

Network Connect (Client VPN) End User Troubleshooting Guide For Windows 7 OS

Revision history

Date	Description	Author/Editor	Version
3/28/2011	Initial release	N. Schettine	1.0
11/21/2013	Edited By	Chandni Kaul	1.1

Contents

Revision history.....	1
Contents.....	1
Error Messages when attempting to sign-in through IVE Credential Provider	2
Using Network Connect from the Programs Menu	5
Errors received during sign on via web browser	6
Problems encountered while VPN-connected	8
Network Connect VPN connection with an Air Card.....	9
Accessing VPN via a public Wi-Fi (Hot Spot).....	12
Network Connect supported platforms.....	13

Error Messages when attempting to sign-in through the IVE Credential Provider (GINA)

IVE Credential Provider Error Message 1



Possible cause: User may have mistyped username and/or password

Solution: Retype credentials and try again.

Possible cause: The computer may not be a member of the domain.

Solution: Verify the machine has not lost domain membership. (Contact your IT administrator)

IVE Credential Provider Error Message 2



Cause: User is trying to access <https://nc1.cio.ny.gov/hsen> when Host Checker is not installed.

Solution: Install Host Checker for the user's profile. Follow the steps outlined below.

Installing Host Checker for the user's profile

1. Sign into the computer with cached domain credentials (see below if the user does not have cached domain credentials).
2. From an external Internet connection, open a web browser and type <https://nc1.cio.ny.gov/hsen> in the URL bar.
3. Enter domain credentials into the Network Connect login page.
4. Host Checker will install and verify security requirements.
5. Select Sign Out from the upper right corner of the Network Connect VPN portal.
6. Log off from Windows.
7. Host Checker has now been installed for the user's domain account. Logging into Windows from this point forward will present the user with the IVE Credential Provider. **The steps listed above are only needed for the first time installation of Host Checker for a user's profile.**

To be performed if the user does not have cached domain credentials on the computer:

1. Connect computer directly to the LAN
2. Login to the computer with domain credentials.
3. Disconnect from the LAN and connect to an external Internet connection.

4. Host Checker still needs to be installed for the user's profile. Proceed with steps 2-6 of the first part of this solution (*Installing Host Checker for the user's profile*).

To be performed if the user does not have cached domain credentials on the computer and does not have the ability to login via a direct LAN connection:

1. Enter domain credentials at the Windows login prompt.
2. At the IVE credential provider login prompt look for the URL that you are connected to. If it displays: <https://nc1.cio.ny.gov/hsen/firstlogon>, select OK to establish a VPN session, and then go to step 5. If the firstlogon URL is not present at this login screen, select Options.
3. From the drop down menu, select the firstlogon URL. If it is not present, manually type this entry in the address bar. Select OK.
4. Make sure your credentials are correct at the IVE credential provider prompt and that the URL now shows the firstlogon URL. Select OK.
5. This will cache the domain account on the device and establish a restricted-use Network Connect VPN session. This connection should not be used for accessing the network as most internal resources are blocked when using the firstlogon URL. Disconnect from VPN by right-clicking the lock icon in the task bar and selecting sign out.
6. Host Checker still needs to be installed for the user's profile. Proceed with steps 2-6 of the first part of this solution (*Installing Host Checker for the user's profile*).

IVE Credential Provider Error Message 3



Possible cause: User has Host Checker installed, but failed one of the security checks (domain, firewall client, incompatible processes).

Solution: Review the section on Host Checker errors and confirm the computer meets specifications (See "Errors received during sign on via web browser" section).

Possible cause: The system date/time on the computer is incorrect. This will make the VPN certificate appear to be invalid.

Solution: Click cancel at the IVE credential provider prompt and log in with cached credentials. Correct the system time and try again.

IVE Credential Provider Error Message 4



Possible cause: There is no Internet connection.

Solution: Make sure that the computer has a connection to the Internet.

Possible Cause: Wireless card is not configured for pre-Windows Internet connection.

Solution: Contact your IT administrator about how to enable NDIS mode for the wireless card or see the section on “Network Connect VPN Connection with an Air Card” of this guide for instructions.

Possible cause: Wireless network is not available.

Solution: Add wireless network to preferred networks list.

1. Click cancel at the IVE credential provider prompt and login with cached domain credentials.
2. Go to Start – Settings – Network Connections – Wireless Network Connection.
3. Right-click Wireless Network Connection and select Properties.
4. Select the Wireless Networks tab.
5. Click Add.
6. Enter the information required for your wireless connection and select OK.
7. Select the new network from the list and move it up into the first position.
8. Select OK to accept changes.
9. Reboot the computer and try again. It is important to note you must allow enough time for the Wireless Network to acquire an IP address before logging in through THE IVE CREDENTIAL PROVIDER.

Possible cause: Your site may require the use of a local proxy to access the Internet

Solution: Configure local proxy in THE IVE CREDENTIAL PROVIDER

1. From the IVE credential provider prompt, select Options.
2. Select the proxy server check box and type in the local network’s proxy information. Select OK. (If you do not know the local network’s proxy information, contact your IT administrator).
3. Select OK at the IVE credential provider prompt.

Possible Cause: URL in IVE credential provider prompt is incorrect.

Solution: Configure IVE credential provider to use proper URL

1. At the IVE credential provider prompt look for the URL that you are connected to. It should display: <https://nc1.cio.ny.gov/hsen> (for existing VPN users) or <https://nc1.cio.ny.gov/hsen/firstlogon> (for first time users without LAN connections). If it does not, select Options.
2. In the URL bar, manually type the appropriate URL entry. Select OK.
3. Make sure your credentials are correct at the IVE credential provider prompt and that the URL now shows the appropriate URL. Select OK.

Using Network Connect from the Programs Menu

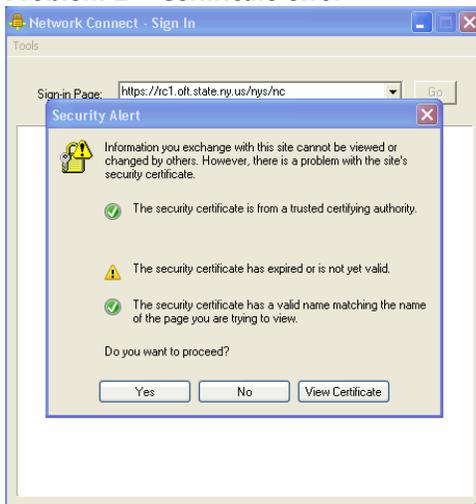
Problem 1 – Address is not valid



Cause: There is no web address in the address bar. This is due to using Network Connect using an account that has never signed into VPN from this computer.

Solution: Insert <https://nc1.cio.ny.gov/hsen> into the address bar and sign in.

Problem 2 – Certificate error

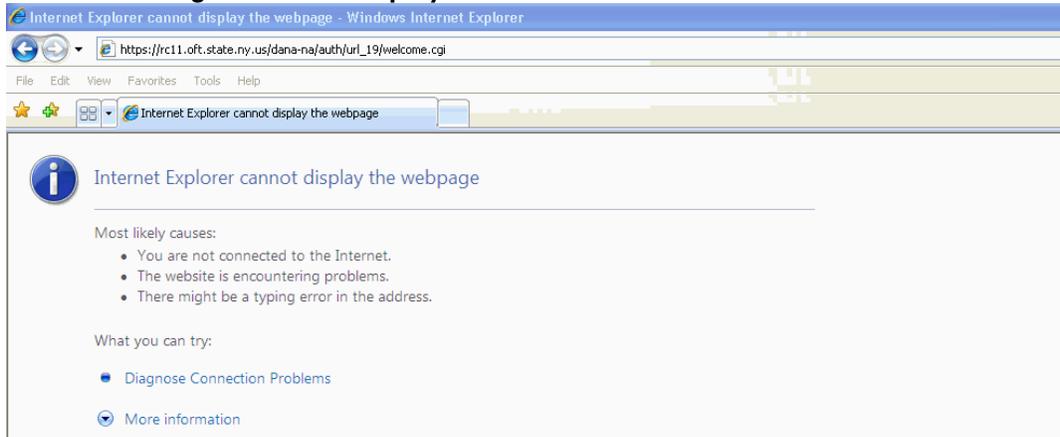


Cause: The system date/time on the computer is incorrect. This will make the VPN certificate appear to be invalid.

Solution: Click cancel at the IVE Credential provider prompt and log in with cached credentials. Correct the system time and try again.

Errors received during sign on via web browser

Problem 1 – Page cannot be displayed



Possible Cause: The VPN URL is incorrect

Solution: Make sure <https://nc1.cio.ny.gov/hsen> is entered in the address bar.

Possible Cause: The user's Internet connection is not working or access to VPN is blocked.

Solution: Attempt to access another site not blocked by the HIPS firewall, such as <http://www.cio.ny.gov>. If it is inaccessible, the Internet connection may not be working properly. If the website is accessible, a local proxy or firewall may be blocking access to VPN. Once you find out if the other website is available contact your IT administrator and relay this information.

Possible Cause: Windows phishing filter is blocking access.

Solution: Turn off phishing filter in Internet Explorer by selecting *Tools-Phishing Filter-Turn off phishing filter*.

Problem 2 - Host Checker Error 1



⚠ Your computer's security is unsatisfactory

Your computer does not meet the following security requirements. Please follow the instructions below to fix these problems. When you are done click **Try Again**.

1. Bonjour Service

Instructions: Your computer is running the Bonjour process. This service is incompatible with Network Connect VPN. If you would like to proceed with using VPN, disable the Bonjour process by pressing Ctrl-Alt-Delete and selecting Task Manager. From the Task Manager search for the name 'mDNSResponder.exe', select it, and then click 'End Process'. Proceed to the Network Connect Sign In page to start your VPN session.

Reasons: found mDNSResponder.exe

Cause: The computer has failed one of the security evaluations assessed by Host Checker.

Solution: Beneath the error, there are steps to follow to correct the problem. For some problems, it may be possible to rectify the issue immediately; others will require the assistance of your IT administrator. See below for a list of errors and solutions.

1. Domain Check

Message: Your computer has been denied access because it is not a member of the domain. Contact the Customer Care Center (CCC) at 1-800-697-1323 if you feel you received the message in error.

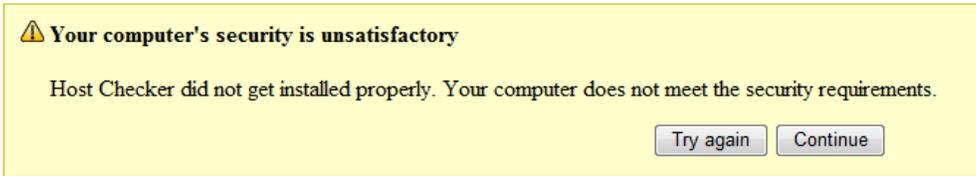
2. Firewall Client Not Detected

Message: Your computer has been denied access because it does not meet security requirements. CIO/OFT requires that a state-issued firewall client is configured and running on your computer. The two acceptable firewall clients include 1) the Symantec Protection Agent or 2) the McAfee Host Intrusion Prevention. If you have been approved for VPN access, but do not have the firewall client installed, you will need to call the Customer Care Center (CCC) at 1-800-697-1323.

3. Bonjour Service

Message: Your computer is running the Bonjour process. This service is incompatible with Network Connect VPN. If you would like to proceed with using VPN, disable the Bonjour process by pressing Ctrl-Alt-Delete and selecting Task Manager. From the Task Manager search for the name 'mDNSResponder.exe', select it, and then click 'End Process'. Proceed to the Network Connect Sign-In page to start your VPN session.

Problem 2 - Host Checker Error 2



Possible Cause: There is a slow or an unreliable Internet connection.

Solution: If the Internet connection is suspect, such as a weak wireless signal, try using a different connection.

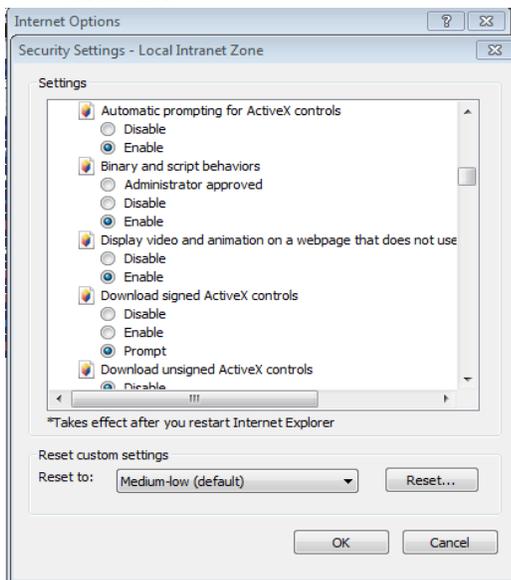
Possible Cause: A corporate proxy may conflict with installing Host Checker properly

Solution: Find a connection outside of the proxy connection and use a non-proxy Internet connection such as DSL or Roadrunner

Possible Cause: The Security settings for IE are too high

Solution: To modify ActiveX settings, follow the steps below

1. Click on **Tools**
2. Select **Internet Options**
3. Select the **Security Tab**
4. Under the Security Tab, click **Custom Level**
5. Enable **Automatic Prompting for ActiveX Controls** to decrease the security setting and click **OK**



Possible Cause: Java is not installed

Solution: Install Java from <https://java.com/en/download/index.jsp>

Possible Cause: An unsupported browsers is being used (ex: Chrome)

Solution: Use a supported browser (refer to Pg.14 for the list of supported platforms)

Problems encountered while VPN-connected

Problem 1 – Internal resources unavailable



Possible Cause: The user has a successful VPN connection but they are unable to access local resources (e.g. Exchange). The user may have established their VPN connection using the <https://nc1.cio.ny.gov/hsen/firstlogon> URL. This URL is intended to cache user credentials on the computer. It does not permit access to internal resources.

Solution: User needs to sign out of this VPN connection and open a browser to the <https://nc1.cio.ny.gov/hsen> URL.

Problem 2 – Session timeout



Cause: The maximum session time or the maximum idle time has been reached.

Solution: The max session time is 24 hours and the idle session timeout is 60 minutes. If any of these events have occurred, select OK. Sign back into the Network Connect VPN client to reestablish the VPN session.

Network Connect VPN connection with an Air Card

Note: An air card is a PCMCIA card that connects to the Internet directly via a wireless data plan from telecommunication providers like Verizon or Sprint. See below for information regarding enabling NDIS mode for several major vendors.

Verizon

Application: VZAccess Manager



Requirements:

Network Adapter (NDIS) will only work if the Verizon network device is on:

- Verizon Wireless Broadband Access
- Verizon National Access coverage

Also the Verizon VZAccess Manager is supported on:

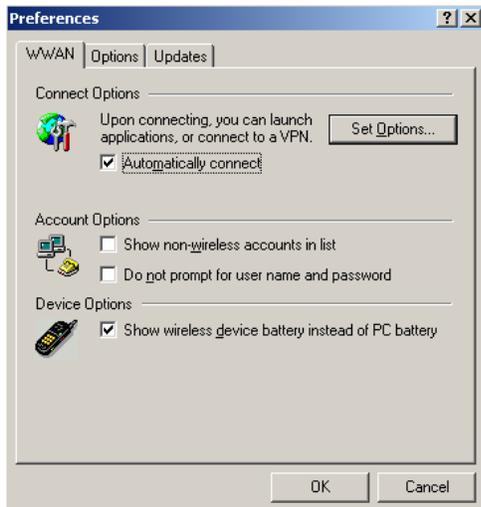
- Windows XP

Note: When enabled, NDIS provides an "always on" Internet connection similar to a standard network interface card (NIC). Also be advised that a NDIS broadband connection will remain active even if VZAccess Manager is closed.

Instructions:

In order to connect to the VPN device with the IVE Credential Provider, there are two steps. First, verify that the device is a Verizon card that runs VZAccess Manager. Secondly, change the Verizon (VZAccess Manager) configuration.

To change the configuration, check the box next to **Automatically Connect**, located within *Tools / Preferences / WWAN* under **Connection Options**. See figure below.



Once the check box is selected, the computer should be rebooted. The connection through the IVE credential provider will now work. This option, once selected, enables NDIS Mode on the device, which allows the card to connect to the Internet before a user signs into Windows. By enabling NDIS, the IVE credential provider is able to initiate a Network Connect session to the state network.

For further information on NDIS Mode open VZAccess Manager and go to *Manager / Help* Search for NDIS.

Sprint

Application: Sprint Mobile Broadband (Sierra)



Requirements:

Network Adapter (NDIS) will only work if the Sprint network device is an:

AirCard 597E ExpressCard

AirCard 595 PC Card

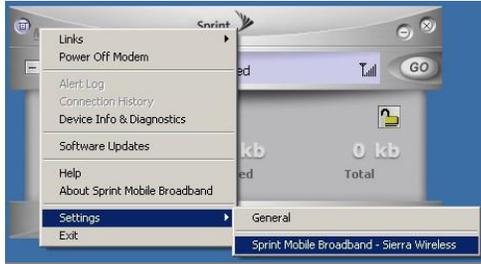
AirCard 595U USB modem

Also the Sprint Mobile Broadband is supported on:

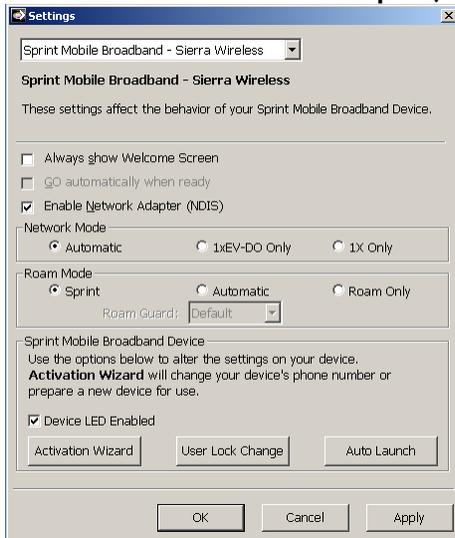
Windows XP with Service Pack 2

Instructions:

There are two steps to connect to the state network with IVE Credential Provider. First, verify that the device is a Sprint card that runs Sprint Mobile Broadband (Sierra). Secondly, change the Sprint configuration. This can be done by checking the box to **Enable Network Adapter (NDIS)**, located within *Menu / Settings / Sprint Mobile Broadband – Sierra Wireless*. See figure below.



Check the **Enable Network Adapter (NDIS)**. See figure below.



Click **Apply** and the settings will be saved.

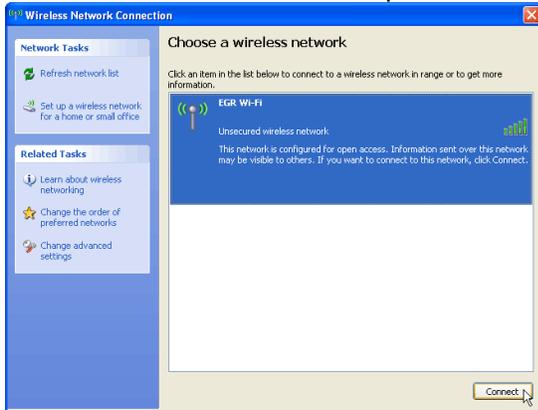
NOTE: On some computers a confirmation window will appear. Accept the changes.

Once the check box is selected, the computer should be rebooted. The connection through the IVE Credential Provider will now work. This option, once selected enables NDIS Mode on the device, which allows the card to connect to the Internet before a user signs into Windows. By enabling NDIS, the IVE Credential Provider is able to initiate a Network Connect session to the state network.

For further information on NDIS Mode open *Sprint Mobile Broadband (Sierra)/Help*. Search for NDIS.

Accessing VPN via a public Wi-Fi (Hot Spot)

1. Connect to a wireless access point. Search for available wireless networks and select **Connect**.



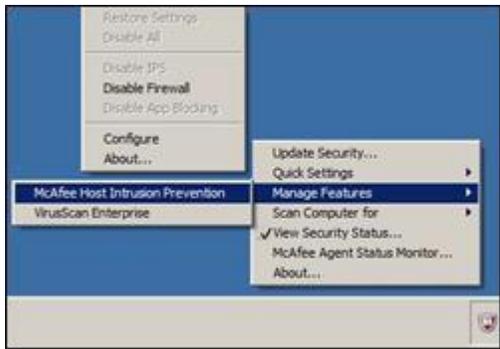
2. Open a browser and access the VPN web page: <https://nc1.cio.ny.gov/hsen>. If “Page cannot be displayed” error is received, try accessing <http://www.cio.ny.gov>. If you receive “Page cannot be displayed” on both sites, close the browser.

3. Disable the firewall.

4. Right-click the **M** icon in the task bar.

5. Right-click **Manage Features | McAfee Host Intrusion Protection**.

6. Select **Disable Firewall**.



McAfee HIPS Agent Disable Firewall

7. Attempt to access and log into the VPN web page again:

- Open Internet Explorer
- Try to access the <http://www.cio.ny.gov> website again. This attempt may show another web page such as a “Panera Welcome Page”. Accept their terms/agreement.
- Once the terms are accepted, now access the <https://nc1.cio.ny.gov/hsen> website and login.

8. After a VPN session is established, re-enable the firewall.

Network Connect supported platforms

To use the Network Connect VPN client, the computer must be running a supported OS, browser, and Java combination.

System requirements		
Version	Operating System	Browsers and Environment
Windows 7	32 bit Enterprise- 32 bit 64 bit	IE 7.0, 8.0, 9.0, 10 Firefox 2.0, 3.0, 4.0, 0 Sun JRE 5, 1.5, .07 and above