Alcatel·Lucent

OmniAccess 3500
Nonstop Laptop Guardian

Release 1.2

End-User Reference Guide

Document Version: 1.2.203

Part Number: 060226-10 Rev A

Published: 09.17.2007

Alcatel-Lucent Proprietary

Table of Contents

Welcome

Welcome to the *OmniAccess 3500 Nonstop Laptop Guardian — Release 1.2 — End-User Reference Guide*. This guide will introduce you to the many functions of the OmniAccess 3500 Nonstop Laptop Guardian (NLG) card and their operation.

For instructions on how to install your card and the client software, see the *OmniAccess 3500 Nonstop Laptop Guardian — Release 1.2 — Card Quick Start Guide*.

OmniAccess 3500 NLG Card Features Overview

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

The card supports the following functions:

- Secure connectivity with your company's network irrespective of your laptop's location and with no action required on your part.
- Automatic switching of network interface serving the connection to your company's network when the current serving interface (e.g., wired Ethernet) is disconnected.
- 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.
- 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).
- 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) to take the execution of time-consuming patch downloads away from the hours when you typically work with your laptop.

Common Operations

The following sections show you how to perform basic OmniAccess 3500 NLG operations on the graphical user interface (GUI) of the OmniAccess 3500 NLG client.

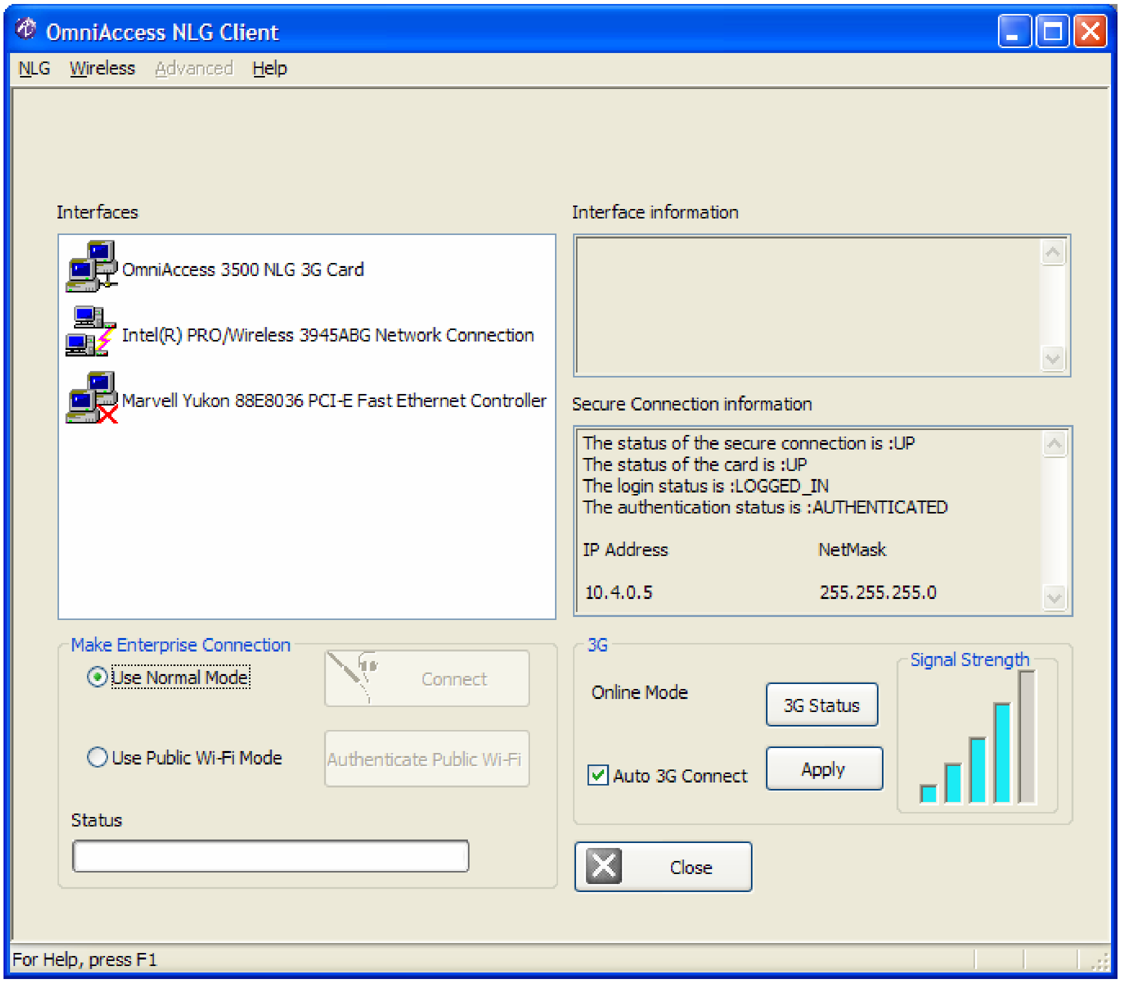
How do I get started?

The client GUI is accessible on your laptop after you have successfully installed the OmniAccess 3500 NLG card (see the *OmniAccess Nonstop Laptop Guardian — Release 1.2 — Card Quick Start Guide* for installation instructions).

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.
- Click Start -> Programs -> OmniAccess 3500 NLG Client Programs -> Alcatel-Lucent -> OmniAccess 3500 NLG -> OmniAccess 3500 NLG Client.

The OmniAccess 3500 NLG Client window appears.



Interfaces:
- OmniAccess 3500 NLG 3G Card
- Intel(R) PRO/Wireless 3945ABG Network Connection
- Marvell Yukon 88E8036 PCI-E Fast Ethernet Controller

Secure Connection information:

The status of the secure connection is :UP
The status of the card is :UP
The login status is :LOGGED_IN
The authentication status is :AUTHENTICATED

IP Address	NetMask
10.4.0.5	255.255.255.0

● Use Normal Mode
○ Use Public Wi-Fi Mode

Online Mode

☑ Auto 3G Connect

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** — Manage the OmniAccess 3500 NLG client. Available options:
  - **Show:** Display the main window of the client GUI.
  - **Configure:** Configure certificate files and user key.
  - **Personal Firewall Settings:** Manage the personal firewall settings on the OmniAccess 3500 NLG card.
  - **Close:** Hide the GUI window.
- **Wireless** — Manage the 3G wireless subscription. Available options:

  - **Modem Activation:** Activate the 3G modem.
  - **Update Data Profile:** Update the wireless parameters in the 3G modem.
  - **Preferences:** Configure roaming and network modes.
- **Advanced** — This menu is not active (grayed out).
- **Help** — Access help documentation.

OMNIACCESS 3500 NLG CLIENT WINDOW SECTIONS

The OmniAccess 3500 NLG Client window contains the following sections:

- The **Interfaces** section lists all network interfaces that are available for access connectivity. A *red 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.
- The **Interface Information** section displays information about the interface that is currently highlighted in the Interfaces section.
- The **Secure Connection Information** section displays parameters for the VPN tunnel (if established) and the authentication status of the end user.
- The **Make Enterprise Connection** section provides access to the controls that are required to connect to your company's network, including the manual selection of the serving interface.
- The **3G** section provides control for and information about the 3G modem that is integrated in the OmniAccess 3500 NLG card.

How do I connect to the company network?

If your 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 red lightning 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 lightning bolt symbol but 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 lightning 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

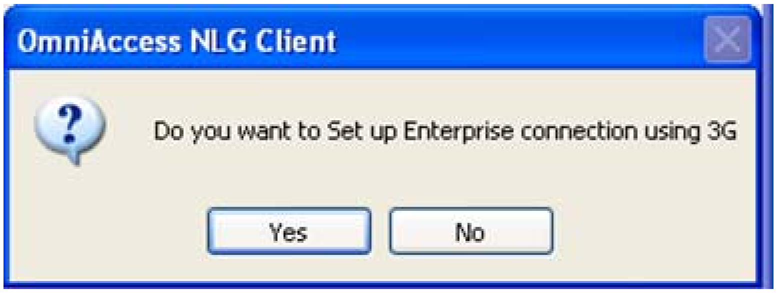
A lower-priority interface is used if no connectivity is available for the higher-priority one(s).

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 Make Enterprise Connection section. The Status bar will show the progress in the establishment of the new connection.

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 NLG Client window, then click **Apply**. If the system subsequently needs to connect via 3G, the following pop-up window appears:



Do you want to Set up Enterprise connection using 3G

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

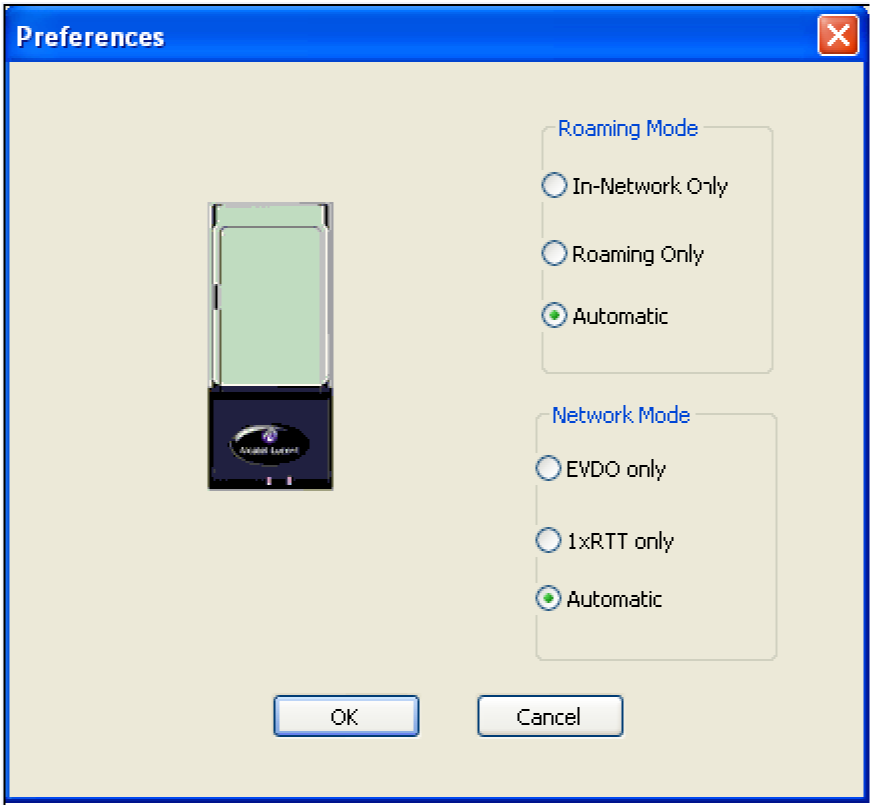
Note: The setting of the Auto 3G Connect checkbox is overridden when the 3G connection is initiated by the OmniAccess 3500 NLG gateway (at times when the laptop may be powered off or not already connected to the gateway).

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 2G 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

Roaming Mode

○ In-Network Only

○ Roaming Only

● Automatic

Network Mode

○ EVDO only

○ 1xRTT only

● Automatic

2. In the Roaming Mode section of the window, select **In-Network Only** (to exclude attachment to a visited network), **Roaming Only** (to exclude attachment to the home network), or **Automatic** (to keep both options available).
3. In the Network Mode section, select **EVDO Only** (for exclusive 3G connectivity), **1xRTT Only** (for exclusive 2G connectivity), or **Automatic** (for keeping both options available).
4. Click **OK** for these settings to become effective.

Note: The 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 (e.g., five minutes):

1. Click **Authenticated Network Access Mode** on the Make Enterprise Connection area of the OmniAccess 3500 NLG Client window.

2. Click **Authenticate**. A browser window opens, asking you to enter the information required to access the public network (the OmniAccess 3500 NLG automatically takes care of the proxy settings for your browser upon entering/exiting this connectivity scenario).
3. After you enter the required information, the OmniAccess 3500 NLG can establish the secure tunnel to your company's network through the public network.

Ho do I view the status of my remote access connection?

You can visually recognize the current status of your connection to your company's network by looking at the OmniAccess 3500 NLG icon in your laptop's icon tray.

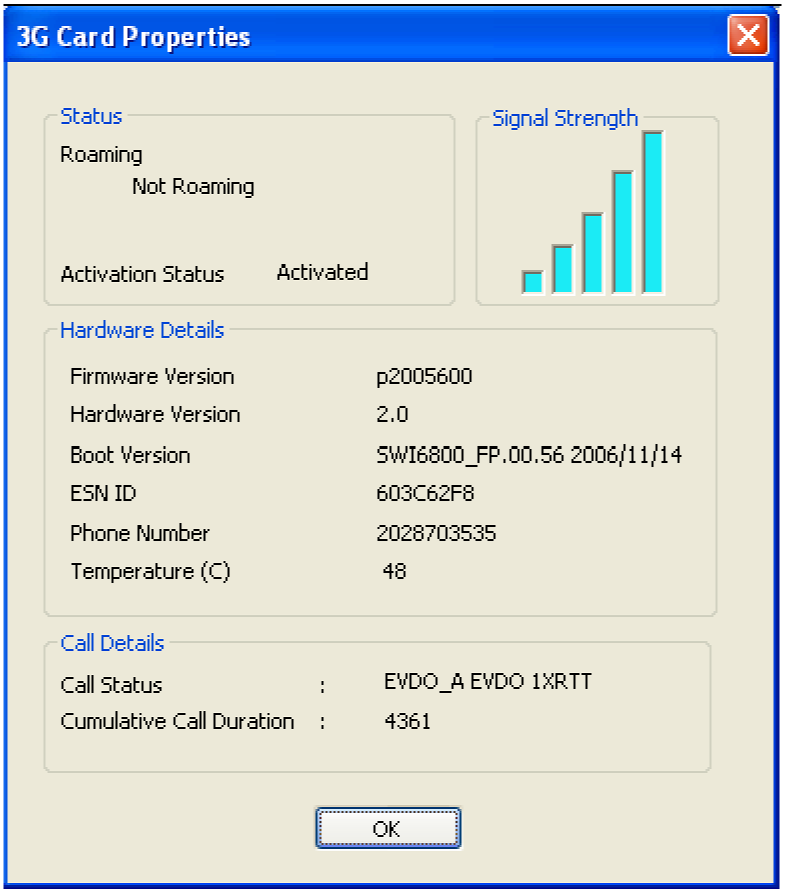
A purple icon indicates that you are currently logged into your company's network. A yellow icon indicates that the VPN tunnel to your company's is available, but you have no access to the network. A red icon indicates that the VPN tunnel to your company's network is not available.

By rolling the mouse pointer over the icon, you can display explicit information about the current status of your card, access connection, VPN tunnel, and network authentication.

The icon will be blinking (in any of the three states described above) when the laptop is working unguarded, under the effect of the One-Time-Password (see the *What if my laptop is lost or stolen*? section below).

How do I view the status of my 3G access connection?

You can view the status of your 3G access connection by clicking **3G Status** on the OmniAccess 3500 NLG Client window. The 3G Card Properties window appears, showing detailed information about the 3G functionality of your OmniAccess 3500 NLG card.



Roaming
Not Roaming

Activation Status Activated

Firmware Version	p2005600
Hardware Version	2.0
Boot Version	SWI6800_FP.00.56 2006/11/14
ESN ID	603C62F8
Phone Number	2028703535
Temperature (C)	48

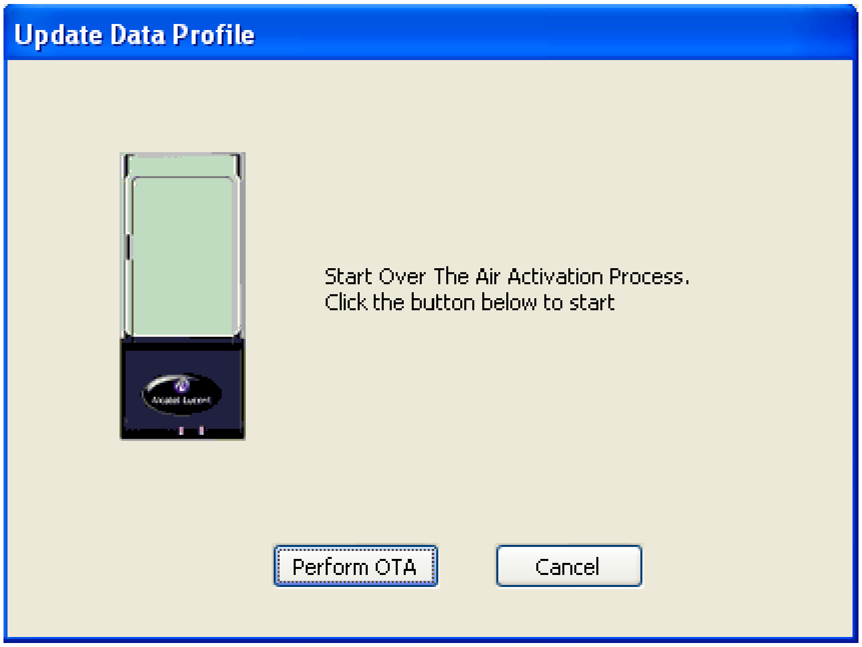
Call Status : EVDO_A EVDO 1XRTT
Cumulative Call Duration : 4361

How do I update the profile of my 3G data subscription?

It is recommended that you periodically update the data profile of your 3G subscription through an iOTA session (you should contact your 3G service provider for a recommended update schedule).

To update the profile, perform the following procedure:

1. On the OmniAccess 3500 NLG Client window, open the **Wireless** menu and click **Update Data Profile**. The Update Data Profile window appears.



Update Data Profile

Start Over The Air Activation Process.
Click the button below to start

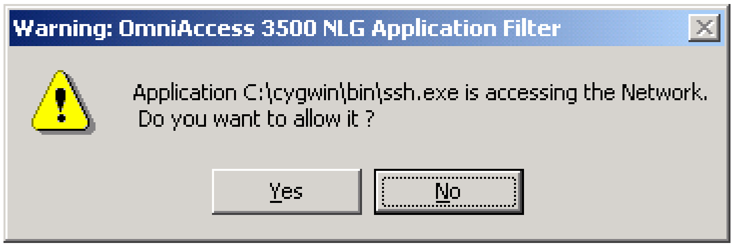
2. Click **Perform OTA**. The 3G wireless parameters inside the 3G modem will be updated.

How do I manage my personal firewall?

ALLOWING AN APPLICATION THROUGH THE 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.

If so configured, 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.



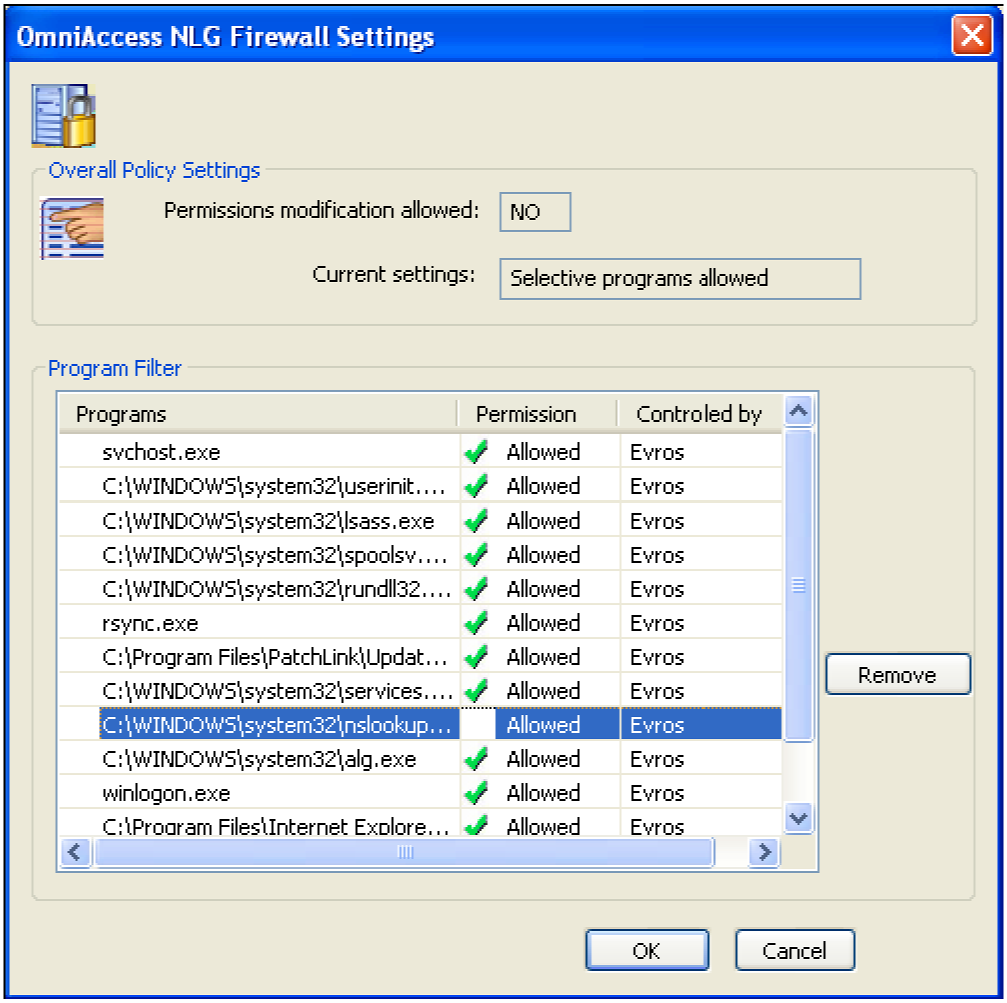
Warning: OmniAccess 3500 NLG Application Filter

Application C:\cygwin\bin\ssh.exe is accessing the Network.
Do you want to allow it ?

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.



Permissions modification allowed: NO

Current settings: Selective programs allowed

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

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.

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?

An encrypted volume can be created in your laptop's hard disk for storage of sensitive data and handled like a separate, secure drive. You, as the end user, install the volume encryption software and select the files to be included in the secure drive, while the administrator assumes exclusive control over the configuration of the encrypted volume. If the laptop is stolen, your IT administrator can remotely delete from your OmniAccess 3500 NLG card the secret password that is needed for decrypting the data in the secure drive. You are encouraged to store all sensitive files in your encrypted volume.

The OmniAccess 3500 NLG Release 1.2 is compatible with the TrueCrypt open-source volume encryption software, Version 4.3a. Other volume encryption solutions or different TrueCrypt versions are currently not supported. For more detailed information about the TrueCrypt open-source software, please refer to the documentation available at www.truecrypt.org. See the following URL for downloading the volume encryption software: http://www.truecrypt.org/downloads.php

Please note the following:

- Accept all default values during the installation. Any deviation from the default values may result in an unsuccessful installation.
- During installation, your keyboard and mouse will be locked for a short time. Do not reboot your laptop as the keyboard and mouse will unlock when the installation completes after a couple of minutes.

See the following URL for detailed installation instructions:
http://www.truecrypt.org/docs/

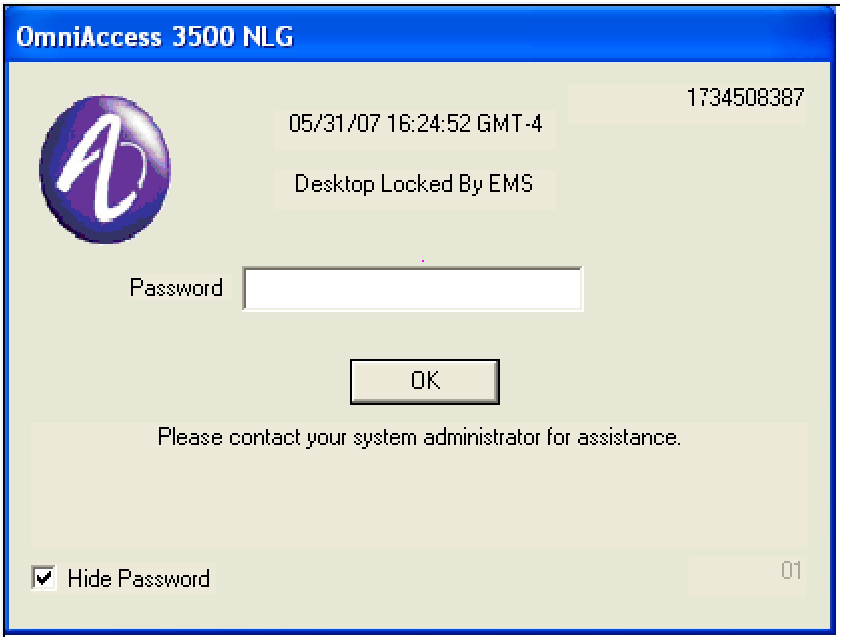
CAUTION: After the TrueCrypt software is installed, you **MUST NEVER** open the TrueCrypt GUI to view/modify the configuration of the encrypted volume. Opening the TrueCrypt GUI may render the data stored in the encrypted volume unreadable.

What if my laptop is lost or stolen?

The OmniAccess 3500 NLG offers many ways to protect the contents of your laptop in the event that the laptop is lost or stolen.

Your administrator can remotely lock your laptop when you realize that the laptop cannot be physically protected from external intrusions (for example, if you inadvertently left your laptop unguarded in a public location). You should call your IT helpdesk immediately after recognizing the ongoing emergency.

A window like the following appears on your laptop's screen after your administrator has locked it:



1734508387

05/31/07 16:24:52 GMT-4

Desktop Locked By EMS

Password

Please contact your system administrator for assistance.

☑ Hide Password

01

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**
Desktop Locked By IT Administrator	The IT administrator has remotely locked the laptop.	Contact the administrator to unlock the laptop. The administrator can unlock the laptop remotely, or pass you a one-time-password (OTP) over the phone.
Secure Tunnel Down	Laptop is out of 3G range, or modem power is off, or otherwise unable to contact the enterprise network.	Return within 3G range, or turn on the modem power, or connect to a different access network (Wi-Fi or Ethernet). -or- Type in the radio password. -or- Contact the 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. -or-

Message	Cause	Possible actions
		Contact the administrator to get an OTP.
Driver Configuration Error	The network drivers on the laptop have been misconfigured.	Contact the administrator to return the network drivers to their proper configuration. -or- Contact the 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 the administrator to get an OTP.
System Integrity Check Failed	An internal check has failed.	Contact the administrator to get an OTP.

If the laptop is lost with no knowledge of where it could be, the end user should notify the administrator immediately. The administrator can determine the laptop location using the GPS capabilities of the OmniAccess 3500 NLG card.

How do I extract the card from my laptop?

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

- Power On — 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.
- Standby/Hibernate/Power Off — 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 may compromise the future operation of your card and laptop.

How do I get help?

If you need assistance using your OmniAccess 3500 NLG card, please contact customer support as follows:

Alcatel-Lucent Enterprise Solutions Division
26801 West Agoura Road
Calabasas, CA 91301 USA

E-mail: support@ind.alcatel.com

Service & Support Website: http://eservice.ind.alcatel.com/
Phone: 800-995-2696

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 (LED A and LED B) on the external end of your OmniAccess 3500 NLG card:

- **LED A (3G Modem):** The 3G Modem LED is closer to the 3G antenna. The LED can be in one of the following states:
  - Off — 3G modem is off, or no 3G signal is detected.
  - Rapid Blinking — 3G signal detected, trying to establish link.
  - Slow blinking — 3G link established.
  - Random blinking — Transmitting data.
- **LED B (OmniAccess 3500 NLG):** The OmniAccess 3500 NLG modem is farther from the antenna. The LED can be in one of the following states:
  - Off — Card is off or VPN tunnel is up.
  - Solid Red — Card is on and VPN tunnel is down.

Radio Frequency and Electrical Specifications

Approvals	Compliant with: IS-856-A (CDMA 1xEV-DO Revision A) IS-856 (CDMA 1xEV-DO Release 0) IS-2000 (CDMA 1xRTT) IS-95 A/B IS-707-A Data IS-637-A SMS IS-683-A Service Provisioning IS-683-B (partial) FCC (ID: RUT-OA3530-S) Industry Canada (ID: 1737G-OA3530-S)
Data Services	CDMA 1xEV-DO Revision A — DL up to 3.1 Mbps, UL up to 1.8 Mbps CDMA 1xEV-DO Release 0 — DL up to 2.4 Mbps, UL up to 153.6 Kbps

	CDMA 1xRTT — DL up to 153.6 Kbps, UL up to 153.6 Kbps
Voltage	+3.3 VDC from PCMCIA Slot
Frequency Bands	800 MHz North American Cellular Band 1900 MHz North American PCS Band GPS Band
Antenna Diversity	Rx Diversity in both 800 MHz and 1900 MHz bands
Temperature Operating Range	IS-98D compliance: -30 to +60 °C Reduced RF performance: +60 to +75 °C
Dimensions	122 mm (L) x 54 mm (W) x 5 mm (H) [15 mm (H) in extended portion only]

Environmental and Mechanical Specifications

Temperature Operating Range	IS-98D compliance: -30 to +60 °C Reduced RF performance: +60 to +75 °C
Dimensions	122 mm (L) x 54 mm (W) x 5 mm (H) [15 mm (H) in extended portion only]

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-OA3530-S — Industry Canada ID: 1737G-OA3530-S

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:

  – Reorient or relocate the receiving antenna

  – Increase the separation between the equipment and receiver

  – Connect the equipment into an outlet on a circuit different from that to which the receiver is connected

  – Consult the dealer or an experienced radio/TV technician for help.

  This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

  – This device may not cause harmful interference, and

  – This device must accept any interference received, including interference that may cause undesirable operations.

  FCC guidelines stipulate that the antenna should be more than 1.7 cm from the user. The highest reported SAR values of the OmniAccess 3500 NLG card by Alcatel-Lucent are:

  – Separation distance of at least 1.7 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 (1.345 mW/g).

  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 OmnniAccess 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.