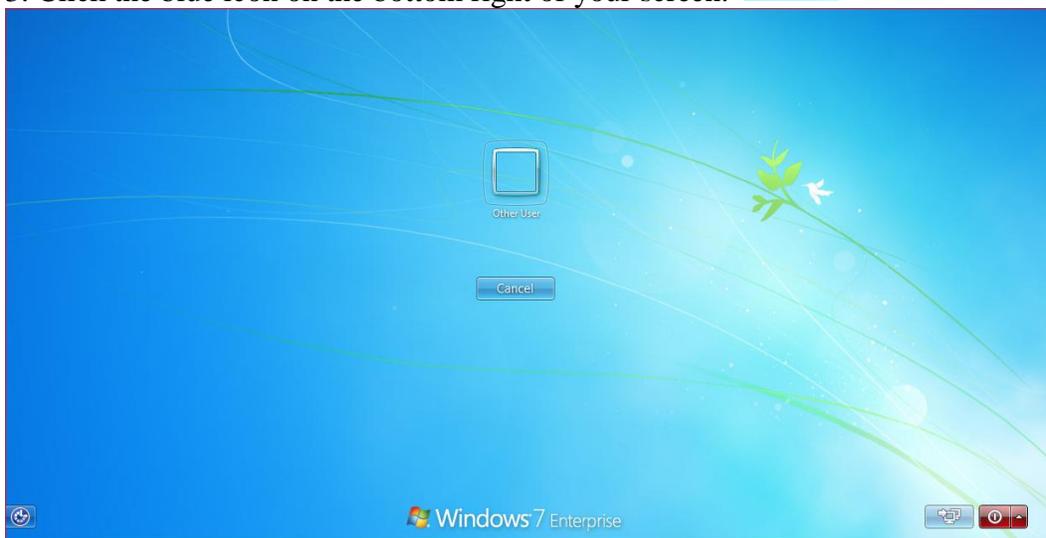
1. When the computer loads, you may need to press, CTRL + ALT + DELETE to log on.



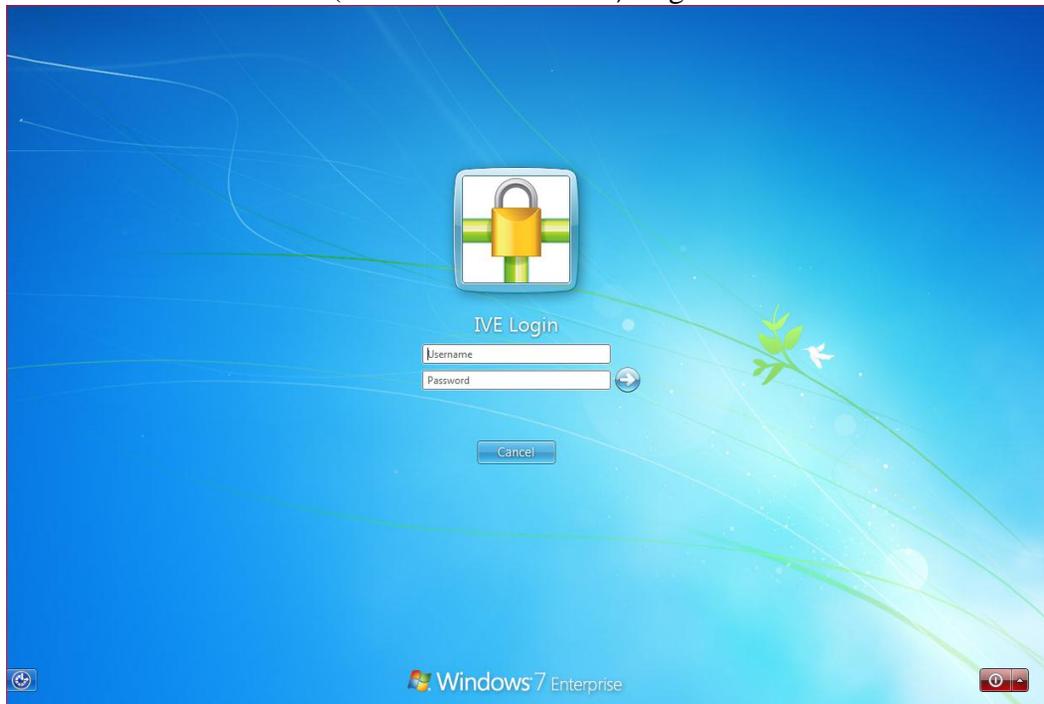
2. Once the Windows Log On screen loads, select “Switch User”



3. Click the blue icon on the bottom right of your screen.



4. This will load the IVE (Instant Virtual Extranet) Login screen.

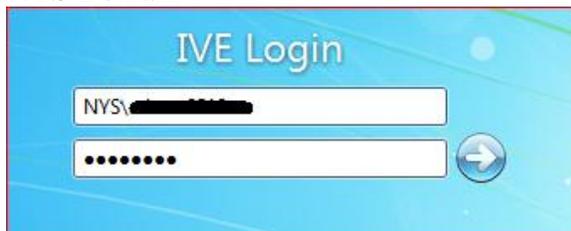


5. Enter your credentials with HSEN\

HSEN Domain



NYS Domain



6. Network Connect will connect to the CIO\OFT state network. This might take a moment.

7. Notice the Network Connect icon in the system tray. The client is loaded and connected to the network. When you hover over the icon with your mouse, it should display *Connected*. To disconnect, double click the Network Connect icon and select *Sign Out*.

If you try to log into the network using the IVE Credential Provider module and there is no network connectivity, you will fail to establish a connection. To resolve this issue, make sure the computer has a network connection. A wireless internet connection with the preferred network set to manually connect may also result in a failed connection. If you are using a wireless network for connectivity, make sure your network is listed in the preferred networks and is set to connect automatically.

Installing Network Connect without stored domain credentials

If access to the state network is available, credentials can be cached (stored on the computer) by physically connecting the computer to the state network and logging into Windows with a valid HSEN or NYS domain account. If the account cannot be cached because access to the state network is unavailable, proceed with the instructions below.

1. An individual with a cached (stored) domain account needs to sign into the computer from an external Internet connection (e.g. Roadrunner or DSL).
2. Launch a web browser and type <https://nc1.cio.ny.gov/hsen/firstlogon> (HSEN users) or <https://nc1.cio.ny.gov/nys/firstlogon> (NYS users) in the URL bar.
3. Sign in with a domain account approved for VPN access.
4. Click Start to begin a Network Connect VPN session.
5. Click OK at the message stating GINA has been enabled.
6. After a Network Connect VPN session has been established, sign out by clicking Sign Out from the menu that appears by right clicking the lock icon in the task bar.
7. Reboot the machine.
8. The actual VPN user (i.e. the individual without cached domain credentials) should then follow the remaining instructions to complete the installation.
9. Sign into Windows with the VPN user's un-cached domain account that is approved for VPN access. When the IVE Credential Provider module prompt appears, click OK to begin a VPN session.
*If authentication is unsuccessful, click the Options button at the IVE Credential Provider screen and verify the URL is correct. First-time users should use either <https://nc1.cio.ny.gov/hsen/firstlogon> (HSEN users) or <https://nc1.cio.ny.gov/nys/firstlogon> (NYS users).
10. Once Windows has loaded and a Network Connect session established, sign out by right clicking the lock icon in the task bar.
11. Remain logged onto the computer. Launch a web browser and type <https://nc1.cio.ny.gov/hsen> (HSEN users) or <https://nc1.cio.ny.gov/nys/> (NYS users) in the URL bar.
12. Sign in with a domain account.
13. Host Checker will install and the Network Connect session will be established.
14. Sign out of Network Connect and then log off from Windows.
15. The domain account has now been cached and Host Checker has been installed for that account. Logging into Windows from this point forward will present the user with the IVE Credential Provider Login prompt. The steps listed above are only needed for the first time installation of Network Connect and Host Checker.

Troubleshooting Juniper Network Connect

Verify the machine meets the minimum requirements

System requirements					
Version	Service Pack	Bit Version	Internet Explorer	Firefox	Java
Windows 7		32 or 64 bit	IE 8.0	Firefox 2.0 Firefox 3.0 Firefox 4.0	Sun JRE 5/1.5.07 and above

Page Can Not Be Displayed

If you receive a page cannot be displayed error when attempting to initiate a VPN connection, ensure:

- You have access to the nc1.cio.ny.gov name on port 443.
 - You can verify this by typing *telnet nc1.cio.ny.gov 443* at the command prompt.
- Verify the URL is typed correct.
 - For HSEN users <https://nc1.cio.ny.gov/hsen>
 - For NYS users <https://nc1.cio.ny.gov/nys>
- You are able to resolve the nc1.cio.ny.gov name. This name will resolve over the Internet, but not internally. Your installation should be completed from an external connection.

No Firewall Detected

You must have the McAfee HIPS product installed on your machine. Determine if the



symbol (McAfee HIPS) is in the system tray at the bottom right of your screen. If it is not,

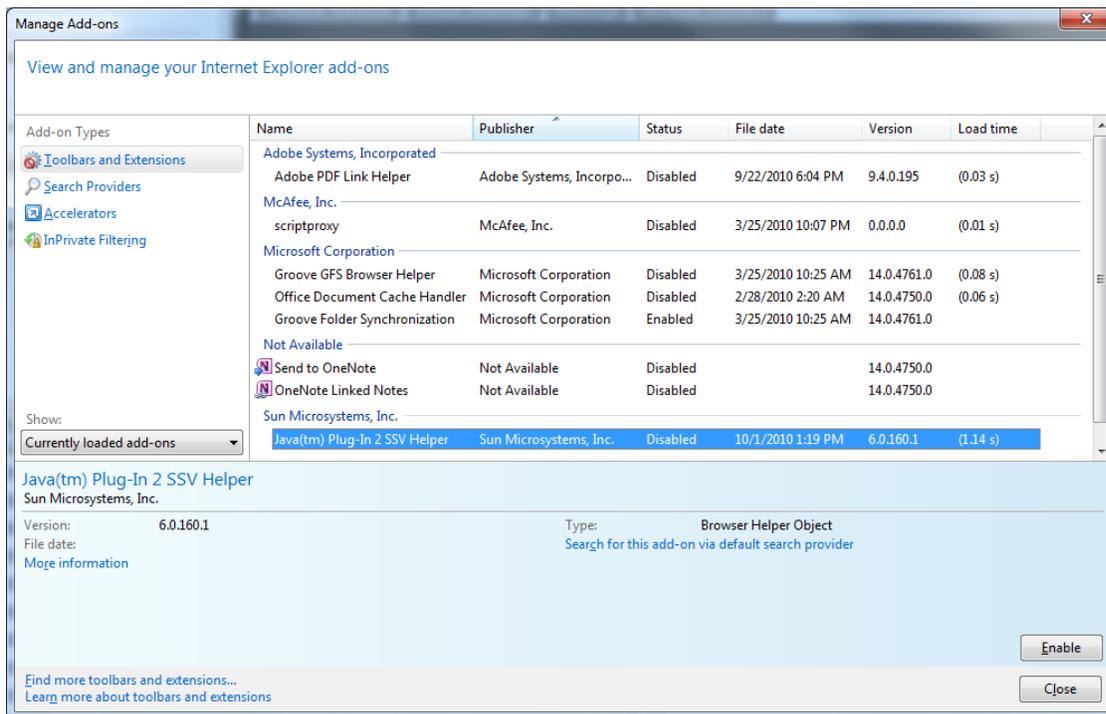
locate the McAfee Shield  in the system tray at the bottom right of your screen. Right click on the icon and go to "Manage Features". If you see McAfee Host Intrusion Prevention listed here or if you found the McAfee HIPS symbol in the system tray, all other components should be in place. If you are unable to find McAfee HIPS you must contact the CIO/OFT Customer Care Center at 1-800-697-1323.

Certain Components Fail To Load

If there is a failure of any of the three main components, namely Host Checker, Network Connect, or the IVE Credential Provider (GINA) module. Verify your Java version meets the minimum requirements and is enabled in your browser.

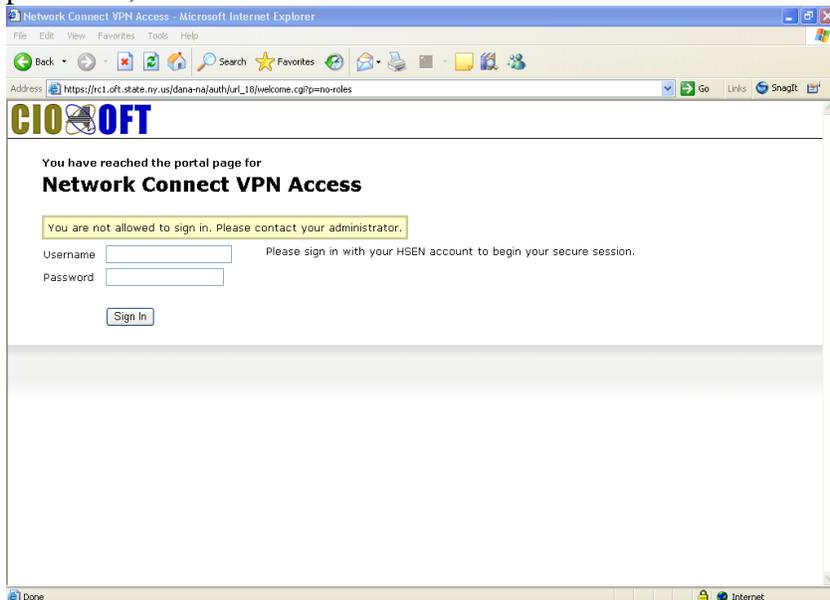
Open internet Explorer

- Click tools
- Internet options
- Click the Programs tab
- Click Manage add-ons
- On the Manage add-ons page verify Toolbars and Extensions is highlighted,
- On the right, Scroll down until you see Sun Microsystems
- Click Java and verify it is enabled.



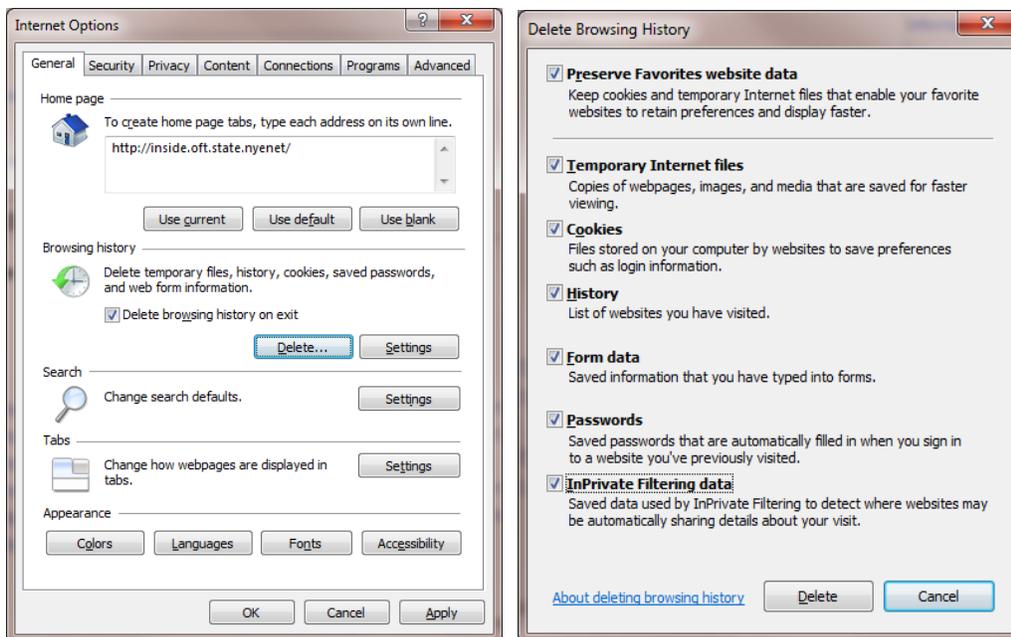
Temporary Internet Files and Cookies Issue:

When attempting to login to the VPN login screen, an error message indicating “You do not have permission to login. Please contact your administrator.” may appear before the login box is presented, as shown below:



The Lack of Permission error message

This may be caused by “congestion” in the temporary files stored by Internet Explorer. In order to remedy this, close the current web browser window, open a new browser, and then go to *Tools -> Internet Options*. This will display the General settings tab. Press the *Delete Cookies* button. A box will appear asking permission to delete all cookies, as shown below.



Click on the *OK* button, which will close the Internet Options screen and return to the browser window. Close all open browser windows and then attempt another Network Connect session either by navigating to the Network Connect URL or through the program files menu.

Selecting *Sign Out* from the Network Connect client menu when finished with the connection will greatly reduce the occurrence of temporary internet file and cookie problems.

IVE Credential Provider (GINA) Login prompt

Problem description:

No error occurs when the Network Connect client is installed but upon next logon, the Network Connect login does not appear.

Solution:

1. The computer must be rebooted after the initial install of the VPN client. Logging off the computer will not initiate the IVE Credential Provider module after installation. After the reboot, the IVE login will appear and from this point forward, a log off from Windows is all that is required to initiate the IVE login.
2. The installation of the VPN client requires that the computer is logged into with a domain account. Local accounts on the workstation will allow the install of the client, but the IVE Credential Provider module component will not install. If this occurs, the client should be uninstalled and then reinstalled with a domain account.

IVE Credential Provider Login does not connect

Problem description:

The connection fails due to a lack of Internet connectivity.

Solution:

1. Make sure Internet connectivity is physically working.
2. If using wireless Internet, make sure the network is listed in the preferred networks and is set to connect automatically.
3. If using an Air Card to connect, make sure that NDIS mode is enabled.

Host Checker

Juniper Host Checker is a security module that is automatically launched before a VPN session is initiated. The software verifies that the connecting computer meets security requirements. The first check verifies that the computer is part of either the NYS or the HSEN Domain. The second check verifies that the McAfee HIPS client is running on the computer. If either of these requirements is not met, a VPN session will not be established.

Further Assistance

If problems are still encountered, you can consult the End User Troubleshooting Guide available at <http://www.cio.ny.gov/vpn/networkconnect.htm>.

If you still are unable to resolve your issue you may contact the Customer Care Center at 1-800-697-1323.