

OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Administrator Release Notes

Document Version: 25.01

Part Number: 032334-10 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 Administrator Release Notes for Release 1.2 of the OmniAccess 3500 Nonstop Laptop Guardian. This document provides detailed information about the product release and all identified issues that may impact the IT-administrator 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

o Issue Date: November 26, 2007

Build: 1.2.25

o Distribution: General availability to all customers

 Hardware: OmniAccess 3500 Nonstop Laptop Guardian Enterprise Gateway, Hardware Revision 1

Software

o Distribution Server: www.nonstopguardian.com (client software only)

o Directory: Link on the main page

Package Files: See Table 1

Sr.	File Name	Description	Size (bytes)	MD5 Hash	Comments
1	NLG-Flash- Image- 1.2.25- V4.raw	Card firmware	TBD	TBD	Pre- installed in the card
2	NLG- Management- Server- pgsqlbin- 1.2.25.rpm	Database software running on the gateway	TBD	TBD	Pre- installed in the gateway

3	NLG- Management- Server- 1.2.25.rpm	Management system software running on the gateway	TBD	TBD	Pre- installed in the gateway
4	NLG- Gateway- 1.2.25.rpm	Gateway software	TBD	TBD	Pre- installed in the gateway
5	NLG- SMSServer- setup- 1.2.25.exe	Software for Microsoft SMS integration to be installed in the SMS server (only if SMS is used)	TBD	TBD	
6	NLG- Gateway- Common- 1.2.25.rpm	Platform software running on the gateway	TBD	TBD	Pre- installed in the gateway

Table 1 - Release 1.2 administrator 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 Gateway Quick Start Guide
- OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Gateway Installation Guide
- OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Administration Guide
- OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Gateway Security Overview
- OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Application Note: Integration of PatchLink Update and Microsoft SMS
- OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Card Quick Start Guide
- OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 End User Reference Guide
- OmniAccess 3500 Nonstop Laptop Guardian Technical Overview

Previous Versions

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
 Gateway Installation Guide for detailed instructions regarding the installation
 and initial configuration of the OmniAccess 3500 NLG gateway.
- 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.

System Requirements

- End user laptop:
 - OS: Microsoft Windows XP SP2
 - o Processor speed: 1 GHz or higher
 - o RAM: 512 MB or higher
 - PCMCIA CardBus slot
 - No VPN client installed in the laptop
- Access to management system GUI:
 - Internet Explorer 6.0 or above or Mozilla Firefox 3.0 or above, installed in any computer with network access.

Contacting Technical Support

Alcatel-Lucent technical support is committed to resolving our customer's technical issues in a timely manner. Customers with inquiries should contact us at:

Region	Phone Number		
North America	1-800-995-2696		
Latin America	+1-877-919-9526		
Europe	+33-388-55-69-29		
Asia Pacific	+65-6240-8484		
Other International	+1-818-878-4507		

Email: support@ind.alcatel.com

Internet: Customers with Alcatel-Lucent service agreements may open cases 24 hours a day via Alcatel-Lucent's support web page at: service.esd.alcatel-lucent.com.

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 MANAGEMENT SYSTEM

The OmniAccess 3500 NLG management system provides the IT administrator with the necessary interfaces for managing the entire OmniAccess 3500 NLG platform, including the gateway, the cards, and the laptops. In Release 1.2 the management system runs on the OmniAccess 3500 NLG gateway.

OMNIACCESS 3500 NLG ENTERPRISE GATEWAY

The OmniAccess 3500 NLG enterprise gateway is an appliance that resides at the edge of the enterprise network and terminates the secure remote access connections for the OmniAccess 3500 NLG cards.

SNMP SUPPORT

Enterprise MIB II support is available on the gateway to monitor network interfaces, TCP/IP stack, operating system, etc. using SNMP. Release 1.2 does not support any OmniAccess 3500 NLG-specific MIB.

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-DOrA 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 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 Release 1.2 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 Release 1.2 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.

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

Gateway

INSTALLATION AND CONFIGURATION

1. Internal tracking ID: 349

Problem Description: Change of super admin id is not forced at the time of installation.

Impact: Gateway may continue to have the default admin password.

Workaround/s: Make sure that you change the admin password after installation of the Gateway. It is also mentioned in the Gateway installation guide.

2. Internal tracking ID: 507

Problem Description: Same or overlapping IP addresses can be configured for the Cards and Laptops address pools.

Impact: Some clients may fail to connect.

Workaround/s: Please verify the configured values before entry.

HIGH AVAILABILITY

3. Internal tracking ID:

Problem Description: There is no redundancy for the Gateway.

Impact: If the Gateway fails then no client can avail the service.

Workaround/s: Keep a backup gateway ready. Periodically backup the configuration on the active gateway (automatic procedure). Restore the configuration on the backup Gateway if the Active one fails.

4. Internal tracking ID: 775

Problem Description: It is not possible to configure a secondary RADIUS server (if RADIUS is used) for the administrators and the end users.

Impact: If the primary Radius server fails then the authentication of administrators and end-users will fail (only if Radius is used for authentication).

Workaround/s: Implement server level redundancy by using virtual servers (server load balancing).

5. Internal tracking ID: 894

Problem Description: It is not possible to configure a secondary Active Directory server or domain name.

Impact: If the configured active directory server fails then the authentication will start failing.

Workaround/s: Use the most reliable active directory server or consider the virtual server option.

6. Internal tracking ID: 1328

Problem Description: Configuration backup does not backup the keytab file.

Impact: If the keytab file is not available with the administrator then the restored gateway will not work.

Workaround/s: Always retain a copy of keytab file on readily accessible media.

USER INTERFACE

7. Internal tracking ID: 993

Problem Description: The certificate used for the management system GUI (https server) cannot be uploaded by the customer.

Impact: Every time the management system GUI is accessed, the certificate warning will appear to the administrator.

Workaround/s: Install the CA certificate on the client computer accessing the management system GUI.

8. Internal tracking ID: 96

Problem Description: For the management system GUI, the browser's back button does not work.

Impact: Inconvenience to the administrator; accidentally hitting the back button will logout the administrator.

Workaround/s: Always use the left side pane menu to browse through the management system GUI sections.

9. Internal tracking ID: 755

Problem Description: Simultaneous multiple logins can be made using the same administrator account.

Impact: Accountability issues. The account may be misused as well.

Workaround/s: Discourage this practice by creating individual administrator accounts for each administrator.

POLICY OBJECTS

10. Internal tracking ID: 805

Problem Description: Users within a user group cannot be modified.

Impact: Accountability issues. Convoluted method for modifying individual user configurations within a user group.

Workaround/s: Instead of editing the user group, change the user group for the desired users.

11. Internal tracking ID: 1127

Problem Description: If the user's "full name" is missing and you ask for the user status then the operation fails.

Impact: Accountability issues. Not able to see the user status for such users.

Workaround/s: Never leave the full name of the user blank.

AUTO VPN

12. Internal tracking ID:

Problem Description: AES is not supported by the encryption acceleration hardware in the card. However the AES algorithm will automatically work using the software based encryption. The encryption acceleration hardware in the gateway supports AES.

Impact: Reduced throughput for the clients making use of AES.

Workaround/s: Avoid using AES if not required.

ACTIVE DIRECTORY IMPORT

13. Internal tracking ID: 1277

Problem Description: While importing a user who is already present in the management system database, a message saying "base key foreign key integrity constraint" is displayed.

Impact: Confusion to the administrator.

Workaround/s: Ignore the message, the operation is successful.

14. Internal tracking ID: 1305

Problem Description: Display name of the user not imported.

Impact: Difficult to identify the imported users.

Workaround/s: Enter the display name manually for the imported users.

PERSONAL FIREWALL

15. Internal tracking ID: 1001

Problem Description: If a change is made to a host or service group that is already used in a personal firewall policy then the changes are not reflected in the policy.

Impact: Desired changes are not reflected in the personal firewall policy.

Workaround/s: Remove the host or the service group from the policy. Make the changes to the host/service group and then reapply the host/service group to the policy.

SMS INTEGRATION

16. Internal tracking ID: 734

Problem Description: Patches available in the card are not applied to the laptop if the gateway is not accessible.

Impact: Application of patches may get delayed.

Workaround/s: Configure the connectivity timeout to a lower value. This will ensure that if the laptop is not connected to the enterprise network then it is in locked state, causing no danger due to pending patch.

17. Internal tracking ID: 735

Problem Description: The patch advertisement may erroneously be declared successful while the patch is in transit.

Impact: The SMS Administrator may get a false notification that the patch has been applied while it is in transit.

Workaround/s: Configure the connectivity timeout to a lower value and encourage the end user to remain always connected. This will reduce the probability of incorrect notification.

PATCHLINK UPDATE INTEGRATION

18. Internal tracking ID:

Problem Description: Patches that have already been downloaded to the card are not applied to the laptop until the tunnel to the gateway is established.

Impact: Application of patches may be delayed.

Workaround/s: Configure a low value for the connectivity timeout. This will ensure that the laptop locks shortly after disconnecting from the enterprise network, minimizing the risk associated with the delayed application of a patch.

Client

Please refer to the OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 End-User Release Notes for information on known issues for the OmniAccess 3500 NLG client (card and laptop).