

**OmniAccess 3500
Nonstop Laptop Guardian
Release 1.2
End-User Reference Guide**

Document Version: 25.05

Part Number: 060226-10 Rev B

Published: 12.18.2007

Alcatel-Lucent Proprietary

Copyright © 2007 Alcatel-Lucent. All rights reserved. This document may not be reproduced in whole or in part without the express written permission of Alcatel-Lucent. Alcatel-Lucent® and the Alcatel-Lucent logo are registered trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners.

Table of Contents

Welcome	1
OmniAccess 3500 NLG Card Features Overview	1
Common Operations	1
How do I get started?	1
OmniAccess 3500 NLG Client window menu options.....	2
OmniAccess 3500 NLG Client window sections	3
OmniAccess 3500 NLG Tray Icon	3
How do I connect to the company network?	4
How do I manually change my serving network interface?	4
How do I select my roaming and network preferences?.....	5
How do I connect from a public hotspot?.....	6
How do I view the status of my 3G access connection?	7
How do I update the profile of my 3G data subscription?	8
How do I manage my personal firewall?	8
Allowing an application through the firewall	8
Viewing personal firewall settings.....	9
Removing an application from the firewall list	10
How do I secure my sensitive data?	10
What if my laptop is lost or stolen?	11
How do I remove the card from my laptop?.....	13
How do I control the power state of the 3G modem on my card?	13
How do I control the power state of my card?.....	13
How do I get help?.....	14
Technical Specifications	14
LED Specifications.....	14
Radio Frequency and Electrical Specifications	14
Environmental and Mechanical Specifications	15
Regulatory Information.....	15
Regulatory Notices	15
Safety and Notices	17
Important Notice	17
Safety and Hazards.....	17
Battery Information	18

Appendix: Error Messages 18

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*.

To ensure that the information you receive is the most accurate available, please

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.

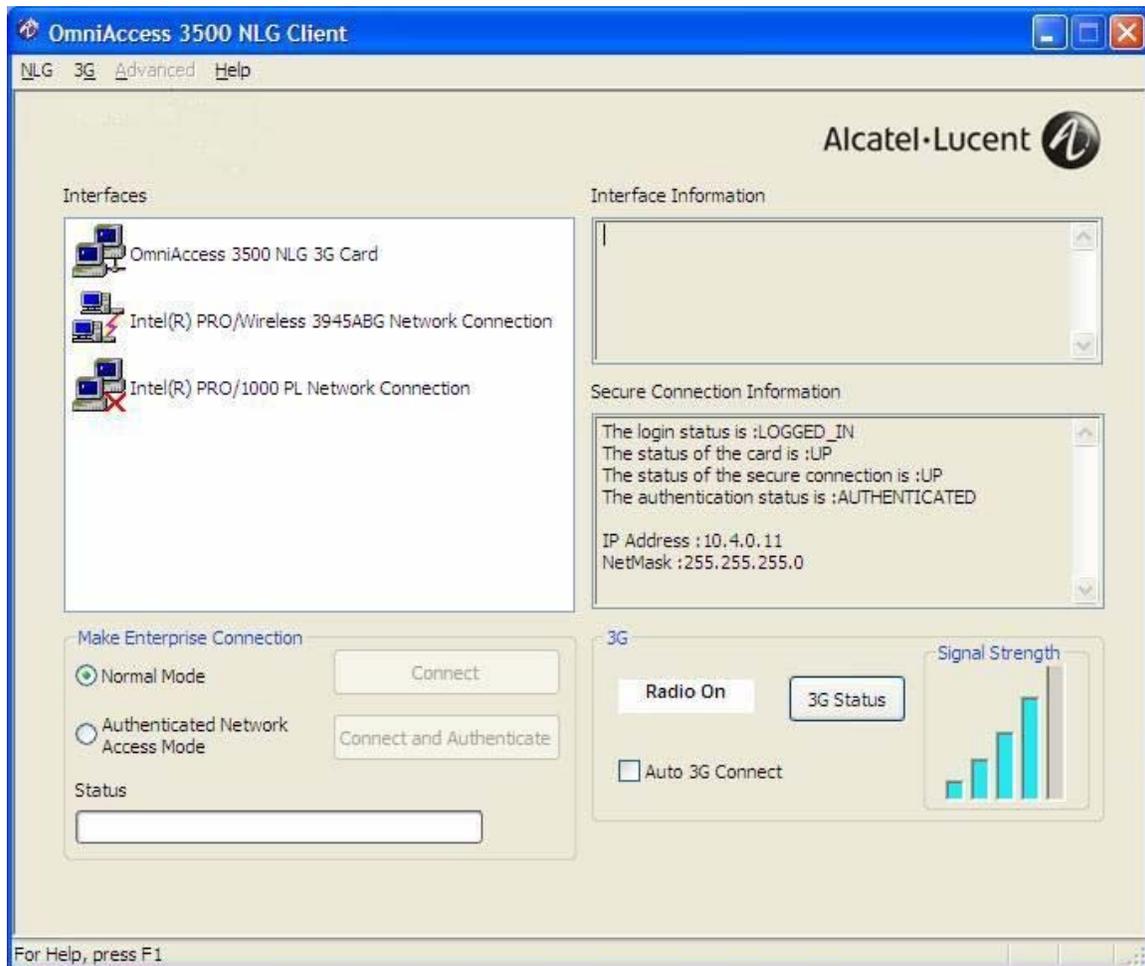
How do I get started?

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.



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.

- **3G** – 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) during normal operation. It can only be accessed by your wireless provider for servicing purposes.
- **Help** – Access help documentation (Adobe Acrobat Reader must be installed in the laptop to view the 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.

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):



- **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.

- Red icon – There is no recognized connectivity between the card and your company's network. The mouse-rollover pop-up message indicates one of the following causes:
 - Card not available
 - No access network available
 - Gateway not available
 - 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 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 (or simply double-click on the desired interface). The Status bar will show the progress in the establishment of the new connection.

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).

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. If the system subsequently needs to connect via 3G, the following pop-up window appears:



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

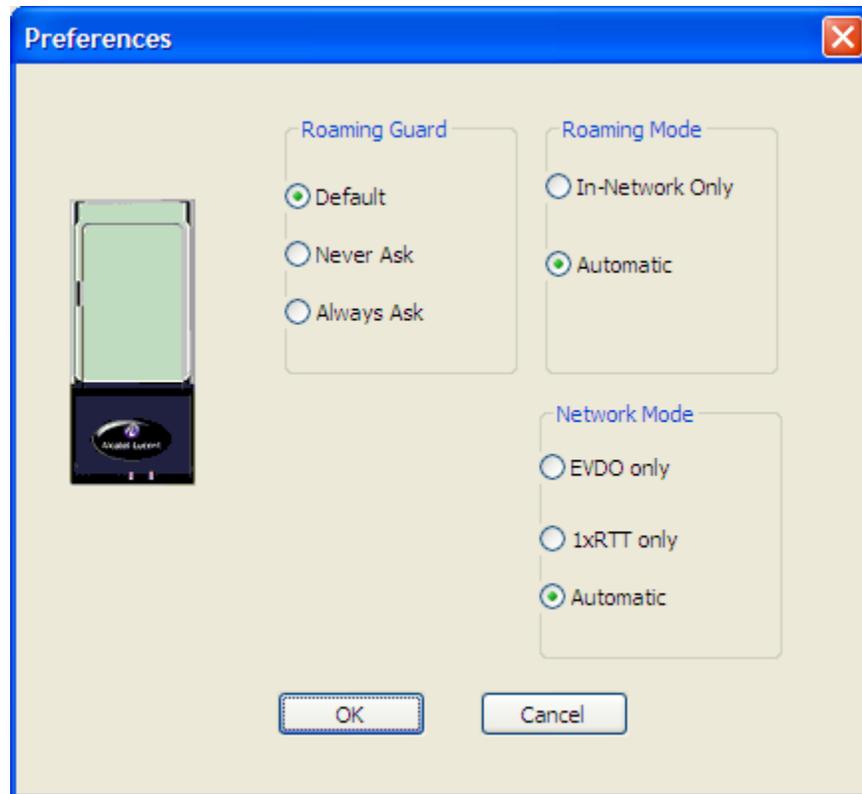
Note: The setting of the Auto 3G Connect checkbox is overridden when the 3G connection is initiated by the OmniAccess 3500 NLG gateway (at times when the laptop may be powered off or not already connected to the gateway).

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.



2. In the Roaming Guard section of the window, select **Default** (to have a pop-up window ask you case by case if you want out-of-network attachment when roaming charges apply), **Never Ask** (to attach out of network with no question when roaming charges apply), or **Always Ask** (to be asked always about out-of-network attachment, even when no roaming charges apply). You can switch the **Default** and **Always Ask** settings to **Never Ask** by clicking the **Never Ask Again** option on any of the pop-up windows that appear on your screen. The setting chosen for this section is irrelevant if the **In-Network Only** option is selected in the Roaming Mode section.
3. In the Roaming Mode section of the window, select **In-Network Only** (to exclude out-of-network attachment) or **Automatic** (to keep both in-network and out-of-network attachment available).
4. 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).
5. Click **OK** for these settings to become effective.

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)

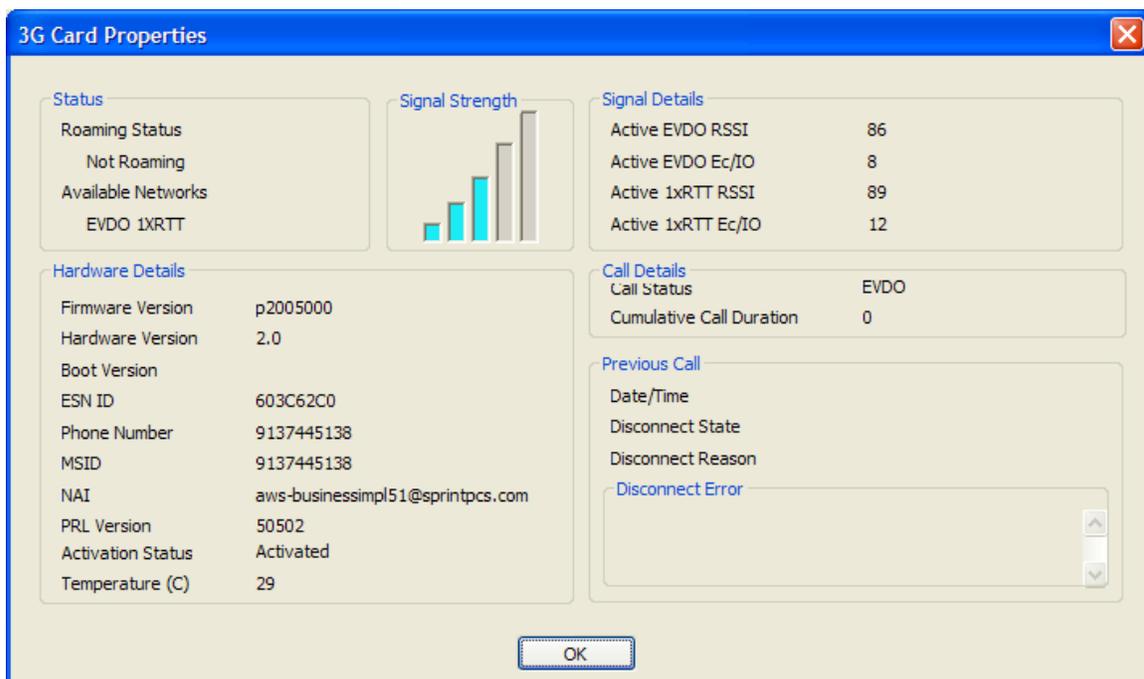
or your credit card information) before granting network access. Since the OmniAccess 3500 NLG cannot know in advance the type of access negotiation implemented at every such place, you will be required to interactively submit your local access credentials.

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 (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 **Connect and 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.

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.

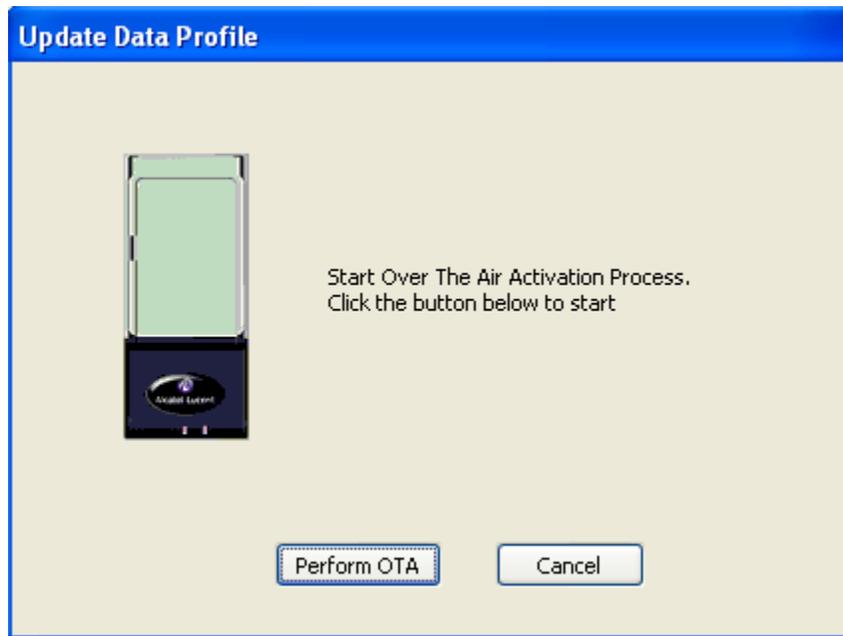


How do I update the profile of my 3G data subscription?

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.



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

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

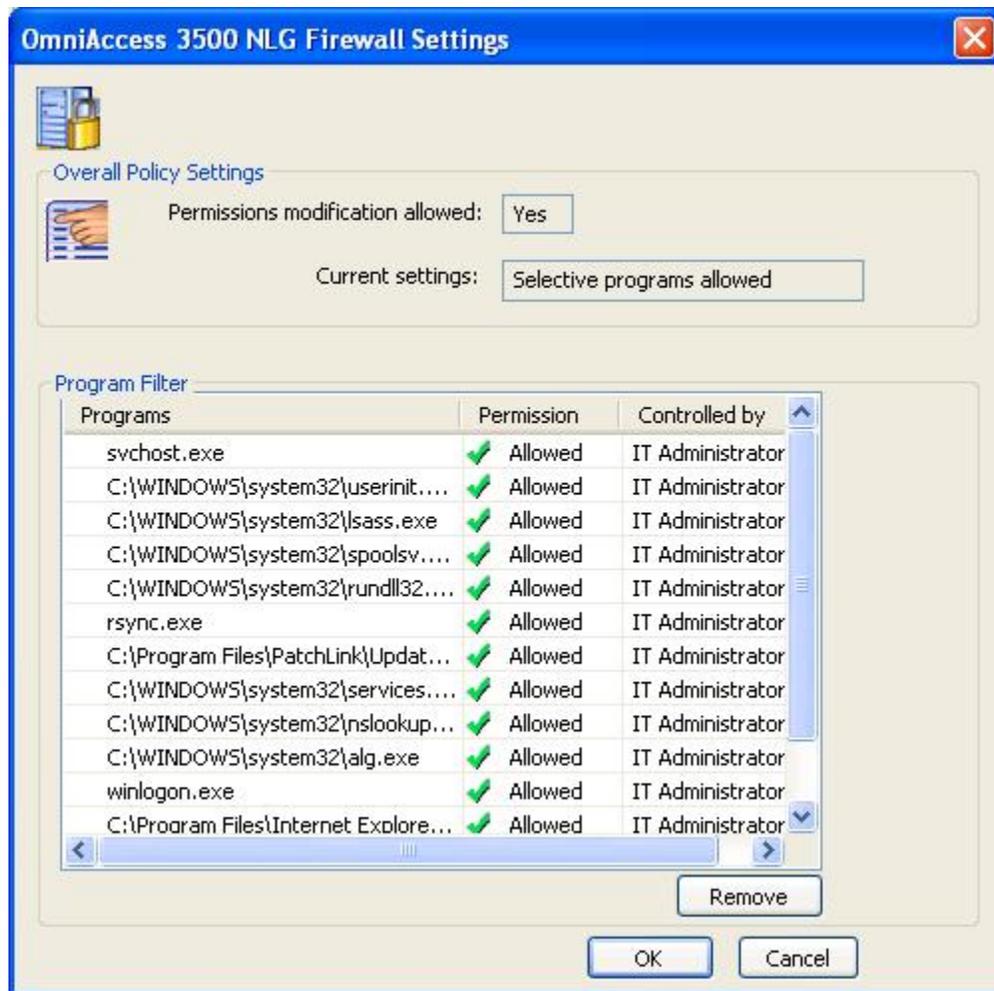
If your personal firewall policy allows you to override its default settings regarding the treatment of certain applications, an OmniAccess 3500 NLG Application Filter window pops up on the laptop screen every time the personal firewall detects an attempt to open a network connection by one of your applications.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



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.



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?

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.

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 use 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 1.2 is only compatible with TrueCrypt Version 4.3a. The software can be downloaded at <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.

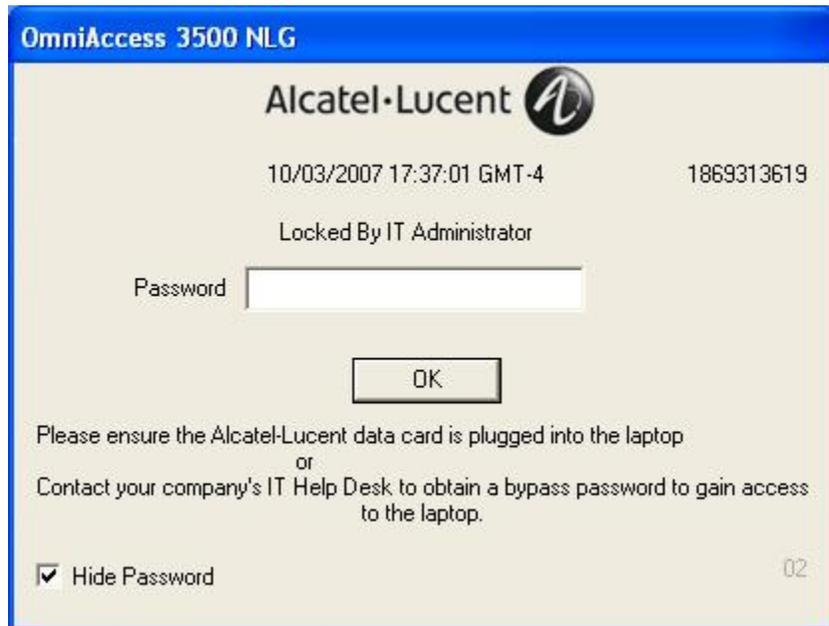
While the secure drive is being create (by request of your IT administrator), your keyboard and mouse will be locked for a short time. Do not reboot your laptop thinking that it has stopped working. The keyboard and mouse will unlock when the secure drive creation completes after a couple of minutes.

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 administrator immediately after recognizing the ongoing emergency.

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



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 pass you a one-time-password (OTP) over the phone.

Message	Cause	Possible actions
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- 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. -or- Contact your IT 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 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.	Contact your IT administrator to get an OTP.

If you receive a one-time password (OTP) from the administrator, you can enter it to regain control of the laptop. 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. You must call your IT administrator to obtain a new OTP if the laptop locks again.

Under the effect of the OTP some of the OmniAccess 3500 NLG controls are temporarily disabled, allowing you to keep using your laptop. During this period you can access any network as you would expect from a regular laptop. However, you must keep the OmniAccess 3500 NLG card inserted in the laptop if you want to retain access to your OmniAccess 3500 NLG-managed encrypted volume.

If the laptop is lost with no knowledge of where it could be, you must notify your IT administrator immediately. The administrator can determine the laptop location and take all necessary measure to protect the laptop contents.

How do I remove the card from my laptop?

Strictly observe the following rules 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 may compromise the future operation of your card and laptop.

How do I control the power state of the 3G modem on my card?

When your laptop is powered on and the card is plugged in, you can push the *power button* on the card with the tip of a ballpoint pen to toggle the 3G modem on and off.

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 my 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 switches to sleep mode if the 3G modem is on and shuts down in 1-2 minutes if the 3G modem is off.
- To shut down your card:
 - If the card is in sleep mode, push the power button and hold it down for about 5 seconds.
 - If the card is on (and therefore plugged into a powered-on laptop) push the button to turn off the 3G modem and remove the card from the laptop. The card will shut down in 1-2 minutes.
- Your card automatically powers on when it is plugged into a laptop that has power.
- Your card includes a *master power switch* (accessible only when the card is removed from the laptop) that you can use to reboot your card if the card stops responding.

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 yellow light: 3G modem is on.
 - Fast-blinking yellow light: 3G modem is transmitting.
- **LED B (Card)** 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 green light: Card is up, VPN tunnel is up.

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

Environmental and Mechanical Specifications

Temperature Operating Range	IS-98D compliance: -30 to +60 °C Caution: Contains Li-Ion battery. Do not expose to high temperature (above +60 °C).
Dimensions	122 mm (L) x 54 mm (W) x 5 mm (H) [15 mm (H) in extended portion only]
SD Card Slot	<i>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.</i>

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 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.
 - 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 your card away from fluids and moisture.

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.

- *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.