Alcatel·Lucent

OmniAccess 3500
Nonstop Laptop Guardian

Release 1.2.42

Administrator Release Notes

Document Version: 42.02

Part Number: 032334-10 Rev C

Published: 02.01.2008

Alcatel-Lucent Proprietary

Welcome

Welcome to the Administrator Release Notes for Release 1.2.42 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. The previous revision of this document (25.01) was issued on 11.27.2007 and was attached to Release 1.2.25 of the OmniAccess 3500 NLG. This document should be read in conjunction with the previous version.

Please note that Release 1.2.42 of the OmniAccess 3500 NLG is a patch release that only fixes bugs found in the previous release.

Release Information

- **Vendor:** Alcatel-Lucent
- **Product:** OmniAccess 3500 Nonstop Laptop Guardian
- **Release:** 1.2.42
  - *Issue Date:* January 29, 2008
  - *Distribution:* General availability to all customers
- **Hardware:** OmniAccess 3500 Nonstop Laptop Guardian Enterprise Gateway, Hardware Revision 1 (there is no change in the gateway hardware compared to Release 1.2.25)
- **Software**
  - *Distribution Server:* www.nonstopguardian.com (client software only)
  - *Directory:* Link on the main page
  - *Package Files:* See Table 1

Sr.	File Name	Description	Size (bytes)	MD5 Hash	Comments
1	NLG-Flash-Image-1.2.42-V4-64.raw	Card firmware	15,194,112	5CCE2BBE16DDA2EB36A4E769655AAACF	Pre-installed in the card

2	NLG-Management-Server-pgsqlbin-1.2.42.rpm	Database software running on the gateway	7,333,807	77D16FBF2DF3287DA4FE978076E4612D	Pre-installed in the gateway
3	NLG-Management-Server-1.2.42.rpm	Management system software running on the gateway	52,570,241	5D65AD452675DBB3EC67D1441A3A100D	Pre-installed in the gateway
4	NLG-Gateway-1.2.42.rpm	Gateway software	19,739,009	03226D5D55842B5BFE4274BAC9E5EA39	Pre-installed in the gateway
5	NLG-SMSServer-setup-1.2.42.exe	Software for Microsoft SMS integration to be installed in the SMS server	3,262,569	E4184EDC6BDF5F81185AACEBC6EEC77B	To be installed only if Microsoft SMS is used
6	NLG-Gateway-Common-1.2.42.rpm	Platform software running on the gateway	661,534	03226D5D55842B5BFE4274BAC9E5EA39	Pre-installed in the gateway

Table 1 - Release 1.2.42 administrator package files

Documentation

Please note that there are no new revisions of the user manuals for this product release (1.2.42). All documents associated with the previous release (1.2.25) are still applicable. All product changes that are visible to the IT administrator and end user are covered in the respective Release Notes documents.

The following list contains all user documents that are available for consultation in addition to the Administrator and End-User Release Notes:

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

Previous Release

This document highlights all known issues of Release 1.2.42 of the OmniAccess 3500 NLG and all incremental changes introduced in Release 1.2.42 with respect to Release 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.
- To achieve proper operation of all components of the OmniAccess 3500 NLG platform, the installed 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
  - Processor speed: 1 GHz or higher
  - RAM: 512 MB or higher
  - PCMCIA CardBus slot
  - No VPN client installed in the laptop
  - Trusted Platform Module (TPM) disabled if 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. The 1024x768 screen resolution (normal font size) is recommended.

Contacting Technical Support

Please contact your Service Provider to address any technical issue that you may encounter in the operation of the OmniAccess 3500 NLG platform. If instructed by your Service Provider to contact Alcatel-Lucent for technical support, please refer to the following contact information:

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

This product release (1.2.42) does not introduce new features compared to the previous release (1.2.25). Please refer to the previous revision (25.01) of this document for a list of the features that are included in this product release.

Issues Fixed

This section lists known issues of Release 1.2.25 that have been fixed in Release 1.2.42:

1. **Internal tracking ID: 775**

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

2. **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.

3. **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.

4. **Internal Tracking ID:**

   Problem Description: The card firmware cannot be upgraded automatically when a new version of the OmniAccess 3500 NLG client software is installed in the laptop.

   Resolution Details: When a new version of the OmniAccess 3500 NLG client software is installed in the laptop, it is now no longer necessary to manually flash the OmniAccess 3500 NLG card with the corresponding firmware version. Instead, after the end user installs the new client software in the laptop, the client software automatically recognizes the card firmware version the next time the card is inserted again, and replaces it if it is obsolete. No intervention is required from the end user or the IT administrator.

5. **Internal Tracking ID:**

Problem Description: The OmniAccess 3500 NLG client software cannot be uninstalled.

Resolution Details: To prevent the end user from bypassing the security and management controls enforced by the OmniAccess 3500 NLG, the end user is normally not allowed to uninstall and remove the OmniAccess 3500 NLG client software from the laptop. However, if the IT administrator concludes that the client software must be uninstalled, Release 1.2.42 now enables uninstallation of the client software by the end user under administrative control. The controlled uninstallation procedure works as follows:

- The end user calls the IT helpdesk.
- The IT helpdesk administrator on the phone instructs the end user to start the uninstallation of the OmniAccess 3500 NLG client software using the *Add-Remove Programs* feature of Windows.
- A pop-up window appears on the screen asking for the uninstallation password. The window displays the current date and time and a screen-count number. The administrator needs this information to generate a One-Time Uninstallation Password (OTUP).
- To generate the OTUP on the management system GUI, the administrator clicks **Users** on the left-hand main menu, selects the desired user, clicks **Configure**, clicks **Generate One Time Password**, enters the information found by the end user on the pop-up window, and clicks **GetPW**. Please note that the OTUP is user-specific and can be used only once within two hours of its generation. The password is not case-sensitive and does include the hyphens that appear on the management system GUI window.
- The end user resumes the uninstallation process by entering the password supplied by the administrator.

The *OmniAccess 3500 Nonstop Laptop Guardian Release 1.2.42 End-User Release Notes* document contains detailed message flows and screen shots.

6. **Internal Tracking ID:**

Problem Description: A redundant RADIUS server for end-user authentication is not supported.

Resolution Details: Release 1.2.42 supports two RADIUS servers (primary and secondary). All authentication requests are first sent to the primary RADIUS server. If the primary server does not respond to a request, the same request is forwarded to the secondary RADIUS server. The secondary RADIUS server becomes now the primary RADIUS server and maintains this role until its first failure to respond to a request. To configure the primary and secondary RADIUS servers on the management system GUI the administrator clicks **Gateway** on the left-hand main menu, clicks **Edit Gateway Settings**, enters the **IP Address**, **Port**, and **Secret** values for the two servers, and clicks **Save**.

Known Issues

This section lists known issues of Release 1.2.42 of the OmniAccess 3500 NLG.

Gateway

INSTALLATION AND CONFIGURATION

1. **Internal tracking ID: 349**

   Problem Description: Change of super admin id is not forced when gateway is installed.

   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. This step is also recommended 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: Verify the configured values before entry.

3. **Internal tracking ID: 1818**

   Problem Description: The *Gateway Configuration and Restore* utility does not restore the pre-existing values of connectivity and OTP timeout (per user) and of radio timeout (per user group). Instead, the default values are set after a restoration (90 days).

   Impact: In case of configuration restore (if the gateway fails) the connectivity, radio, and OTP timeout are set to the maximum value permitted.

   Workaround/s: After configuration restore, make sure to configure these values correctly for all users and user groups.

4. **Internal tracking ID: 655**

   Problem Description: There is no mechanism for the recovery of a lost super administrator’s password.

   Impact: The super admin account may become unusable if the password is lost.

   Workaround/s: Store the super administrator’s password in a safe place. Also create immediately upon gateway installation at least one more administrator account in addition to the super administrator one, so that the administrative functions can be carried out using the other account.

HIGH AVAILABILITY

5. **Internal tracking ID:**

   Problem Description: There is no redundancy for the gateway.

   Impact: If the OmniAccess 3500 NLG gateway fails, 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 gateway fails.

6. **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 of the end users will start failing.

Workaround/s: Use the most reliable Active Directory server or consider the virtual server option.

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 that is used for accessing the management system GUI.

8. **Internal tracking ID: 96**

   Problem Description: On 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 pane menu on the left-hand side of the GUI window 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.

10. **Internal tracking ID: 1834**

    Problem Description: Some of the management system GUI windows, specifically the *Gateway Configuration* window, may appear jumbled up.

    Impact: Accountability issues. Not able to carry out the desired configuration changes.

    Workaround/s: Use of Internet Explorer 6.0 with 1024x768 screen resolution shall fix this problem.

OPERATION

11. **Internal tracking ID: 1840**

    Problem Description: Sometime the user status information, including indication of whether the card is currently inside or outside the laptop, is not shown correctly. If the tunnel is not active, the status shown is the last known at the time of the request and is only updated after completion of the remote wakeup procedure.

Impact: Incorrect status information.

Workaround/s: If the status information is critical, always recheck the desired status entry again 10 minutes after issuing the status request.

Policy Objects

12. **Internal tracking ID: 805**

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

    Impact: Accountability issues. The method for modifying individual user configurations within a user group is convoluted.

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

Auto VPN

13. **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.

14. **Internal tracking ID: 1024**

    Problem Description: If RADIUS is used for end-user authentication then any user having a valid RADIUS account can use the OmniAccess 3500 MLG-enabled laptop.

    Impact: This is not a bug. Some enterprises may like it this way. However, this behavior may be an issue for enterprises that want to have a strict binding between the laptop, the OmniAccess 3500 NLG card, and the user.

    Workaround/s: If you want to have a strict binding between the laptop, the OmniAccess 3500 NLG card, and the user, do not use the RADIUS-based authentication and use instead the default Active-Di rectory authentication method.

15. **Internal tracking ID: 1471**

    Problem Description: Switching from the default 3DES encryption to AES encryption does not work.

    Impact: Because of the configuration issue, it is not possible to use AES in this release.

    Workaround/s: There is no known workaround at the moment. Continue using 3DES in place of AES.

RADIUS-Based Authentication

16. **Internal Tracking ID: 1892, 1893**

Problem Description: It is not possible to change the authentication method from RADIUS (Lax or Strict) to Domain (Active Directory) after the RADIUS selection has been saved in the initial configuration.

Impact: Once RADIUS is selected, Domain is no longer an available option. Trying to switch from RADIUS to Domain will compromise the configuration of all OmniAccess 3500 NLG components.

Workaround/s: Make a conclusive decision about the authentication method (RADIUS or Domain) before installing the gateway.

17. **Internal Tracking ID: 1892, 1893**

Problem Description: Switching the authentication method from Domain to RADIUS (Lax or Strict) when the RADIUS configuration parameters are already populated or changing the configuration of the RADIUS server parameters when a secondary RADIUS server is configured may not work.

Impact: Once an authentication method is selected and configured, changing any portion of the configuration may compromise the configuration of all OmniAccess 3500 NLG components.

Workaround/s: In general, it is always preferable to make a conclusive decision about the authentication method (RADIUS or Domain) and its configuration before installing the gateway. However, in the specific cases outlined in the Problem Description the following procedure can be used to ensure a successful update of the configuration parameters for the authentication method:

- Click **Gateway** and **Edit Gateway Settings**.
- On the *Gateway Configuration* window, enter incorrect values for all RADIUS-server fields (IP address, port, secret).
- Save the incorrect values. The gateway will reboot.
- Click **Gateway** and **Edit Gateway Settings**.
- On the *Gateway Configuration* window, enter the desired values for all RADIUS-server fields (IP address, port, secret).
- Save the correct configuration. The gateway will reboot.
- Check the Rules table in the Connection Manager settings (click **Configure Advanced Settings** and click **Rules** to view the *Gateway Configure -> Rule Information* window). The Rule table may show two duplicate rules (106 and 108). This is not a problem if the two rules are identical.

ACTIVE DIRECTORY IMPORT

18. **Internal tracking ID: 1305**

Problem Description: The display name of the user is not imported.

Impact: Difficult to identify the imported users.

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

PERSONAL FIREWALL

19. **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

20. **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.

21. **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.

22. **Internal tracking ID: 1571**

    Problem Description: Patches delivered to the laptop do not get installed. This happens because the virtual IP address of the laptop is not registered with the DNS and therefore the SMS client on the laptop is not able to connect to the SMS management point (residing either on the SMS server or on a separate server).The SMS management point hence never gets to know that a patch is waiting to be installed.

    Impact: The patches sent to the laptop may not be applied.

    Workaround/s: For the patches to be delivered successfully, the admin shall take care of following:

    - Add to the DNS a reverse lookup zone for the virtual IP address range assigned to the laptops.
    - Add the virtual IP address range assigned to the laptops to the site boundaries of the SMS server.

PATCHLINK UPDATE INTEGRATION

23. **Internal tracking ID:**

Problem Description: PatchLink Update 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.

24. **Internal tracking ID: 1885**

    Problem Description: The status of the AWT facility is not properly reflected in the management system GUI.

    Impact: Once AWT is enabled it is not possible to disable it because the management system GUI will not show the option of disabling it.

    Workaround/s: There is no workaround for this. However there is no harm in leaving the AWT enabled all the time.

ANTI-TAMPERING

25. **Internal tracking ID: 866**

    Problem Description: It is possible to uninstall the OmniAccess 3500 NLG client software from the laptop by restoring Windows to a previous checkpoint.

    Impact: The end user may get rid of the security and management controls enforced by the OmniAccess 3500 NLG.

    Workaround/s: To prevent this from happening, please delete all previous checkpoints after installing the OmniAccess 3500 NLG software.

26. **Internal tracking ID: 1848**

    Problem Description: The One-Time Password issued for one user also works for another user.

    Impact: Not a desirable behavior from a security perspective.

    Workaround/s: This happens if the base password configured for both users is the same. Please make sure that a unique base password is configured for each user. In the future the base password will be generated automatically.

Client

Please refer to the OmniAccess 3500 Nonstop Laptop Guardian Release 1.2.42 End-User Release Notes for information on known issues for the OmniAccess 3500 NLG client (card and laptop).