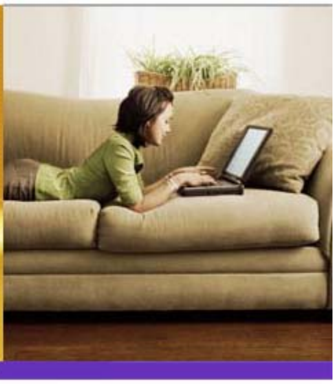
Alcatel·Lucent

OmniAccess 3500
Nonstop Laptop Guardian
Release 1.6
End User Reference Guide (HSPA)



Document Version: 022.01

Part No.060246-00 Rev. A

Published: 09.21.2008

Table of Contents

Welcome

Welcome to the *OmniAccess 3500 Nonstop Laptop Guardian Release 1.6 End-User Reference Guide*. This guide will introduce you to the many functions of the OmniAccess 3500 Nonstop Laptop Guardian (NLG) card and its operation.

For instructions on how to install or upgrade your card and the client software, see the *OmniAccess 3500 Nonstop Laptop Guardian Release 1.6 Card Quick Start Guide*. *It is recommended to have the Windows XP Service Pack 3 (SP3) patch installed for Windows XP on your laptop.*

Overview of OmniAccess 3500 NLG Card Features

The OmniAccess 3500 NLG card keeps your laptop within the security perimeter of your company's network and provides the same user experience at all times, irrespective of where you are.

The card supports the following functions:

- Secure connectivity to your company's network irrespective of your laptop's location and without requiring user intervention.
- Single sign-on – Just use your domain authentication credentials for secure remote access to the enterprise network.
- Automatic switchovers to the next best network interface if the company's network can no longer be reached using the existing interface.
- Easy manual switching of network interface serving the connection to your company's network when the laptop senses a surrounding access network with better performance.
- Option to use the OmniAccess 3500 NLG card as a smart card. You just need to enter a PIN (instead of domain credentials) to securely access your company's network.
- Integrated Personal Firewall to protect your laptop from attackers and to restrict the set of applications that are allowed to access the network.
- Encrypted volume for storage of sensitive data in your laptop's hard disk. Configuration and management of the encrypted volume are fully transparent to you (no passwords to enter and maintain). *The OmniAccess 3500 NLG Release 1.6 supports volume encryption for Truecrypt versions 4.3a, 5.1a, and 6.0a.*
- Protection of the data stored in your laptop in case it is lost or stolen. Your IT administrator can remotely lock the laptop or destroy the keys that are required for decryption of the encrypted volume contents.
- Integration of common patch management applications (Microsoft SMS, PatchLink Update).
- The same laptop can be shared by multiple users if so configured by the IT administrator.
- Interoperation with full hard disk encryption solutions.

SYSTEM CONFIGURATION

The OmniAccess 3500 NLG card works with Windows-based laptops with the following minimum configuration:

- CPU: X86 1GHz
- Memory: 512 MB
- Free hard disk space: 1 GB
- Operating system: Windows XP Professional (Service Pack 3 patch is recommended), or Tablet edition
- One PC Cardbus slot

Note:- Windows XP Home edition can also be used, but only if the laptop is configured for RADIUS authentication.

The OmniAccess 3500 NLG card and client software present the following interfaces for interaction with the end user:

- OmniAccess 3500 NLG client GUI
- OmniAccess 3500 NLG tray icon
- LEDs on the OmniAccess 3500 NLG card
- Radio On/Off button on the OmniAccess 3500 NLG card.

Common Operations

The following sections shows you how to perform basic operations with your OmniAccess 3500 NLG card and with the graphical user interface of the client software that comes with the card. *(For installation procedure refer to OmniAccess Nonstop Laptop Guardian Release 1.6 Card Quick Start Guide)*

How do I use my laptop?

You can keep using your laptop as always, with no extra steps required. Your OmniAccess 3500 NLG card automatically keeps your laptop connected to your company's network whenever network connectivity is available. The OmniAccess 3500 NLG tray icon displays the status of your connection**.** If your administrator has configured an encrypted volume for your laptop, the OmniAccess 3500 NLG automatically mounts it to your file system.

Only a few specialized operations require you to access the OmniAccess 3500 NLG client GUI on your laptop. Many of the client GUI commands can also be accessed by right-clicking on the tray icon.

How do I log into my laptop?

Important: - The laptop login procedure varies depending on the authentication method that your administrator has configured for your user account. The following options are available:

- **Domain** (Default) - You log into your laptop by entering your Windows Domain username and password on the Windows logon prompt. The procedure also gives you access to your company's network, whether you are connected from within the premises of your company or from a remote location.

  Note: If you are logging into your Windows domain for the first time after installing the OmniAccess 3500 NLG client software (your laptop has no cached credentials), please wait for the light of the card LED to turn amber before entering your Windows Domain username and password.

- **Smart Card**: At the Windows logon prompt, press the **Ctrl-Alt-Backspace** key combination to display the PIN prompt. Enter your PIN to start using the laptop and access your corporate network. Note that the smart Authentication works only if you are using the keyboard of your laptop, any external keyboard may not work. Please contact your administrator if you don't know the PIN.

  Note: If your user account is configured for smart-card login, the Windows logon prompt shows the message "Please insert the card". Hitting the Ctrl-Alt-Backspace key combination is equivalent to physically inserting/extracting a smart card in/from your laptop.

  If the card is coming up from sleep mode then wait until the card's NLG LED stops blinking and gives a steady light before entering authentication credentials.

- **Domain and Smart Card**: Your user account may be configured for both authentication methods. In this case you choose your preferred authentication procedure every time you login.

How do I interpret the state of the card LEDs?

There are two LEDs on the OmniAccess 3500 NLG card as described below:

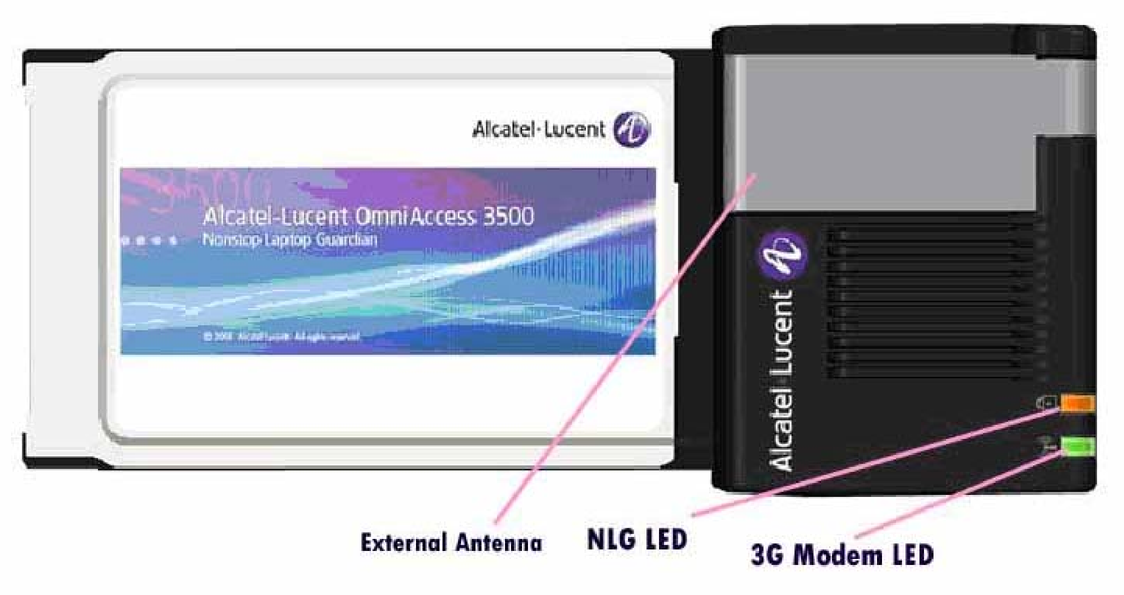


Figure 1: OmniAccess 3500 NLG Card (HSPA)

- **3G Modem LED** can be in one of the following states:
  - No light: 3G modem is off.
  - Slow-blinking amber light: 3G modem is on.
  - Fast-blinking yellow light: 3G modem is transmitting data.
- **NLG LED** can be in one of the following states:
  - No light: Card is in sleep mode or off.
  - Solid red light: Card is up, VPN tunnel is down.
  - Solid amber light: Tunnel is up but not authenticated. Only management traffic can flow across the Card and the Gateway but no user traffic.
  - Solid green light: Card is up, VPN tunnel is up and the user has been authenticated. Both user and management traffic can flow.

Note: To receive the 3G signal the external antenna of the card must be raised."

How do I interpret the state of OmniAccess 3500 NLG tray icon

OMNIACCESS 3500 NLG TRAY ICON

You find an icon with the Alcatel-Lucent infinity logo added to your laptop's icon tray. The color of the icon provides visual indication of the current status of your connection to the enterprise network (roll over the icon with your mouse to have a more detailed status description displayed):

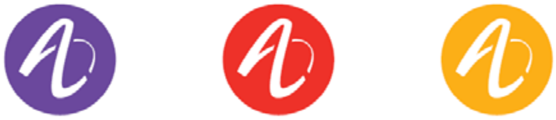


Figure 2: OmniAccess 3500 NLG tray icon colors

- Purple icon — You have full access to your company's network. The mouse-rollover pop-up message shows the type of access network in use and the strength of the 3G signal.
- Yellow icon — The card is connected to the OmniAccess 3500 NLG gateway in your company's network, but you don't have access to the network. Only management transactions can take place between the card and the gateway. The mouse-rollover pop-up message shows the type of access network in use and the strength of the 3G signal. This happens only when a valid user is not logged into the laptop.
- Red icon — there is no connectivity between the card and your company's network or an error has occurred in the operation of the card. The mouse-rollover pop-up message will show further information about the error condition, such as:
  - Not Connected

- Radio timeout along with the time left over if the 3G modem has been turned off.
- Laptop is working unguarded under the effect of the One-Time-Password. It will also show the duration left till you can continue using the laptop. (See section *One Time Password (OTP*.

How do I switch Off (On) the 3G modem on my card?

In some environments (e.g. on board of airplanes that are landing or taking off) regulatory restrictions require that all radio equipments shall be turned off. The OmniAccess 3500 NLG card allows you to selectively turn off the integrated 3G Radio Modem allowing you to continue using the laptop and the functionality provided by the OmniAccess 3500 NLG card except for 3G connectivity.

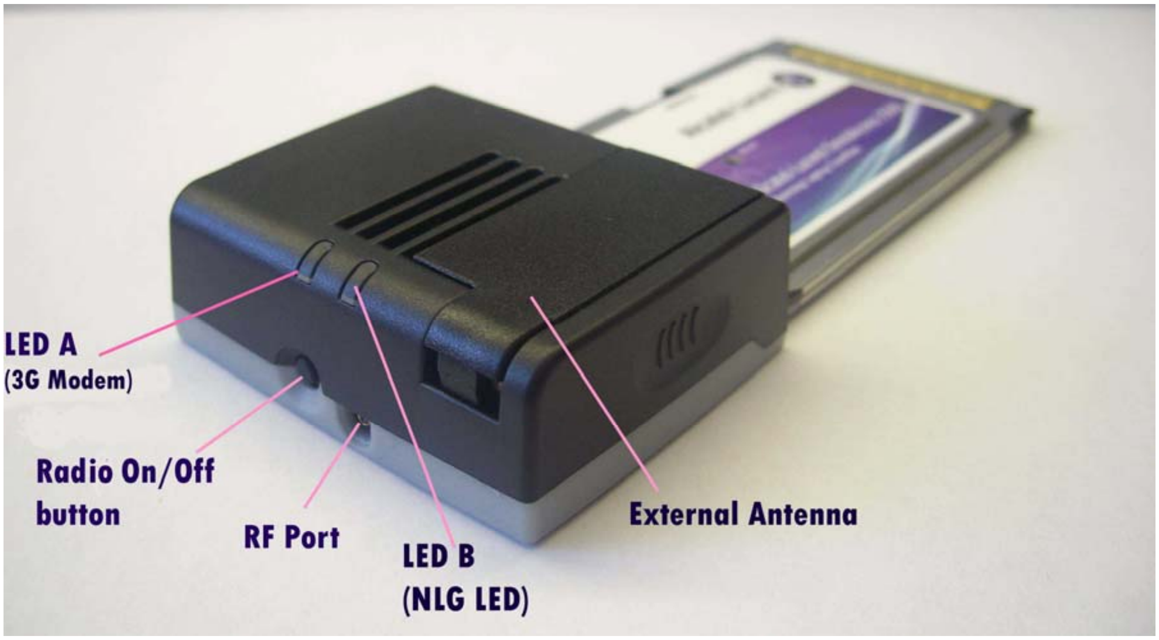


Figure 3: OmniAccess 3500 NLG card (HSPA)

To toggle the power state (turn Off or On) of the 3G Radio modem, push the *Radio On-Off button* located on the front of the card with the tip of a ballpoint pen.

Note: The power state of the 3G modem is always remembered throughout a reboot event. After the laptop or the card reboots the 3G modem is in the same power state as before the reboot started.

How do I control the power state of the OmniAccess 3500 NLG Card?

As your laptop goes into Standby/Hibernate/Shutdown state with the card plugged in, or as the card is removed from the laptop, the card automatically switches to sleep mode (shutdown) in 10 minutes if the 3G modem is on and in 1-2 minutes if the 3G modem is off to preserve the integrate battery charge. Your card automatically powers on when it is plugged into a laptop that has power.

However if you need to manually shut down the power to the card for the reasons like shipping then it can be done by any of the method listed below:

- Take the card out of the laptop (see also *How do I remove the card from my laptop?*?) Press and hold the Radio On/Off button for 5 seconds. It will turn off the card. The power will restore automatically when inserted into a powered laptop.
- Press the *Reset switch* (accessible only when the card is removed from the laptop) to turn OFF the power to card completely.

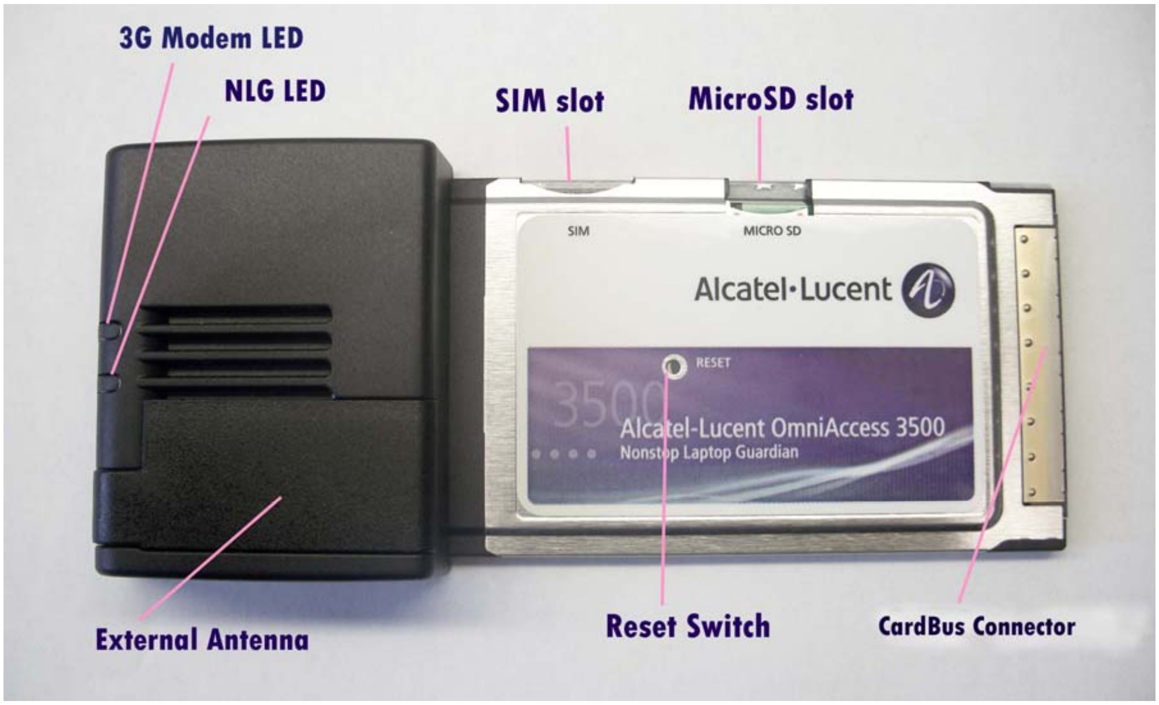


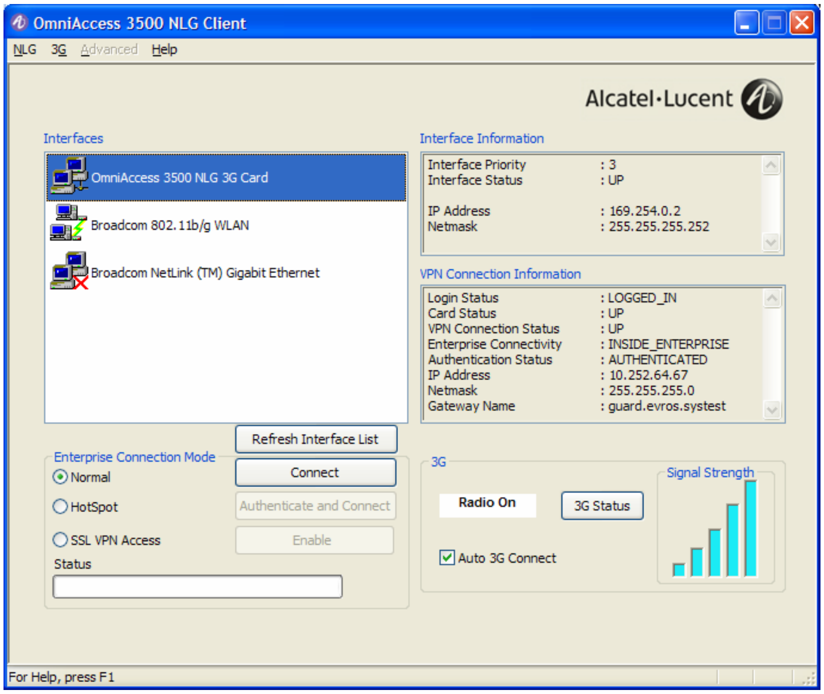
Figure 4: OmniAccess 3500 NLG card

How do I access the OmniAccess 3500 NLG client GUI?

You can open the OmniAccess 3500 NLG client GUI in one of the following ways:

- Double-click on the OmniAccess 3500 NLG desktop icon.
- Double-click on the OmniAccess 3500 NLG Tray icon at the Notification area.
- Click **Start > Programs > OmniAccess 3500 NLG Client Programs > Alcatel-Lucent > OmniAccess 3500 NLG > OmniAccess 3500 NLG Client**.

The OmniAccess 3500 NLG Client Window appears (shown on the next page)



Interface Priority : 3
Interface Status : UP

IP Address : 169.254.0.2
Netmask : 255.255.255.252

Login Status : LOGGED_IN
Card Status : UP
VPN Connection Status : UP
Enterprise Connectivity : INSIDE_ENTERPRISE
Authentication Status : AUTHENTICATED
IP Address : 10.252.64.67
Netmask : 255.255.255.0
Gateway Name : guard.evros.systest

● Normal
○ HotSpot
○ SSL VPN Access

☑ Auto 3G Connect

Figure 5: OmniAccess 3500 Nonstop Laptop Guardian (NLG) client window

OMNIACCESS 3500 NLG CLIENT WINDOW MENU OPTIONS

The menu bar at the top of the *OmniAccess 3500 NLG Client* window contains the following menus:

- **NLG** — Management of the OmniAccess 3500 NLG card. Available options:
  - **Configure:** Configuration of basic parameters for operation of the OmniAccess 3500 NLG card (name of the gateway designated for remote connectivity and certificates needed for establishment of the IPsec tunnel).
  - **Personal Firewall Settings:** Configuration of the personal firewall that resides in the OmniAccess 3500 NLG card.
  - **Retrieve Logs:** Retrieves both card and the laptop logs and deposits in a folder named as NLGLogs on the desktop. If the Winzip is installed on the laptop then it automatically creates the zip file named as NLGLogs.zip
  - **Reset Card:** Reboot the card without having to remove it from the laptop. This command works only if the connection between the laptop and the card is fully functional.
  - **Card Upgrade:** Upgrades OmniAccess 3500 Nonstop Laptop Guardian Card.
  - **Card Information:** View the card configuration.
  - **Close:** Hide the client GUI window.
- **3G** — Management of the 3G wireless modem. Normal operation of the OmniAccess 3500 NLG card does not require the functions that are accessible from this menu. Available options:

  - **Preferences:** Management of preferences for Roaming, Bearer, and Network
  - **Unblock SIM:** The end user can unlock the SIM.
  - **Reset SIM PIN:** The end user can reset the SIM PIN.
  - **New Profile:** The end user can create a profile to connect to the network with compression selection for IP Header, data and Authentication type.
  - **Open Profile:** The end user can open an existing profile**.**
  - **Delete Profile:** The end user can delete an existing profile.
- **Advanced** — This menu is not active (grayed out) during normal operation. It can only be accessed by your wireless provider for servicing purposes.
- **Help** — Support Information. Available options:
  - **User Manual:** Access help documentation (Adobe Acrobat Reader must be installed in the laptop to view the documentation).
  - **About OmniAccess 3500 NLG Client -** Displays the software version running on the laptop.

OMNIACCESS 3500 NLG CLIENT WINDOW

The OmniAccess 3500 NLG Client window contains the following sections:

- The **Interfaces** section lists all network interfaces that are available for connectivity to your company's netwrok. A *green lightning bolt* symbol is added to the icon of the network interface that currently serves the access connection. A *red diagonal cross* symbol is added to the icons of the available network interfaces that are currently not serving the access connection. You can view configuration and status information for an interface by clicking on the corresponding icon.

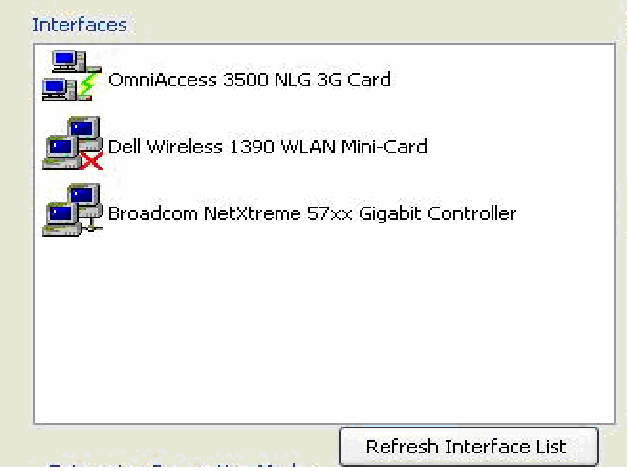
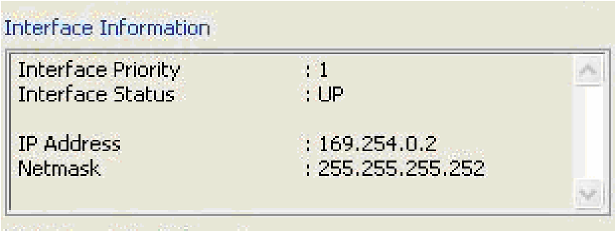

Interfaces
OmniAccess 3500 NLG 3G Card
Dell Wireless 1390 WLAN Mini-Card
Broadcom NetXtreme 57xx Gigabit Controller
Refresh Interface List

Figure 6: Interfaces section of the OmniAccess 3500 NLG Client window

- The **Interface Information** section displays information about the interface that is currently highlighted in the Interfaces section.



Interface Information

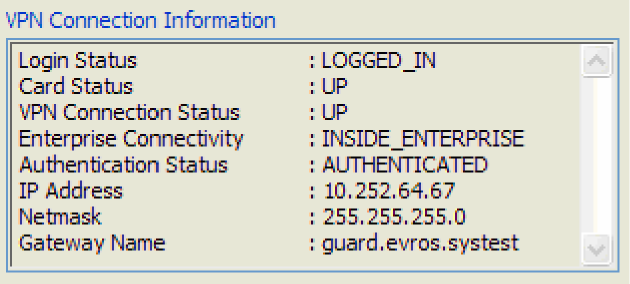
Interface Priority : 1
Interface Status : UP

IP Address : 169.254.0.2
Netmask : 255.255.255.252

Figure 7: Interface Information section of the OmniAccess 3500 NLG Client window

- The **VPN Connection Information** section displays parameters for the VPN tunnel (if established); the authentication status of the end user and the name of the gateway to which the end user is currently connected. This tab also displays your IP Address, Login Status , card Status.

  Enterprise Connectivity: displays OUTSIDE_ENTERPRISE i.e the laptop has a tunnel established to the WAN interface of the gateway and if it shows as INSIDE_ENTERPRISE than the laptop has a tunnel established to the LAN interface of the gateway.

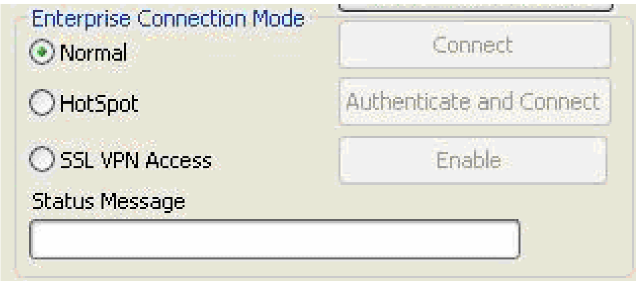


VPN Connection Information

Login Status : LOGGED_IN
Card Status : UP
VPN Connection Status : UP
Enterprise Connectivity : INSIDE_ENTERPRISE
Authentication Status : AUTHENTICATED
IP Address : 10.252.64.67
Netmask : 255.255.255.0
Gateway Name : guard.evros.systest

Figure 8: VPN Connection Information section of the OmniAccess 3500 NLG Client window

- The **Enterprise Connection Mode** section provides access to the controls that are required to connect to your company's network, including the manual selection of the serving interface. Available Options:



Enterprise Connection Mode

● Normal
○ HotSpot
○ SSL VPN Access

Status Message

Figure 9: Enterprise Connection Mode section of the OmniAccess 3500 NLG Client window

  - **Normal:** To manually connect to the company network, please select any of the available network interfaces listed under Interfaces section and press the "Connect" button.
  - **Hotspot:** If you want to connect over a paid network (e.g. Wi-Fi hotspots) where additional authentication needs to be performed then please select the desired interface (Wi-Fi or Ethernet), check the HotSpot radio button and then

press 'Authenticate and Connect' button next to it. While establishing connection via hotspot if you get either "Action Cancelled" or "The page cannot be displayed" window then try refreshing the browser page. For more on connecting to public. (See also *How do I connect from a public hotspot?)*

- **SSL VPN Access:** Situations where the OmniAccess 3500 NLG card cannot reach the company's gateway because IPSec traffic is blocked by the visited network, end user can establish connection to the company's SSL VPN server by selecting available loop back or wireless interfaces from the Interfaces section and pressing the "Enable" button to get an access to the company's SSL VPN portal.

- The **3G** section provides control for and information about the 3G modem that is integrated in the OmniAccess 3500 NLG card. Available Options:

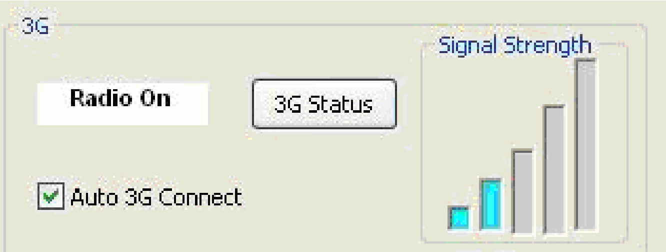
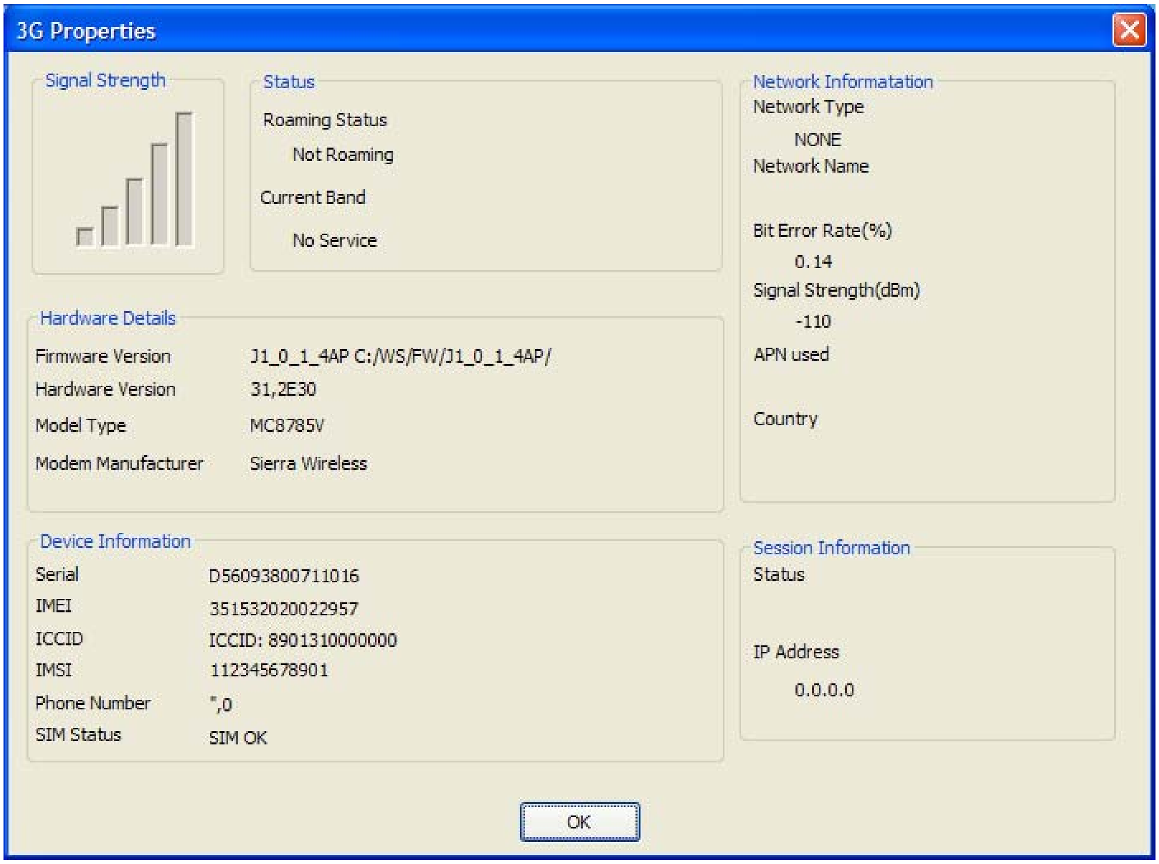


Figure 10: 3G Section of the OmniAccess 3500 NLG Client window

- **Radio ON/OFF**: The 3G modem integrated in the OmniAccess 3500 NLG card can be switched On or Off from the toggle switch located at the center of the OmniAccess 3500 NLG card. A small window in this section will show the current status of the 3G modem. "Radio ON" status means the modem is On and connection over 3G are available. "Radio OFF" status means the modem is Off and connection over 3G cannot be established. To change the status, please toggle the switch on the Card.
- **Auto 3G Connect**: If the check box is checked then the connection over 3G interface will be made automatically if required. Otherwise you will be prompted before connecting over 3G.
- **3G Status**: Pressing of this button will open up a new screen displaying more detailed information about 3G modem and its status. The content of this screen will be different based on the type of OmniAccess 3500 NLG card used as shown in Figure 11. You would not require this information for normal operation. It is only useful if you are facing any problem related to connecting over 3G.



3G Properties

Signal Strength

Status

Roaming Status

Not Roaming

Current Band

No Service

Network Informatation

Network Type

NONE

Network Name

Bit Error Rate(%)

0.14

Signal Strength(dBm)

-110

APN used

Country

Hardware Details

Firmware Version J1_0_1_4AP C:/WS/FW/J1_0_1_4AP/

Hardware Version 31,2E30

Model Type MC8785V

Modem Manufacturer Sierra Wireless

Device Information

Serial D56093800711016

IMEI 351532020022957

ICCID ICCID: 8901310000000

IMSI 112345678901

Phone Number ",0

SIM Status SIM OK

Session Information

Status

IP Address

0.0.0.0

Figure 11: 3G Properties window

- **Signal Strength**: Number of bars displays the percentage of signal strength.
- **Status**: Displays Roaming and current band information.
- **Network Information:** Displays Network type, network name etc.
- **Hardware Details:** displays version related information about the hardware, firmware, model type and manufacturer.
- **Device information:** Displays cards information.
- **Session Information:** displays the status of the current session.

How do I connect to the company network?

If the OmniAccess 3500 NLG card has been properly activated and configured and at least one of the network interfaces has connectivity to the Internet, the OmniAccess 3500 NLG will automatically connect you to your company's network over a secure tunnel. The Interfaces section of the client GUI window will show the green lightening bolt symbol next to the interface that is currently serving the network connection.

Be sure that you are logged into your laptop with the user ID and password (NT Domain credentials) provided by your IT administrator for access to your company's network. If you use a different set of credentials to log into your laptop, you will see the lightening bolt color as yellow and you will have no access to your company's network.

Depending on network conditions, access to your company's network may not be immediately available after you log into your laptop. The appearance of the lightening bolt symbol will indicate when the secure tunnel to your company's network is established.

After your laptop boots up, one of the following three network interfaces, in the order of priority given below, is used for establishing a connection:

1. Ethernet on your laptop
2. Wi-Fi on your laptop
3. 3G wireless on your OmniAccess 3500 NLG card

A lower-priority interface is used if no connectivity is available for the higher-priority one(s).

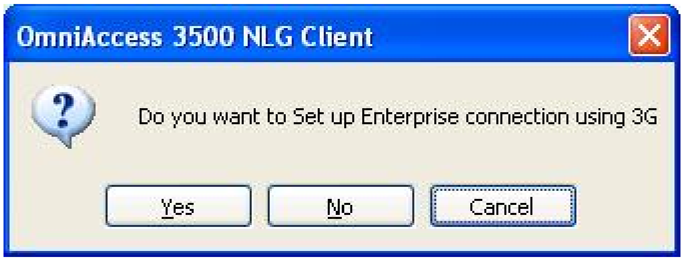
Once a connection has been established, the serving interface does not change unless the corresponding access network becomes unavailable (in which case the OmniAccess 3500 NLG automatically establishes a new connection over the available access network with the highest priority) or you switch it manually.

How do I manually change my serving network interface?

If you are connected to your company's network through the 3G modem on your OmniAccess 3500 NLG card and a Wi-Fi access point or an Ethernet outlet become available near you, you may want to switch your serving interface to experience faster network access. To manually switch from one interface to another, simply select the desired interface in the Interfaces section of the OmniAccess 3500 NLG Client window and click **Connect** in the Enterprise Connection Mode section (or simply double-click on the desired interface). The Status bar will show the progress in the establishment of the new connection.

What if my 3G plan is not unlimited?

If you do not want the OmniAccess 3500 NLG to automatically use the 3G connection (for example, because your 3G service provider charges you based on traffic), uncheck the **Auto 3G Connect** checkbox in the 3G section of the OmniAccess 3500 NLG Client window. If the system subsequently needs to connect via 3G, the following pop-up window appears:



OmniAccess 3500 NLG Client

Do you want to Set up Enterprise connection using 3G

Figure 12: Auto 3G prompt window

Click **Yes** or **No**, depending on whether you want to use the 3G interface to connect to your company's network.

If you are connected to your company's network through the 3G modem on your OmniAccess 3500 NLG card and you want to drop the 3G connection without replacing it with another connection, select the OmniAccess 3500 NLG card in the Interfaces section of the OmniAccess 3500 NLG Client window and click the **Disconnect** button (the **Disconnect** button is available only if the **Auto 3G Connect** option is not set).

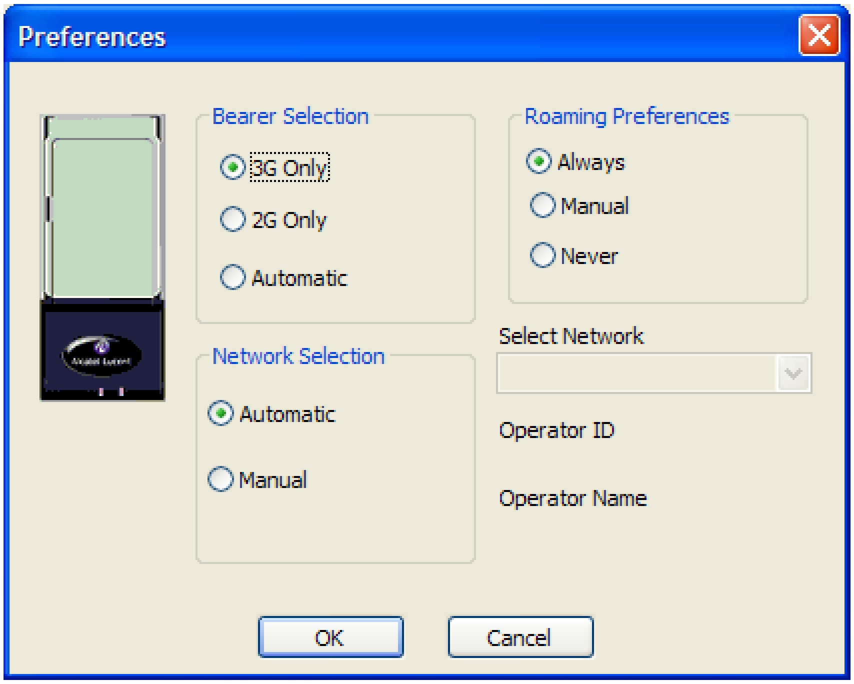
Note: The setting of the Auto 3G Connect checkbox is overridden when the 3G connection is initiated by the OmniAccess 3500 NLG gateway (at times when the laptop may be powered off or not already connected to the gateway).

How do I select my roaming and network preferences?

To avoid paying the extra connectivity fees that wireless service providers different than yours may charge when you roam through their networks (being attached to a *visited network* instead of your *home network*), you can prevent your 3G modem from connecting to a visited network by disabling its roaming capability. You can also prevent your modem from attaching to low-bandwidth wireless networks.

To select your preferred roaming and networking modes, do the following:

1. On the OmniAccess 3500 NLG Client window, from the Wireless menu, click **Preferences**. The Preferences window appears.



Preferences

Bearer Selection

● 3G Only

○ 2G Only

○ Automatic

Network Selection

● Automatic

○ Manual

Roaming Preferences

● Always

○ Manual

○ Never

Select Network

Operator ID

Operator Name

Figure 13: 3G Preferences Window

2. In the Bearer selection section of window you can select the type of carrier **2G, 3G or Automatic**.
3. In the Roaming section of the window, you can set the 3G preference to Automatic, Manual or Never. Selecting Never will disable roaming for the OmniAccess 3500 NLG. Select **Automatic** (to keep both in-network and out-of-

network attachment available). If you select manual then the network available will be displayed in the Select Network drop down drop down list.

Note: The Roaming Guard, Roaming Mode, and Network Mode settings are overridden when the 3G connection is initiated by the OmniAccess 3500 NLG gateway (at times when the laptop may be powered off or not already connected to the gateway).

How do I connect from a public hotspot?

Wi-Fi access points and Ethernet outlets in hotels and other public places often require you to enter additional credentials (for example, a local user ID and password or your credit card information) before granting network access. Since the OmniAccess 3500 NLG cannot know in advance the type of access negotiation implemented at every such place, you will be required to interactively submit your local access credentials.

To establish connectivity from a location that requires the submission of local-access credentials, you must complete the following procedure within the time allowed by your IT administrator (Default configured is five minutes):

1. Select the desired interface (Wi-Fi or Ethernet) to make the connection.
2. Select the **Hotspot** radio button and Click **Authenticate and Connect** button.
3. A window will appear asking for the proxy information. Please leave this blank and simply hit the OK button.
4. Now an Internet Explorer window opens, displaying information about the visited hotspot and asking you to enter the information required to access the public network.
5. After you enter the required information, the OmniAccess 3500 NLG can establish a secure tunnel to your company's network through the public network.

Note: While establishing connection via hotspot if you get either "Action Cancelled" or "The page cannot be displayed" window then try refreshing the browser page

Authentication and Security

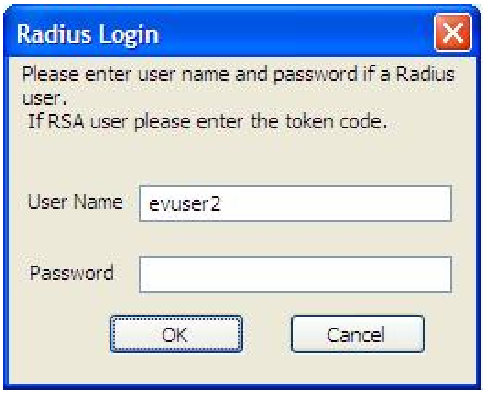
RADIUS only: How can I access the network using RSA SecureID?

If your user account is configured for RADIUS authentication, you may have to use RSA SecureID to access your network. The following two sections describe the access procedures for the first login after configuration of the RSA SecureID access method and for all subsequent logins.

FIRST RSA SECUREID LOGIN

Follow the steps below the first time you access your network as an RSA SecureID user:

1. On the RADIUS Login prompt window (**Error! Reference source not found.**), fill the *User Name* field with your login name and the *Password* field with the *tokencode* displayed on the RSA Secure ID device. Click **OK**.



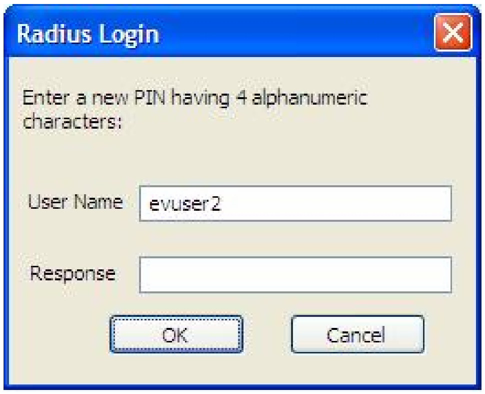
Please enter user name and password if a Radius user.
If RSA user please enter the token code.

User Name: evuser2

Password:

Figure 14: RADIUS Login prompt window for first login

2. A second RADIUS Login prompt window appears (**Error! Reference source not found.**). Fill the *Response* field with your PIN (the PIN can be a 4-8 character numeric or alphanumeric string, depending on the configuration of your user account). Click **OK**.



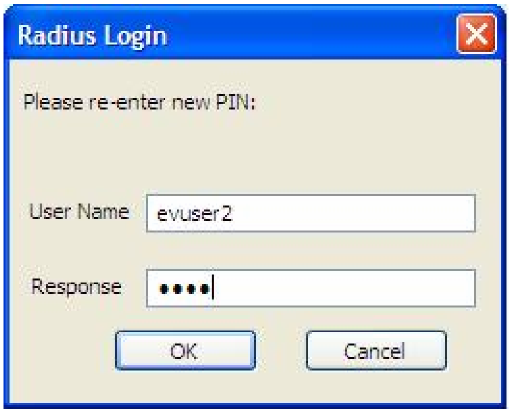
Enter a new PIN having 4 alphanumeric characters:

User Name: evuser2

Response:

Figure 15: Second RADIUS Login prompt window for first login

3. A third RADIUS Login prompt window appears (**Error! Reference source not found.**). Enter again your PIN in the *Response* field. Click **OK**.



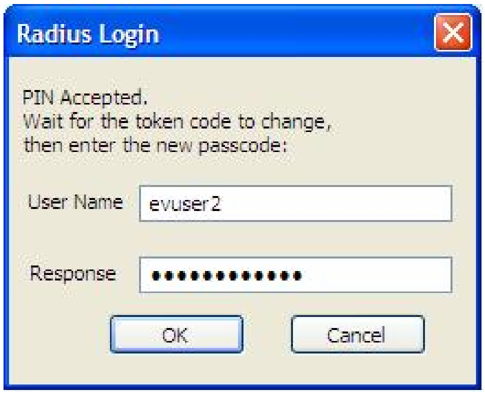
Please re-enter new PIN:

User Name: evuser2

Response: ••••

Figure 16: Third RADIUS Login prompt window for first login

4. A fourth RADIUS Login prompt window appears (**Error! Reference source not found.**). Fill the Response field with your *passcode* (PIN + *tokencode*) after the *tokencode* has changed value on the RSA SecureID display. Click **OK.**



Radius Login

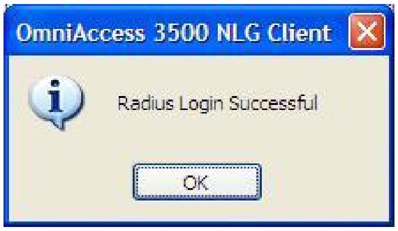
PIN Accepted.
Wait for the token code to change,
then enter the new passcode:

User Name: evuser2

Response: ●●●●●●●●●●●●

Figure 17: Fourth RADIUS Login prompt window for first login

5. A login confirmation window appears (**Error! Reference source not found.**) if you have entered all credentials successfully.



OmniAccess 3500 NLG Client

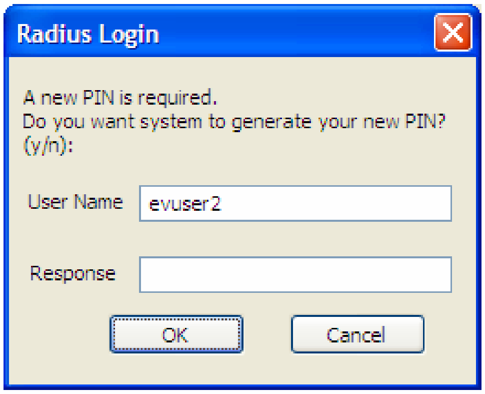
Radius Login Successful

Figure 18: RADIUS Login confirmation window for first login

Note: If you enter wrong values for your credentials (whether the PIN or the token code) for three consecutive times, you will be placed in next token-code mode*. In this mode, you will have to enter the correct* passcode *twice.*

System Generated PIN

RSA Authentication Manager can be configured by the administrator such that the user can either get a System generated PIN or user can enter a new PIN. You can receive a system - generated PIN by entering ‘Y’ in the *Response* field as shown below if RSA manager is configured for the cards.


Radius Login

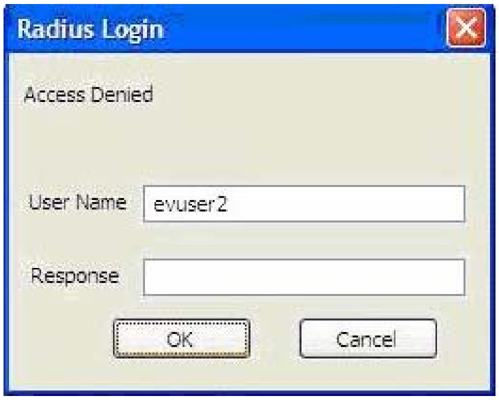
A new PIN is required.
Do you want system to generate your new PIN?
(y/n):

User Name: evuser2

Response:

Figure 19: System Generated PIN

In case you are not satisfied with the systems generated PIN and want another pin to be generated by the system then you can also do so by entering ‘N’ at the next *Response* field.


Radius Login

Access Denied

User Name: evuser2

Response:

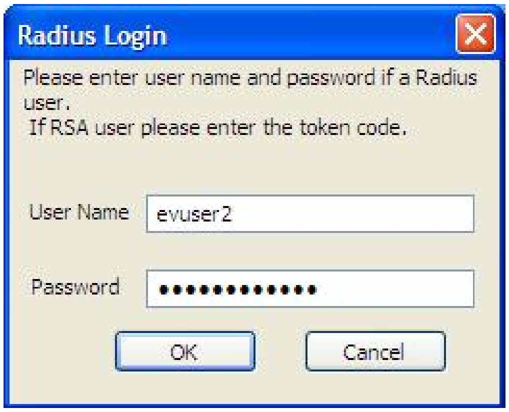
Figure 20: Access Denied

Important Note: - *If you get an Access denied screen at this point then close the application and restart. This feature is under modification.

SUBSEQUENT RSA SECUREID LOGINS

The following procedure applies to all RSA SecureID logins following the first one:

1. On the RADIUS Login prompt window (Figure 21**Error! Reference source not found.**), fill the *User Name* field with your login name and the *Password* field with your current *passcode* (PIN + *tokencode* currently displayed on the RSA SecureID device). Click **OK**.



Radius Login

Please enter user name and password if a Radius user.
If RSA user please enter the token code.

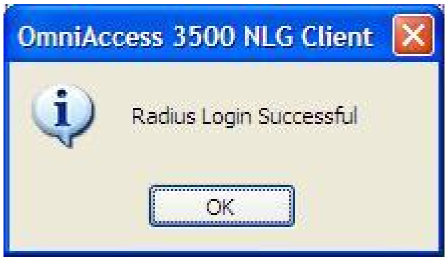
User Name: evuser2

Password: ●●●●●●●●●●●●

Figure 21: RADIUS Login prompt window for returning user

The Pin is a 4 -8 digit number configured at the Administrator end and the Token code is an 8 digit number displayed on the RSA Secure ID Authenticator device.

2. If the credentials you entered are correct, Radius Login Successful should appear.



OmniAccess 3500 NLG Client

Radius Login Successful

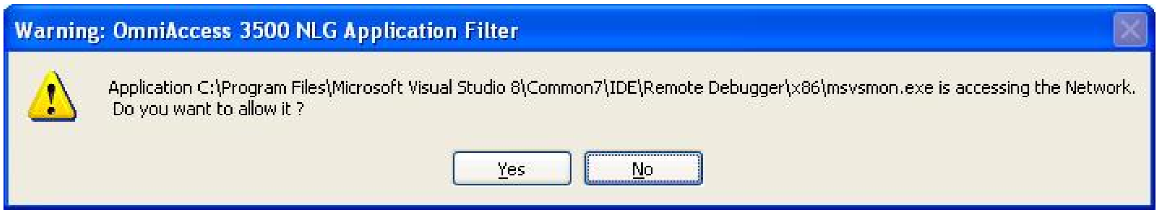
Figure 22: Successful RADIUS Login

How do I manage my personal firewall?

The personal firewall that resides in your OmniAccess 3500 NLG card may prevent some applications in the laptop from opening network connections. However, a setting in your personal firewall policy may allow you to override the default decision of the personal firewall.

ALLOWING AN APPLICATION THROUGH THE FIREWALL

If your personal firewall policy allows you to override its default settings regarding the treatment of certain applications, an OmniAccess 3500 NLG Application Filter window pops up on the laptop screen every time the personal firewall detects an attempt to open a network connection by one of your applications. The window offers you the option to allow (click **Yes**) or deny (click **No**) the network connection.



Warning: OmniAccess 3500 NLG Application Filter

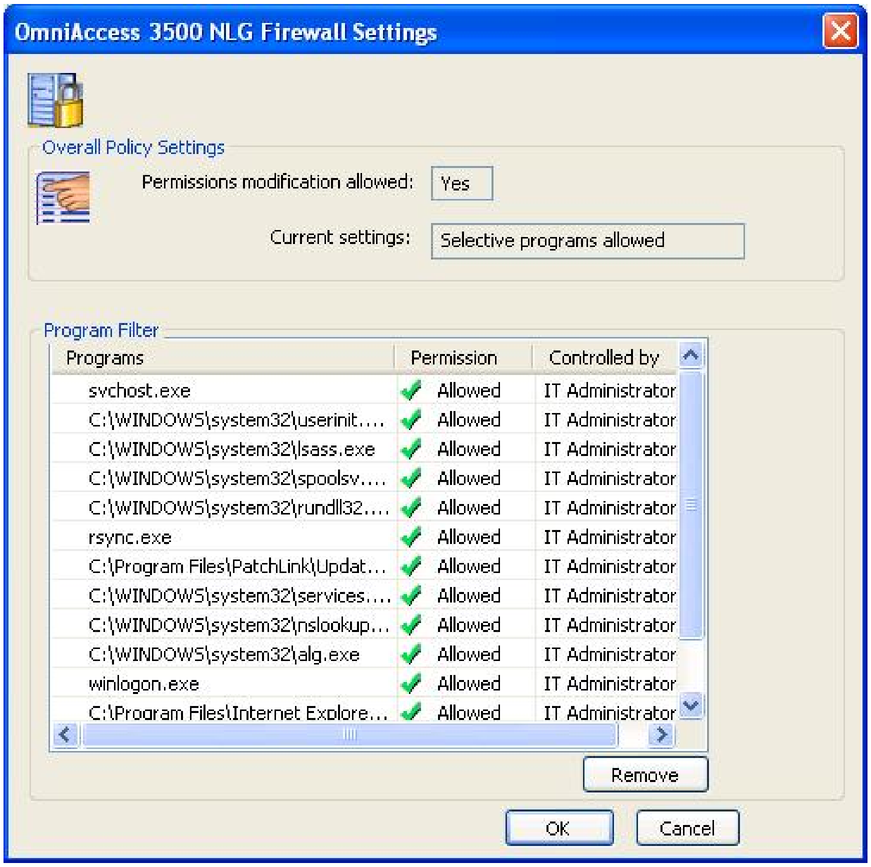
Application C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\Remote Debugger\x86\msvsmon.exe is accessing the Network.
Do you want to allow it ?

Figure 23: Personal Firewall Application prompt

The personal firewall will remember your answer for all future attempts to open a network connection by the same application. If you want to change your decision for the application, you need to remove the application from the list of applications for which the personal firewall has a set allow/deny policy (see the instructions in the *Removing* an application from the firewall list section below). The next time the application tries to open a network connection, you will be asked again if you want to allow or deny the connection request.

VIEWING PERSONAL FIREWALL SETTINGS

The **Personal Firewall Settings** option in the **NLG** menu opens a window with the list off all the applications running on your laptop for which the personal firewall has a set allow/deny rule.



OmniAccess 3500 NLG Firewall Settings

Overall Policy Settings

Permissions modification allowed: Yes

Current settings: Selective programs allowed

Program Filter

Programs	Permission	Controlled by
svchost.exe	✓ Allowed	IT Administrator
C:\WINDOWS\system32\userinit....	✓ Allowed	IT Administrator
C:\WINDOWS\system32\lsass.exe	✓ Allowed	IT Administrator
C:\WINDOWS\system32\spoolsv....	✓ Allowed	IT Administrator
C:\WINDOWS\system32\rundll32....	✓ Allowed	IT Administrator
rsync.exe	✓ Allowed	IT Administrator
C:\Program Files\PatchLink\Updat...	✓ Allowed	IT Administrator
C:\WINDOWS\system32\services....	✓ Allowed	IT Administrator
C:\WINDOWS\system32\nslookup...	✓ Allowed	IT Administrator
C:\WINDOWS\system32\alg.exe	✓ Allowed	IT Administrator
winlogon.exe	✓ Allowed	IT Administrator
C:\Program Files\Internet Explore...	✓ Allowed	IT Administrator

Figure 24: Personal Firewall Settings window

REMOVING AN APPLICATION FROM THE FIREWALL LIST

You can delete an application from the list of applications that are allowed or denied through the personal firewall, provided that you have permission to do so. You have permission to manage the handling of the application in the personal firewall if the <User> value is shown next to the application in the "Controlled by" column. The <User> value can only be found next to applications for which you have been previously asked for an allow/deny decision. Your personal firewall policy may prevent you from ever making the decision about any application.

Do the following to remove an application from the personal firewall list:

1. On the OmniAccess 3500 NLG Client window, open the **NLG** menu and click **Personal Firewall Settings.** The OmniAccess 3500 NLG Firewall Settings window appears.
2. Click an application to highlight it and then click **Remove**. If you have the necessary permission, the personal firewall removes the application from the list of applications with set allow/deny rule. You will be asked to set the rule again the next time the application tries to open a network connection.

   Note: If you try to remove an application over which you have no control, an error message appears, stating that the item you selected is not under your control. You will not be allowed to remove the item.

How do I secure my sensitive data?

Your IT administrator may decide to create an encrypted drive in your laptop's hard disk for storage of sensitive data. In that case you are encouraged to store all sensitive files in the secure drive only. If the laptop is lost or stolen, your IT administrator can remotely remove from the OmniAccess 3500 NLG card the secret password that is needed for decrypting the data in the secure drive thus making the data stored in the encrypted volume inaccessible to anyone.

No extra steps are required to operate the secure drive. The OmniAccess 3500 NLG automatically mounts the drive after you successfully log into the laptop with your Windows NT account. You will have no access to the secure drive if you are logged-in using any other account (e.g., a Guest account) to log into your laptop.

Warning: The secure drive is created and maintained using the TrueCrypt open source software. To avoid the loss of the sensitive data stored in the secure drive you should never use the TrueCrypt user interface for any purpose (e.g., to modify the secure drive configuration). Please contact your IT administrator if you need assistance with your secure drive.

If your IT administrator decides to create the secure drive after you have started using your OmniAccess 3500 NLG card, the installation of the TrueCrypt software may be either automatic (driven by your company's IT solution for remote software distribution and installation) or manual. If you are required to manually install the TrueCrypt software, please note the following:

- The OmniAccess 3500 NLG Release 1.6 is compatible with TrueCrypt Version 4.3a 5.1a, 6.0a. The latest version of the software can be downloaded from http://www.truecrypt.org/downloads.php.

- For all information about the TrueCrypt software, please refer to the documentation available at http://www.truecrypt.org.
- Accept all default values during the installation. Any deviation from the default values may compromise the installation.

While the secure drive is being created (by request of your IT administrator), your keyboard and mouse will be locked for a short time. Do not reboot your laptop during this process. . The keyboard and mouse will unlock when the secure drive creation completes after a couple of minutes.

USING A LAPTOP THAT IS CONFIGURED FOR SMART CARD LOGIN

You can skip this section if your laptop is configured for the default NT Domain login.

If the laptop is configured for smart card login, everything remains the same except the following:

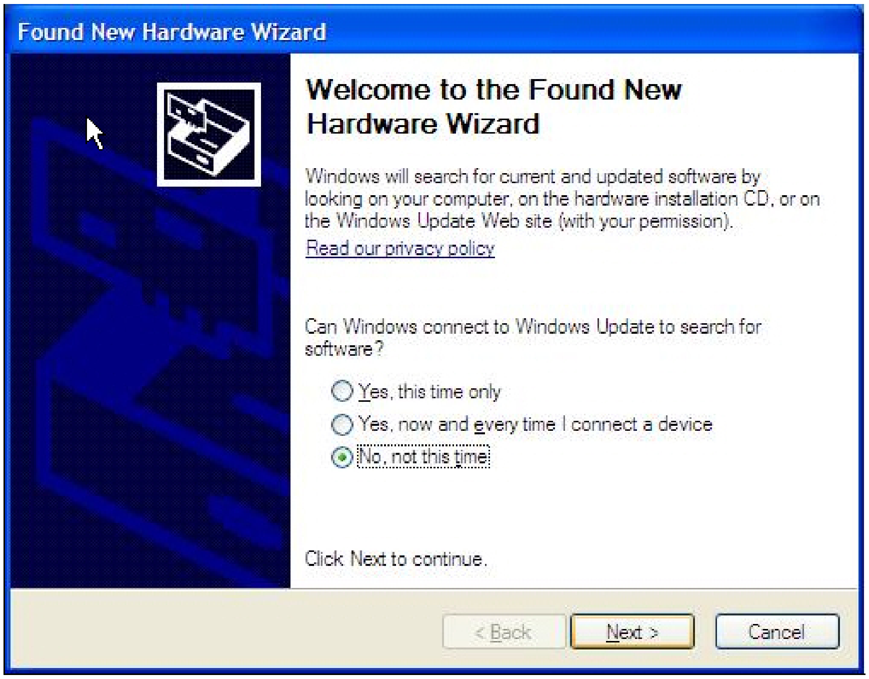
1. To start the login and logout procedures you must press the **Ctrl-Alt-Backspace** key combination instead of the **Ctrl-Alt-Delete** combination. To login, please enter your six digit PIN. Default PIN is 123456, and it should be changed using the steps described below. Note that the smart card - Authentication works only if you are using laptop key, any external keyboard may not authenticate.
2. To complete the login procedure you must enter a six-digit PIN instead of your NT Domain username and password.
3. To change the login PIN, click **Start > Run**, type the command <pintool>, and click **OK**. You finish by entering the old PIN and the new one.
4. Your login certificate is removed from your card and your smart card login is disabled after four consecutive unsuccessful login attempts made with an invalid PIN.
5. If the smart card login is disabled in your laptop you must contact your IT helpdesk to re-enable it. After the smart card login is re-enabled, the PIN is reset to a fixed default value (<123456>). For security reasons, you should invoke the *pintool* command to customize the PIN value immediately after the smart card login is re-enabled.
6. If you press the **Ctrl-Alt-Backspace** key combination after having logged into your laptop using the same sequence and your PIN, you may observe different behaviors depending on the *Group Policy* settings that your administrator has applied to your laptop. Note that the smart card - Authentication works only if you are using laptop key, any external keyboard may not authenticate. The following options are available: (i) <No Action>; (ii) <Lock Workstation> (to temporarily lock your laptop); and (iii) <Force Logoff> (to close your user session). You can verify the settings for you laptop by entering the *gpedit.msc* command at the **Start>Run** prompt and then checking the value of the *Local computer Policy>Computer Configuration>Windows Settings>Security Settings>Local Policies>Security Options>Interactive logon: Smart card removal behavior* policy.

Note: - If your laptop is coming out of sleep mode or hibernate mode than the NLG LED will blink a red light for few seconds. Wait until it turns to a solid red light and then login by pressing **Ctrl-Alt-Backspace**.

DRIVER INSTALLATION FOR PREBOOT LOADING

If your administrator has enabled Preboot settings for your smart card then you need to install serial driver as shown in the procedure below.

1. Reboot the laptop. You will get Found New Hardware screen



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).

Read our privacy policy

Can Windows connect to Windows Update to search for software?

○ Yes, this time only

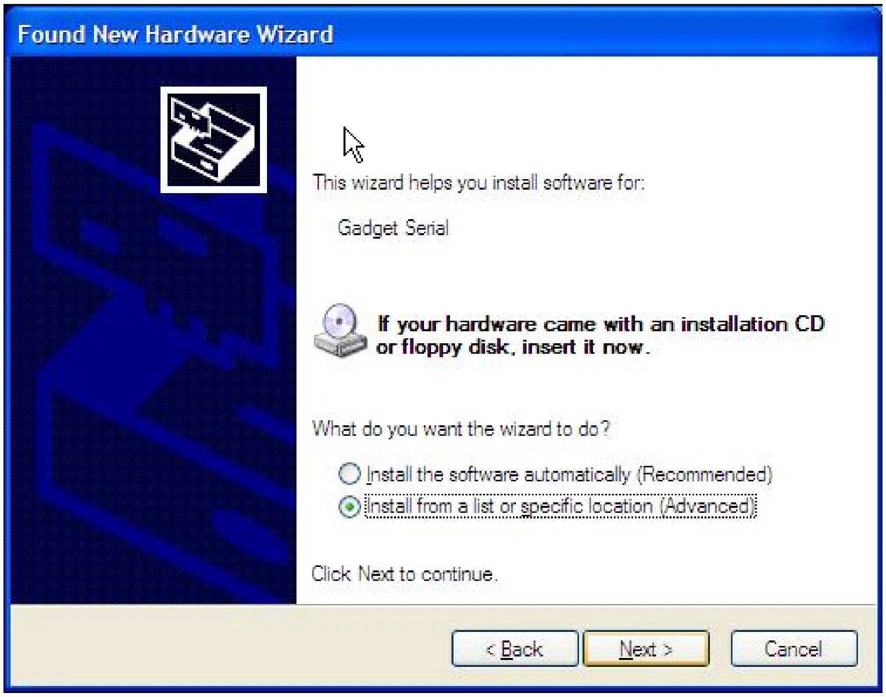
○ Yes, now and every time I connect a device

● No, not this time

Click Next to continue.

Figure 25: Found New Hardware Wizard

2. Click No, not this time



Found New Hardware Wizard

This wizard helps you install software for:

Gadget Serial

If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

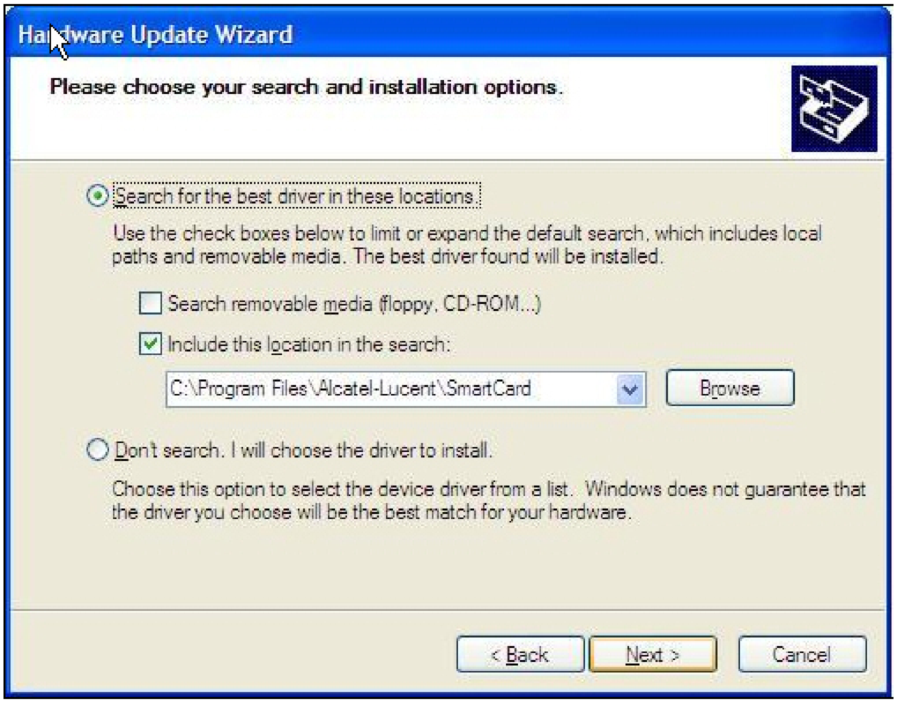
○ Install the software automatically (Recommended)

● Install from a list or specific location (Advanced)

Click Next to continue.

Figure 26: Found New Hardware

3. Select option: Install from a list or specific location (Advance)



Hardware Update Wizard

Please choose your search and installation options.

● Search for the best driver in these locations.

Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.

□ Search removable media (floppy, CD-ROM...)

☑ Include this location in the search:

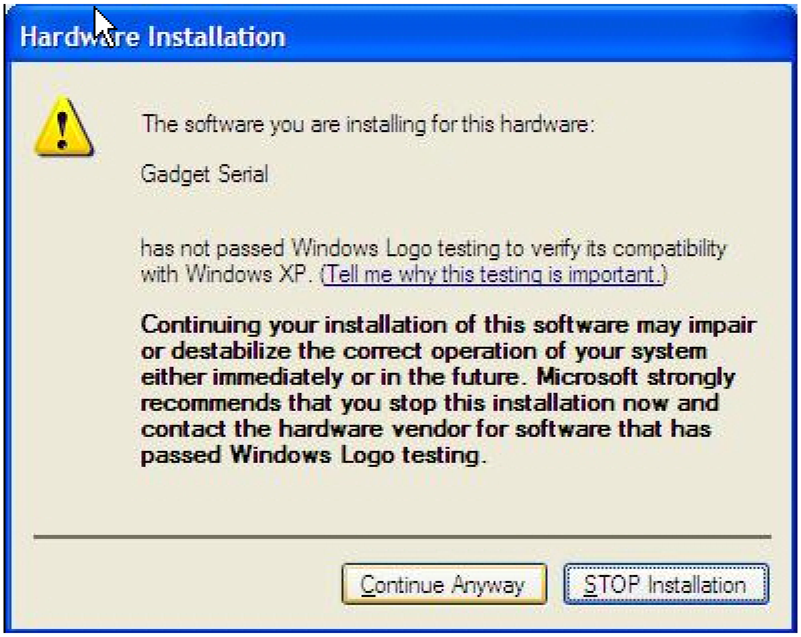
C:\Program Files\Alcatel-Lucent\SmartCard

○ Don't search. I will choose the driver to install.

Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.

Figure 27: Locating the Serial driver path

4. Now Select option: Search for the best driver in these locations. Check option Include this location and browse to locate path : **C:\Program Files\Alcatel-Lucent\SmartCard**



Hardware Installation

The software you are installing for this hardware:

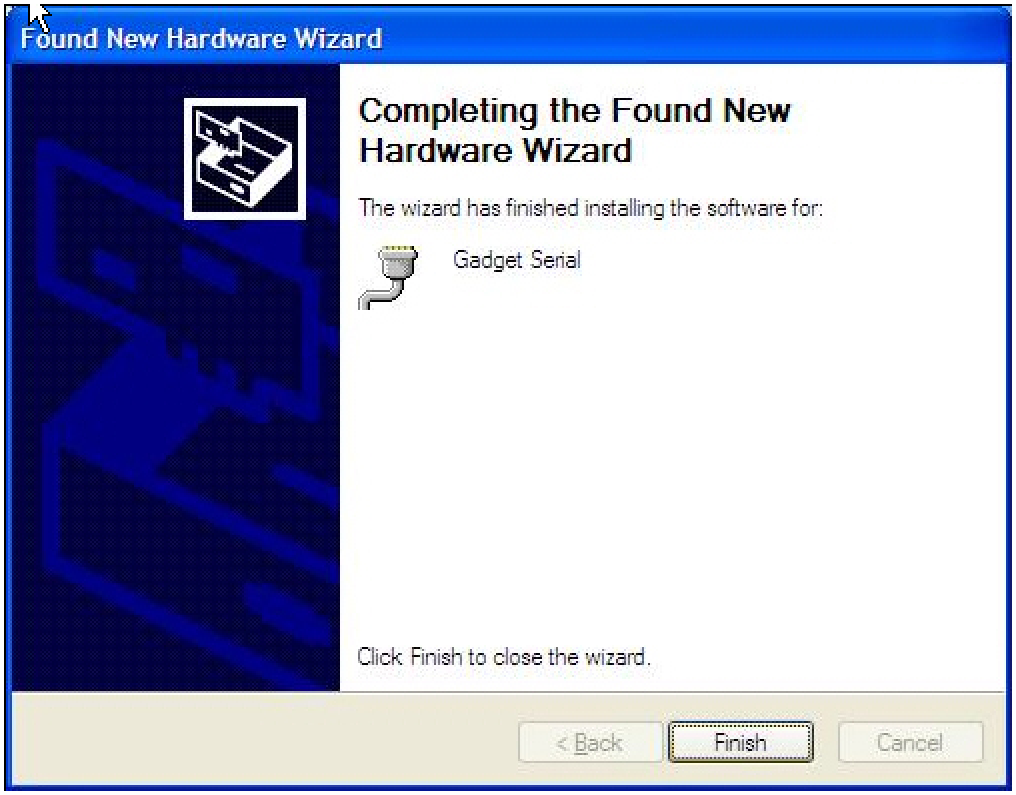
Gadget Serial

has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)

Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.

Figure 28: Gadget Serial warning

5. You will get a Hardware Installation screen. Click **Continue Anyway.**



Completing the Found New Hardware Wizard

The wizard has finished installing the software for:

Gadget Serial

Click Finish to close the wizard.

Figure 29: Gadget Serial software installed

6. Click **Finish** to complete.

Card, Laptop and SIM

How do I remove the card from my laptop?

Strictly observe the following procedure for extraction of the card depending on the power state of your laptop:

- Laptop in *Power On* state — You MUST stop the OmniAccess 3500 NLG card device on the **Safely Remove Hardware** Windows utility before you physically extract the card from the CardBus slot in your laptop. Failure to run the Safely Remove Hardware utility may compromise the future operation of your card and laptop.
- Laptop in *Standby/Hibernate/Power Off* state — You MAY extract the OmniAccess 3500 NLG card from the CardBus slot after your laptop enters the Standby, Hibernate, or Power Off mode. In that case, you MUST always plug the card back into the CardBus slot before your laptop powers up again. Failure to plug the card back in before power-up will result in NLG-locking of the laptop.

How to upgrade modem firmware?

Follow the procedure to upgrade the firmware of OmniAccess 3500 Nonstop Laptop Guardian Card (EVDO).

1. **Click 3G** > Upgrade Modem Firmware on main menu
2. Click **OK** on the confirmation box to start the upgrade

How do I insert SIM in OmniAccess 3500 Nonstop Laptop Guardian Card?

Insert the SIM card in the SIM slot (Figure 4). The cut on the SIM should be at the left side and directed towards the LED when inserting the card to the slot. *Reset the Card after inserting the SIM else SIM will not be detected.*

How to take out the SIM (Subscribers Identity Module) from OmniAccess 3500 Nonstop Laptop Guardian Card?

Important: Removing the SIM card requires the card to be switched off.

Switch off your OmniAccess 3500 Nonstop Laptop Guardian Card after safely removing the Card from Laptop whenever you are taking the SIM (Subscribers Integrity Module) Card Out of the OmniAccess 3500 Nonstop Laptop Guardian Card.

What if my laptop is lost or stolen?

Please call your IT Helpdesk immediately. They may be able to take the following actions:

1. Remotely lock the laptop to prevent any access to it.
2. Get the physical location of the laptop. You may ask the location as it may help you retrieve the laptop.
3. Remotely remove the password for the encrypted volume making the sensitive data inaccessible.

What if my laptop is locked?

To protect your laptop/ data stored in the encrypted volume/ the network it may be necessary to lock your laptop further denying any access to it. There are two types of locks:

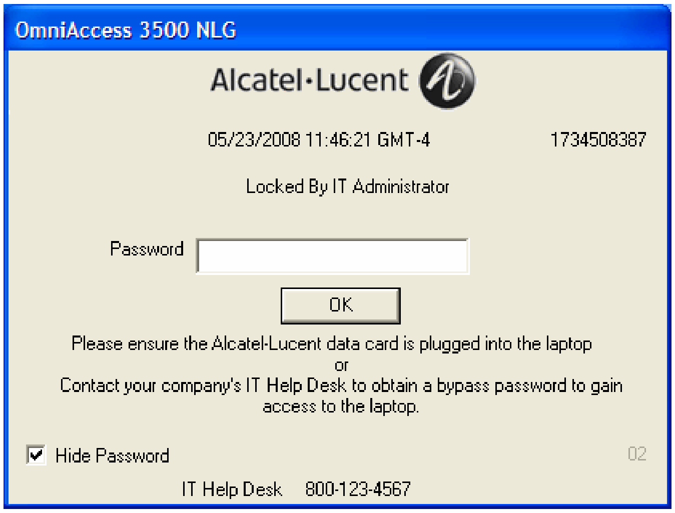
1. **Windows Lock** – In such cases the Windows standard lock screen will appear. However there would be another pop-up window with the reason for locking the laptop.

   Normally this is done for less severe situations prompting you to take an action. In the current release it will happen only if you have turned off the 3G radio modem by pressing the switch in front of the card.

   To unlock, you can either turn on the 3G radio modem by again pressing the switch if the operating environment no longer requires the modem to be off (e.g. the airplane landing and takeoff is complete) else press Ctrl-Alt-Del and enter your domain password.

2. **NLG Lock** – This prevents any further access to the laptop and is done for high-risk events threatening the integrity of the laptop, data stored or the network. A lock screen similar to the one on Figure 30 will appear indicating the reason for locking and other information. The administrator’s contact information is also displayed at the bottom of the screen.

Unlocking can be done only by rectifying the cause of lock or by getting the One Time Password (OTP) from the administrator which will allow the access to the laptop for the limited duration as determined by the administrator.



05/23/2008 11:46:21 GMT-4 1734508387

Locked By IT Administrator

Please ensure the Alcatel-Lucent data card is plugged into the laptop
or
Contact your company's IT Help Desk to obtain a bypass password to gain access to the laptop.

IT Help Desk 800-123-4567

Figure 30: Sample Lock Screen

The following table shows all possible messages that may appear on the OmniAccess 3500 NLG window when your laptop is locked, the cause of the message, and actions that you can take to unlock the laptop.

Message	**Cause**	**Possible actions**
Locked By IT Administrator	The IT administrator has remotely locked the laptop.	Contact your IT administrator to unlock the laptop. The administrator can unlock the laptop remotely, or provide you a one-time-password (OTP) over the phone.
Secure Tunnel Down	Laptop has not been able to connect to your company's network for the duration specified by your administrator.	Return within 3G range, or turn on the modem power, or connect to a different access network (Wi-Fi or Ethernet). -or- Contact your IT administrator to get an OTP.
Card Communication Failed	Laptop is unable to communicate with the OmniAccess 3500 NLG card.	Re-insert the OmniAccess 3500 NLG card -or- Remove the card, toggle the battery switch, and re-insert the card.

Message	Cause	Possible actions
		-or- Contact your IT administrator to get an OTP.
Driver Configuration Error for <Interface>	The network drivers on the laptop have been misconfigured.	Contact the administrator to return the network drivers to their proper configuration. -or- Contact your IT administrator to get an OTP.
File Integrity Check Failed	An OmniAccess 3500 NLG critical file is missing or corrupt.	Restart the laptop to see if the OmniAccess 3500 NLG client software was able to recover the file. -or- Contact your IT administrator to get an OTP.
System Integrity Check Failed	An internal check has failed.	Restart the laptop and if it does not solve the problem then contact your IT administrator to get an OTP.
Invalid Card	The laptop and the OmniAccess 3500 NLG card are tied one-to-one. If the card inserted in the laptop is not the card configured for that laptop, the laptop locks. For the HSPA version of the card, the laptop locks also when the SIM is swapped.	Replace the correct card or contact your IT administrator to get an OTP.

One Time Password (OTP)

UNLOCKING LAPTOP USING ONE TIME PASSWORD (OTP)

If your laptop is locked and you are unable to rectify the cause, then you can still use your laptop for a limited duration by getting OTP from your administrator. To get OTP and unlock the laptop, following procedure may be used:

1. Please call your administrator using the contact information listed at the bottom of the lock screen.
2. In addition to verifying your identity and the need for OTP, you will be asked for the following information from the lock screen. The value in the () shows the sample values as displayed in Figure 30.

- Date (05/23/2008)
- Time (11:46:21)
- Timezone (GMT-4)
- Screen Count (1734508387)

3. You will be provided with a password consisting of small words separated by hyphens (-) such as MOT-SHOW-ROLL-FOUR-HYMN-ROVE. Please enter this password on your lock screen and hit OK to unlock the laptop.

   Note: Hyphens (-) are part of the password and you need to enter them. The OTP is not case sensitive. For the ease of typing the password you may uncheck the 'Hide Password' option if the environment permits.

The laptop then remains operational for a fixed amount of time, after which it locks again if in the meantime you have not removed the cause of the initial lock event.

Note that under the effect of the OTP some of important safety controls normally provided by OmniAccess 3500 NLG controls are disabled, therefore it is highly recommended to avoid being under OTP as far as possible.

After unlocking the laptop using OTP, you can connect directly to Internet using any of the laptop interfaces (cannot use the 3G interface) as you would do from a normal laptop. The access to the files stored in the encrypted volume will be available only if the OmniAccess 3500 NLG card is accessible.

The time remaining under the OTP can be seen by keeping the cursor on the OmniAccess 3500 NLG tray icon for few seconds. Your laptop will lock after the expiry of the OTP duration if the corrective action is not completed before the expiry of OTP. Of course you may always request another OTP from the administrator at the expiry.

SECURE CONNECTIVITY UNDER OTP

After your laptop enters the OTP mode of operation, you must manually select your preferred interface to establish the secure tunnel to the enterprise and gain access to the enterprise network.

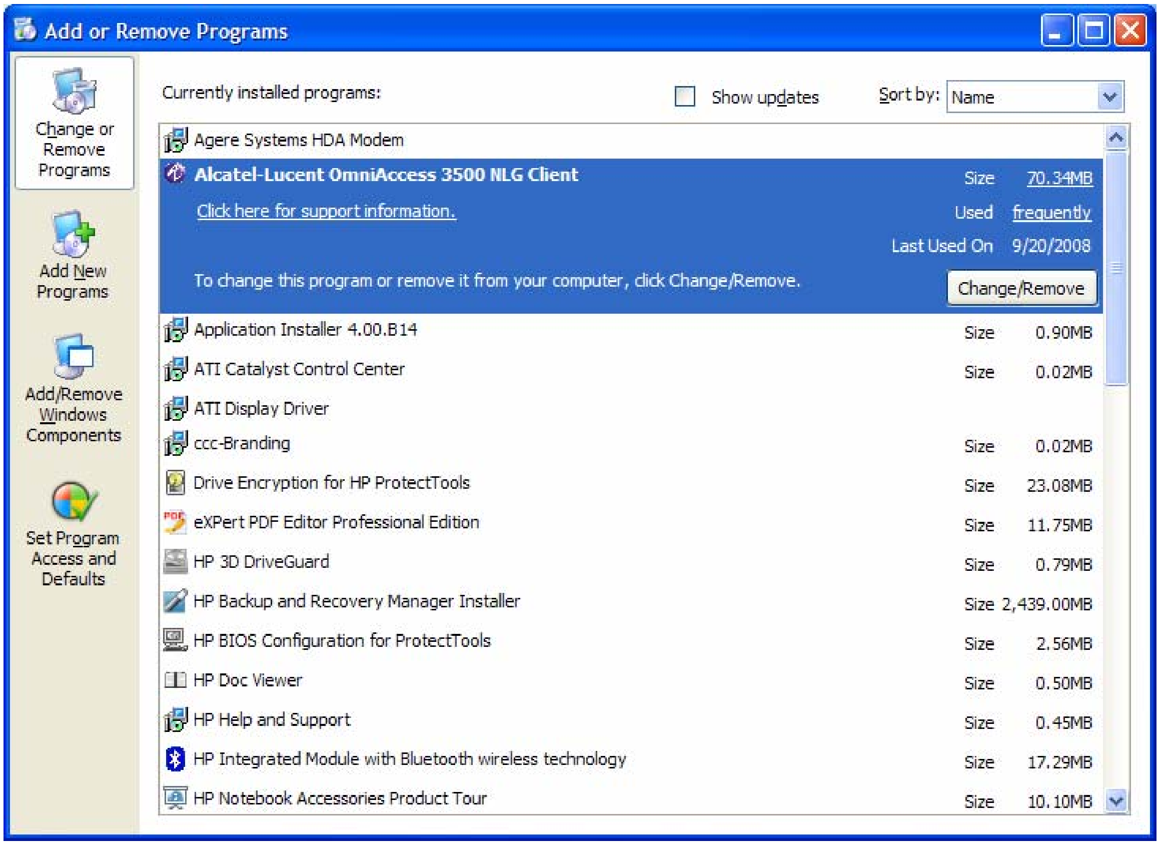
Your laptop may be in one of the following two states after entering the OTP mode:

1. There is no secure tunnel to the enterprise.
   - Select your preferred interface out of the ones that are currently available.
   - Click the **Connect** button.
2. The card is securely connected to the enterprise via the 3G interface but you are not authenticated with the network.
   - Uncheck the **Auto 3G** option (if currently checked).
   - Select the 3G interface and click **Disconnect** (the **Connect** button turns into a **Disconnect** button if the **Auto 3G** option is unchecked and the 3G interface is currently supporting the secure tunnel to the enterprise).
   - After the tunnel goes down, select the 3G interface and click **Connect**. After the tunnel comes back you will also be authenticated with your network.
   - Check the **Auto 3G** option if it was checked originally.

UNINSTALLING THE OMNIACCESS 3500 NLG CLIENT SOFTWARE

To uninstall the software follow the below procedure:

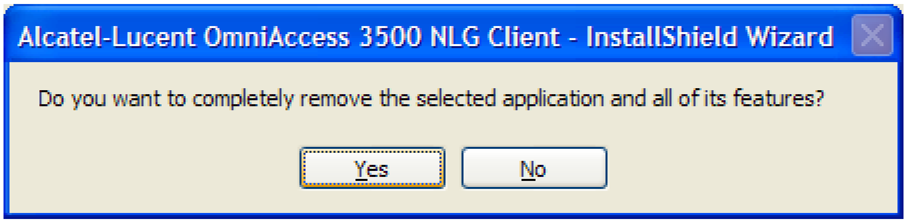
1. Click **Start > Settings > Control Panel**. Double-click **Add or Remove Programs**. Highlight the OmniAccess 3500 NLG entry and click **Remove**.


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
Currently installed programs:
□ Show updates
Sort by: Name
Change/Remove

Agere Systems HDA Modem		
Alcatel-Lucent OmniAccess 3500 NLG Client	Size	70.34MB
Click here for support information.	Used	frequently
	Last Used On	9/20/2008
To change this program or remove it from your computer, click Change/Remove.		
Application Installer 4.00.B14	Size	0.90MB
ATI Catalyst Control Center	Size	0.02MB
ATI Display Driver		
ccc-Branding	Size	0.02MB
Drive Encryption for HP ProtectTools	Size	23.08MB
eXPert PDF Editor Professional Edition	Size	11.75MB
HP 3D DriveGuard	Size	0.79MB
HP Backup and Recovery Manager Installer	Size	2,439.00MB
HP BIOS Configuration for ProtectTools	Size	2.56MB
HP Doc Viewer	Size	0.50MB
HP Help and Support	Size	0.45MB
HP Integrated Module with Bluetooth wireless technology	Size	17.29MB
HP Notebook Accessories Product Tour	Size	10.10MB

Figure 31

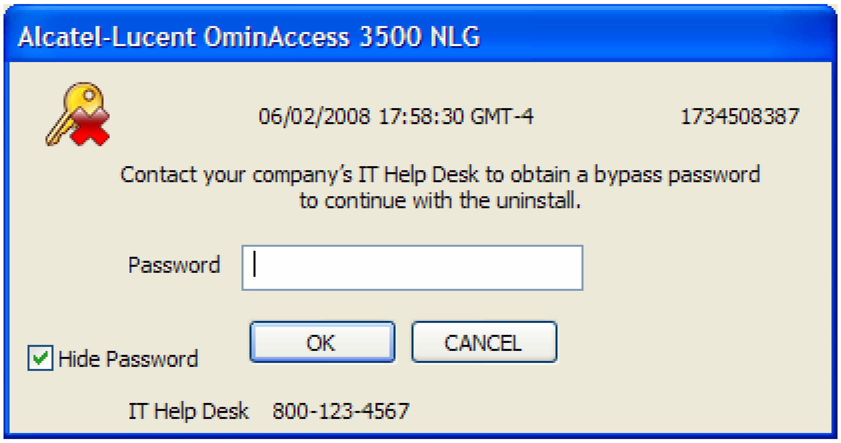
2. InstallationShield Wizard will appear. Click on **Next**.


Alcatel-Lucent OmniAccess 3500 NLG Client - InstallShield Wizard
Yes
No

Do you want to completely remove the selected application and all of its features?

Figure 32

3. Now click **Yes** to completely remove the software. Right after the uninstallation wizard starts running, the Uninstallation NLG Lock window of Figure 33 appears. You must obtain a valid OTP from your administrator before you can proceed with the uninstallation.



Alcatel-Lucent OminAccess 3500 NLG

06/02/2008 17:58:30 GMT-4 1734508387

Contact your company's IT Help Desk to obtain a bypass password to continue with the uninstall.

Password

☑ Hide Password

IT Help Desk 800-123-4567

Figure 33: Uninstallation NLG Lock window

Note: - You can run the uninstallation procedure directly from your corporate account if you logged into it using your NT Domain credentials (username and password). If instead you logged into the account using your smart card PIN, you must first log out and then log back into a non-smart card account with administrative privileges (e.g., the local Administrator account or an NT Domain account) before you can start the uninstallation procedure.

How to terminate the OTP mode of operation?

To get out of OTP mode after rectifying the problem, you should manually connect to your company's network using any of the interfaces. After the connection is established, please call the administrator or the helpdesk to issue a remote unlock command. This will take your laptop out of OTP mode and all OmniAccess 3500 NLG protection will be again enforced. Optionally your administrator might have issued an unlock command in advance. In this case your laptop will come out of OTP mode immediately after the connection to the Gateway is established and there is not need to call the administrator.

How do I get help?

If you need assistance using your OmniAccess 3500 NLG card, please contact your IT administrator.

Technical Specifications

This section presents LED, radio, electrical, environmental, and mechanical specifications for your OmniAccess 3500 NLG card.

LED Specifications

You find two LED bars on the external end of your OmniAccess 3500 NLG card. From left to right under the Alcatel-Lucent logo:

- **LED A (3G Modem)** can be in one of the following states:
  - No light: 3G modem is off.
  - Slow-blinking amber light: 3G modem is on.
  - Fast-blinking amber light: 3G modem is transmitting.
- **LED B (NLG)** can be in one of the following states:
  - No light: Card is in sleep mode or off.
  - Solid red light: Card is up, and can accept user input from Host (e.g. authentication credentials when applicable).
  - Solid amber light: Tunnel is up but user is not authenticated. Only management traffic can flow across the card and the gateway but no user traffic.
  - Solid green light: card is up, VPN tunnel is up and user is authenticated. Indicates that user has access to enterprise network.

Radio Frequency and Electrical Specifications

Approvals	Compliant with: CE GCF FCC IC IEEE 1725: In progress PTCRB: TBD
Data Services	850/900/1800/1900/2100 MHz WCDMA — DL up to 7.2 Mbps, UL up to 2.0 Mbps
Voltage	+3.3 VDC from PCMCIA Slot
Frequency Bands	850/1900/2100MHz WCDMA

	Power class 3 (+24dBm) 850/900MHz GSM/GPRS/EDGE GSM Power class 4/EDGE E2 1800/1900 MHz GSM/GPRS/EDGE GSM Power Class 1/EDGE E2 GPS/1575.42 MHz
Antenna Diversity	850/900/1800/1900/2100 MHz

Environmental and Mechanical Specifications

Temperature Operating Range	Operating Temperature: -25 to +60º C Storage Temperature: -30 to +85º C **Caution:** Contains Li-Ion battery. Do not expose to high temperature (above +60 °C).
Dimensions	138 mm (L) x 60 mm (W) x 5 mm (H) [15 mm (H) in extended portion only] Weight: 105- 110 g (3.7 – 3.88 oz)

Software and Additional Features

Software	OmniAccess 3500 NLG firmware
Battery	Internal Li-Ion rechargeable (not user replaceable) On/Off button for WCDMA modem.
Additional features	*The SD card slot is not operational in this release of the OmniAccess 3500 NLG card. Do not insert an SD card in the slot.*
	SIM card Slot
	Master reset switch

Regulatory Information

This section contains important regulatory notices about your OmniAccess 3500 NLG card.

Regulatory Notices

The design of the OmniAccess 3500 NLG card complies with U.S. Federal Communications Commission (FCC) and Industry Canada (IC) guidelines respecting safety levels of radio frequency (RF) exposure for portable devices, which in turn are consistent with the following safety standards previously set by Canadian, U.S. and international standards bodies:

- ANSI / IEEE C95.1-1999, IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3kHz to 300 GHz
- National Council on Radiation Protection and Measurements (NCRP) Report 86, 1986, Biological Effects and Exposure Criteria for Radio Frequency Electromagnetic Fields
- Health Canada, Safety Code 6, 1999, Limits of Human Exposure to Radio frequency Electromagnetic Fields in the Frequency Range from 3 kHz to 300 GHz
- International Commission on Non-Ionizing Radiation Protection (ICNIRP) 1998, Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz).

FCC ID: RUT-OA3541 — Industry Canada ID: 1737G-OA3541

CAUTION: The OmniAccess 3500 NLG card has been tested for compliance with FCC/IC RF exposure limits in the laptop computer(s) configurations with the side loading PC Card slot and can be used in laptop computers with substantially similar physical dimensions, construction, and electrical and RF characteristics. This PC card must not be co-located or operated in conjunction with any other antenna or transmitter. Use of this device in any other configuration may exceed the FCC RF Exposure compliance limit. **Note:** If this PC Card is intended for use in any other portable device, you are responsible for separate approval to satisfy the SAR requirements of Part 2.1093 of FCC rules.

Where appropriate, the use of the equipment is subject to the following conditions:

- **WARNING (EMI) — United States FCC Information**: This equipment has been tested and found to comply with the limits for a class B computing device peripheral, pursuant to Parts 15, 22, and 24 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

  This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful Section 4B: Regulatory Information 91 interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation.

  If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- o Reorient or relocate the receiving antenna
- o Increase the separation between the equipment and receiver
- o Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- o Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules and with RSS-210 of Industry Canada. Operation is subject to the following two conditions:

- o This device may not cause harmful interference, and
- o This device must accept any interference received, including interference that may cause undesirable operations.

FCC guidelines stipulate that the antenna should be more than 1 cm from the user. The highest reported SAR values of the OmniAccess 3500 NLG card by Alcatel-Lucent are:

- o Separation distance of at least 1 cm needs to be maintained to user's lap with OmniAccess 3500 NLG card inserted into the bottom PC Card slot of the laptop computer (0.633 W/kg).

CAUTION: Any changes or modifications not expressly approved by Alcatel-Lucent could void the user's authority to use the equipment.

- **WARNING (EMI) — Canada:** This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference causing equipment standard entitled "Digital Apparatus," ICES-003 of the Department of Communications.

  Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par le ministre des Communications.

  If you have purchased this product under a United States Government contract, it shall be subject to restrictions as set forth in subparagraph (c)(1)(ii) of Defense Federal Acquisitions Regulations (DFARs) Section 252.227-7013 for Department of Defense contracts, and as set forth in Federal Acquisitions Regulations (FARs) Section 52.227-19 for civilian agency contracts or any successor regulations. If further government regulations apply, it is your responsibility to ensure compliance with such regulations.

Safety and Notices

This section provides important information about the radio performance and safe use of your OmniAccess 3500 NLG card.

Important Notice

Because of the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the OmniAccess 3500 NLG card by Alcatel-Lucent are used in a normal manner with a well-constructed network, they should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Alcatel-Lucent accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the OmniAccess 3500 NLG card by Alcatel-Lucent, or for failure of the OmniAccess 3500 NLG card by Alcatel-Lucent to transmit or receive such data.

Safety and Hazards

Do not operate the OmniAccess 3500 NLG card by Alcatel-Lucent in areas where blasting is in progress, where explosive atmospheres may be present, near medical equipment, life support equipment, or any equipment which may be susceptible to any form of radio interference. In such areas, the OmniAccess 3500 NLG card by Alcatel-Lucent MUST BE POWERED OFF. It can transmit signals that could interfere with this equipment.

Do not operate the OmniAccess 3500 NLG card by Alcatel-Lucent in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the OmniAccess 3500 NLG card by Alcatel-Lucent MUST BE POWERED OFF. When operating, it can transmit signals that could interfere with various onboard systems.

The driver or operator of any vehicle should not operate the OmniAccess 3500 NLG card by Alcatel-Lucent while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some jurisdictions, operating such communications devices while in control of a vehicle is an offense.

Battery Information

Your OmniAccess 3500 NLG card has an internal Li-Ion rechargeable battery.

- The battery gets charged when the card is plugged into your laptop and the laptop is powered on.
- The battery gets discharged when the 3G modem is on and one of the following conditions holds:
  - The card is not plugged into your laptop.
  - The card is plugged into your laptop, the laptop is powered on, and the 3G modem is transmitting at maximum power because network coverage is bad at your current location.

  - o The card is plugged into your laptop, and the laptop is in Standby/Hibernate/Shutdown mode.

- If the battery is out of charge, plug the card into the laptop, connect the laptop to a power source, and leave the laptop powered up for at least two hours.

The battery has a limited number of charge cycles and may eventually need to be replaced. Note that the battery is not user replaceable: if the battery stops working, please contact your IT administrator, which can make arrangements to have the battery replaced and disposed of by your 3G service provider.

The battery can be damaged if the card is dropped or exposed to extreme temperatures. Always try to keep the card at room temperature. A card with a hot or cold battery may temporarily not work, even when the battery is fully charged. Li-Ion batteries are particularly affected by temperatures below 0 °C (32 °F). The battery should not be charged at temperatures below 0 °C (32 °F) or above 45 °C (113 °F).

Do not place your card in areas that may get very hot, such as on or near a cooking surface, cooking appliance, iron, or radiator. Keep you card away from fluids and moisture.

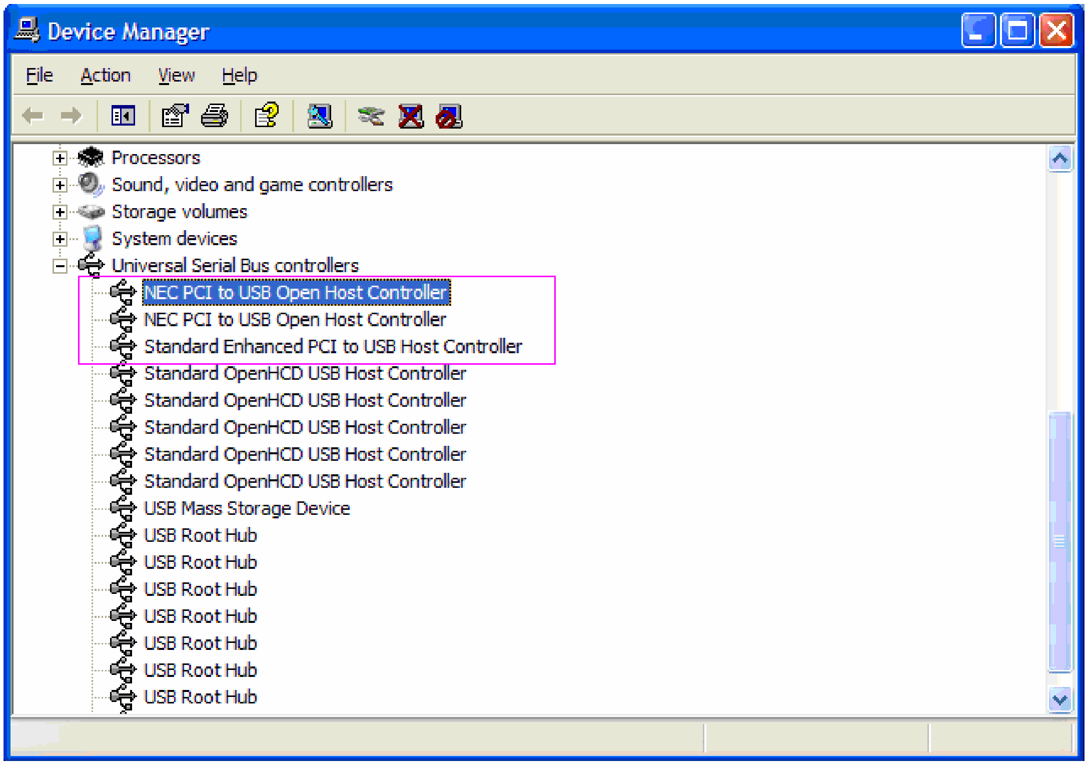
Appendix: How to check if card is a defunct?

Any card that passes the below test is NOT a Defunct card.

1. Reboot the laptop.
2. Turn off the card and then turn it back on
3. Insert in the laptop
4. Check Device Manager for following Controllers:

For EVDO Card check (Three controllers)	For HSPA Cards check (Two controllers)
▪ 2 x NEC PCI to USB Open Host Controller ▪ 1 x Standard Enhanced PCI to USB controller	▪ 2 x NEC PCI to USB Open Host Controller

*HSPA Cards have an extra SIM card Slot and External Antenna



Processors
Sound, video and game controllers
Storage volumes
System devices
Universal Serial Bus controllers
NEC PCI to USB Open Host Controller
NEC PCI to USB Open Host Controller
Standard Enhanced PCI to USB Host Controller
Standard OpenHCD USB Host Controller
Standard OpenHCD USB Host Controller
Standard OpenHCD USB Host Controller
Standard OpenHCD USB Host Controller
Standard OpenHCD USB Host Controller
USB Mass Storage Device
USB Root Hub
USB Root Hub
USB Root Hub
USB Root Hub
USB Root Hub
USB Root Hub
USB Root Hub

Figure 34

5. After a maximum of two minutes the red LED and the Yellow LED must come on. The Yellow LED will be blinking (EVDO) or steady (HSDPA).

6. If the card is plugged in a host with our host software then you should observe the followings:

- The card is recognized as the OmniAccess NLG 3500
- ping 169.254.0.1 succeeds
- If you push the 3G button, the modem information is there
- If you see the signal strength and in a decent signal area, there is signal strength

4. Card is charged (let in the slot for 1 hour), radio is ON, and when pulled out of the slot, after about 15 seconds the RED LED turns off, while the yellow LED starts blinking.

If a card is received as DOA (i.e. fails any of the above) following are possible resolutions:
1. If it fails 1: Cardbus controller is not responding or card is not powered, switch problem (look at J1 connector, NEC chip, power circuit).
2. If it fails 2: Card failed to boot > memory/fhash or OMAP problem
3. If it fails 3: Modem either not connected or antenna not connected or modem problem
4. If it fails 4: battery is not charging and/or connector is missing.

Appendix: Error Messages

The following error messages may be displayed on the bottom left of the main OmniAccess 3500 NLG client GUI window:

- *Error: Certificates not uploaded to the client card. Please use the NLG>Configure menu to upload certificates.*

  The certificates needed for authentication of the OmniAccess 3500 NLG card are missing. Make sure you have the full set (CA Certificate, User Certificate, and User Key) before trying to install them again. Contact your IT administrator if you are missing any of the required items.

- *Error: Card to certificate mapping failed at the gateway. Please contact your IT Administrator.*

  The User Certificate currently installed in your card may be outdated or incorrect. Contact your IT administrator to obtain a new User Certificate. If Card ID changes from EMS then it also shows the same error message.

- Error: Gateway name resolution failed. Please check the Gateway Name configured using **NLG>Configure** menu.

  The OmniAccess 3500 NLG client cannot find the IP address associated with the Gateway Name value currently configured in your card. Please check and correct the Gateway Name for any typing errors. If the problem persists contact your IT administrator.

- *Error: Gateway not reachable. Please check the Gateway Name configured using NLG>Configure menu.*

  It is not possible to reach the OmniAccess 3500 NLG gateway in your enterprise network. Make sure that the access network you are currently using has Internet connectivity and does not block outgoing VPN (IPsec) traffic. If the problem persists try a different access network.

- *Error in establishing connection over 3G. Please contact your service provider.*

  Connectivity to your enterprise network cannot be established using the 3G modem on your card. Make sure that your OmniAccess 3500 NLG card has been activated for 3G service. Also check if you are currently roaming into the network of a different service provider (a triangle next to the 3G signal level bars on the main client GUI window indicates this condition) and then if roaming is enabled for your card (**3G>Preferences** menu option). Contact your 3G service provider for further help.

- *Error: No license assigned to the card at the gateway. Please contact your IT Administrator.*

  There is no license currently assigned to your card. Contact your IT administrator to have a valid license assigned to your card.

- *Error: License for the card expired at the gateway. Please contact your IT Administrator.*

  The license allocated to your card has expired. Contact your IT administrator to request a license renewal.

- *Error: Domain Authentication Failed (Generic Error).*

  Your enterprise network could not authenticate you. The reason for the authentication failure is unknown. Contact your IT administrator if the problem persists.

  You are currently not logged into your valid NT domain account for the OmniAccess 3500 NLG (e.g., a local account on the laptop or an NT domain account that is not recognized by the OmniAccess 3500 NLG). Log out and then log into your valid NT domain account. Contact your IT administrator if the problem persists.

- *Error: Domain Authentication Failed (Domain Controller could not be contacted).*

  Your enterprise network could not authenticate you because the network's domain controller could not be reached. Contact your IT administrator if the problem persists.

- *Error: Domain Authentication Failed (Gateway Authentication Module could not be contacted).*

  The gateway failed to complete your authentication. Contact your IT administrator if the problem persists.

- *Error: Domain Authentication Failed (Laptop not in Domain). Please contact your IT Administrator.*

  Your enterprise network could not authenticate you because your laptop is not assigned to the appropriate network domain. Contact your IT administrator to have your laptop assigned to the appropriate network domain.

- *Error: Connection to 3G failed. Please contact your IT administrator.*

  The authentication to the 3G network might have failed then please contact your service provider.

- *Error: Timeout Waiting for response from Enterprise*

  The 3G connection is successful but the gateway is not responding to the NLG 3500 card. Please contact your IT administrator.