

**OmniAccess 3500
Nonstop Laptop Guardian
Release 1.2
End-User Release Notes**

Document Version: 25.01

Part Number: 032335-10 Rev B

Published: 11.27.2007

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.

Welcome

Welcome to the End-User Release Notes for Release 1.2 of the OmniAccess 3500 Nonstop Laptop Guardian. The document provides detailed information about the product release and all identified issues that may impact the end-user experience of the solution. This revision of the document (25.01) refers to build 1.2.25 of the OmniAccess 3500 NLG. The previous revision of this document (1.2.703) was issued on 10.10.2007 and was attached to build 1.2.7.

Release Information

- **Vendor:** Alcatel-Lucent
- **Product:** OmniAccess 3500 Nonstop Laptop Guardian
- **Release:** 1.2
 - *Issue Date:* November 26, 2007
 - *Build:* 1.2.25
 - *Distribution:* General availability to all customers
- **Hardware:** OmniAccess 3500 Nonstop Laptop Guardian Card with EV-DOa (Sprint) Modem, Hardware Revision 4
- **Software**
 - *Distribution Server:* www.nonstopguardian.com
 - *Directory:* Link on the main page
 - *Package Files:* See Table 1

Sr.	File Name	Description	Size (bytes)	MD5 Hash	Comments
1	NLG-Client-setup-1.2.25-NLGMonitor-Enabled.exe	First-time installation of client software in the laptop	15,190,016	90E82E62A3A3FB39C125128C93E26CD8	Self executable

2	Alcatel-Lucent 3500 NLGClient Software Upgrade-1.2.25-V3.msi	Upgrade from previous release of client software	20,395,008		Self executable
---	--	--	------------	--	-----------------

Table 1 - Release 1.2 end-user package files (build 1.2.25)

Documentation

- OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Features Overview
- OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Card Quick Start Guide
- OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 End-User Reference Guide

Previous Releases

Since Release 1.2 is the first commercial release of the OmniAccess 3500 NLG, there is no previous release of the product to be used for comparison. This document highlights all incremental changes that exist between builds 1.2.7 and 1.2.25.

Installation/Upgrade Instructions

- Please refer to the *OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Card Quick Start Guide* for detailed instructions regarding the installation of the OmniAccess 3500 NLG card and client software.
- The version number must be the same for the laptop client software, the OmniAccess 3500 NLG card firmware, and the OmniAccess 3500 NLG gateway software. Please verify with your IT helpdesk in case of doubt.

System Requirements

- End user laptop:
 - OS: Microsoft Windows XP SP2
 - Processor speed: 1 GHz or higher
 - RAM: 512 MB or higher
 - PCMCIA CardBus slot
 - No VPN client installed in the laptop.

Contacting Technical Support

Please contact your IT helpdesk to address any technical issue that you may encounter in the operation of your OmniAccess 3500 NLG card and laptop.

New Features

Here is the list of new features included in this release. Please refer to the *OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Features Overview* document for more information about the features.

Platform

OMNIACCESS 3500 NLG CLIENT

The OmniAccess 3500 NLG client is the combination of a Type II (CardBus) PC Card (the OmniAccess 3500 NLG card) and the client software installed in the laptop. The card includes a local processor, a flash memory card, and an EV-DO_rA modem. All card components are powered by an on-card rechargeable battery. All traffic to and from the laptop network interfaces is routed via the card where it can be processed by the OmniAccess 3500 NLG applications running on the card. The OmniAccess 3500 NLG-enabled laptop is inoperable without the card.

ANTI-TAMPERING

To ensure that the OmniAccess 3500 NLG-enforced security and management controls are not disabled, anti-tampering measures are incorporated in the solution.

Release 1.2 supports the following anti-tampering control actions:

- Laptop lockdown (the laptop becomes unusable)
- Lockdown of data stored in the encrypted volume
- Network access control by runtime modification of the policies that drive the operation of the integrated personal firewall.

Events that trigger anti-tampering actions include:

- Card removal from the laptop
- Uninstallation of the OmniAccess 3500 NLG client software
- Tampering with OmniAccess 3500 NLG components.

ONE TIME PASSWORD

If the laptop is locked by effect of an anti-tamper control action but a legitimate need remains to use the laptop, the administrator can pass to the end user a one-time password that unlocks the laptop for a limited amount of time (set by the administrator).

RADIO PASSWORD

The card includes a power button to switch off the 3G modem when required by specific regulations (e.g., in an airplane that is taking off or landing). However, it is generally not desirable to leave the 3G modem off for a prolonged time. To discourage

the end user from doing so, the laptop automatically locks after the 3G modem remains off for a time of configurable duration (set by the administrator). The legitimate end user can unlock the laptop using the Windows logon password.

Applications

AUTO-VPN

The OmniAccess 3500 NLG supports transparent IPsec-based secure connectivity to the enterprise network. The user has no involvement in the establishment, maintenance, and interruption of the secure access session. The card embeds a standards-based IPsec client that automatically establishes and maintains the IPsec tunnel to the enterprise network. The end user is not required to supply a separate set of authentication credentials to establish the connection. The usual authentication mechanism (e.g., submission of Windows NT credentials) is used to obtain access to the enterprise network (single sign-on feature).

RADIUS BASED AUTHENTICATION

RADIUS-based authentication can optionally be added for network access. As a result, various authentication methods that rely on RADIUS for their message exchanges (e.g., SecureID) can be adopted for end-user authentication. The RADIUS-based mechanism can either coexist with an Active Directory infrastructure or operate in complete autonomy.

MOBILITY MANAGEMENT

The OmniAccess 3500 NLG supports the automatic and manual transfer of the laptop access link (vertical handover) between heterogeneous access networks (Ethernet, Wi-Fi, 3G cellular). The IP address seen by the applications does not change during the handover, so that the network application session remains intact at every network transition.

PERSONAL FIREWALL

The OmniAccess 3500 NLG card includes a personal firewall for protection of the end user laptop. The administrator manages the set of packet filtering and application filtering rules that drive the operation of the personal firewall, called the personal firewall policy, through the management system. The packet filter component of the personal firewall supports stateful packet inspection (SPI) for all traffic that the laptop exchanges in both directions with the access network. The application filter restricts the set of laptop applications that are allowed to open network connections.

NETWORK ACCESS CONTROL ENFORCEMENT

The OmniAccess 3500 NLG can force the laptop to communicate exclusively with the enterprise network, preventing simultaneous access connections and direct access to the public Internet.

ASSISTED FILE TRANSFER

As an underlying framework to many OmniAccess 3500 NLG applications, the Assisted File Transfer (AFT) feature enables the automatic synchronization of two remote folders, one located on the laptop and the other located on a file server in the

enterprise network. The file transfer continues even when the laptop is powered down.

SMS INTEGRATION

The OmniAccess 3500 NLG transparently integrates with the Microsoft Systems Management Server (MS-SMS) application to extend its reach, enabling the execution of patch downloads at times when the laptop is not powered on.

PATCHLINK UPDATE INTEGRATION

The OmniAccess 3500 NLG enhances the patch download capabilities of the PatchLink Update application (a Lumension Security product) by helping it reduce the total time needed to distribute the software updates to the mobile devices. Copies of a new software package are cached in the OmniAccess 3500 NLG cards of the target laptop collection as soon as the package becomes available.

ASSET MANAGEMENT

The OmniAccess 3500 NLG includes a proprietary asset management application that enables monitoring of laptop assets and status at any time the OmniAccess 3500 NLG card is reachable and independently of the power state of the laptop.

REMOTE LOCK

The administrator can make a laptop unusable by issuing a remote lock command through the management system. The IT administrator can also issue a remote unlock command.

VOLUME ENCRYPTION

The OmniAccess 3500 NLG interoperates with the TrueCrypt open software for creation and management of an encrypted volume in the laptop hard disk. The laptop automatically mounts the encrypted volume after the end user successfully logs in. The administrator has exclusive control over the password stored in the card and can remotely erase it if the laptop is reported lost or stolen.

FILE TRACKER

The file tracker application allows the administrator to obtain a list of the files stored in the encrypted volume at any time. This capability can be used to enforce the storage policies of the enterprise for sensitive data and to identify the contents that are at risk in a lost/stolen laptop.

REMOTE KILL

The administrator can remotely render the critical data stored in the encrypted volume on the laptop's hard disk unreadable by anyone.

GEOTRACK

The administrator can obtain the geographical location of the OmniAccess 3500 NLG card whenever needed. The request for the card location is issued through the management system and shown on a browser window using commercial mapping software (Microsoft Earth) with interactive map navigation capabilities. The location of the laptop at every login event is also recorded.

Feature Enhancements over Build 1.2.7

RETRIEVE THE CARD LOGS

The option to retrieve logs from the OmniAccess 3500 NLG card has been added to the client GUI (**NLG->Retrieve Card Logs**) in order to support the debugging of issues that the end user is most likely to face. The execution of the command transfers the card logs to the laptop's desktop, making them easy to upload to the IT helpdesk together with the laptop logs.

ENHANCED CONTROL OF 3G ROAMING OPTIONS

Added control capabilities are now available for the end user with respect to the selection of 3G roaming options.

- Roaming Mode selection – Available options: <In-Network Only>, <Automatic>.
- Network Mode – Available options: <EVDO only>, <1xRTT only>, <Automatic>.
- Roaming Guard – Available options: <Default>, <Always Ask>, <Never Ask>.

UPGRADE OF OMNIACCESS 3500 NLG CLIENT SOFTWARE

The OmniAccess 3500 NLG client software on the laptop and the firmware on the OmniAccess 3500 NLG card can be simultaneously upgraded with a single installation program that runs on the laptop. The upgrade image is released as an executable Microsoft installer file (.msi extension).

Warning: Please contact your IT helpdesk if you need to upgrade your OmniAccess 3500 NLG client software.

Issues Fixed

Since Release 1.2 is the first commercial release of the OmniAccess 3500 NLG product, there are no entries in this section.

Known Issues

CARD HARDWARE

There are no known issues with the OmniAccess 3500 NLG card hardware at the time of release of this document.

INSTALLATION AND CONFIGURATION

1. Internal tracking ID: 1247

Problem Description: No direct support available for uninstalling the OmniAccess 3500 NLG client software.

Impact: There is no straightforward method available to uninstall the OmniAccess 3500 NLG client software. Please note that the uninstallation of the OmniAccess 3500 NLG client software is in any case not desirable as it will remove all the OmniAccess 3500 NLG functionality and protection, and expose the laptop to the usual security risks.

Workaround/s: In case of emergency, any of the following methods can be used to uninstall the OmniAccess 3500 NLG client software under the supervision of your IT administrator:

- If any Windows System Restore point created before the installation of the OmniAccess 3500 NLG client software is available, the laptop can be brought back to the state of that restore point. If the laptop is in locked state, it must first be unlocked using a one-time password. Please consider that invoking a restore point will also undo all the system changes that occurred after the restore point was created, not only the installation of the client software.
- Boot the laptop using an external medium and then uninstall the OmniAccess 3500 NLG client software.
- Re-image the laptop (install a new copy of the operating system).

2. Internal tracking ID: 1247

Problem Description: The laptop may lock immediately after installing the OmniAccess 3500 NLG client software if earlier versions of the client software were ever loaded on the laptop before.

Impact: The installation of the OmniAccess 3500 NLG client software is not successful.

Workaround/s: This happens because some older versions of the OmniAccess 3500 NLG software (only used in trials) failed to execute a complete cleanup when uninstalled. Find and remove the *tampercheck* folder in the Windows registry of the laptop before installing the OmniAccess 3500 NLG software.

STARTUP AND SHUTDOWN

3. Internal tracking ID:

Problem Description: For the first time after installation of the OmniAccess 3500 NLG client software or if for some reason the laptop does not have cached credentials then the end user may not be able to login immediately after the Windows logon prompt appears.

Impact: Unable to login.

Workaround/s: Wait for the VPN tunnel to come up before attempting to login. The right-hand LED on the card (LED B) indicates the tunnel status. If the tunnel does not come up, login to a local account on the laptop (e.g., Administrator), establish the tunnel using the OmniAccess 3500 NLG GUI, logout, and then login to your regular domain account.

4. Internal tracking ID: 1561

Problem Description: In extremely rare occasions, connectivity to the gateway may not be restored when the laptop recovers from standby/hibernation mode.

Impact: Unable to connect to the gateway.

Workaround/s: Reboot the laptop.

5. Internal tracking ID:

Problem Description: The laptop locks for about two minutes after recovering from standby/ hibernation mode.

Impact: Unable to use the laptop for 1-2 minutes.

Workaround/s: This is a deliberate behavior of the solution, meant to protect the integrity of the laptop and of the data stored in the laptop at times when the OmniAccess 3500 NLG card is not functional (the card is booting up). There is no workaround at the moment. Efforts are being made to reduce the duration of the locking period (by making the card boot faster).

OPERATION

6. Internal tracking ID: 1237

Problem Description: In extremely rare occasions the end user may get a message indicating that the ecmservice.exe crashed.

Impact: The user will no longer be able to establish the connection to the enterprise network.

Workaround/s: Rebooting the laptop will fix this problem.

7. Internal tracking ID: 1228

Problem Description: In extremely rare occasions the 3G interface is not shown in the laptop GUI, though it is operational.

Impact: Confusion to the end user: if the card is inserted, why is the 3G interface not listed?

Workaround/s: Wait for 3 minutes. The card may be rebooting after having detected an abnormal situation. If the 3G interface is still not shown after 3 minutes, reboot the laptop or logoff and login again. The interface will show up again correctly.

8. Internal tracking ID:

Problem Description: In rare occasions the OmniAccess 3500 NLG tray icon may not reflect the correct status of the laptop/card.

Impact: Confusion to the end user.

Workaround/s: Please wait for about two minutes and see if the situation corrects itself. If not, log out and login again.

INTEROPERATION

9. Internal tracking ID:

Problem Description: The OmniAccess 3500 NLG client software does not operate properly in presence of other IPsec VPN clients.

Impact: If the OmniAccess 3500 NLG client software is installed in a laptop that already has an installed IPsec client the OmniAccess 3500 NLG functionality may be compromised (e.g., the VPN tunnel may not come up).

Workaround/s: Uninstall any pre-existing IPsec client before installing of the OmniAccess 3500 NLG client software in the laptop.

10. Internal tracking ID:

Problem Description: User-installed Cygwin software may not work or stop working after installing the OmniAccess 3500 NLG client software.

Impact: The Cygwin application may not work for the end user.

Workaround/s: The installation of the OmniAccess 3500 NLG client software includes a particular version of Cygwin. Please make sure that your installed version of Cygwin is the same as the one installed with the OmniAccess 3500 NLG client software. Two different versions of Cygwin cannot coexist.

ANTI-TAMPERING

11. Internal tracking ID: 1244

Problem Description: The OmniAccess 3500 NLG client software can be uninstalled using the Windows restore utility.

Impact: An attacker that manages to log into the laptop may get rid of the enterprise-enforced security controls. However, logging into the laptop is not sufficient to obtain access to the sensitive data stored in the encrypted volume.

Workaround/s: To prevent anyone from removing the client software by invoking an older restore point, make sure that there are no Windows System Restore points in the laptop when the OmniAccess 3500 NLG client software is installed.

12. Internal tracking ID:

Problem Description: The OmniAccess 3500 NLG-enabled laptop can be booted using an external boot medium.

Impact: Someone having physical access to the laptop may get rid of the enterprise enforced security controls. Still this would not give access to the sensitive data stored in the encrypted volume.

Workaround/s: To prevent the capability to boot the laptop from an external medium, first disable in the BIOS the booting from all external means such as CD, USB, network, etc., and then password-lock the BIOS.

13. Internal tracking ID: 767

Problem Description: It is not possible to connect to the enterprise network while the one-time password is in effect, not even with a third-party IPsec client.

Impact: The end user may not be able to access the enterprise network.

Workaround/s: This is a security requirement. However this behavior will be reviewed and possibly modified in the next release of the OmniAccess 3500 NLG platform based on customer feedback.

AUTO VPN

14. Internal tracking ID:

Problem Description: The laptop cannot be connected directly to the Internet.

Impact: Direct access to the Internet is not possible even if needed.

Workaround/s: This is a security feature and is requested by most customers. In case of emergency, pull the card out of the laptop, get the one time password from your administrator, unlock the laptop and, for the duration of the one time

password, connect the laptop directly to the public Internet using one of its local network interfaces.

MOBILITY MANAGEMENT

15. Internal tracking ID: 1202

Problem Description: In extremely rare occasions the captive portal web page (hotspot authentication screen) does not appear automatically.

Impact: The end-user is not able to authenticate with the hotspot network.

Workaround/s: Open the web browser manually and try accessing any web page. That should bring up the authentication screen from the hotspot service provider.

PERSONAL FIREWALL

16. Internal tracking ID: 1261

Problem Description: In extremely rare occasions the personal firewall policies may not be applied correctly.

Impact: The end-user is not able to access a particular resource or an application is unable to access the network.

Workaround/s: Shutdown the laptop, wait for two minutes and then restart the laptop. A plain restart may not fix the problem.

TRUECRYPT INTEGRATION

17. Internal tracking ID: 1261

Problem Description: In extremely rare occasions the encrypted volume may not mount.

Impact: The end-user is not able to access the files stored in the encrypted volume.

Workaround/s: Shutdown the laptop, wait for two minutes and then restart the laptop. A plain restart may not fix the problem.

RADIUS AUTHENTICATION

18. Internal tracking ID: 1024

Problem Description: Any user with a valid RADIUS login can log into the laptop.

Impact: Accountability issue. Of course the illegitimate user needs to know the password on the laptop.

Workaround/s: For some enterprise customers this may be a desirable behavior, hence the treatment of this behavior will be finalized in the next release of the OmniAccess 3500 NLG platform based on customer feedback.