

**OmniAccess 3500
Nonstop Laptop Guardian
Release 1.2
Administration Guide**

Document Version: 25.02

Part Number: 060228-10 Rev B

Published: 12.11.2007

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

About This Document	1
The OmniAccess 3500 NLG Library	1
Contacting Technical Support	2
Chapter 1. OmniAccess 3500 NLG Platform Components	3
OmniAccess 3500 NLG Gateway	3
OmniAccess 3500 NLG Card	5
Management System Software	5
Chapter 2. OmniAccess 3500 NLG Initialization Tasks	6
Working with the Management System GUI	6
Launching the Management System GUI	7
Logging into the Management System GUI	7
Window Navigation	8
Common Operations	9
Technical Support Information	10
Logging Out of the Management System GUI	11
Initial Configuration of Gateway Parameters	11
Administrator Accounts	13
Administrators	13
Authentication Methods	14
Remote Access Provisioning	16
Connection Manager—Settings	16
File Upload	22
License Manager	23
End User Provisioning	27
Users and User Groups	27
OmniAccess 3500 NLG Cards	32
Laptops	35
Application Provisioning	36
Device Management Applications	36
Personal Firewall	39
Chapter 3. OmniAccess 3500 NLG Runtime Administration Functions	53
Viewing Laptop Asset Information	53
Viewing User Status Information	54

Viewing the Laptop Location	55
Laptop Remote Lock	57
Laptop Remote Unlock	57
One-Time Password Generation.....	58
Encrypted Volume Management	59
Connection Manager - Show Information	65
Logs and Alarms	66
Log Viewer.....	66
Log History	67
Syslog.....	68
Chapter 4. OmniAccess 3500 NLG Infrastructure Maintenance	70
Backing Up and Restoring the OmniAccess 3500 NLG Gateway Configuration.....	70
Automatic Backup Configuration.....	70
Restoration Procedure.....	75
Upgrading the OmniAccess 3500 NLG Gateway Configuration	77
Configuration Upgrade.....	77
Chapter 5. OmniAccess 3500 NLG Administrative Information Base	79
Devices	79
Users.....	99
Hosts.....	111
Services	113
Policies	114
Fault Manager	122
License Manager	125
Management Access.....	126
Configuration Manager	129
Utilities	132

About This Document

The OmniAccess 3500 Nonstop Laptop Guardian (NLG) administrator finds in this document general information about the OmniAccess 3500 NLG Release 1.2 (R1.2) product and detailed information on the use of the management system Graphical User Interface (GUI) and on the maintenance of the OmniAccess 3500 NLG gateway.

The document is divided into the following chapters:

- Chapter 1, *OmniAccess 3500 NLG Platform Components*, provides an overview of the components that make up the OmniAccess 3500 NLG.
- Chapter 2, *OmniAccess 3500 NLG Initialization Tasks*, details configuration and provisioning tasks that the administrator performs on the OmniAccess 3500 NLG components prior to their deployment.
- Chapter 3, *OmniAccess 3500 NLG Runtime Administration Functions*, describes tasks that the administrator performs at runtime on the deployed OmniAccess 3500 NLG components.
- Chapter 4, *OmniAccess 3500 NLG Infrastructure Maintenance*, illustrates procedures for servicing and upgrading the OmniAccess 3500 NLG gateway (including the management system software that runs on it).
- Chapter 5, *OmniAccess 3500 NLG Administrative Information Base*, contains detailed descriptions for all information objects that are accessible through the management system GUI. The OmniAccess 3500 NLG administrator should refer to this chapter to better understand the meaning and intended use of the objects that compose the information base.

The OmniAccess 3500 NLG Library

Other documents in the OmniAccess 3500 NLG library include the following:

- The *OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Gateway Quick Start Guide* (available at: http://www1.alcatel-lucent.com/enterprise/en/resource_library/user_manuals.html) provides the IT administrator/technician with an overview of the OmniAccess 3500 NLG gateway and with the minimum information needed to set up the gateway and connect it to the network.
- The *OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Gateway Installation Guide* (available at: http://www1.alcatel-lucent.com/enterprise/en/resource_library/user_manuals.html) provides the IT administrator/technician with detailed instructions for the installation and initial configuration of the OmniAccess 3500 NLG gateway.
- The *OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Application Note: Integration of PatchLink Update and Microsoft SMS* (available at: http://www1.alcatel-lucent.com/enterprise/en/resource_library/user_manuals.html) provides the IT administrator with instructions for the integration of the OmniAccess 3500 NLG platform with the PatchLink Update and Systems Management Server (SMS)

applications (PatchLink Update is a Lumension Security product; SMS is a Microsoft product).

- The *OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Card Quick Start Guide* (available at: http://www1.alcatel-lucent.com/enterprise/en/resource_library/user_manuals.html) provides the end user with an overview of the OmniAccess 3500 NLG card and with the necessary information for its installation.
- The *OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 End User Reference Guide* (available at: http://www1.alcatel-lucent.com/enterprise/en/resource_library/user_manuals.html) provides the end user with instructions for the daily operation of the OmniAccess 3500 NLG card.
- The *OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Features Overview* presents the feature set composition for the current release of the product.
- The *OmniAccess 3500 Nonstop Laptop Guardian Technical Overview* presents release-independent information about the product's technology and features.

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.

Chapter 1. OmniAccess 3500 NLG Platform Components

The OmniAccess 3500 NLG platform is built on the following three logical components:

- OmniAccess 3500 NLG gateway – An enhanced remote access server that deploys at the edge of the enterprise network.
- OmniAccess 3500 NLG card – An intelligent EV-DOrA data card that plugs into the end-user laptop and includes a processor, non-volatile memory, and independent power.
- Management system software – A management platform that can be installed in any general-purpose enterprise server (including the OmniAccess 3500 NLG gateway). In the OmniAccess 3500 NLG R1.2 the management system software is always embedded in the OmniAccess 3500 NLG gateway.

Figure 1 displays the OmniAccess 3500 NLG platform components.

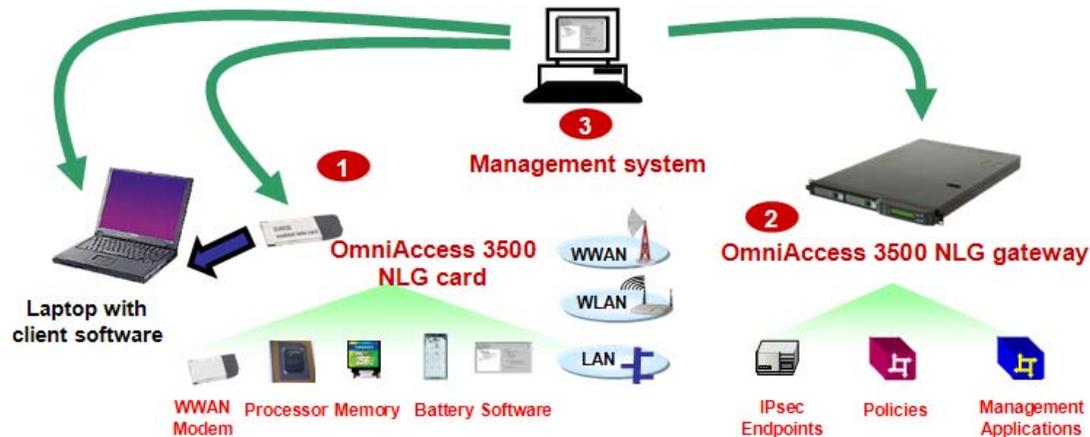


Figure 1 - OmniAccess 3500 NLG platform components

After receiving the box with the OmniAccess 3500 NLG card, the end user downloads the client software (a collection of Windows drivers and applications that enable the laptop for OmniAccess 3500 NLG functionality) from the OmniAccess 3500 NLG support website (the URL is printed on the end user welcome card that comes with the box). The laptop activates the client software the first time the card is plugged in.

OmniAccess 3500 NLG Gateway

The OmniAccess 3500 NLG gateway combines the following physical and functional elements:

- Two network interfaces (10/100/1000 Mbps Ethernet), of which one is external (handling traffic to and from the public Internet) and one internal (facing the inner portion of the enterprise network).
- A processing subsystem (CPU, OS, and management system software) that implements the OmniAccess 3500 NLG functions.

- A hardware acceleration module for IPsec encryption/decryption, key management, and compression.
- A hard disk for storage of local information and application caching.
- A secure management interface for driving all OmniAccess 3500 NLG operation, administration, management, and provisioning (OAM&P) procedures.

The OmniAccess 3500 NLG gateway terminates the secure remote-access tunnels, manages user credentials and security policies (up to 16K users in the OmniAccess 3500 NLG R1.2), and provides storage and file transfer capabilities in support of third-party remote-access and device-management applications. The OmniAccess 3500 NLG gateway also cooperates with the OmniAccess 3500 NLG card in ensuring that vertical handovers (run-time connectivity switchovers from one laptop interface to another) are not disruptive to running network applications.

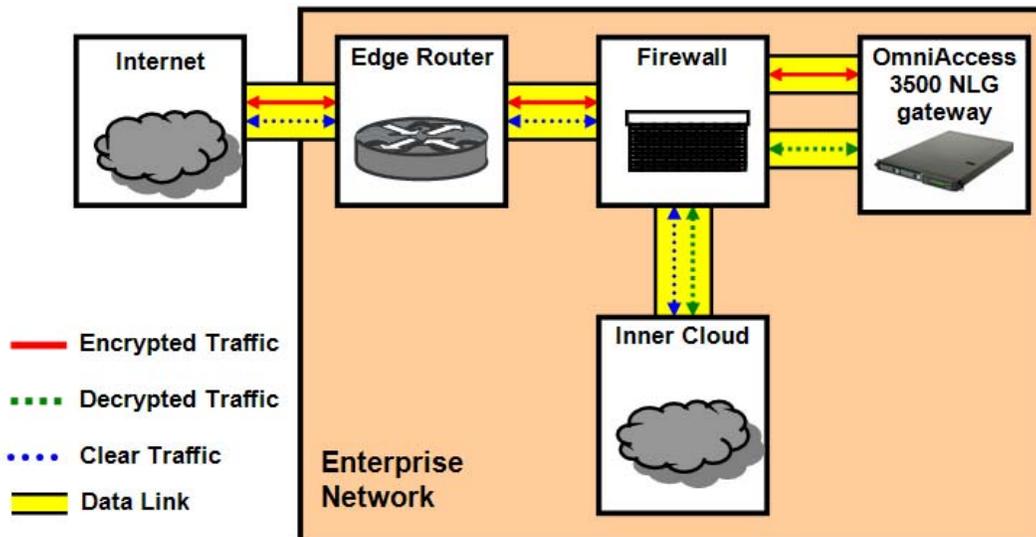


Figure 2 - Recommended placement of the OmniAccess 3500 NLG gateway within the network

The OmniAccess 3500 NLG gateway is best deployed as a stub of the enterprise firewall at the edge of the enterprise network (Figure 2): the firewall and the OmniAccess 3500 NLG gateway exchange encrypted traffic over the external interface of the gateway and decrypted traffic over its internal interface. This way the firewall can apply full protection both to the external interface of the OmniAccess 3500 NLG gateway and to the inner portion of the enterprise network. Alternative, sub-optimal arrangements can also be adopted to match topological and functional peculiarities that may be found in the pre-existing network infrastructure.

Multiple instances of the OmniAccess 3500 NLG gateway can be deployed within the same enterprise network to increase capacity and extend geographical coverage and service availability. In the OmniAccess 3500 NLG R1.2, each OmniAccess 3500 NLG gateway is installed with its own management system instance and serves its own set

of OmniAccess 3500 NLG cards. The gateway's physical location can be either intra-premises or extra-premises (e.g., in a data center).

For detailed information on installing the OmniAccess 3500 NLG gateway, see the *OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Gateway Installation Guide*. For information on the maintenance of the OmniAccess 3500 NLG gateway software, see the chapter entitled *OmniAccess 3500 Nonstop Laptop Guardian Infrastructure Maintenance* in this document.

OmniAccess 3500 NLG Card

The OmniAccess 3500 NLG card is a CardBus device that can be field-installed in a laptop with a PCMCIA slot. The card contains a local processor, flash memory, and a 3G modem (EV-DO Release A), all powered by an on-card rechargeable battery. During normal operation, the card draws power from the laptop. The rechargeable battery supplies power when the laptop is in standby mode or in shutdown mode.

The OmniAccess 3500 NLG card works with Windows-based laptops with the following minimum configuration:

- CPU: X86 1GHz
- Memory: 512 MB
- Free hard disk space: 1 GB
- Operating system: Windows XP Home, Professional, or Tablet edition
- One PC Cardbus slot

For information on installing the OmniAccess 3500 NLG card and the client software, see the *OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Card Quick Start Guide*.

Management System Software

The management system is the sole management portal to the OmniAccess 3500 NLG gateway, cards, and laptops. It is a software-only component that can be installed in any Linux server with adequate resources, including the OmniAccess 3500 NLG gateway (in the OmniAccess 3500 NLG R1.2 the gateway is actually the only option available for the installation of the management system software).

Chapter 2. OmniAccess 3500 NLG Initialization Tasks

The management system performs all OAM&P functions for the OmniAccess 3500 NLG platform. The management system GUI is the single entry point to those functions for the IT administrator.

This chapter explains how to:

- Launch the management system GUI, log into an administrator account, browse through the GUI sections, and log out of the administrator account.
- Perform initialization tasks from the management system GUI, including the following:
 - Completing the gateway installation – After installing the gateway or upgrading its software, you must configure parameters that enable the gateway interoperation with the other functional components of the corporate network.
 - Configuring administrator accounts – You can add administrator accounts to the system, as well as view, edit, and delete existing administrator information (including the authentication method).
 - Configuring RADIUS servers for administrator authentication – You can configure RADIUS servers for administrator accounts that do not use locally-defined credentials for authentication.
 - Configuring the connection manager – You can set configuration parameters and view status information for the functional components of the OmniAccess 3500 NLG gateway that define how the remote access connections are established.
 - Managing licenses – You can create, delete, and renew user licenses.
 - Provisioning users – You must complete certain tasks before starting deployment of the OmniAccess 3500 NLG cards, such as configuring a user group and associating it with a personal firewall policy, and adding a new user to a user group.
 - Provisioning cards – You can add and delete OmniAccess 3500 NLG card instances, or edit their configuration.
 - Provisioning laptops – You can add and delete laptop instances, or edit their configuration.
 - Setting up the assisted file transfer facility – You can configure your IT applications for automatic offline synchronization between laptop and enterprise folders.
 - Managing policies – You can configure the personal firewall policies that are installed in the OmniAccess 3500 NLG cards.

Working with the Management System GUI

The management system GUI is a web server application that runs on the OmniAccess 3500 NLG R1.2 gateway. Every instance of the management system has exclusive control over the OmniAccess 3500 NLG gateway where it is installed.

Launching the Management System GUI

To launch the management system GUI, you must open a web browser and connect to the HTTPS URL of the target GUI instance. The procedure is the same irrespective of whether you are working from a remote terminal or at the console of the OmniAccess 3500 NLG gateway that hosts the management system.

Logging into the Management System GUI

1. After you launch the GUI, the login window appears (Figure 3).



Figure 3 - Login window

2. Enter your Administrator ID and Password.
3. Click **Login**.
4. A banner window appears (Figure 4).

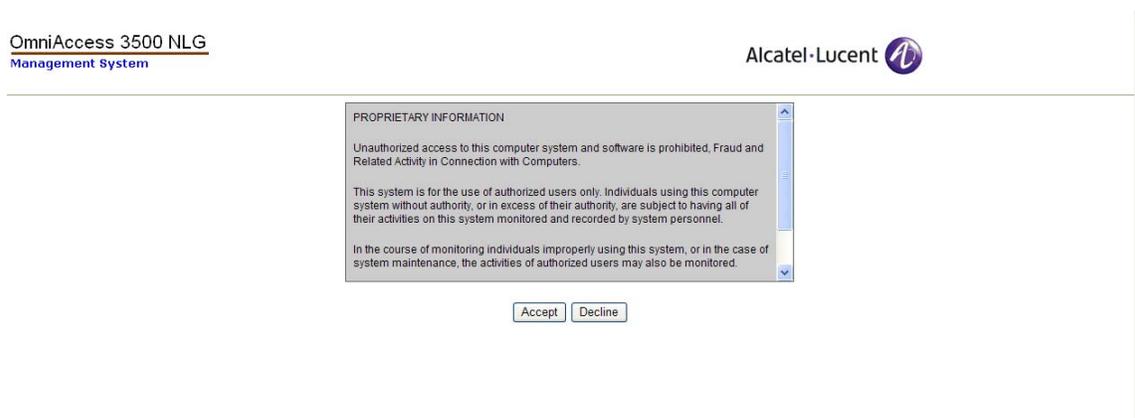


Figure 4 - Banner window

5. Click **Accept** to log into the GUI.

Note: To customize your banner page, contact the OmniAccess 3500 NLG customer support.

6. Next, the Home window appears (Figure 5). This window displays system settings information. You can click **Home** at any time during your GUI session to return to the Home page.

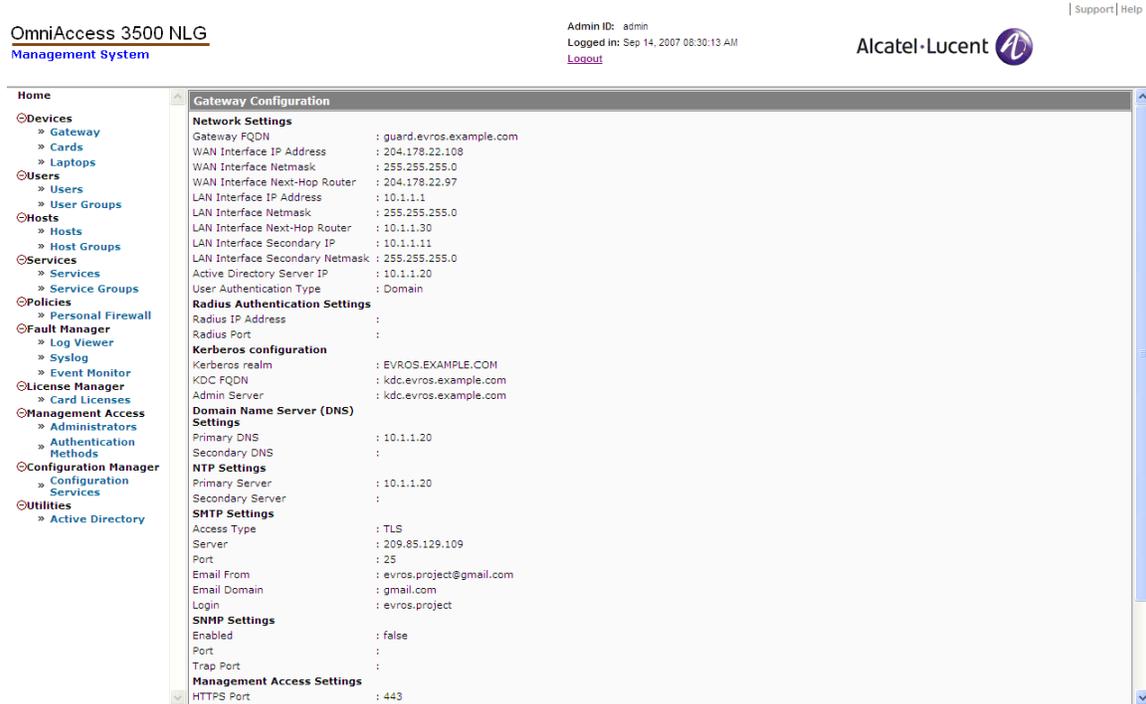


Figure 5 - Home window

Note: The first time you log into the management system GUI after installing the gateway or upgrading its software, you will find most settings still undefined. Please follow the instructions in the section Initial Configuration of Gateway Parameters for completing the initialization of the OmniAccess 3500 NLG gateway before moving on to other administrative tasks.

Window Navigation

The OmniAccess 3500 NLG configurable objects are accessible by clicking on them in the menu bar on the left-hand side of the GUI window. Object windows have the following format:

- First row: window name
- Second row: action tabs (see the *Common Operations* section below for common action tabs)
- Third row: field descriptions. Click on a field description to apply that field as the sorting criterion for the listed objects.

Common Operations

Most objects allow the following operations:

- **New** – Click this button to create a new instance of the object.
- **Open** – Click this button to view information about an object instance. Fields on the Open windows are read-only.
- **Edit** – Click this button to modify settings for an object instance.
- **Delete** – Click this button to remove an object instance from the system. A message will appear asking you to confirm the deletion. Click **Yes** to delete the object you selected.
- **Status** – Click this button to update the status for an object instance and review it.
- **Configure** – Click this button to perform configuration actions on an object instance.

To complete actions on a window, click one of the following buttons that appear at the bottom of the window:

- After viewing information on a window, click **OK**.
- After changing information on a window, click **Save**.
- To exit a window without saving changes, click **Cancel**.

Note: Always use the GUI's interface buttons to navigate. With some browsers (e.g., Internet Explorer) using the browser's navigation buttons will result in being sent to an error window (login session expiration) and then back to the login window.

You can access online support information at any time by clicking the **Support** link that appears at the top right corner of every window (see the *Technical Support Information* section below for more details).

You can access online help information (a web reproduction of this document) at any time by clicking the **Help** link that appears at the top right corner of every window.

Technical Support Information

Click the **Support** button at the top right of any window to see technical support contact information in the Gateway Support Information window (Figure 6).

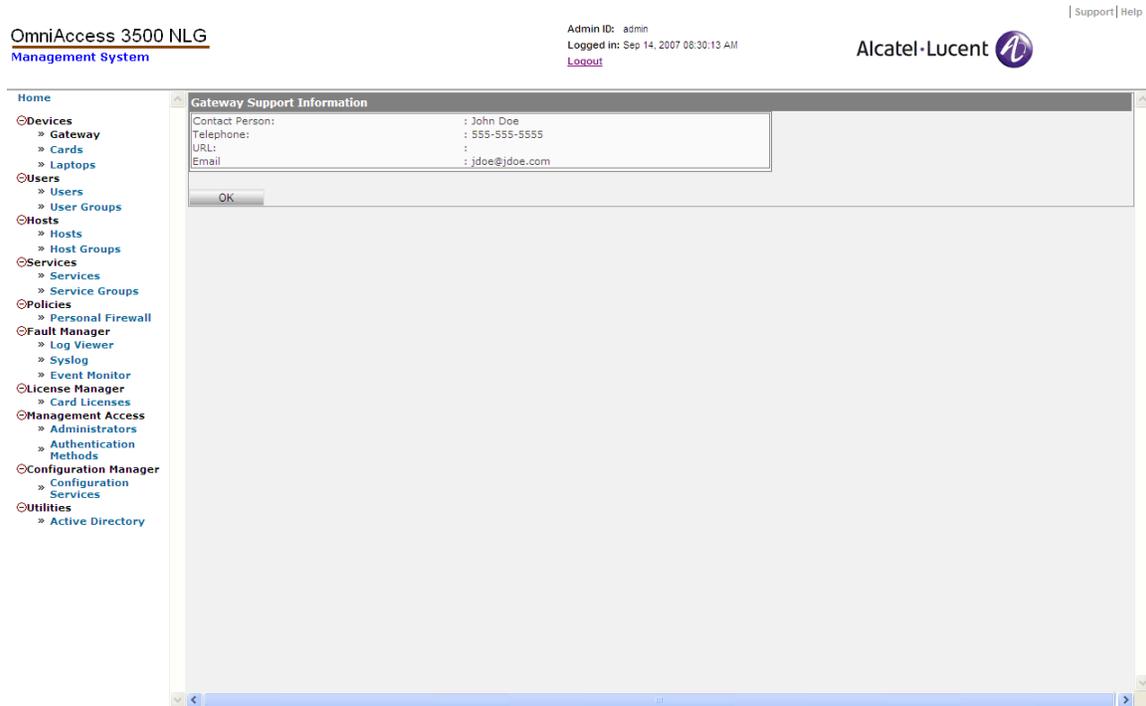


Figure 6 - Gateway Support Information

Support information can be added or edited using the following procedure:

1. Click **Gateway** on the main menu.
2. Click **Edit Support Information**. The Edit Gateway Support Information window appears (Figure 7).
3. Type support contact information into the fields or edit the existing information.
4. Click **Save**.

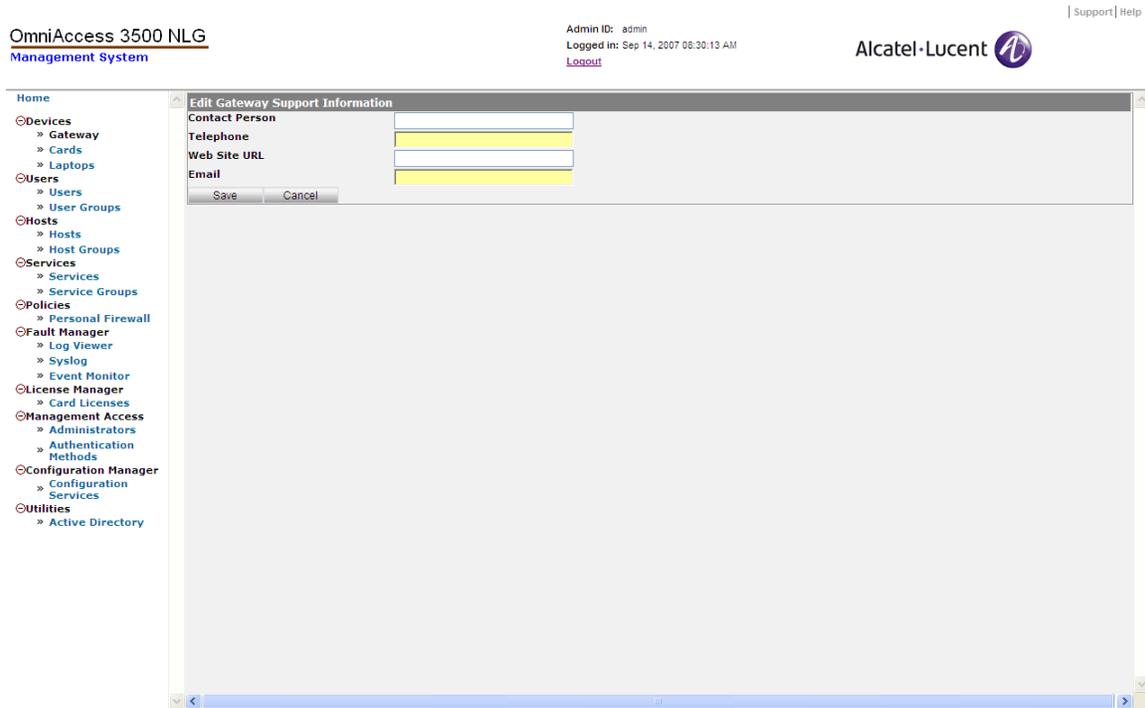


Figure 7 - Edit Gateway Support Information

Logging Out of the Management System GUI

1. To log out of the management system GUI, click the **Logout** link near the top of the window (see Figure 8 for the location of the **Logout** link).
2. Alternatively, you can exit the application by closing the web browser window.

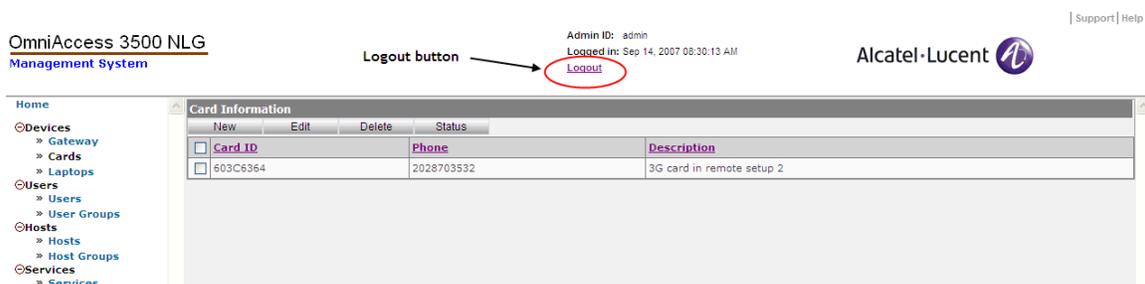


Figure 8 - Logout button

Initial Configuration of Gateway Parameters

After physical installation of the OmniAccess 3500 NLG gateway or installation of a software upgrade, you must configure the gateway for interoperability with the other nodes of your network. This section describes the procedure for this initial configuration.

1. The first time the management system GUI is opened, the Gateway Settings window appears (Figure 9). Click **New**.



Figure 9 - Gateway Settings

2. The Gateway Configuration (Add) window appears (Figure 10).



Figure 10 - Gateway Configuration (Add)

3. Type the appropriate information into the fields that do not contain default values (see the *Gateway* portion of the *Devices* section in Chapter 5, *OmniAccess 3500 NLG Administrative Information Base*, for a detailed description of each field).
4. Click **Save** when you are finished entering information.
5. A window appears stating that the operation has been successful.
6. The gateway will reboot and resume operation with the last saved configuration.

Administrator Accounts

The management system admits one super administrator account (pre-configured) and multiple plain administrator accounts (configured exclusively by the super administrator). The super administrator can create, modify, and delete plain administrator accounts through the Management Access section of the management system GUI. Plain administrators cannot configure other administrator accounts. The super administrator and all plain administrators have identical administrative privileges over all configurable objects of the management system GUI. No more than one login session per administrator account can be active at any time.

The super administrator always uses locally-defined credentials to log into the management system GUI. For every plain administrator account, instead, the super administrator can choose between local and RADIUS-based authentication. RADIUS is a distributed client/server system that secures networks against unauthorized access. The OmniAccess 3500 NLG management system integrates a RADIUS client for communication with the RADIUS server(s) that may be deployed within the enterprise network. The Management Access section of the management system GUI includes facilities for configuring the RADIUS servers for RADIUS-based authentication of the plain administrators.

Administrators

The super administrator can use this GUI object to add, view, edit, and delete administrator accounts.

To add an administrator:

1. Click **Administrators** on the main menu.
2. On the Administrators Information window, click **New**. The Administrators Information (Add) window appears (Figure 11), displaying the following fields:
 - Login ID: The login ID for the administrator account you are creating.
 - Authentication Method: Select <Local> (for authentication based on locally defined username and password) or <RADIUS> (for authentication by a RADIUS server).
 - RADIUS Server: From the drop-down menu, select <None> (if the selected authentication method is <Local>) or the pre-populated IP address of a RADIUS server (if the selected authentication method is <RADIUS>).
 - First Name: The first name of the new administrator.
 - Last Name: The last name of the new administrator.

- Password: The password of the new administrator. The value assigned to this field is relevant only if the selected authentication method is <Local>. If the selected authentication method is <RADIUS>, the password needed by the administrator for authentication is set separately through the RADIUS infrastructure.
- Re-enter Password: Re-enter the password of the new administrator (relevant only if the authentication method is set to <Local>).
- Email: The email address of the new administrator.
- Address: The mailing address of the new administrator.
- City: The city of the new administrator.
- State: The state of the new administrator.
- Country: The country of the new administrator.
- Zip: The zip code of the new administrator.
- Phone: The new administrator's office phone number.
- Mobile: The new administrator's mobile phone number.

3. Click Save.

The screenshot displays the 'Administrator Information (Add)' form within the OmniAccess 3500 NLG Management System. The interface includes a top navigation bar with the system name, user information (Admin ID: admin, Logged in: Sep 14, 2007 08:30:13 AM), and the Alcatel-Lucent logo. A left-hand navigation tree lists various system components such as Devices, Users, Hosts, Services, Policies, Fault Manager, License Manager, Management Access, Configuration Manager, and Utilities. The main content area contains the 'Administrator Information (Add)' form with the following fields: Login ID (text input), Authentication Method (dropdown menu set to 'Local'), Radius Server (dropdown menu set to 'None'), First Name (text input), Last Name (text input), Password (text input), ReEnter Password (text input), Email (text input), Address (text input), City (text input), State (text input), Country (text input), Zip (text input), Phone (text input), and Mobile (text input). At the bottom of the form are 'Save' and 'Cancel' buttons.

Figure 11 - Administrators Information (Add)

Authentication Methods

The OmniAccess 3500 NLG R1.2 supports the following two methods for authentication of a plain administrator:

1. Local — The management system authenticates the administrator with locally configured login ID and password (default method).
2. RADIUS — A RADIUS server installed in the network authenticates the administrator with a login ID that is configured with the administrator account and a password that is remotely assigned according to the applicable RADIUS-supported authentication method.

The super administrator can use the Authentication Methods object of the management system GUI to configure the RADIUS servers that support non-local authentication methods for the plain administrators. Each administrator is assigned to one of the available RADIUS servers. To access this object, click **Authentication Methods** under Management Access and then click **RADIUS Server**.

To add a RADIUS configuration:

1. On the RADIUS Server Configuration window, click **New**. The RADIUS Configurations (Add) window appears (Figure 12), displaying the following fields:
 - o Server IP Address: IP address of the RADIUS server you are adding.
 - o Authentication Port: UDP port for the authentication requests (default: 1812).
 - o Accounting Port: UDP port for the accounting requests (default: 1813).
Currently not used.
 - o Timeout (seconds): Time interval (in seconds) between consecutive retransmissions of the same request from the OmniAccess 3500 NLG gateway to the RADIUS server if the gateway receives no reply from the RADIUS server (default: 30).
 - o Shared Secret: Authentication key used for all RADIUS exchanges between the gateway and the RADIUS server. The key must match the authentication method set for the RADIUS daemon.
 - o Authentication Method: Authentication method supported by the RADIUS server. Available options: <CHAP> (challenge-based) and <PAP> (simple password).
2. Click **Save**.

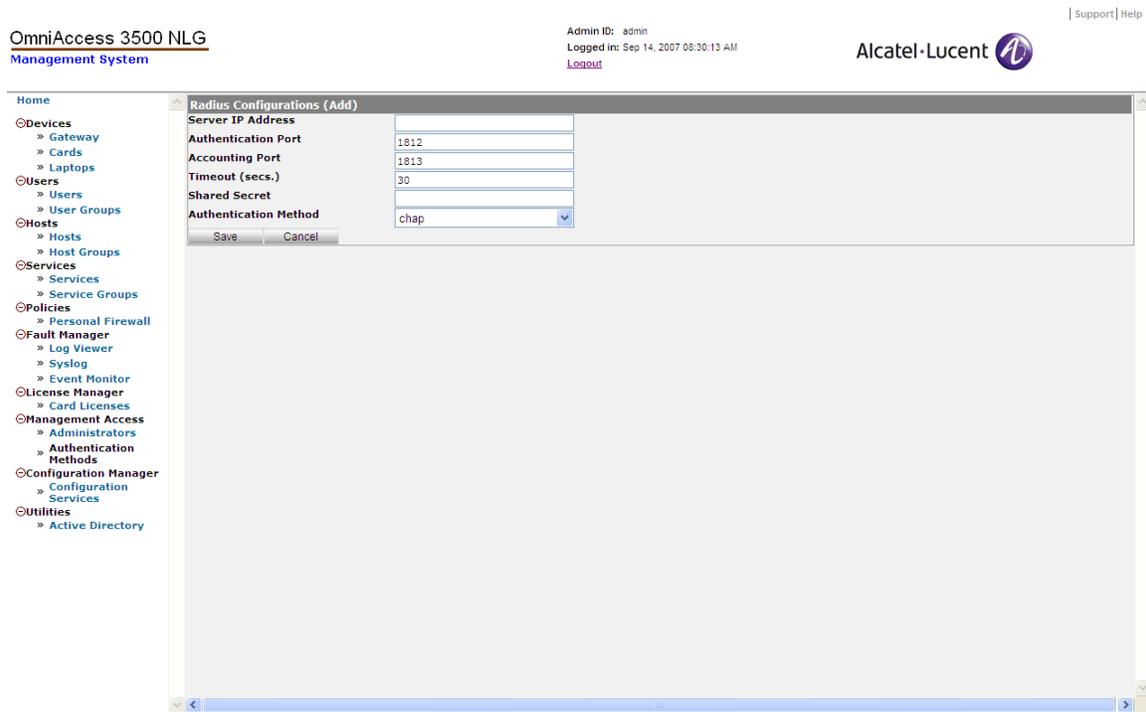


Figure 12 - Radius Configurations (Add)

Remote Access Provisioning

The infrastructural components needed to establish the remote access connections to the gateway, including the OmniAccess 3500 NLG licenses, are provisioned through the following sections of the management system GUI:

1. **Connection Manager—Settings:** Configuration of address pools, server addresses, packet classification rules, and tunnel profiles, needed by the OmniAccess 3500 NLG gateway to handle the remote requests for IPsec tunnel establishment. You can create new objects by clicking the **New** button and entering the required information, or you can view/remove existing objects by selecting an object and clicking the **Open/Delete** button. Please note that to modify any parameter of a Connection Manager object, you must first delete the object and then create a new one with the desired parameter values. See the following sections for more details.
2. **Gateway—File Upload:** Installation of the files needed by the gateway to participate in all secure transactions with its network peers (including the OmniAccess 3500 NLG cards).
3. **License Manager:** Installation of the service licenses that enable connectivity between the OmniAccess 3500 NLG cards and the gateway.

Connection Manager—Settings

The Connection Manager—Settings section of the management system GUI provides control over gateway objects that are needed for configuration of the remote access connections.

ADDRESS POOL

Address pools are sets of IP addresses from which the gateway draws the pair of VPN addresses that it assigns to the OmniAccess 3500 NLG card and associated laptop upon establishment of the IPsec tunnel. The addresses for the card and for the laptop are drawn from different, disjoint sets. Multiple sets can be assigned to the cards (Card sets) and to the laptops (Laptop sets).

To add an address pool:

1. Click **Gateway** on the main menu and then click **Configure Advanced Settings**.
2. On the Configure menu, click **Address Pool**.
3. Click **New**. An Connection Manager Address Pool (Add) window appears (Figure 13), displaying the following fields:
 - IP Address: The base IP address for the definition of the IP address range from which the OmniAccess 3500 NLG gateway draws the pair of VPN addresses.
 - Netmask (x.x.x.x): The netmask for the definition of the IP address range from which the OmniAccess 3500 NLG gateway draws the pair of VPN addresses. The Netmask value must be expressed as an IP address (e.g., <255.255.255.0>).
 - Type: The platform component that will receive the VPN addresses out of this address pool. Select <Card> or <Laptop> from the drop-down menu.
4. Click **Save**.

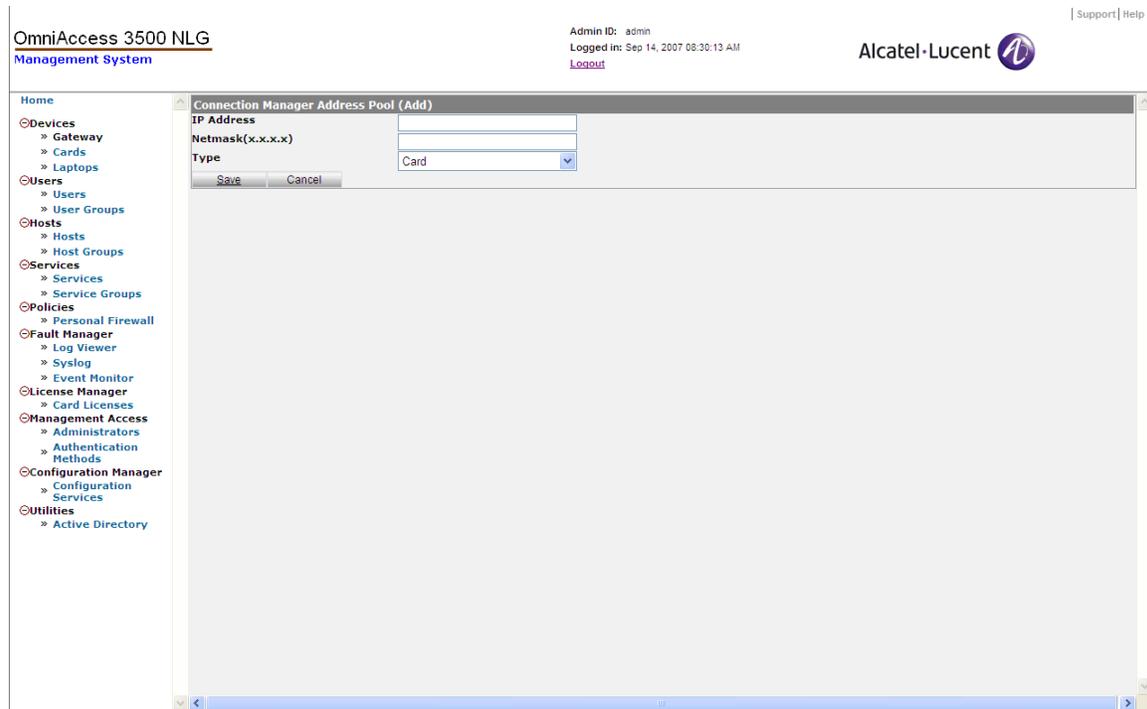


Figure 13 - Connection Manager Address Pool (Add)

SERVER TABLE

The Server Table allows the configuration of the DNS, WINS, and default-gateway addresses that the gateway passes to the card and laptop together with the VPN addresses. Only one address can be set for each type of server.

To add a server table entry:

1. Click **Gateway** on the main menu and then click **Configure Advanced Settings**.
2. On the Configure menu, click **Server Table**.
3. Click **New**. A Connection Manager Server Table (Add) window appears (Figure 14), displaying the following fields:
 - o **Type**: The type of server for which the address is being configured. Options (choose one): <DNS> (DNS server), <WINS> (WINS server), and <GUARD_PRIVATE_IP> (IP address of the LAN:1 virtual interface of the gateway).
 - o **Primary IP Address**: IP address of the first network server being configured.
 - o **Secondary IP Address**: IP address of the second network server being configured.
4. Click **Save**.

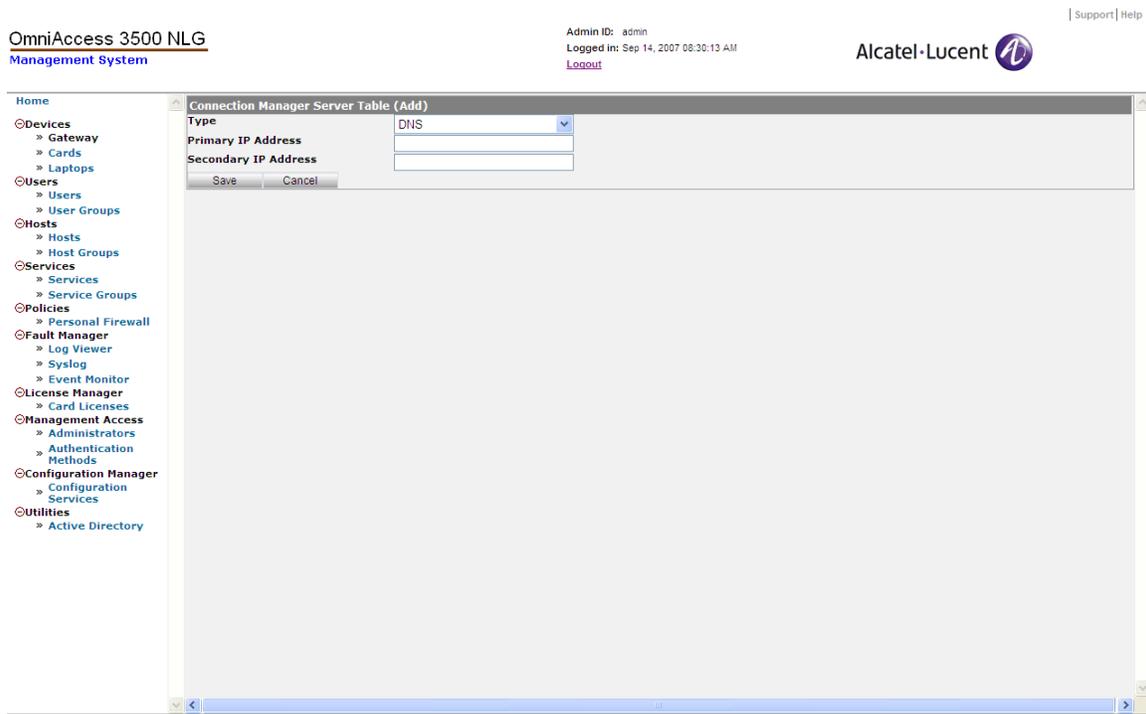


Figure 14 - Connection Manager Server Table (Add)

RULES

The entries of the Rule Information table define the packet classification behavior for the firewall and IPsec endpoint that are embedded in the OmniAccess 3500 NLG gateway.

The embedded firewall can be used to restrict the network traffic that the gateway exchanges over its interfaces, assuming the function of an enterprise firewall in a network where an enterprise firewall may not be already deployed. The firewall rules may or may not be associated with existing IPsec tunnels.

The embedded IPsec endpoint handles the requests to open IKEv2 and IPsec security associations that the OmniAccess 3500 NLG cards originate from their current locations. The gateway uses the IPsec endpoint rules to match incoming IKEv2 requests with sets of IKEv2/IPsec parameters (Tunnel Table entries) to be used in the configuration of the resulting security associations.

To add a packet classification rule:

1. Click **Gateway** on the main menu and then click **Configure Advanced Settings**.
2. On the Configure menu, click **Rules**.
3. Click **New**. A Connection Manager Rules (Add) window appears (Figure 15), displaying the following fields:
 - **Precedence:** Rule precedence with respect to other rules defined in the same context. The priority of the rule is higher with a higher precedence value.
 - **Type:** Rule type, to be chosen out of <Pass> (accept all packets matching the rule), <Drop> (drop all packets matching the rule), and <Reject> (drop all packets matching the rule and for each dropped packet notify the sender).
 - **Protocol:** Protocol Identifier value carried by the packets that match the rule. Options (choose one): <IP>, <TCP>, <UDP>, <ICMP>.
 - **Source IP/[Mask]:** Range of IP addresses to be checked against the source IP address field in the packet header.
 - **Source Port Low, Source Port High:** Range of port values to be checked against the source port field in the packet header.
 - **Destination IP/[Mask]:** Range of IP addresses to be checked against the destination IP address field in the packet header.
 - **Destination Port Low, Destination Port High:** Range of port values to be checked against the destination port field in the packet header.
 - **Interface Name:** Network interface on the OmniAccess 3500 NLG gateway where the packet filter rule applies. Options (choose one): <WAN> (for the WAN/public interface of the gateway), <LAN> (for the LAN/private interface of the gateway)).
 - **Local Stack Direction:** Packet direction with respect to the local IP stack of the OmniAccess 3500 NLG gateway. Options (choose one): <ANY> (the rule applies to traffic in any direction), <From> (the rule only applies to traffic from the local IP stack, i.e., outgoing traffic), <To> (the rule only applies to traffic to the local IP stack, i.e., incoming traffic).
 - **Tunnel Direction:** This object enables the association of the packet classification rule with a tunnel profile. Options (choose one): <None> (no tunnel is to be associated with the rule, which is therefore strictly a packet filtering rule), <To Tunnel> (packets matching the rule are dispatched through an IPsec tunnel whose profile is identified by the <To Tunnel> value; if an

existing IPsec tunnel is not found for a matching packet, it is created before the packet is delivered), <From Tunnel> (packets matching the rule are received from an IPsec tunnel whose profile is identified by the <From Tunnel> value; if a remote request to open an IPsec tunnel is received on a packet whose header matches the rule, the OmniAccess 3500 NLG gateway uses the tunnel profile specified in the <From Tunnel> value to conduct the subsequent negotiations).

- To Tunnel: Name of the tunnel profile for the IPsec tunnel that dispatches the matching packet.
- From Tunnel: Name of the tunnel profile for the IPsec tunnel over which the matching packet is received.

4. Click Save.

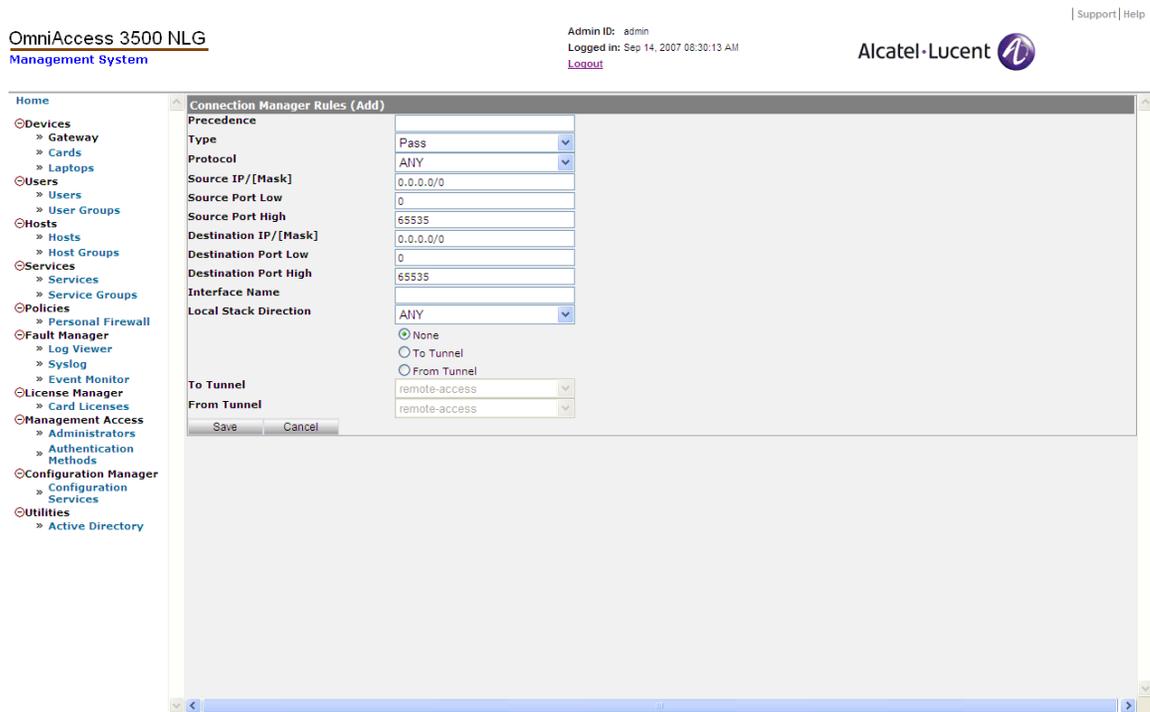


Figure 15 - Connection Manager Rules (Add)

TUNNEL TABLE

The Tunnel Table contains a list of tunnel profiles used to define the parameters of the IKE and IPsec Security Associations that are created either by the OmniAccess 3500 NLG gateway or by request of the OmniAccess 3500 NLG cards. More specifically, the configuration of the Tunnel Table entries drives the run-time selection of the hashing and encryption algorithms used for message authentication and content protection in the IKEv2 and IPsec exchanges.

To add a tunnel profile:

1. Click **Gateway** on the main menu and then click **Configure Advanced Settings**.
2. On the Configure menu, click **Tunnel Table**.

3. Click **New**. A Connection Manager Tunnel Table (Add) window appears (Figure 16), displaying the following fields:
 - **Name:** Name of the tunnel profile.
 - **Identity Type:** Type of identifier used to designate the local tunnel endpoint (residing on the OmniAccess 3500 NLG gateway) in the security association negotiations. Options (choose one): <EMAIL> (email address, as in <user@domain.ext>), <FQDN> (Fully Qualified Domain Name, as in <hostname.localdomain.ext>), <DN> (Distinguished Name, used for identification of an entry in an LDAP directory, as in <dn: cn=John Doe,dc=example,dc=com>, where <cn=John Doe> is the Relative Distinguished Name of the entry and <dc=example,dc=com> is the Distinguished Name of the parent entry).
 - **Identity:** Identity value for the local tunnel endpoint, specified in the format required by the <Identity Type> value.
 - **Algorithms to be used for IPsec Negotiations:** Encryption and hashing algorithm to be used in the IPsec tunnel. Options (choose one): <3DES-SHA1>, <AES128-SHA1>, <AES192-SHA1>, <AES256-SHA1> (3DES, AES128, AES192, and AES256 are the encryption algorithms available for selection; the hashing algorithm is SHA-1 in all cases).
 - **Algorithms to be used for IKE Negotiations:** Encryption and hashing algorithm to be used for protection of the IKEv2 exchanges. Options (choose one): <3DES-SHA1>, <AES128-SHA1>, <AES192-SHA1>, <AES256-SHA1> (3DES, AES128, AES192, and AES256 are the encryption algorithms available for selection; the hashing algorithm is SHA-1 in all cases).
 - **Lifetime of the IKE SA in seconds:** Maximum duration of the IKEv2 Security Association that controls the IPsec tunnel between the OmniAccess 3500 NLG card and the OmniAccess 3500 NLG gateway.
 - **Lifetime of the IPsec SA in seconds:** Maximum duration of the IPsec Security Association that carries encrypted packets from one end of the secure remote access connection to the other (i.e., maximum lifetime of a remote-access tunnel).
4. Click **Save**.

Note: As the OmniAccess 3500 NLG gateway is first installed, the Rules Table contains a default set of pre-defined rules. Within the set, the rules with precedence 78, 79, and 150 must be replicated for every new tunnel profile that is added to the Tunnel Table. When the first Tunnel Table entry is created, delete the current version of each rule and replace it with a new version that includes reference to the Tunnel Table entry in the To Tunnel or From Tunnel field. For subsequent replications of the rules, simply create new rules with identical structure as the existing ones, but with reference to the appropriate Tunnel Table entry.

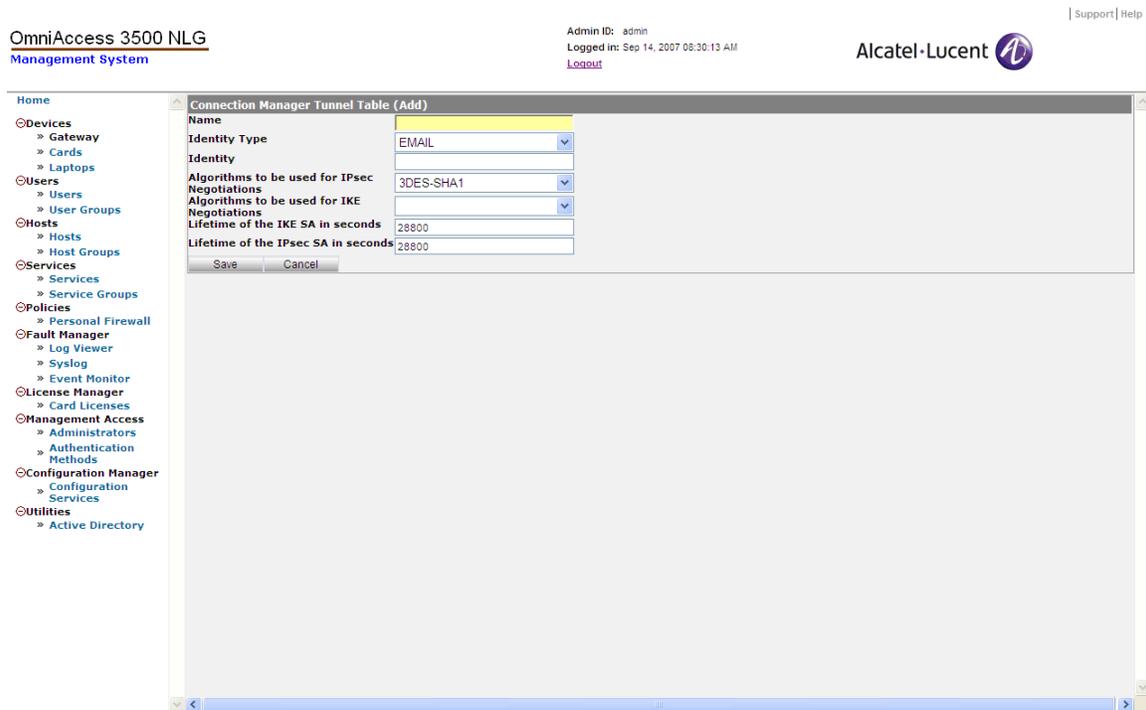


Figure 16 - Connection Manager Tunnel Table (Add)

To view/delete information for an address pool, a server table entry, a filter rule, or a tunnel table entry:

1. Click **Gateway** on the main menu and then click **Configure Advanced Settings**.
2. On the **Configure** menu, click **Address Pool**, **Server Table**, **Rule**, or **Tunnel Table**, depending on the type of information you want to view.
3. A **Gateway Configure** window opens, displaying your selection.
4. Click the checkbox next to an item to select it.
5. Click **Open** to view the object details and then **OK** when you want to return to the **Gateway Settings** window. Click **Delete** and then **OK** to remove the object and return to the **Gateway Settings** window.

File Upload

The following files must be installed in the gateway to enable its participation in secure transactions with other network nodes:

- **Keytab File:** File containing the credentials of the gateway for authentication with the Active Directory Server (ADS). The file must necessarily be uploaded to the gateway before any interaction with the Active Directory (AD) infrastructure can start. This includes the case where the method used for authentication of one or more user groups changes from RADIUS to AD.
- **CA Certificate:** Digital certificate of the Certificate Authority (CA), which includes the CA's public key and digital signature. The same CA certificate is installed in the OmniAccess 3500 NLG cards.

- CA Certificate Revocation List: List of certificates issued by the Certificate Authority that have been revoked before their natural expiration.
- Gateway Certificate: Certificate (public key) of the gateway, used by peer network nodes for encryption of the messages that they send to the gateway.
- Gateway Private Key: Secret key used by the gateway to decrypt the messages that it receives from peer network nodes (including the OmniAccess 3500 NLG cards).

To install the security files:

1. Click **Gateway** on the main menu.
2. Click **File Upload**. The Gateway Configuration File Upload window appears (Figure 17).
3. Browse through the file system of your computer to find the appropriate files to fill out each of the following fields: Keytab File, CA Certificate, CA Certificate Revocation List, Gateway Certificate, and Gateway Private Key.
4. Click **Upload Files**.

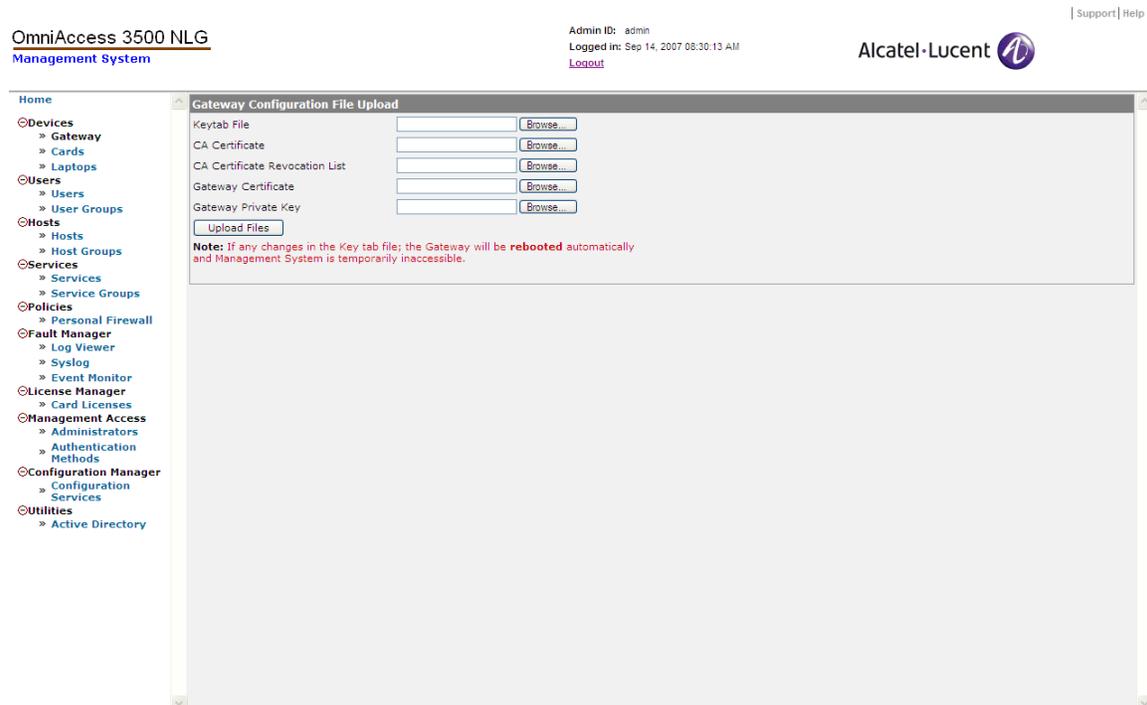


Figure 17 - Gateway Configuration File Upload

License Manager

Only cards that are covered by a valid OmniAccess 3500 NLG license issued by Alcatel-Lucent can establish the VPN tunnel to the gateway.

Every license is strictly associated with the service provider that offers broadband wireless access to the 3G subscriptions of the cards. The duration of a license can be 1 month, 3 months, 6 months, 1 year, 2 years, or unlimited. The number of end users in the license defines the maximum number of end users that can be provisioned in the

management system at any time. If necessary, a license can be issued for a single end user. The customer enterprise specifies all license parameters upon ordering the license file.

A sample license file looks like the following:

```
testlic
100
xyzwireless
01/01/2007
12/31/2007
mGyXdE0Fd8xBN0eeyVukrE1lu319baKyIu5OMfxIPWAJiRzp//U17g==
```

The meaning of each line in the file is as follows:

- The first line (`testlic` in the example) is the license identifier, unique for every license.
- The second line (`100` in the example) is the number of users.
- The third line (`xyzwireless` in the example) is the service provider for which this license is valid.
- The fourth line (`01/01/2007` in the example) indicates the start date for the license in mm/dd/yyyy format.
- The fifth line (`12/31/2007` in the example) indicates the end date for the license in mm/dd/yyyy format.
- The sixth and last line (`mGyXdE0Fd8xBN0eeyVukrE1lu319baKyIu5OMfxIPWAJiRzp//U17g==` in the example) is a digital signature of the first five license lines and of the Gateway Certificate ID that is set with the procedure described in the *Initial Configuration of Gateway Parameters* section above (the installation of the actual certificate is described in the *File Upload* section, also above).

The License Manager section of the management system GUI allows you to view/create/renew/delete your card licenses.

To add a license:

1. Click **Card Licenses** on the main menu.
2. On the Card Licenses window, click **New**. The Card License Upload window appears (Figure 18), displaying the following field:
 - License File: Browse through your computer's file system to find the license file previously obtained from Alcatel-Lucent and assign it to this text box.
3. Click **Upload License**. If this license is valid, a new entry will appear on the Card Licenses window.

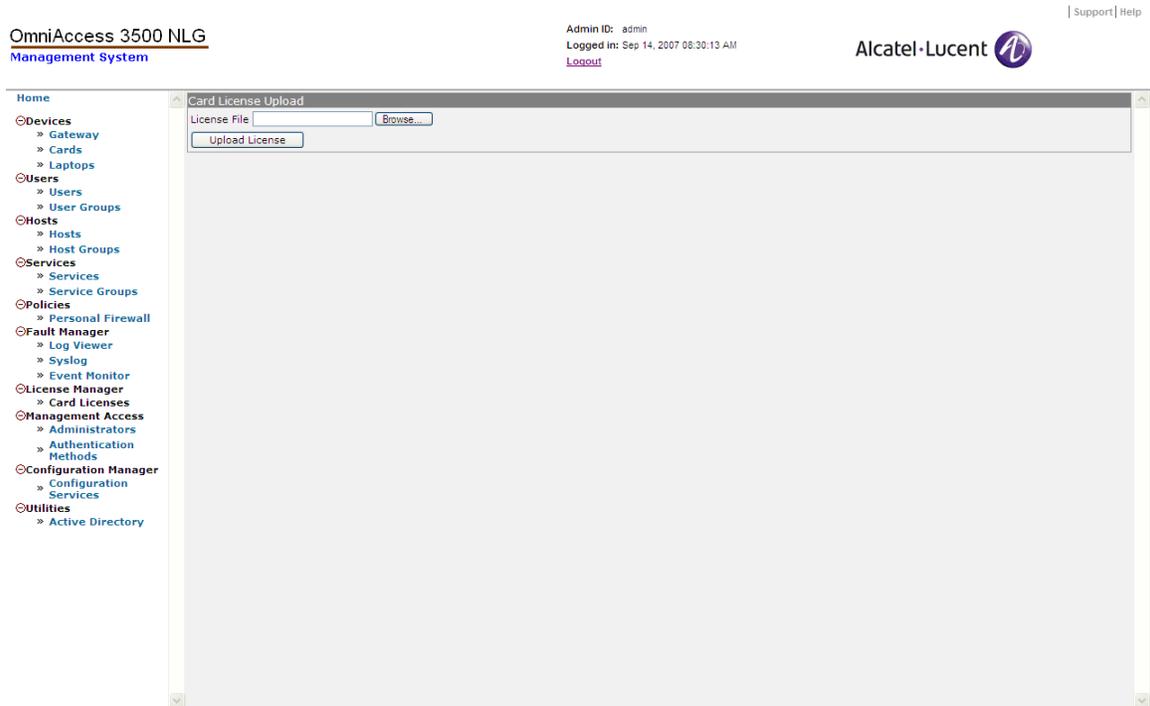


Figure 18 - Card License Upload

To view detailed information for all your licenses:

1. On the main menu, click Card Licenses. The Card Licenses window appears (Figure 19), displaying the following fields for each entry:
 - Name: Unique name that identifies the license.
 - Service Provider: Service provider for which this license is valid.
 - Max. Licenses: Maximum number of users served by this license that can be provisioned in the management system at any given time.
 - Available: Number of users that can still be provisioned with this license.
 - Start Date: Start date for this license in mm/dd/yyyy format.
 - End Date: End date for this license in mm/dd/yyyy format

OmniAccess 3500 NLG Management System

Admin ID: admin
 Logged in: Sep 14, 2007 08:30:13 AM
[Logout](#)

Alcatel-Lucent

Home

- Devices
 - Gateway
 - Cards
 - Laptops
- Users
 - User Groups
- Hosts
 - Hosts
 - Host Groups
- Services
 - Services
 - Service Groups
- Policies
 - Personal Firewall
- Fault Manager
 - Log Viewer
 - Syslog
 - Event Monitor
- License Manager
 - Card Licenses
- Management Access
 - Administrators
 - Authentication Methods
- Configuration Manager
 - Configuration Services
- Utilities
 - Active Directory

Card Licenses

<input type="checkbox"/>	Name	Service Provider	Max. Licenses	Available	Start Date	End Date
<input type="checkbox"/>	testlic-sprint	sprint	100	100	01/01/2007	12/31/2007
<input type="checkbox"/>	testlic	verizon	100	99	01/01/2007	12/31/2007

Figure 19 - Card Licenses

The same information can be displayed for a single license by clicking the checkbox next to the license name and then clicking **Open** (Figure 20).

OmniAccess 3500 NLG Management System

Admin ID: admin
 Logged in: Sep 14, 2007 08:30:13 AM
[Logout](#)

Alcatel-Lucent

Home

- Devices
 - Gateway
 - Cards
 - Laptops
- Users
 - User Groups
- Hosts
 - Hosts
 - Host Groups
- Services
 - Services
 - Service Groups
- Policies
 - Personal Firewall
- Fault Manager
 - Log Viewer
 - Syslog
 - Event Monitor
- License Manager
 - Card Licenses
- Management Access
 - Administrators
 - Authentication Methods
- Configuration Manager
 - Configuration Services
- Utilities
 - Active Directory

Card License Information

Name	: testlic
Maximum Licenses	: 100
Available Licenses	: 99
Service Provider	: verizon
Start Date	: 01/01/2007
End Date	: 12/31/2007

OK

Figure 20 - Card License Information

To renew a license:

1. On the Card Licenses window, click **Renew**.
2. The Card License Upload window appears.
3. Follow the same procedure described above for adding a new license in order to replace the old license file with a new one.

End User Provisioning

This section explains how to provision OmniAccess 3500 NLG cards and associated laptops and users.

The following tasks must be completed on the management system GUI before starting deployment of the OmniAccess3500 NLG cards:

1. Configure a user group.
2. Associate the user group with a personal firewall policy.

The following tasks must be completed on the management system GUI before deploying a new card:

1. Add a new user.
2. Place the new user into an existing user group.
3. Create a user license for the card.

Warning: To prevent the end user from arbitrarily removing the OmniAccess 3500 NLG client software from the laptop without losing the data it contains, the administrator must ensure that no Windows System Restore point exists in the laptop when the client software is installed.

Users and User Groups

Users can be administered either individually, or can be assigned to a user group and have administrative functions assigned to the group as a whole.

To manually add a user to the system:

1. Click **Users** on the main menu.
2. From the User Information menu, click **New**. The User Information (Add) window appears (Figure 21), displaying the following fields:
 - o **Login:** The login name of the user (e.g., jdoe).
 - o **Domain:** The Windows domain name for the user. If the enterprise uses a RADIUS-based method instead of an Active Directory infrastructure to authenticate the end users for network access, the Domain field should be filled with the Laptop ID as set up in the laptop configuration.
 - o **Full Name:** The real name of the user (e.g., John Doe).
 - o **Base Unlock Password:** Base password used to generate the One-Time Password (OTP). Do not use special characters (such as #, @, &) in this field.

- Connectivity Timeout (sec): Total laptop power-on time during which the laptop is allowed to work without VPN tunnel to the OmniAccess 3500 NLG gateway. The corresponding timer is reset every time the IPsec tunnel to the gateway is established while the laptop is powered on. A warning pops up on the laptop's screen five minutes before expiration of the connectivity timeout. If the timeout expires, the laptop locks and can only be unlocked with an OTP received from the IT helpdesk.
 - OTP Valid Time (sec): Amount of time that the laptop will remain unlocked after the one-time password has been successfully entered. After this time interval expires, all tamper checks are enabled again.
 - Card ID: The Electronic Serial Number (ESN) of the card assigned to this user. One card only can be assigned to a given user.
 - Laptop ID: The laptop assigned to this user. One laptop only can be assigned to a given user.
 - User Group: The user group to which the user belongs. A given user can belong to only one user group.
 - Certificate ID: The identifier of the Digital Certificate that is used in the activation of the card. The identifier must be expressed in the format: <CN=value>, where *CN* stands for *common name* and *value* is the common name of the certificate (available in the *Subject* field of the certificate). *Please note that this parameter is case-sensitive.*
 - License ID: Select a license name from the pull-down menu. The user can connect to the enterprise between the start and end dates specified in the license you have selected.
3. Click **Save**.

The screenshot displays the 'User Information (Add)' window in the OmniAccess 3500 NLG Management System. The window title is 'User Information (Add)'. The form contains the following fields:

- Login:
- Domain:
- Full Name:
- Base Unlock Password:
- Connectivity Timeout(sec):
- OTP Valid Time(sec):
- Card ID:
- Laptop ID:
- User Group:
- Certificate ID:
- License ID:

At the bottom of the form are 'Save' and 'Cancel' buttons. The left sidebar shows a navigation tree with categories like Devices, Users, Hosts, Services, Policies, Fault Manager, License Manager, Management Access, Configuration Manager, and Utilities. The top right corner shows 'Admin ID: admin', 'Logged in: Sep 14, 2007 08:30:13 AM', and a 'Logout' link. The Alcatel-Lucent logo is also present.

Figure 21 - User Information (Add)

Once you have added users, you can add them to user groups. You can have as many user groups as you like. A given user can belong to only one user group.

To manually add a user group:

1. First you must add users to the system. Follow the instructions above to add a user.
2. Next, add the users to a user group. From the User Groups Information menu, click **New**. The User Group Information (Add) window appears (Figure 22), displaying the following fields:
 - Name: Type in a name for the new user group.
 - Description: An optional field into which you can type any additional information.
 - Radio Timeout (sec): A switch on the OmniAccess 3500 NLG card turns the 3G modem on and off. The radio timeout field indicates how long the switch can remain in the off position with the laptop powered on before the Windows Lock screen appears on the laptop's monitor. The lock screen can be unlocked using the Windows Logon credentials, but only as long as the Connectivity Timeout does not expire.
 - Policy: The Personal Firewall Policy that is installed in all the OmniAccess 3500 NLG cards of this user group.
3. Click **Save**.

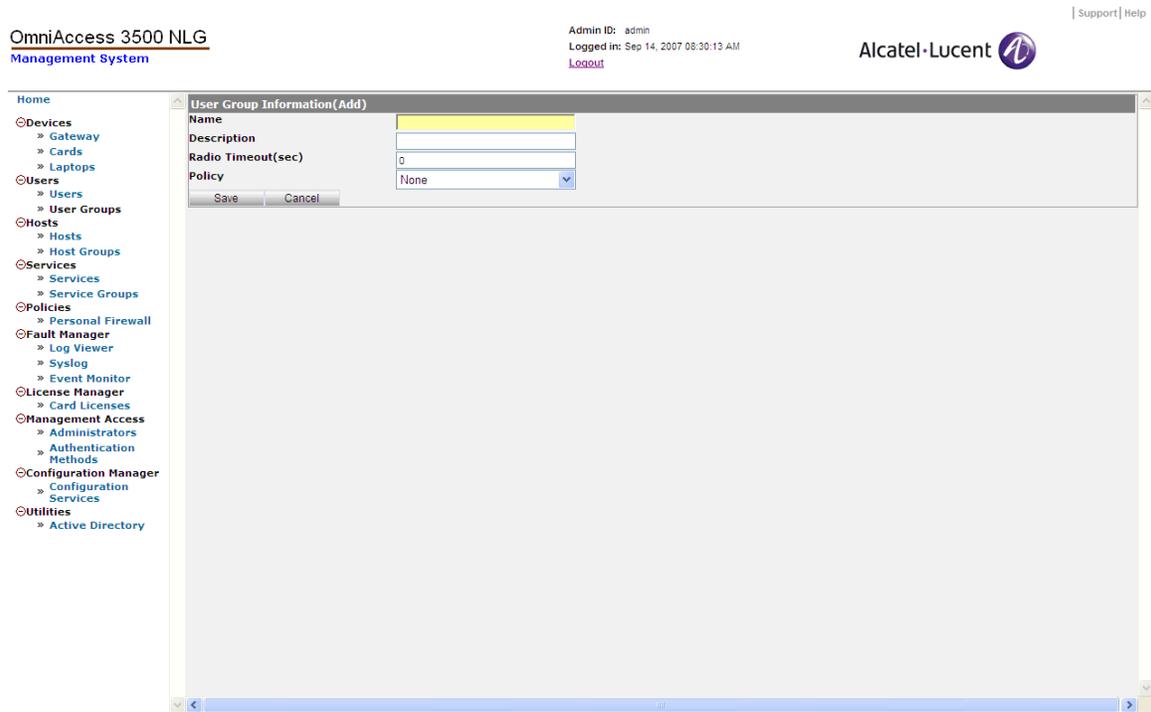


Figure 22 - User Group Information (Add)

You can modify the list of users for a group by editing user groups. The same fields whose initialization is described above can be modified for an existing user group.

You can also import user and user group information automatically from your Active Directory Server (ADS), which is particularly useful when the number of OmniAccess 3500 NLG users to add or re-configure is large.

To configure a new automatic ADS import profile for a user group:

1. Click **Active Directory** on the main menu and then click **New** in the Active Directory - Server Configuration window. The Active Directory Import User Information window appears (Figure 23).

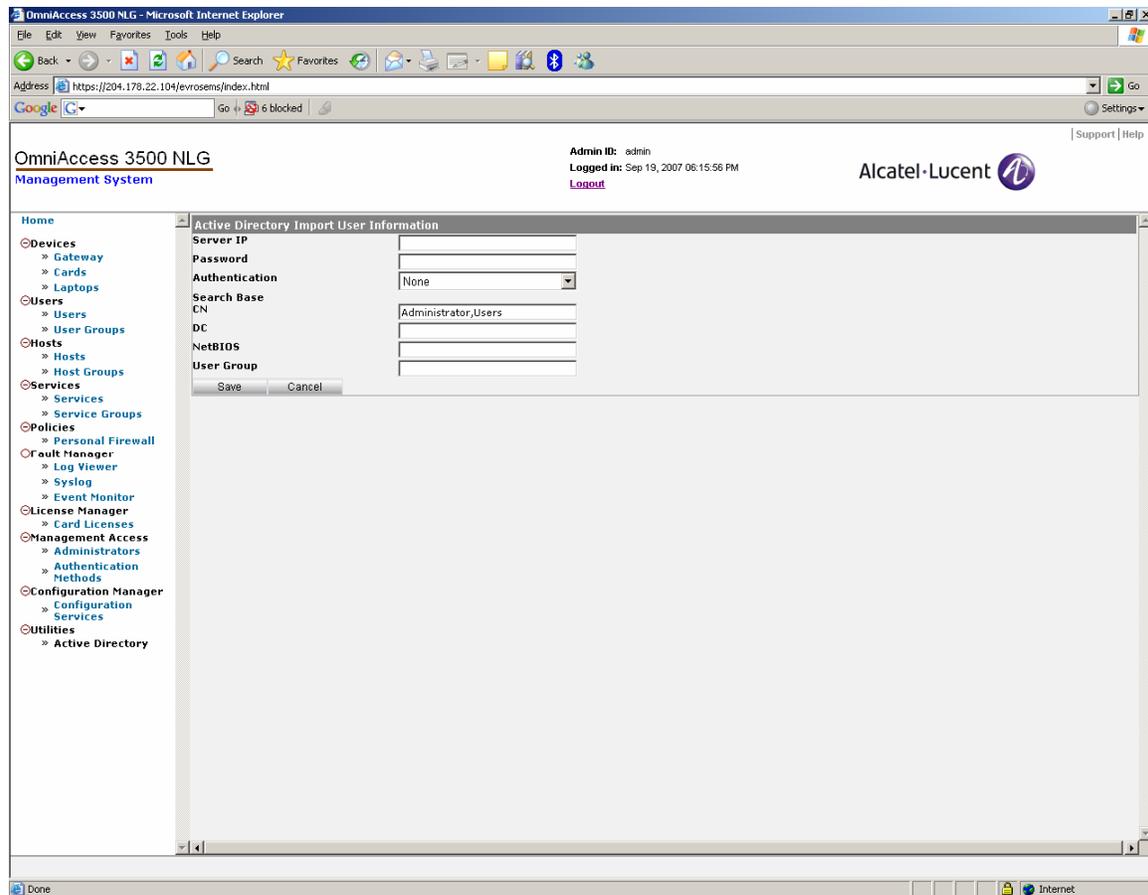


Figure 23 - Active Directory Import User Information

2. Enter the necessary information for the following fields:
 - Server IP: IP address of the ADS to be used as the source of the user record.
 - Password: Password needed for access to the ADS.
 - Authentication: Type of authentication required for access by the ADS. The <Simple> option is typical for Active Directory.
 - Search Base CN: Common name; for example, Administrator, Users.
 - DC: Domain name (e.g., evros.example.com).
 - NetBIOS: The NetBIOS name corresponding to the Domain name (e.g., "evros" in the domain name evros.example.com).
 - User Group: Name of the user group to be imported from the ADS.
3. Click **Save**.

To import user records based on a pre-configured automatic import profile:

1. Click **Active Directory** on the main menu, select the checkbox next to a server configuration entry in the Active Directory - Server Configuration window, and then click **Import**.

2. The management system connects to the ADS, retrieving data for the target user group.
3. Click **OK** on the Active Directory User Import window.

If an automatic import profile includes users that are already present in the management system database, the execution of the automatic import transaction based on that profile does not modify the records of those users. When completed, the transaction shows a **Status: Failed!** message with a list of the users whose records could not be imported because they already exist in the management system database. If you wish to automatically update a user record that already exists in the management system database, you must first delete the old record and then invoke the automatic import procedure with a profile that includes the target user.

OmniAccess 3500 NLG Cards

Once users are configured, you can provision OmniAccess 3500 NLG card information. This must be done before connecting a card to the OmniAccess 3500 NLG gateway; otherwise, the card will not be recognized by the system and will be denied access to the enterprise network.

You can perform the following administrative functions for the cards:

- View card information.
- Add a card to the system.
- Edit card information.
- Delete a card.
- Update and review the status of a card.

To add an OmniAccess 3500 NLG card to the system:

1. To access this function, click **Cards** on the main menu.
2. On the Card Information menu, click **New**. The Card (Add) window appears (Figure 24), displaying the following fields:
 - Card ID (ESN #): The Electronic Serial Number (ESN) of the card.
 - Service Provider: The company that is providing 3G wireless service to the card.
 - Description: An optional field in which you can type any additional information.
 - Phone # (MSID): The 10-digit telephone number associated with the OmniAccess 3500 NLG card, assigned by the service provider.
3. Click **Save**.
4. Repeat this procedure for each card that you want to connect to the OmniAccess 3500 NLG gateway.

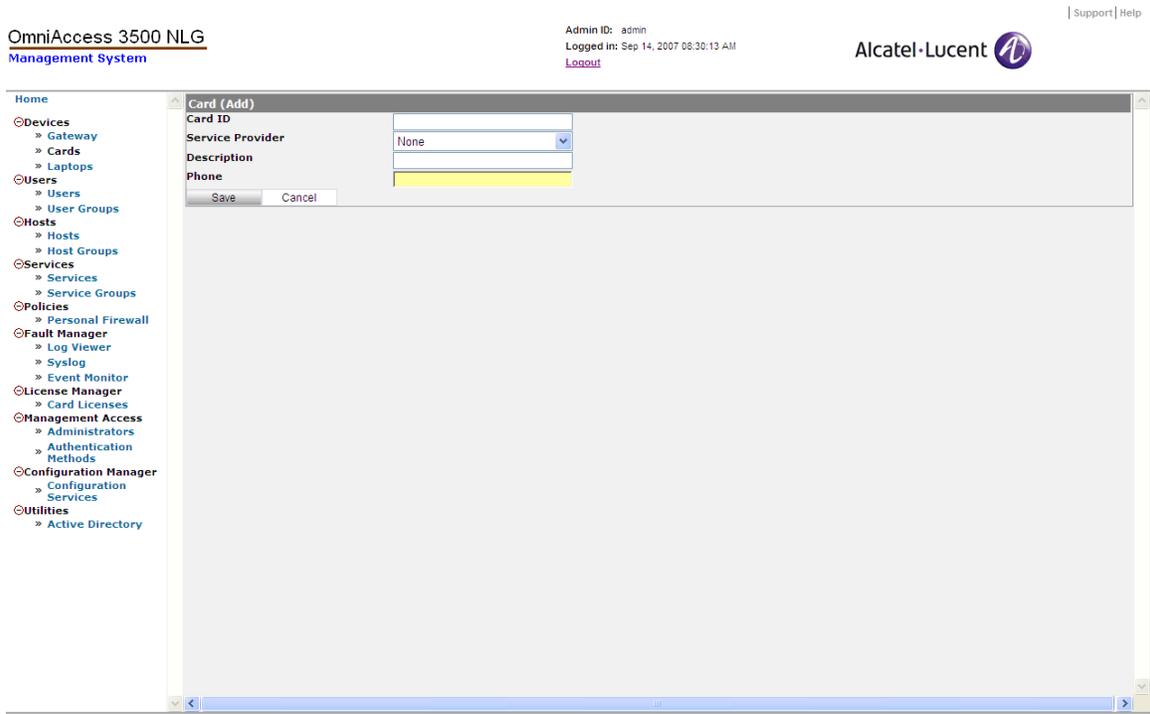


Figure 24 - Card (Add)

To view information for all cards:

- After you click **Cards** on the left-hand side of the main menu, the Card Information window appears (Figure 25). This window shows a list of cards in the OmniAccess 3500 NLG system.

OmniAccess 3500 NLG Management System

Admin ID: admin
 Logged in: Sep 14, 2007 08:30:13 AM
[Logout](#)

Alcatel-Lucent

Home

- ⊖ Devices
 - Gateway
 - Cards
 - Laptops
- ⊖ Users
 - Users
 - User Groups
- ⊖ Hosts
 - Hosts
 - Host Groups
- ⊖ Services
 - Services
 - Service Groups
- ⊖ Policies
 - Personal Firewall
- ⊖ Fault Manager
 - Log Viewer
 - Syslog
 - Event Monitor
- ⊖ License Manager
 - Card Licenses
- ⊖ Management Access
 - Administrators
 - Authentication Methods
- ⊖ Configuration Manager
 - Configuration Services
- ⊖ Utilities
 - Active Directory

Card Information

Card ID	Phone	Description
<input type="checkbox"/> 603C6364	2028703532	3G card in remote setup 2

Figure 25 - Card Information

To view the status of an OmniAccess 3500 NLG card:

1. From the Card Information menu, click the checkbox next to a card to select it.
2. Click **Status**. The Card Status window appears (Figure 26), displaying the following fields:
 - Card ID: The ESN (Electronic Serial Number) of the card. ESN is a unique identification number for the card provided by the manufacturer.
 - VPN IP Address: The VPN IP Address assigned to the card when the tunnel is established.
 - VPN Status: Current status of the IPsec tunnel between the OmniAccess 3500 NLG card and its target OmniAccess 3500 NLG gateway.
 - Last Connection Status: Indicates whether the card is plugged into the laptop or not. Possible values are <Card Inside Laptop> and <Card Outside Laptop>.
 - Modem Activation Time: The time when the card was activated with the Service Provider.
 - Last Connection Time: The last time the card connected to the OmniAccess 3500 NLG gateway.
3. Click **OK**.

OmniAccess 3500 NLG Management System

Admin ID: admin
 Logged in: Sep 14, 2007 08:30:13 AM
[Logout](#)

Alcatel-Lucent

Home

- Devices
 - Gateway
 - Cards
 - Laptops
- Users
 - Users
 - User Groups
- Hosts
 - Hosts
 - Host Groups
- Services
 - Services
 - Service Groups
- Policies
 - Personal Firewall
- Fault Manager
 - Log Viewer
 - Syslog
 - Event Monitor
- License Manager
 - Card Licenses
- Management Access
 - Administrators
 - Authentication Methods
- Configuration Manager
 - Configuration
 - Services
- Utilities
 - Active Directory

Card (Status)

Card Status Information

Card ID	: 603C6364
VPN IP Address	: 10.3.0.11
VPN Status	: CARD_UP
Last Connection Status	: CARD_INSIDE_LAPTOP
Modem Activation Time	:
Last Connection Time	: Fri Sep 14 08:02:40 2007

Note: The status information displayed on this page is the last known status. To get the current status please refresh this screen after about a minute. If you have already refreshed once then please ignore this message.

OK

Figure 26 - Card (Status)

Laptops

This section of the management system GUI allows you to view information for and configure laptops. Click **Laptops** on the main menu to access this function.

You can perform the following administrative functions for laptops:

- Add a laptop.
- Edit laptop information.
- Delete a laptop.

To add a laptop:

1. On the Active Laptop Information menu, click **New**. The Laptop (Add) window appears (Figure 27), displaying the following fields:
 - Laptop ID: A unique name for the laptop.
 - Description: An optional field in which you can type any additional information.
2. Click **Save**.

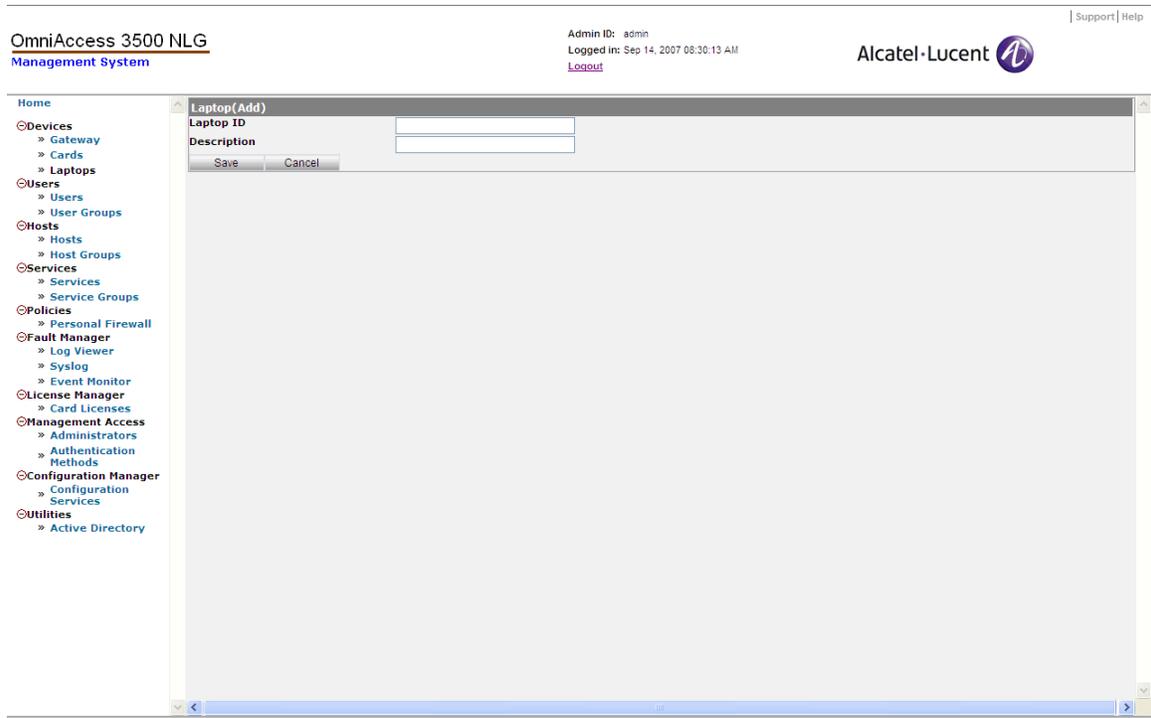


Figure 27 - Laptop (Add)

Application Provisioning

To support certain IT applications at runtime, you must first provision the infrastructure that supports them. This section describes the provisioning tasks that prepare the OmniAccess 3500 NLG platform for support of the following IT applications:

- Device management applications, such as asset inventory maintenance and patch management.
- Security applications, such as management of the personal firewall that is installed in the OmniAccess 3500 NLG card.

Device Management Applications

The OmniAccess 3500 NLG R1.2 supports a proprietary application (called ASSETMGMT) for maintaining inventories of the software assets in the deployed laptops, and two third-party solutions for the management of patch downloads (PatchLink Update by Lumension Security and SMS by Microsoft).

The Assisted File Transfer (AFT) facility of the OmniAccess 3500 NLG platform provides the foundation for integration of the ASSETMGMT and Microsoft SMS applications. The first subsection that follows describes the AFT facility, its support for the ASSETMGMT and Microsoft SMS applications, and the configuration steps needed to integrate other IT applications. The second subsection that follows references the document that describes all the configuration steps needed for integration of the OmniAccess 3500 NLG R1.2 with the PatchLink Update and SMS applications, including the steps that are external to the OmniAccess 3500 NLG platform.

ASSISTED FILE TRANSFER

The Assisted File Transfer facility allows you to synchronize the contents of laptop and enterprise folders via the OmniAccess 3500 NLG card, staging information in the card when either the laptop or the OmniAccess 3500 NLG gateway is not reachable. This feature is configured per application; that is, you specify for each application the enterprise folder and the laptop folder that need to be kept in sync. The enterprise folder is a Windows share that is available for export and is mounted from the respective application server into the file system of the OmniAccess 3500 NLG gateway. The direction of the synchronization — from the enterprise to the laptop, or vice versa — is a mandatory configuration parameter. When the direction is from the enterprise to the laptop, the enterprise folder is replicated to the specified OmniAccess 3500 NLG laptop folder. When the direction is from the laptop to the enterprise, the files in the laptop folder are copied into the enterprise folder. It is also possible to bind application table entries with user groups, so that for every application the directory synchronization only applies to the laptops of the associated user groups. The default group called BROADCAST corresponds to all users.

To configure an application for use of the AFT facility, you must create a new entry in the Application Table associated with the AFT and set all necessary parameters. There is one pre-configured application in the Application Table, called ASSETMGMT (Figure 28). ASSETMGMT is the OmniAccess 3500 NLG internal application that periodically transfers laptop asset information from the laptop to the gateway over the AFT facility. You can view status information for a given laptop asset (out of the following list: Programs, Services, Processes, Partitions, System Information, Operating System, Personal Firewall, TrueCrypt Encrypted Volume) by clicking the asset name on the User Configurations window (to access the User Configurations window click **Users** on the main menu, click the checkbox next to the desired user, and finally click **Configure**).

OmniAccess 3500 NLG Management System

Admin ID: admin
Logged in: Sep 14, 2007 08:30:13 AM
[Logout](#)

Alcatel-Lucent

Home

- ⊖ Devices
 - Gateway
 - Cards
 - Laptops
- ⊖ Users
 - User Groups
- ⊖ Hosts
 - Hosts
 - Host Groups
- ⊖ Services
 - Service Groups
- ⊖ Policies
 - Personal Firewall
- ⊖ Fault Manager
 - Log Viewer
 - Syslog
- ⊖ Event Monitor
- ⊖ License Manager
 - Card Licenses
- ⊖ Management Access
 - Administrators
 - Authentication Methods
- ⊖ Configuration Manager
 - Configuration Services
- ⊖ Utilities
 - Active Directory

Gateway-> Application Table Information

Application Name	Shared Path	User Name	Domain Name	Laptop Directory	Laptop Directory Owner	Direction	Max Disk Space
<input type="checkbox"/> ASSETMGMT		root		assetinfo		Laptop_To_Enterprise	0

OK

Figure 28 - Application Table Information

To add an entry to the application table for the AFT facility:

1. Click **Gateway** on the main menu and then click **Configure Advanced Settings**.
2. On the Configure menu, under Assisted File Transfer, click **Application Table**. The Application Table Information window (Figure 28) appears, displaying the following fields:
 - Application Name: Name of the application that will be configured to use the Assisted File Transfer facility (e.g., <testapp>).
 - Shared Path: Windows share to be mounted on the gateway file system (e.g., <///server1/testappdir>, where <server1> is the IP address or hostname of the application server and <testappdir> is the path of the directory to be synchronized).
 - User Name: User name with permission to mount the share.
 - Domain Name: Domain of the server that hosts the share.
 - Laptop Directory: Folder on the laptop that will be created for the application (if it does not exist already).
 - Laptop Directory Owner: The domain account to which the ownership of files in this laptop folder is assigned.
 - Direction: Replication direction (choose between <Laptop_To_Enterprise> and <Enterprise_To_Laptop>).
 - Max Disk Size (MB): Maximum storage space (in MB) allocated for the application (on the laptop, card, and gateway).

- User Groups: Sets of users that participate in the Assisted File Transfer transactions for the application being configured.

3. Click Save.

Note: If you use the Mozilla Firefox browser to access the management system GUI and the browser is configured to remember the passwords that you enter on the management system GUI windows, a pop-up window will appear when you click the Save button, asking whether or not you want to change one of the passwords that the browser had previously saved. Either answer will not compromise the configuration of the application table entry. However, to avoid the inconvenience of dealing with the pop-up window, it is recommended to configure the browser so that it does not remember any password at the URL of the management system GUI.

INTEGRATION OF PATCHLINK UPDATE AND MICROSOFT SMS

For all information needed to configure the integration of the PatchLink Update and SMS applications with the OmniAccess 3500 NLG R1.2, please refer to the following document: *OmniAccess 3500 NLG Release 1.2 Application Note: Integration of PatchLink Update and Microsoft SMS.*

Personal Firewall

The Policies section of the management system GUI allows the configuration of the personal firewall policies that are installed in the OmniAccess 3500 NLG cards. A personal firewall policy regulates the network activity of the end user. The personal firewall policy has scope exclusively over the network traffic exchanged by the OmniAccess 3500 laptop and not over the traffic that terminates at the card.

The same personal firewall policy is installed in the OmniAccess 3500 NLG cards of all users in the same user group. Each user group is bound to a single personal firewall policy. Whenever the policy changes, the same modification applies to the personal firewalls of all users in the group.

A personal firewall policy consists of packet filter rules and application filter rules.

- A packet filter rule defines the treatment of individual packets that traverse the personal firewall in the OmniAccess 3500 NLG card. The following steps must be completed prior to the configuration of a packet filter rule:
 1. Define its services (TCP/UDP port numbers) and assign them to a service group (aggregation of multiple TCP/UDP port numbers).
 2. Define its hosts (sets of contiguous IP addresses) and assign them to a host group (aggregation of multiple IP address ranges).
- An application filter rule decides on the opening of laptop-terminated connections for the target application whenever the application requests such an opening.

To begin configuring a personal firewall policy, first create the necessary service instances. A service is where the binding between TCP/UDP port numbers and service/application names is defined.

1. Click Services on the main menu.
2. On the Services Information menu, click New. The Service Information (Add) window appears (Figure 29), displaying the following fields:

- o Name: Type a name for the service you want to add.
 - o Port: The port number of the service.
3. Click Save.

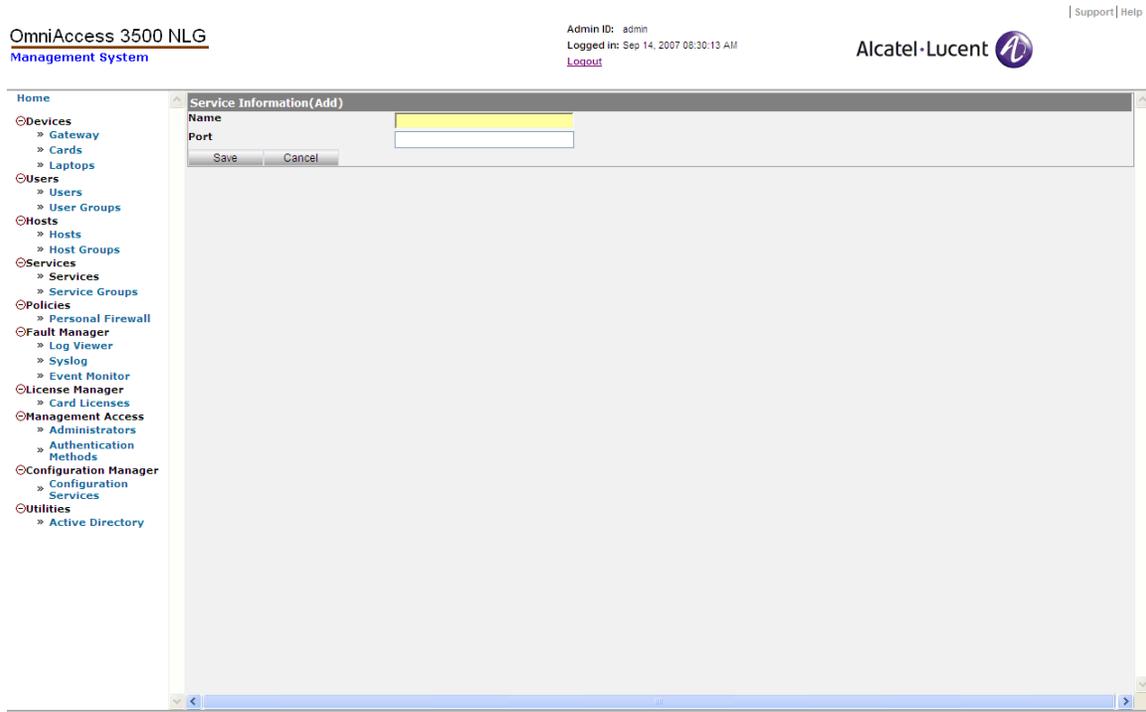


Figure 29 - Service Information (Add)

Next, create a service group, which is simply a group of previously defined services.

4. Click **Service Groups** on the main menu.
5. On the Service Group Information menu, click **New**. The Service Group Information (Add) window appears (Figure 30), displaying the following fields:
- o Group ID: Type a numeric user ID representing the service group you want to add.
 - o Name: Type the name of the service group you want to add.
 - o Services: Click on a user ID in the Available list and move it to the Selected list by clicking the appropriate arrow key. This adds services to the new service group.
6. Click Save.

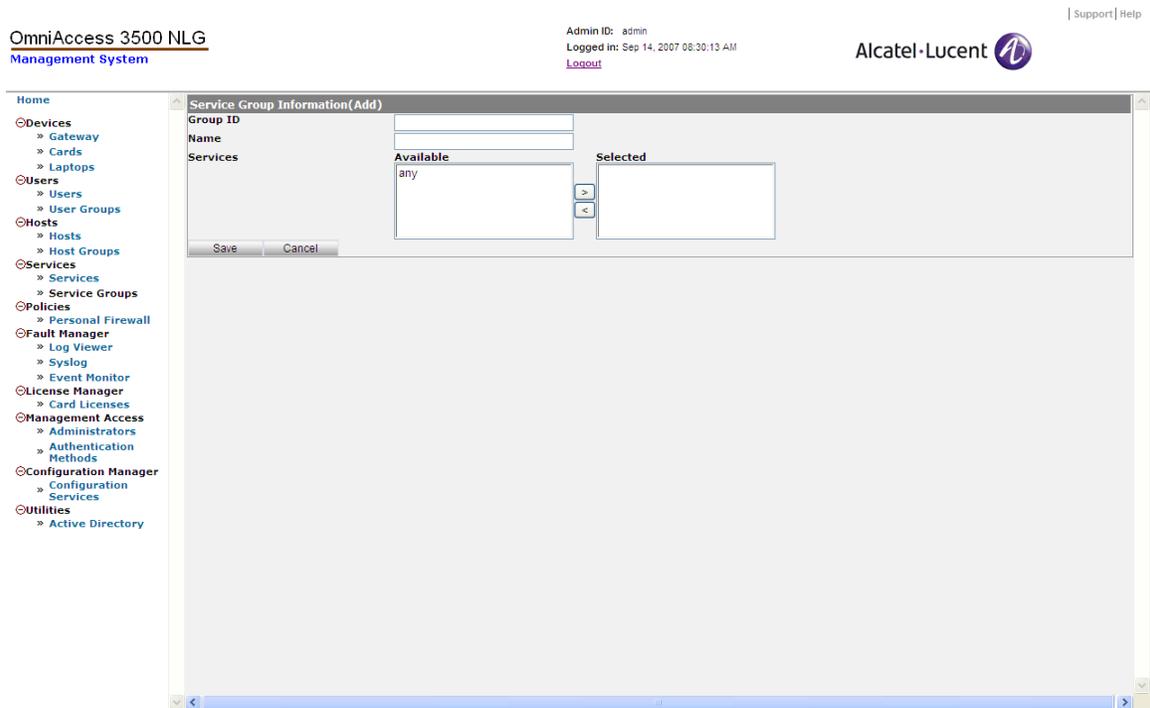


Figure 30 - Service Group Information (Add)

Now create a host object. The host object designates a set of IP addresses that will later be included in a host group and thereby in a packet filter rule.

7. Click **Hosts** on the main menu.
8. On the Host menu, click **New**. The Host (Add) window appears (Figure 31), displaying the following fields:
 - Host Name: A name that uniquely identifies the host.
 - Description: Type in any descriptive text about the new host.
 - Host: A valid IP address in the target IP address range.
 - Mask (1-32): The network mask used for identification of the entire range (the integer expresses the number of right-most bits to be set at 0 in the network mask address).
9. Click **Save**.

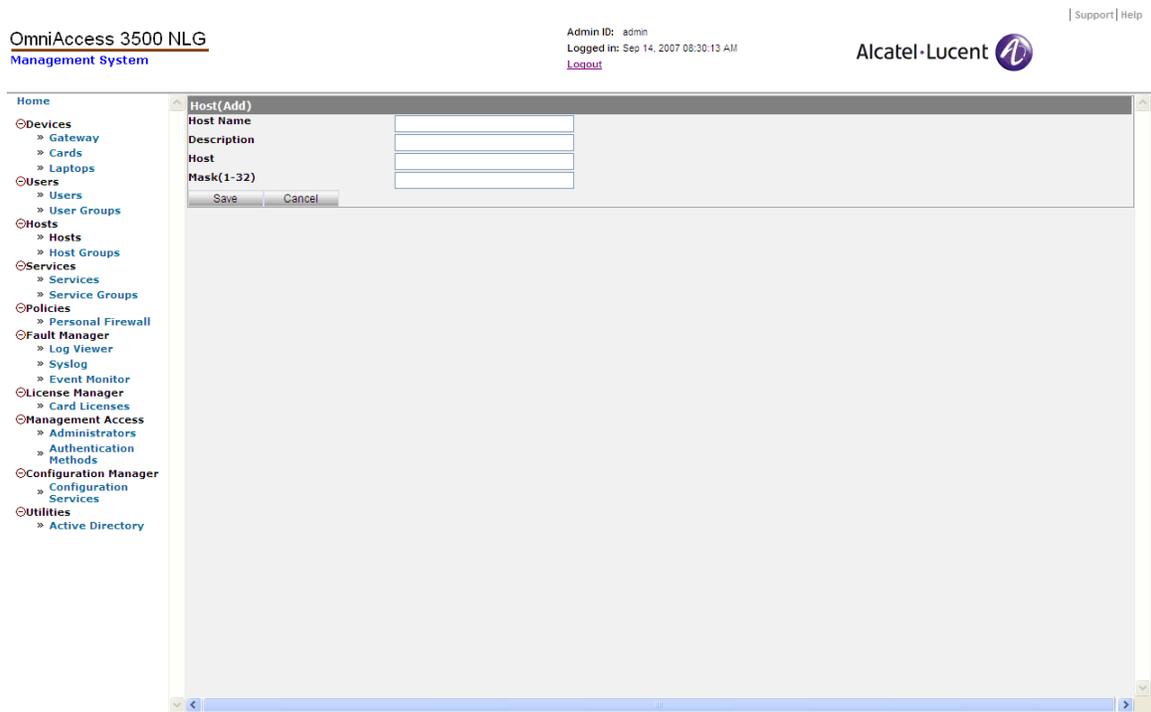


Figure 31 - Host (Add)

Now create a host group. A host group contains a list of IP address ranges that are currently configured for inclusion in packet filtering rules for personal firewall policies.

10. Click **Host Groups** on the main menu.
11. On the Host Groups menu, click **New**. The Host Group (Add) window appears (Figure 32), displaying the following fields:
 - Host Group Name: A number that uniquely identifies the host group.
 - Description: Type in any descriptive text about the new host group.
 - Hosts: Click on a host name in the Available Hosts list and move it to the Selected Hosts list by clicking the appropriate arrow key. This adds the host to the new host group.
12. Click **Save**.

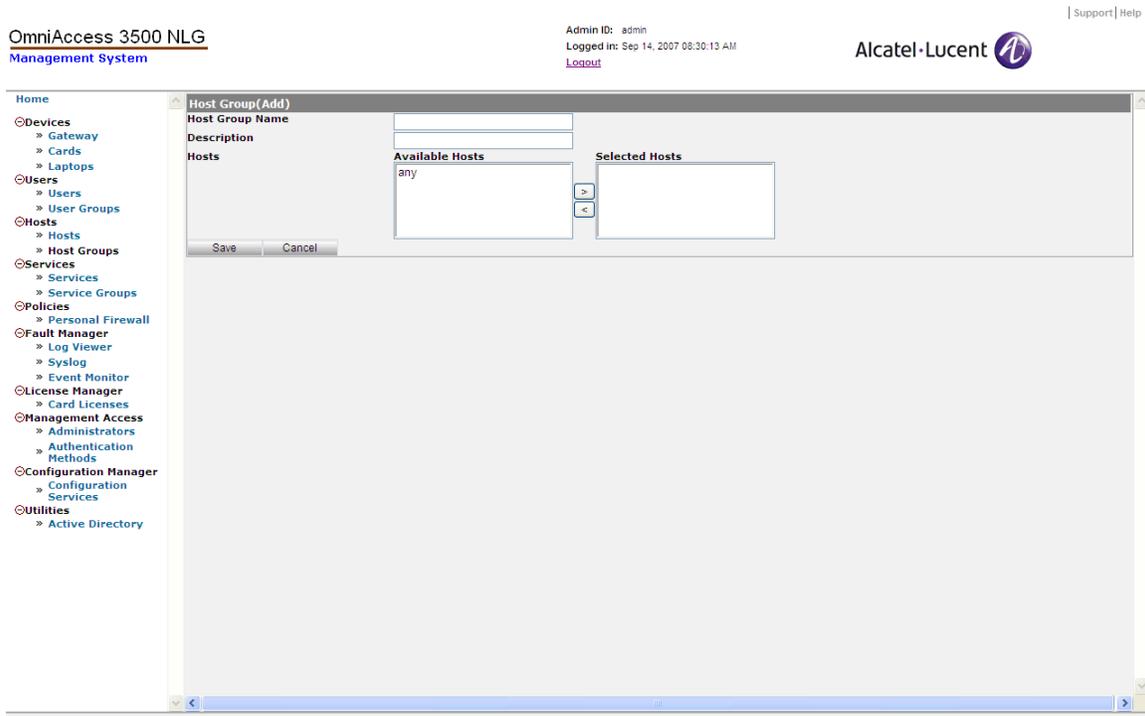


Figure 32 - Host Group (Add)

Next, create the packet filter rules. The default packet filter rule is the “drop” rule: if a packet does not match any of the packet rules specified in the personal firewall policy, the packet is dropped. The packet filter rules that are explicitly created define exceptions to the default behavior.

13. Click **Personal Firewall** on the main menu.
14. On the Policies - Personal Firewall menu, click **Packet Filter Rules**. The Packet Filter Rules Definitions window appears.
15. Click **New**. The Packet Filter Rules (Add) window appears (Figure 33), displaying the following fields:
 - Rule Name: Type a name for the new rule.
 - Direction: Whether the direction of the packets matching the rule is inbound (to the laptop) or outbound (from the laptop).
 - IP Addresses: Set of IP address ranges including the address of a packet matching the packet filter rule (destination IP address for outgoing packets, source IP address for incoming packets).
 - Source Ports: The ports from which the network traffic is originating.
 - Destination Ports: The ports to which the network traffic is going.
 - Protocol: Select a protocol from the drop-down list (for example, UDP, TCP, ICMP, or IP).
 - Rule Action: Select an action to take for this rule from the drop-down list (Accept or Drop).

16. Click Save.

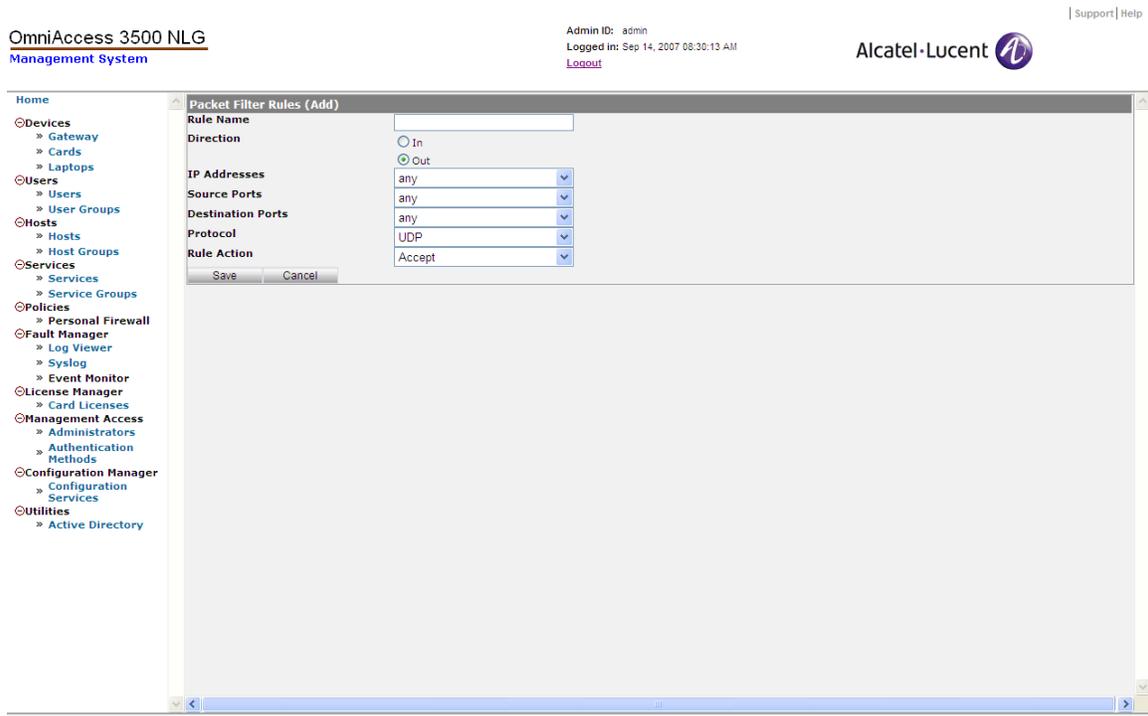


Figure 33 - Packet Filter Rules (Add)

Next, create the list of applications for inclusion in application groups and application filter rules.

17. Click Personal Firewall, then Applications. The Applications window appears.
18. Click New. The Applications window appears (Figure 34), displaying the following fields:
 - o Application Name: Name of the application.
 - o Executable File: Name of the executable file that implements the application.
19. Click Save.

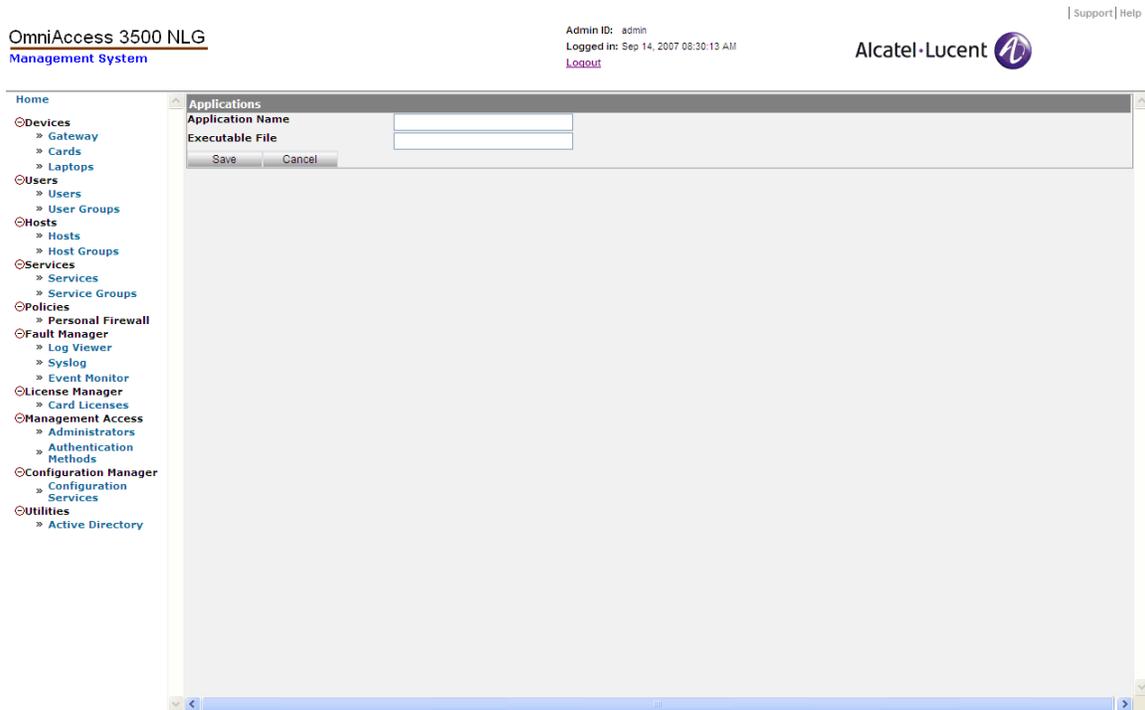


Figure 34 - Applications

Next, create the list of application groups for inclusion in the application filter rules.

20. Click **Personal Firewall**, then **Application Group**. The Applications Group Information window appears.
21. Click **New**. The Application Group window appears (Figure 35), displaying the following fields:
 - Group Name: Name of the application group.
 - Applications: Drop-down menu with the list of applications that can be added to the application group. Once an application is selected, click **Add** to include it in the group list.
22. Click **Save** when the list of applications is complete.

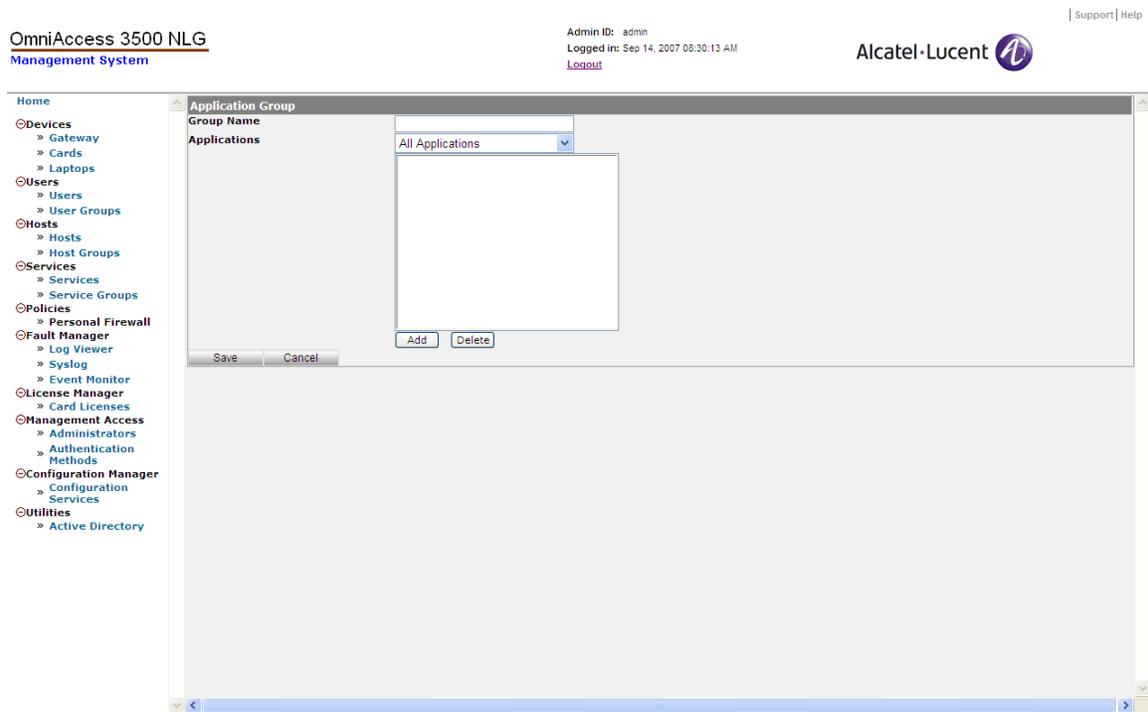


Figure 35 - Application Group

Now create the personal firewall policy.

23. Click **Personal Firewall**, then **Firewall Policy**. The Firewall Policy Definitions window appears.
24. Click **New**. The Firewall Policy Settings (Add) window appears.

On the General tab

The screenshot shows the OmniAccess 3500 NLG Management System interface. At the top, it displays 'OmniAccess 3500 NLG Management System' and 'Admin ID: admin' with a 'Logout' link. The Alcatel-Lucent logo is in the top right. A left-hand navigation tree includes categories like Devices, Users, Hosts, Services, Policies, Fault Manager, License Manager, Management Access, Configuration Manager, and Utilities. The main window is titled 'Firewall Policy Settings (Add)' and has four tabs: General, Rules, Applications, and Application Groups. The 'General' tab is selected and contains the following fields:

- Policy Name: [Text input field]
- User Control: allow deny
- Hotelling Scenario**
- Unsecured connectivity duration: [300]
- Re-activation wait period: [60]

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

25. Figure 36), enter information for the following fields:

- Policy Name: A unique alphanumeric identifier for the personal firewall policy.
- User Control: Whether the user will have control to allow or deny network connections requested by applications. Possible values are <Allow> and <Deny>.
- Hotelling Scenario – Unsecured Connectivity Duration: First timeout used in the Captive Portal Management algorithm, which regulates open access to the Internet during the negotiation of local access credentials with an access point provider. The timeout, expressed in seconds, defines the extension of the time window during which the end user can negotiate the access credentials with the access point provider, in a connectivity scenario that is not secured by the inclusion of the OmniAccess 3500 NLG Gateway in the data path.
- Hotelling Scenario: Re-activation Wait Period: Second timeout used in the Captive Portal Management algorithm, which regulates open access to the Internet during the negotiation of local access credentials with an access point provider. The timeout, expressed in seconds, defines the extension of the blackout interval between consecutive attempts to obtain access credentials from the access point provider. The blackout interval prevents the end user from causing continuous exposure of the laptop to external attacks with lengthy credential negotiation procedures.

26. Click Save.

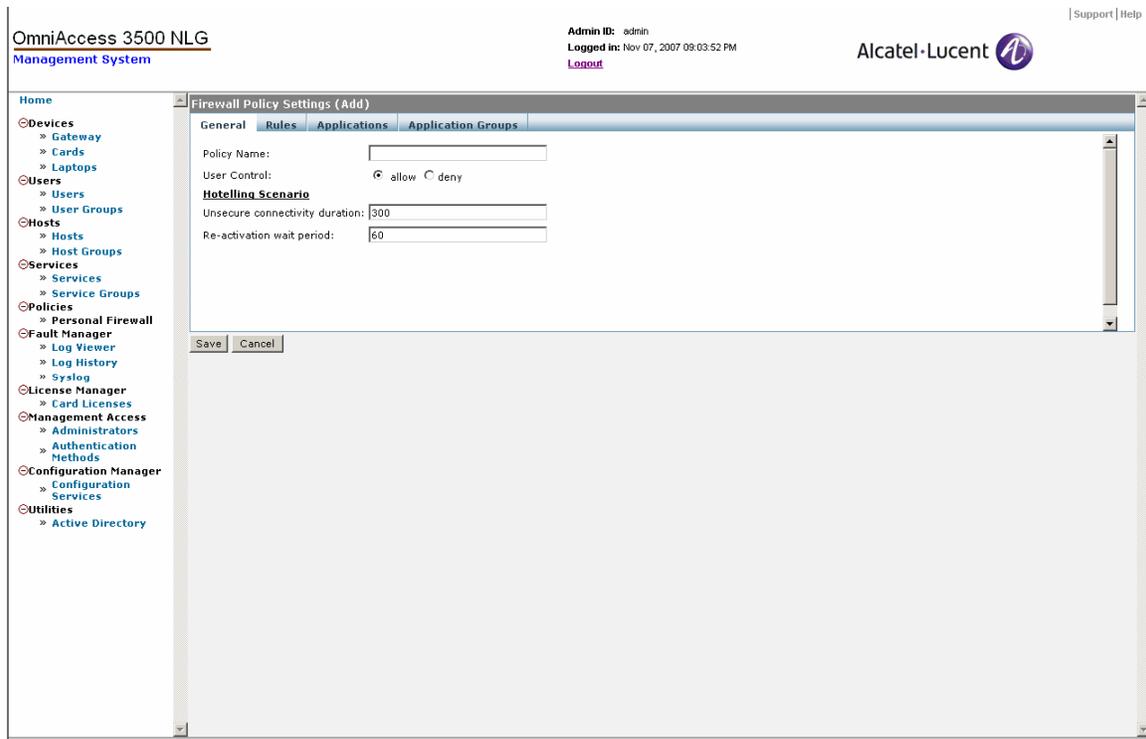


Figure 36 - Firewall Policy Settings General tab

27. On the Rules tab (Figure 37), enter information for the following fields:
 - Rule name: A unique alphanumeric identifier for the packet filter rule to be included in the personal firewall policy.
 - Precedence: A priority level for designation of the order in which the packet filter rule will be executed (i.e., compared with the packet header) with respect to other rules. Higher precedence value means that the rule will be executed first. The first rule that matches the packet header determines the action on the packet.
28. Click Save.

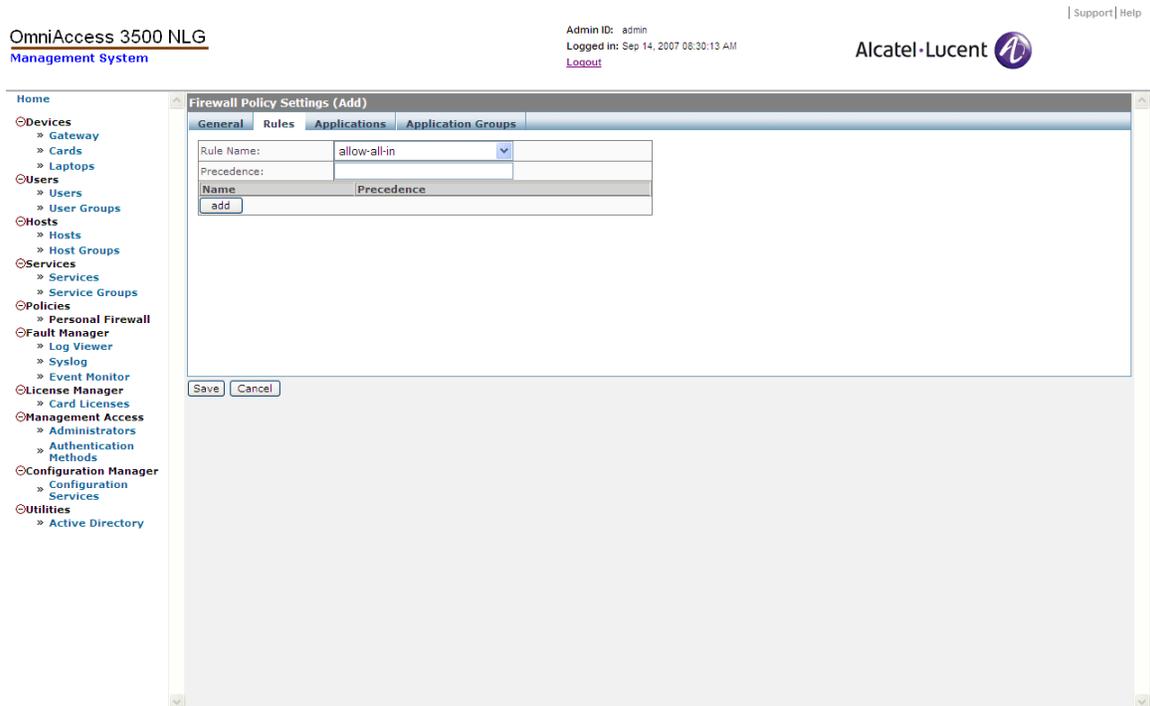


Figure 37 - Firewall Policy Settings Rules tab

29. On the **Applications** tab (Figure 38), enter information for the following fields:
 - Applications: List of applications in the application filter table that contributes to the definition of the personal firewall policy.
 - Network Access: While a packet filter rule is always an allow rule (a packet matching the rule is allowed through the filter), an application filter rule can be set as either an allow rule (the application is always allowed to open a remote connection) or a deny rule (the application is never allowed to open a remote connection).
30. Click **Save**.

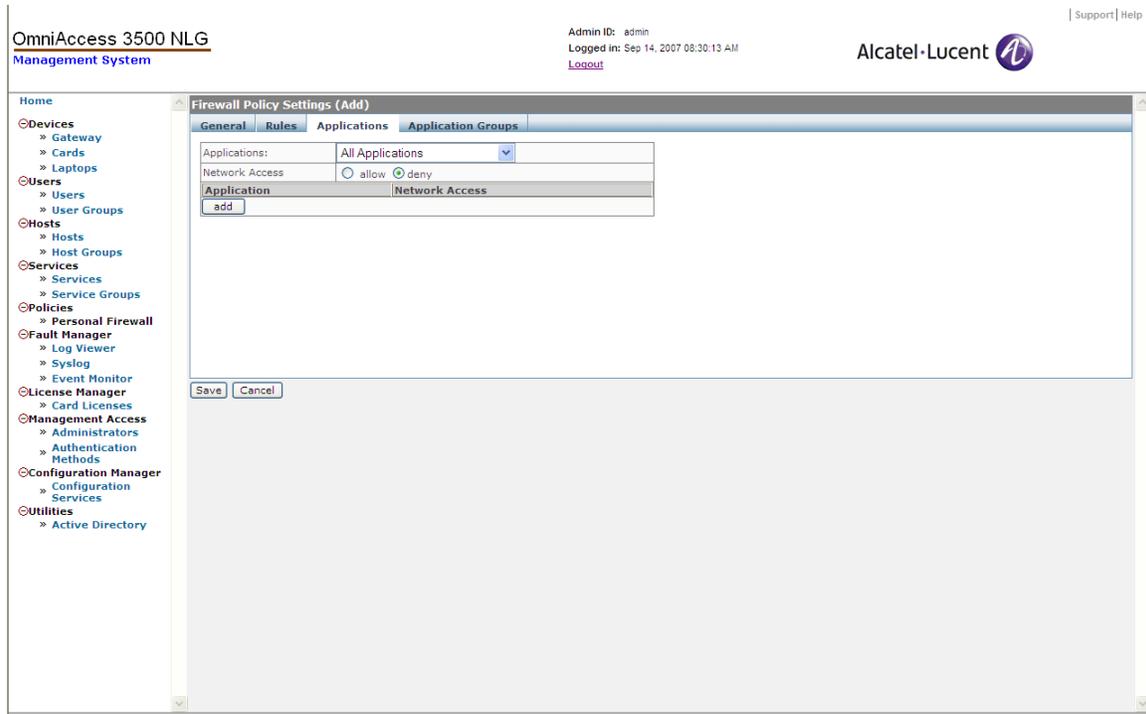


Figure 38 - Firewall Policy Settings Applications tab

31. On the **Application Groups** tab (Figure 39), enter information for the following fields:
 - **Application Groups:** List of application groups in the application filter table that contribute to the definition of the personal firewall policy. Application groups are used to simplify the specification of personal firewall policies, especially when a large number of applications require explicit inclusion in the application filter table.
 - **Network Access:** While a packet filter rule is always an allow rule (a packet matching the rule is allowed through the filter), an application group filter rule can be set as either an allow rule (the application group is always allowed to open a remote connection) or a deny rule (the application group is never allowed to open a remote connection).
32. Click **Save**.

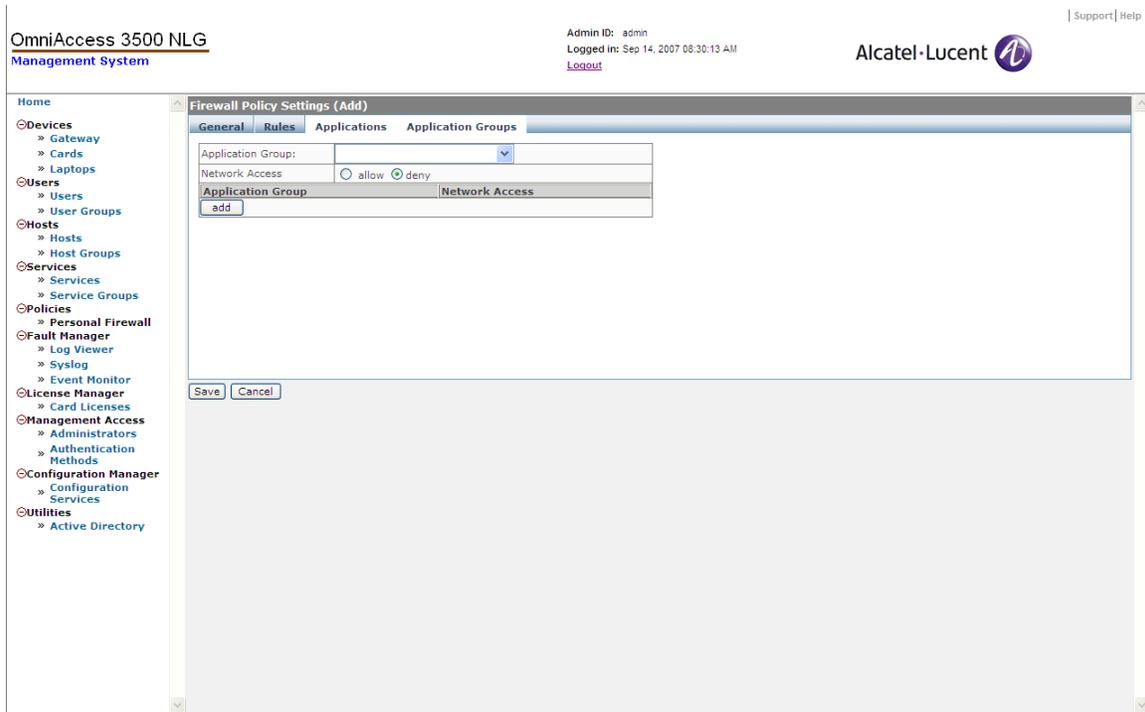
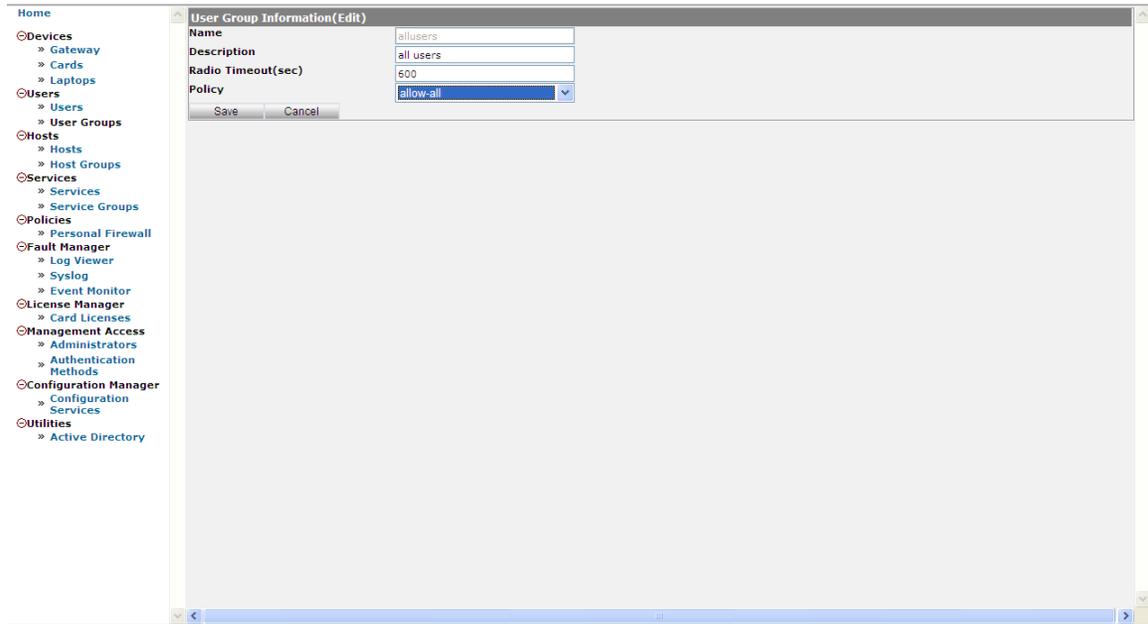


Figure 39 - Firewall Policy Settings Application Groups tab

Now apply the firewall policy to a user group.

33. Click **User Groups**. The User Group Information window appears.
34. Click the checkbox next to a User Group to select it.
35. Click **Edit**. The User Group Information window appears (Figure 40). Select the Firewall Policy that you want to apply from the Policy drop-down list.
36. Click **Save**.



The screenshot displays the 'User Group Information (Edit)' web interface. On the left is a navigation tree with categories like Devices, Users, Hosts, Services, Policies, Fault Manager, License Manager, Management Access, Configuration Manager, and Utilities. The main content area contains a form with the following fields:

Name	allusers
Description	all users
Radio Timeout(sec)	600
Policy	allow-all

At the bottom of the form are 'Save' and 'Cancel' buttons.

Figure 40 - User Group Information (Edit)

Chapter 3. OmniAccess 3500 NLG Runtime Administration Functions

This chapter describes tasks that are performed during runtime, after deployment of the OmniAccess 3500 NLG cards. Runtime tasks include the following:

- Viewing laptop asset information – Display asset information for a user’s laptop.
- Viewing laptop location – Display location information for a user’s laptop.
- Remotely locking a laptop – Remotely lock a user’s laptop for security reasons. You can later unlock the same laptop or generate a one-time password for the end user to temporarily disable all OmniAccess 3500 NLG functions in the laptop.
- Managing the encrypted volume of a laptop – Create/delete/view status for an encrypted volume, and change/remove the secret password needed for decryption of the volume contents.
- Viewing log information – View logs and alarms stored in the management system database.
- View status information for current access connections – View current settings, status variables, and traffic statistics.

Viewing Laptop Asset Information

The Asset Management function runs periodically and allows you to display information about laptop assets.

1. Click **Users** on the main menu.
2. Click the checkbox next to a user to select it and then click **Configure**. The User Configurations window appears (Figure 41).

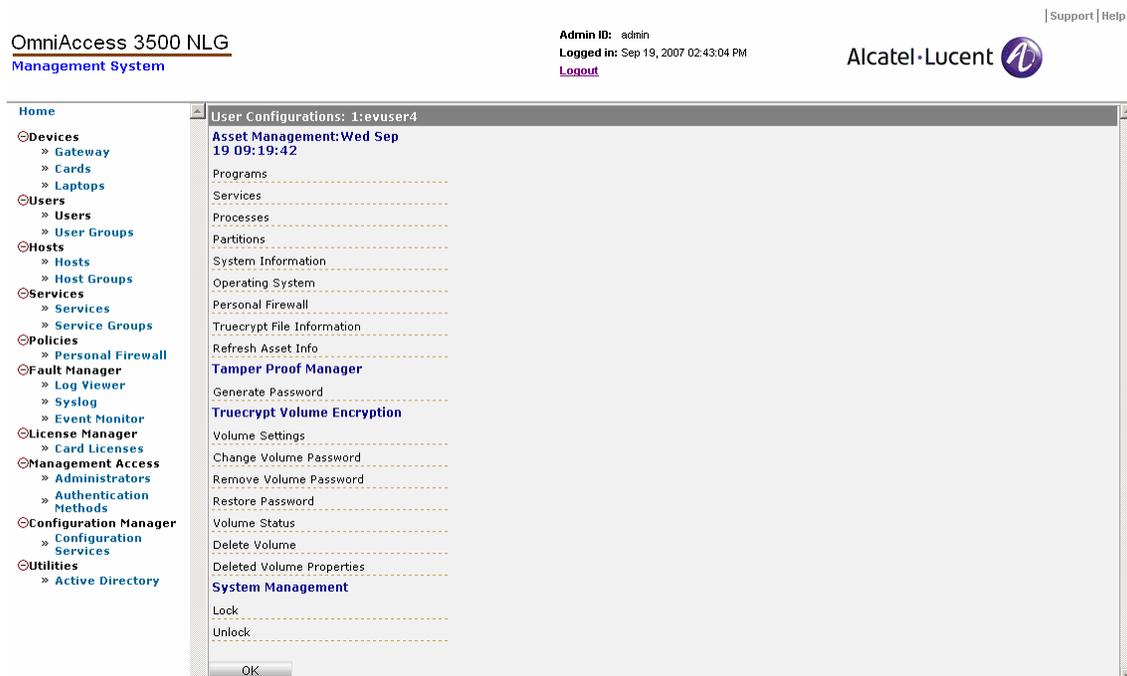


Figure 41 - User Configurations

3. To view laptop asset information, select one of the options under the Asset Management menu, as follows:
 - Programs: Applications installed in the user's laptop.
 - Services: Services installed in the user's laptop.
 - Processes: Processes running on the user's laptop.
 - Partitions: Partition table entries.
 - System Information: System-related information, such as Manufacturer, Model, CPU version, etc.
 - Operating System: Operating system installed in the user's laptop.
 - Personal Firewall: Applications for which the personal firewall policy has set allow/deny rules with respect to network access.
 - TrueCrypt File Information: Information about the files stored in the encrypted volume of the user's laptop.
 - Refresh Asset Info: Click this link to trigger a refresh of all the asset management entries.

Viewing User Status Information

The management system maintains comprehensive status information for every user and the associated laptop and card.

To view a user's status information:

4. Click **Users** on the main menu.

5. Click the checkbox next to a user to select it and then click **Status**.
6. On the Status Information of User window, click **User Status**. The User Status Information window appears (Figure 42).
7. Click **OK**.

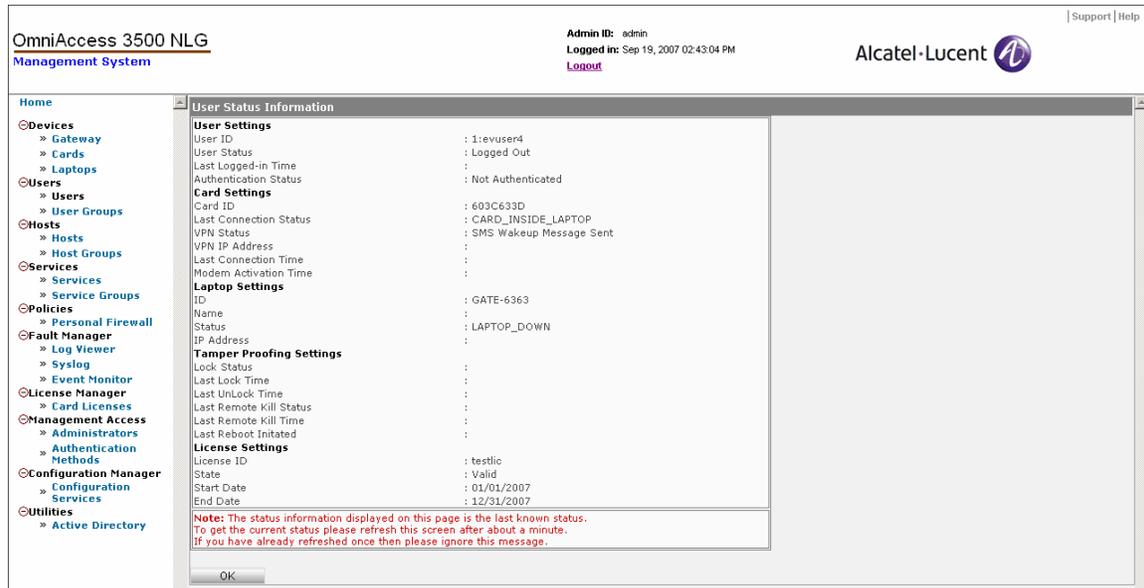


Figure 42 - User Status Information

Viewing the Laptop Location

You can view the current location of the laptop or the location where the user most recently logged into the laptop.

To view a laptop's location:

1. Click **Users** on the main menu.
2. Click the checkbox next to a user to select it and then click **Status**.
3. Click one of the following:
 - o **View Current Location** to see the current location of the laptop.
 - o **View Login Location** to see the location where the user last logged into the laptop.
4. A Proprietary Information window appears (Figure 43). Type your administrator password into the text box and click **Accept** to proceed.

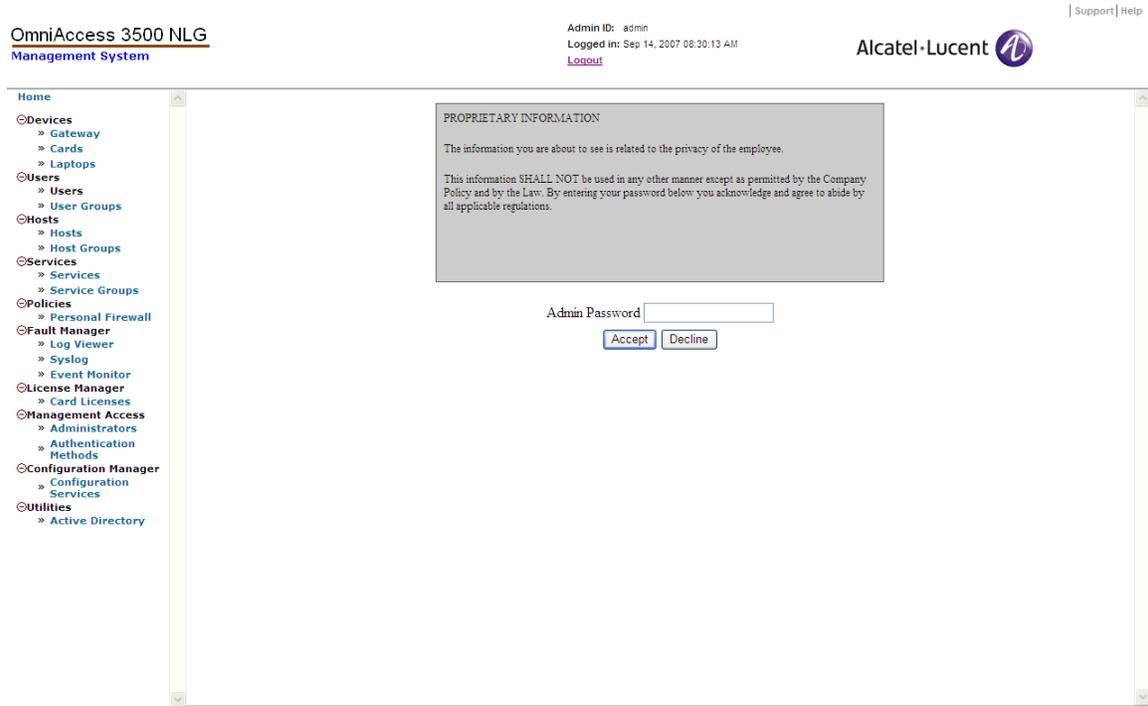


Figure 43 - Proprietary Information window

5. A map similar to the one shown in Figure 44 appears. If the laptop's location cannot be retrieved, a corresponding message will appear.

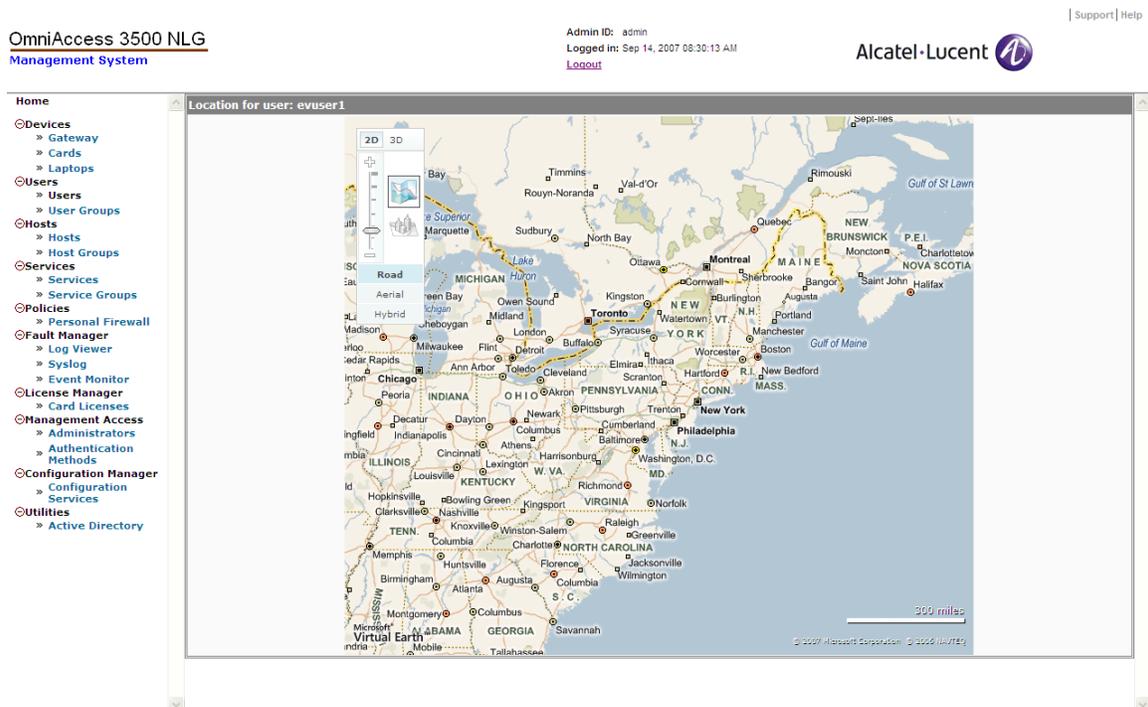


Figure 44 - Current User Location map

Laptop Remote Lock

The IT administrator can remotely lock the laptop when the end user realizes that the laptop cannot be physically protected from external intrusions (for example, if the laptop was inadvertently left unguarded in a public location).

To remotely lock a laptop:

1. Click **Users** on the main menu.
2. Click the checkbox next to a user to select it, then click **Configure**.
3. On the User Configurations window, click **Lock** under the System Management menu.
4. Click **Yes** to lock the laptop.
5. A window appears on the laptop indicating that the laptop has been locked (Figure 45).

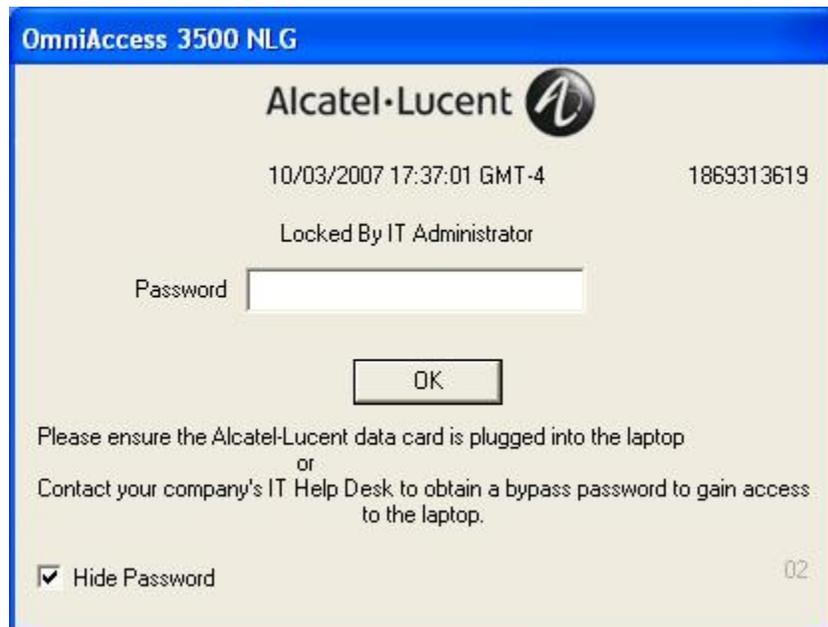


Figure 45 - Laptop locked window

Laptop Remote Unlock

The IT administrator can issue a remote unlock command through the management system to unlock a laptop that had previously been locked by issuing a remote lock command.

To remotely unlock a laptop:

1. Click **Users** on the main menu.
2. Click the checkbox next to a user to select it and then click **Configure**.
3. On the User Configurations window, click **Unlock** under the System Management menu.

4. Click **Yes** to unlock the laptop.
5. A message appears stating that the laptop has been unlocked.

One-Time Password Generation

The OmniAccess 3500 NLG can lock the laptop under several circumstances, both manually (remote lock command issued by the IT administrator) and automatically (upon detection of certain events like tamper attempts, etc.). While locked, the laptop shows on the window a numeric key (the screen count) and a password prompt. To unlock the laptop, the legitimate end user must call the IT desk and read the screen count value to the IT administrator. If the end user is eligible for unlocking, the IT administrator generates a one-time password (OTP) using the screen count and communicates it to the end user. The end user enters the OTP to regain control of the laptop. The OTP expires upon its first use. All OmniAccess 3500 NLG controls are disabled for a period of configurable duration, during which the end user is expected to remove the cause of the initial lock. Upon expiration of the controlless interval, the laptop either locks again (if the cause of the lock has not been removed) or restores all OmniAccess 3500 NLG controls (if the cause of the lock has been successfully removed).

To generate a one-time password for a locked laptop:

1. Click **Users** on the main menu.
2. Click the checkbox next to a user to select it, then click **Configure**.
3. On the User Configurations menu, click **Generate One Time Password** under the Tamper Proof Manager menu. The Tamper Proofing Settings – Get One Time Password window appears (Figure 46), displaying the following fields:
 - **User ID:** Type the user ID corresponding to the laptop you are locking.
 - **Current Date (mm/dd/yyyy):** Type the date displayed on the lock screen of the laptop.
 - **Current Time (hh:mm:ss):** Type the time of the day displayed on the lock screen of the laptop.
 - **Time Zone:** Type the time zone displayed on the lock screen of the laptop.
 - **Screen Count:** Type the number that appears in the upper right-hand corner of the pop-up window on the laptop screen (in Figure 45, this number is 1734508387).

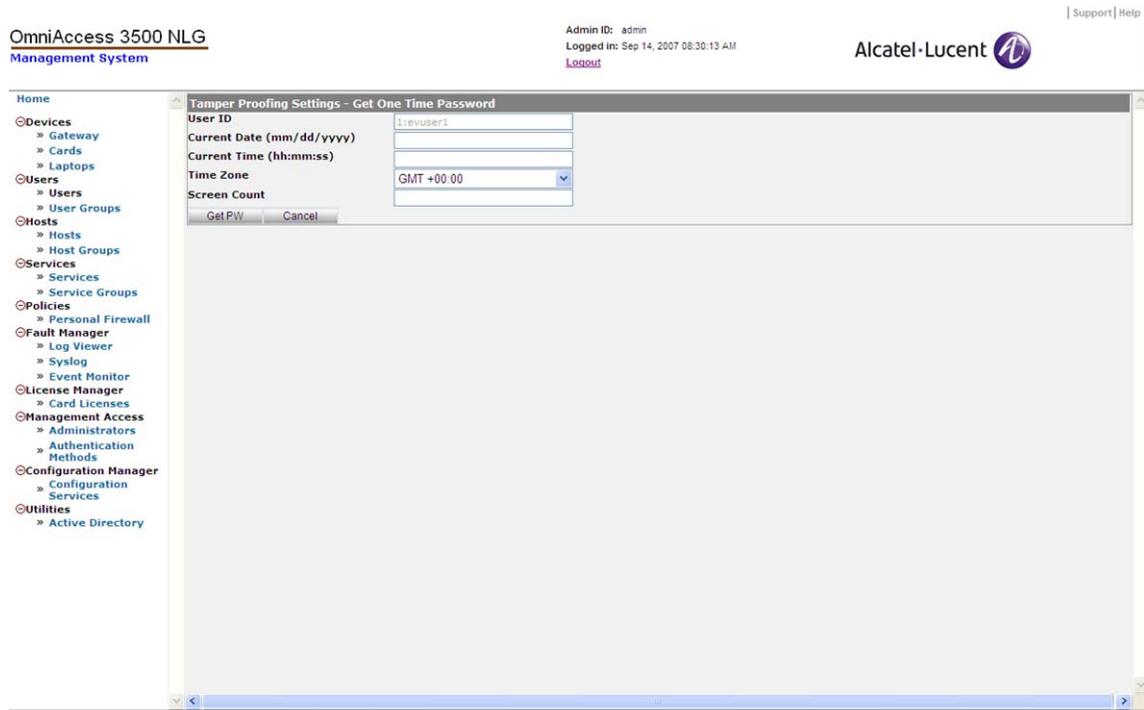


Figure 46 - Tamper Proofing Settings - Get One Time Password

- Click **Get PW**. A window appears displaying a new one-time password. The end-user must type this password (including any hyphen it may include) into the Password field on the window on the laptop to unlock the laptop. (They must uncheck the Hide Password box if they want the password to display on the window as they are typing it.)

Encrypted Volume Management

An encrypted volume can be created in the laptop hard disk for storage of sensitive data. While the selection of the files to be included in the encrypted volume is left to the end user, the OmniAccess 3500 NLG assumes exclusive administrative control over the encrypted volume. Through the management system GUI, the administrator sets the configuration parameters of the encrypted volume (some of the parameters, such as the encryption algorithm and the hash algorithm, are set per user group, while other parameters, such as the drive identifier, the maximum size, and the secret password needed for encryption/decryption of the volume contents, are set per individual user). The end user can access neither the configuration parameters, nor the secret password, which is stored in the OmniAccess 3500 NLG card and never accessible from the laptop. If the laptop is stolen, the contents of the encrypted volume can be protected from malicious access by remotely deleting the secret password from the card. The management system retains the last password used to encrypt the data, so that it can be utilized to retrieve the data if the laptop is ever recovered.

This section describes the configuration of the encrypted volume, the management of the secret password, and the monitoring of the volume status.

To configure common volume encryption parameters within a user group:

1. Click **User Groups** on the main menu.
2. Click the checkbox next to a user group to select it and then click **Configure**.
3. On the User Group Configurations window, click **Group Volume Settings**.
4. The Group TrueCrypt Settings (New) window appears (Figure 47), showing the following fields:
 - Group Name: Identifier of the user group, shown to remind the IT administrator of the user group for which the encrypted volume is being configured.
 - Encryption Algorithm: Algorithm used for encryption of the volume contents. Available options are:
 - AES (default)
 - Serpent
 - Twofish
 - AES-Twofish
 - AES-Twofish-Serpent
 - Serpent-AES
 - Serpent-Twofish-AES
 - Twofish-Serpent
 - Hash Algorithm: Algorithm used for random generation of the volume master key. Available options are:
 - RIPEMD-160 (default)
 - SHA-1
 - Whirlpool
 - File Format: Type of file system for the encrypted volume. Available options are:
 - FAT (default)
 - NTFS (this option does not work for end users that do not have administrator privileges on their laptops).

Note: Windows XP supports NTFS. Earlier Windows versions and Linux support FAT.

5. Click **Save** to save the TrueCrypt settings for the user group.

Note: The values of the user group parameters for TrueCrypt are not retroactively applied. When one or more user group values change, only the encrypted volumes that are created after the change reflect the new values.

Note: Since every user group parameter for TrueCrypt has an assigned default value, the configuration of the user group parameters for TrueCrypt is only necessary when one or more of those values requires modification.

Note: If you delete your selection for the values of the user group parameters for TrueCrypt, the default values are automatically restored for those parameters.

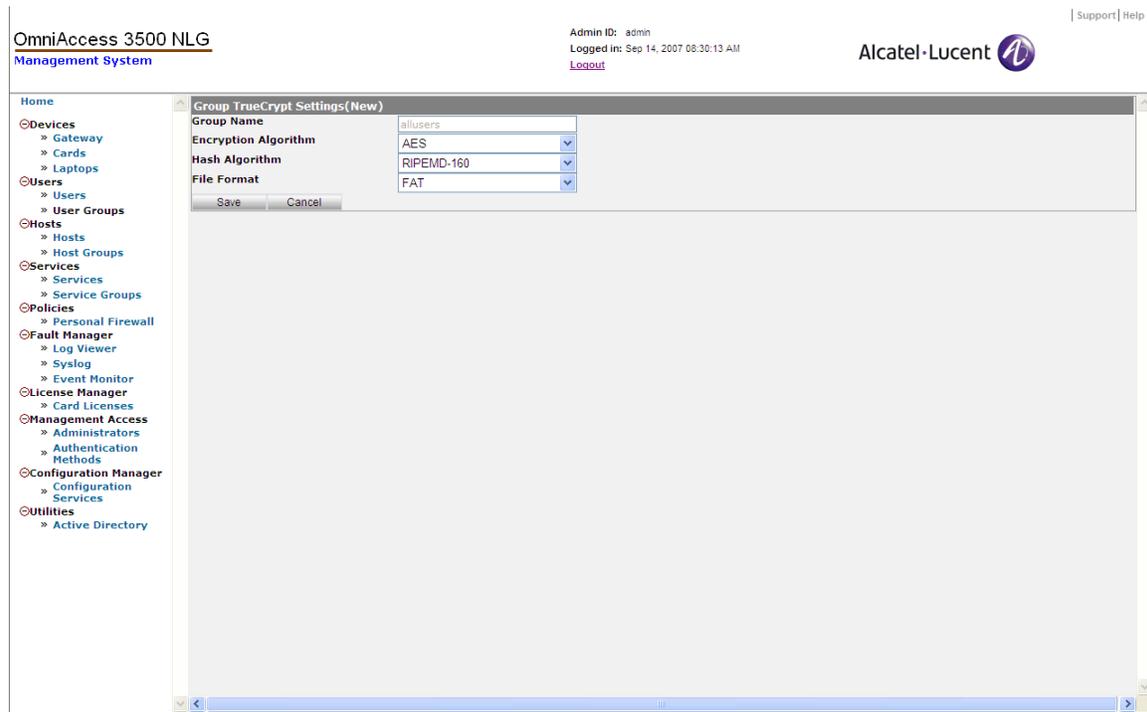


Figure 47 - TrueCrypt User Group Settings

To create an encrypted volume:

1. Click **Users** on the main menu.
2. Click the checkbox next to a user to select it and then click **Configure**.
3. On the User Configurations window, click **Volume Settings** under the TrueCrypt Volume Encryption menu.
4. The TrueCrypt Settings window appears (Figure 48), with the following parameters to be configured:
 - User ID: Numeric identifier of the end user (read-only field).
 - Volume Path: Location of the encrypted volume in the laptop hard disk. The assigned value must be a valid, unused path and can point to a file with any type of extension.
 - Mount Drive: Drive identifier assigned to the encrypted volume once mounted. The assigned value must be a valid, unused drive identifier.
 - Volume Size (MB): Space allocated to the encrypted volume in the laptop hard disk. The assigned value must not exceed the space that is currently available on the laptop's hard disk.
 - Volume Enabled: Flag for enabling/disabling the mounting of the encrypted volume on the laptop's file system. The flag must be checked in order for the

creation of the encrypted volume to proceed the next time the laptop connects to the gateway after the volume settings are saved.

5. Click **Save** to save the configuration settings and enable the creation of the encrypted volume.

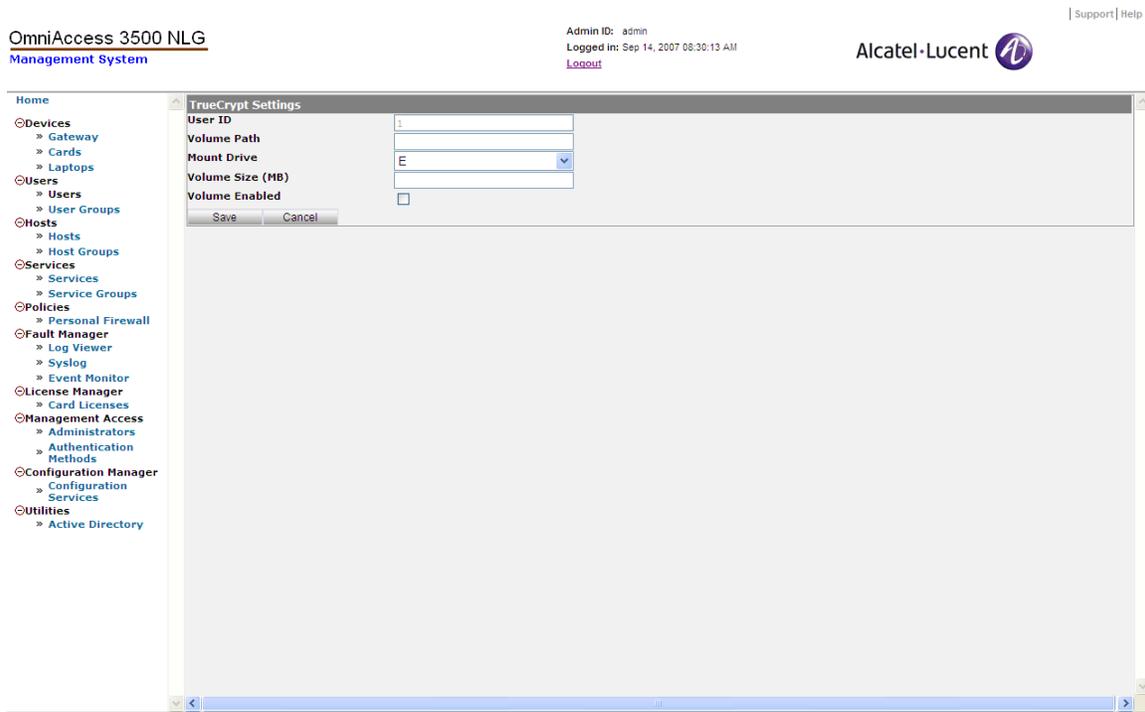


Figure 48 - TrueCrypt Settings

To relinquish administrative control over an existing encrypted volume:

1. Click **Users** on the main menu.
2. Click the checkbox next to a user to select it and then click **Configure**.
3. On the User Configurations window, click **Delete Volume** under the TrueCrypt Volume Encryption menu.
4. Click **OK** to issue the Delete Volume command and return to the User Information window.

The administrator should relinquish administrative control over an existing volume only after having carefully concluded that the encrypted volume will never be needed again by the end user (for example, if the end user is no longer with the company). Please note that the Delete Volume command does not remove the encrypted volume from the laptop hard disk and does not always make the contents of the encrypted volume immediately inaccessible to the end user. The administrator must resort instead to the Remove Password command in all emergency cases where access to the encrypted volume contents must be immediately denied ("Remote Kill" feature). If control over the volume is erroneously relinquished and a user wants to recover data from the deleted volume, the Deleted Volume Properties feature can be used to recover the volume path and password, as in the following procedure.

To display the properties of a volume that was previously released by the administrator:

1. Click **Users** on the main menu.
2. Click the checkbox next to a user to select it and then click **Configure**.
3. On the User Configurations window, click **Deleted Volume Properties** under the TrueCrypt Volume Encryption menu.
4. The Deleted Volume Information window appears (Figure 49), displaying all data needed for reconfiguration of the same volume in the laptop's hard disk.

Note: The restoration of a relinquished encrypted volume cannot be performed remotely by the administrator through the management system. Instead, the end user must enter the necessary parameters locally, through the user interface that comes with the encrypted volume software.

5. Click **OK**.

Only the end user can physically remove the encrypted volume from the laptop hard disk, by deleting the file corresponding to the volume path after the administrator has relinquished administrative control over it.

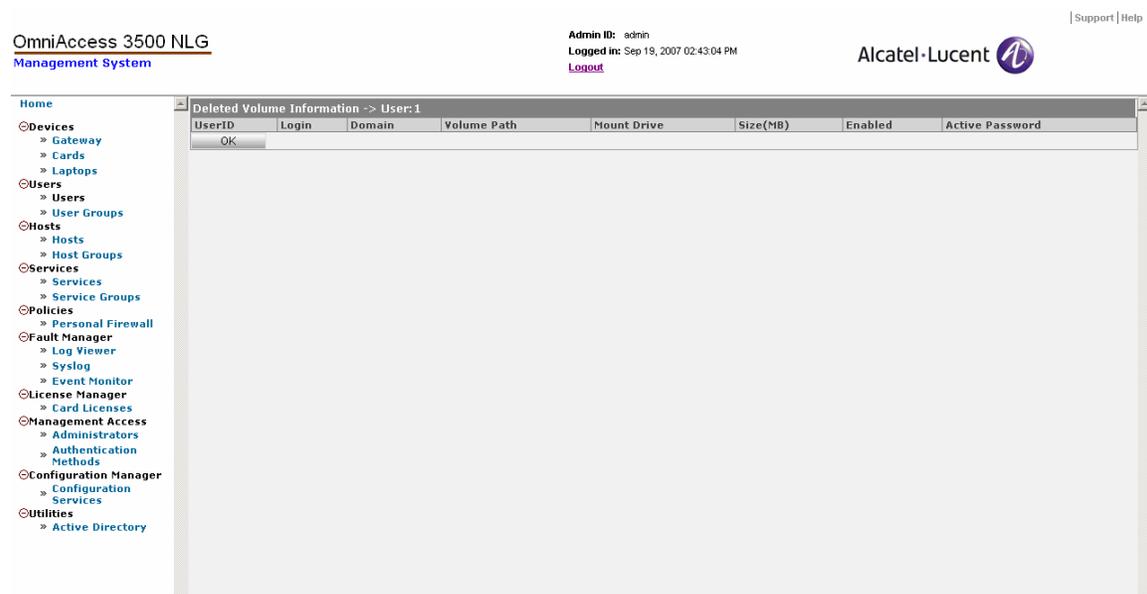


Figure 49 - Deleted Volume Information

To change the secret password stored in the OmniAccess 3500 NLG card:

1. Click **Users** on the main menu.
2. Click the checkbox next to a user to select it and then click **Configure**.
3. On the User Configurations window, click **Volume Settings** under the TrueCrypt Volume Encryption menu.
4. If the check box next to Volume Enable is currently checked, click it to uncheck it and click **Save**.

5. On the User Configurations window, click **Change Volume Password** under the TrueCrypt Volume Encryption menu.
6. Click **Yes** to issue the password change command and return to the User Configurations window.
7. Click **Volume Status** and verify the Password Change Status reported on the TrueCrypt Status Information window. Then click **OK**.
8. If the password change has been successful, click **Volume Settings** under the TrueCrypt Volume Encryption menu and click the Volume Enable checkbox on the TrueCrypt Settings (Edit) window.
9. Click **Save**.

To delete the secret password and immediately make the contents of the encrypted volume impossible to access (Remote Kill feature):

1. Click **Users** on the main menu.
2. Click the checkbox next to a user to select it and then click **Configure**.
3. On the User Configurations window, click **Remove Volume Password** under the TrueCrypt Volume Encryption menu.
4. Click **Yes** to issue the password deletion command and return to the User Information window.

Note: To immediately deny access to the encrypted volume contents without deleting the volume you must use the Remove Volume Password command. Other methods, such as unchecking the Volume Enabled flag, are not immediately effective and may not prevent the decryption of the volume contents.

To restore the secret password stored in the OmniAccess 3500 NLG card:

1. Click **Users** on the main menu.
2. Click the checkbox next to a user to select it and then click **Configure**.
3. On the User Configurations window, click **Restore Password** under the TrueCrypt Volume Encryption menu.
4. Click **Yes** to issue the password restore command and return to the User Information window.

To verify the status of a previously submitted volume encryption command (volume creation/deletion, password change/removal):

1. Click **Users** on the main menu.
2. Click the checkbox next to a user to select it and then click **Configure**.
3. On the User Configurations window, click **Volume Status** under the TrueCrypt Volume Encryption menu.
4. The TrueCrypt Status Information window appears, showing the following fields:
 - User ID: Numeric identifier of the user.
 - Volume Path: Location of the encrypted volume in the laptop hard disk.
 - Mount Drive: Drive name assigned to the encrypted volume.

- Volume Size: Hard disk space allocated to the encrypted volume (in MB).
 - Volume Status: Status of the encrypted volume (whether or not created and mounted).
 - Password Change Status: Status of execution of a command previously issued to change or delete the secret password.
 - Password Change Time: Time of completion of the Password Change/Delete command.
 - Active Password: Last password successfully stored in the OmniAccess 3500 NLG card.
5. Click **OK** to return to the User Information window.

To delete TrueCrypt Volume Encryption settings from a user group:

1. Click **User Groups** on the main menu.
2. Click the checkbox next to a user group to select it and then click **Configure**.
3. On the User Group Configurations window, click **Delete Group Volume**.
4. A confirmation window appears, asking if you are sure you want to delete group volume settings.
5. Click **Yes** to delete the settings.

Connection Manager - Show Information

This section of the management system GUI allows you to display status information for the remote access connections that are currently established between the OmniAccess 3500 NLG cards and the gateway. (Refer to Chapter 5, OmniAccess 3500 NLG Administrative Information Base, to see detailed field information.)

Status information can be displayed for the following items:

- SA-IKE — List of the IKE Security Associations that currently exist between the OmniAccess 3500 NLG gateway and remotely connected OmniAccess 3500 NLG cards.
- SA-IPsec — List of the IPsec Security Associations that currently exist between the OmniAccess 3500 NLG gateway and remotely connected OmniAccess 3500 NLG cards.
- Flows — List of the objects that the OmniAccess 3500 NLG gateway instantiates for stateful packet inspection purposes. When a packet arrives at the firewall embedded in the OmniAccess 3500 NLG gateway, the firewall first tries to match it with a previously established flow object. If no matching flow object is found, the firewall tries to match the packet with one of its configured rules. If one or more matches are found, a new flow object is created according to the matching rule with the highest precedence. If no matching rule is found, the default rule (drop) is applied to the packet.
- Global Information — List of traffic statistics collected since the OmniAccess 3500 NLG gateway was last restarted.

To view status information:

1. Click **Gateway** on the main menu, then click **Configure Advanced Settings**.
2. On the Configure menu, under Connection Manager -Show Information, click **SA-IKE**, **SA-IPsec**, **Flows**, or **Global Information**, depending on the type of information you wish to view.
3. A window containing information about the OmniAccess 3500 NLG gateway you have selected appears (Figure 50 shows the Global Information window as an example).

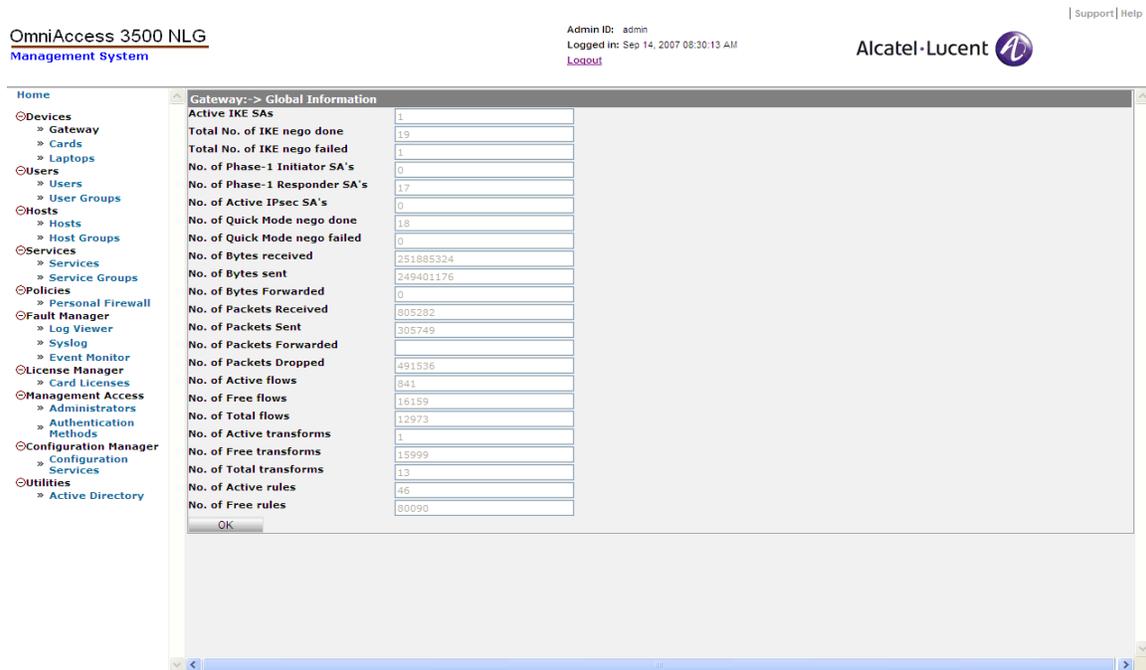


Figure 50 - Gateway Global Information

Logs and Alarms

The Fault Manager application allows you to view system status information in different formats. In addition, you can use the Syslog function to have logs forwarded to a specific server.

Log Viewer

The Log Viewer function allows you to view the most recent logs stored in the system's database.

To view all logs:

1. On the Fault Manager menu, click **Log Viewer**. The Server Log Viewer window appears (Figure 51), displaying the following fields:
 - o Local Time: The local time at which the event took place.
 - o IP Address: The IP address of the module on which the event took place.

- Event ID: The type of the logged event.
- Module Name: The name of the module by which the log is filtered.
- Severity: The alarm severity.
- Message: Any additional information about the event.

OmniAccess 3500 NLG Management System

Admin ID: admin
Logged in: Nov 07, 2007 09:03:52 PM
[Logout](#)

Alcatel-Lucent

Time	IP Address	Event ID	Module Name	Severity	Message
11/07/2007 09:03:52	10.1.1.13	MS_SERVER_LOGIN1860623611	MS_SERVER_LOGIN	INFO	Successfully logged in to the Management Server
11/07/2007 09:03:52	10.1.1.13	MS_SERVER_LOGIN1555579627	MS_SERVER_LOGIN	INFO	Start verifying the admin logon credentials
11/07/2007 08:03:29	10.1.1.13	MS_SERVER_LOGIN-199163439	MS_SERVER_LOGIN	INFO	Successfully logged in to the Management Server
11/07/2007 08:03:29	10.1.1.13	MS_SERVER_LOGIN-1289785888	MS_SERVER_LOGIN	INFO	Start verifying the admin logon credentials
11/07/2007 02:17:46	10.1.1.13	MS_SERVER_LOGIN096829240	MS_SERVER_LOGIN	INFO	Successfully logged in to the Management Server
11/07/2007 02:17:46	10.1.1.13	MS_SERVER_LOGIN-1979617803	MS_SERVER_LOGIN	INFO	Start verifying the admin logon credentials
11/06/2007 10:28:08	10.1.1.13	MS_SERVER_LOGIN-896537793	MS_SERVER_LOGIN	INFO	Successfully logged in to the Management Server
11/06/2007 10:28:08	10.1.1.13	MS_SERVER_LOGIN-1576015036	MS_SERVER_LOGIN	INFO	Start verifying the admin logon credentials

Refresh (mins.):

Figure 51 - Server Log Viewer

Log History

The Log History function provides access to an extended set of archived event logs.

1. On the Fault Manager menu, click **Log History**. The Server Log History window appears (Figure 52), displaying the following fields:
 - Time: The local time when the log was created.
 - GMT Time: The GMT time the alarm occurred.
 - IP Address: The IP address of the device where the alarm occurred.
 - Event ID: The identifier of the software module that triggered the alarm.
 - Module Name: Name of the software module that generated the log.
 - Severity: The alarm severity.
 - Message: Any additional information about the event.
 - Refresh (mins.): Type a number in this field to indicate how often you would like this window to refresh (default: 1 minute).

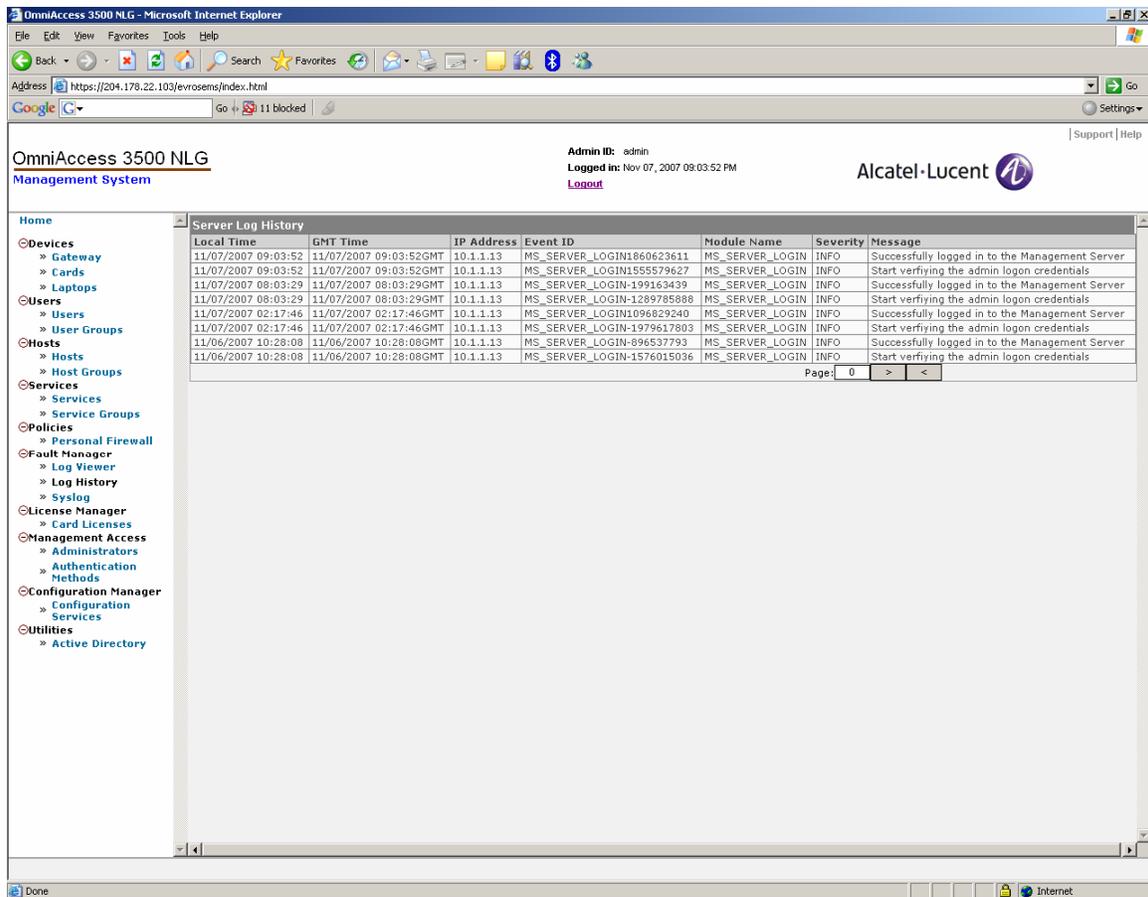


Figure 52 - Server Log History

Syslog

All log messages are sent to the management system and displayed on the GUI. The syslog function allows you to have logs also forwarded to a particular server.

1. On the Fault Manager menu, click **Syslog**. The Syslog Server Settings window appears (Figure 53), displaying the following fields:
 - o Primary Server: The first Server to which you want to forward logs.
 - o Secondary Server: A second Server to which you want to forward logs.
 - o Port: The port number to which you want to forward logs.
 - o Forward Logs: Click this checkbox to forward logs; leave unchecked to not forward.
2. Click **Save**.

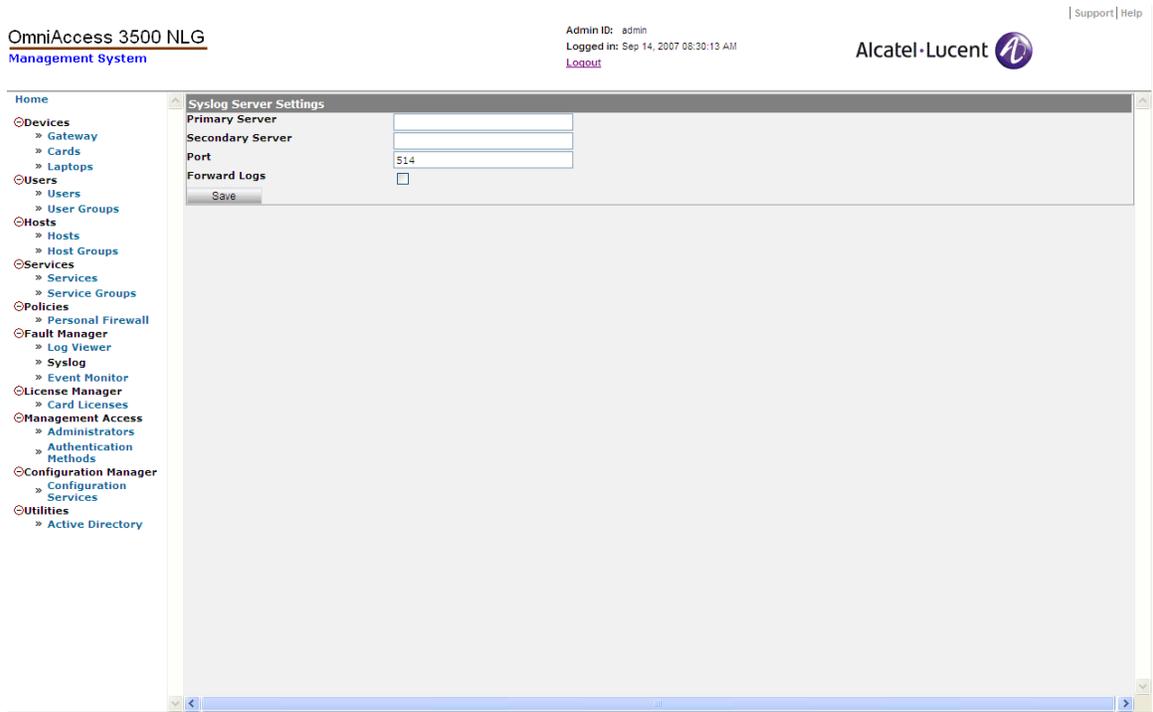


Figure 53 - Syslog Server Settings

Chapter 4. OmniAccess 3500 NLG Infrastructure Maintenance

This chapter describes the procedures that are needed for maintenance of the infrastructural components of the OmniAccess 3500 NLG platform after they are installed.

Backing Up and Restoring the OmniAccess 3500 NLG Gateway Configuration

The backup-and-restore procedures described in this section should be applied to recover from the complete failure of an OmniAccess 3500 NLG gateway unit, when the failed unit is replaced with a new one.

The criticality of the specific OmniAccess 3500 NLG gateway instance drives the choice for the backup frequency and for the location of the backup repository. At a minimum, it is recommended to backup the configuration data at least once a day, and to store the backup files in two geographically separated backup repository sites.

Automatic Backup Configuration

The following steps are required for configuration of the automatic backup procedure:

1. Make sure that the gateway already has all the files that it needs to establish secure connections with other network nodes:
 - Keytab File: File containing the credentials of the gateway for authentication with the Active Directory Server (ADS). The file must necessarily be uploaded to the gateway before any interaction with the Active Directory (AD) infrastructure can start. This includes the case where the method used for authentication of one or more user groups changes from RADIUS to AD.
 - CA Certificate: Digital certificate of the Certificate Authority (CA), which includes the CA's public key and digital signature. The same CA certificate is installed in the OmniAccess 3500 NLG cards.
 - CA Certificate Revocation List: List of certificates issued by the Certificate Authority that have been revoked before their natural expiration.
 - Gateway Certificate: Certificate (public key) of the gateway, used by peer network nodes for encryption of the messages they send to the gateway.
 - Gateway Private Key: Secret key used by the gateway to decrypt the messages it receives from peer network nodes (including the OmniAccess 3500 NLG cards).

In the unlikely case that the files listed have not already been uploaded, follow the procedure described in the *File Upload* section of this document (page 22) to install the files in the gateway.

2. Add a pass rule to the Rules table (through the [Gateway|Configure Advanced Settings|Rules|New] command path) to allow traffic from the gateway to the designated backup server. The rule is typically set for the Ethernet interface of the gateway that faces the private portion of the enterprise network (LAN). In the

example of Figure 54, <10.1.1.9> is the IP address of the private interface (LAN) of the gateway.

The screenshot shows the 'Connection Manager Rules (Add)' configuration window in the Alcatel-Lucent OmniAccess 3500 NLG Management System. The window is titled 'Connection Manager Rules (Add)' and contains the following fields and options:

- Precedence:** (Empty text field)
- Type:** Pass (Dropdown menu)
- Protocol:** ANY (Dropdown menu)
- Source IP/[Mask]:** 0.0.0.0/0 (Text field)
- Source Port Low:** 0 (Text field)
- Source Port High:** 65535 (Text field)
- Destination IP/[Mask]:** 0.0.0.0/0 (Text field)
- Destination Port Low:** 0 (Text field)
- Destination Port High:** 65535 (Text field)
- Interface Name:** (Empty text field)
- Local Stack Direction:** ANY (Dropdown menu)
- To Tunnel:** None, To Tunnel, From Tunnel (Radio buttons)
- From Tunnel:** remote-access (Dropdown menu)

At the bottom left of the form, there are 'Save' and 'Cancel' buttons. The background shows the management system's navigation tree on the left and the Alcatel-Lucent logo on the right.

Figure 54 - Connection Manager Rules (Add)

3. Set the parameters for the automatic backup procedure through the Configuration Services section of the management system GUI.

To set the configuration parameters for the automatic backup procedure:

1. Click **Configuration Services** on the main menu.
2. On the Configuration Manager window (Figure 55), click **Gateway Public Key**.

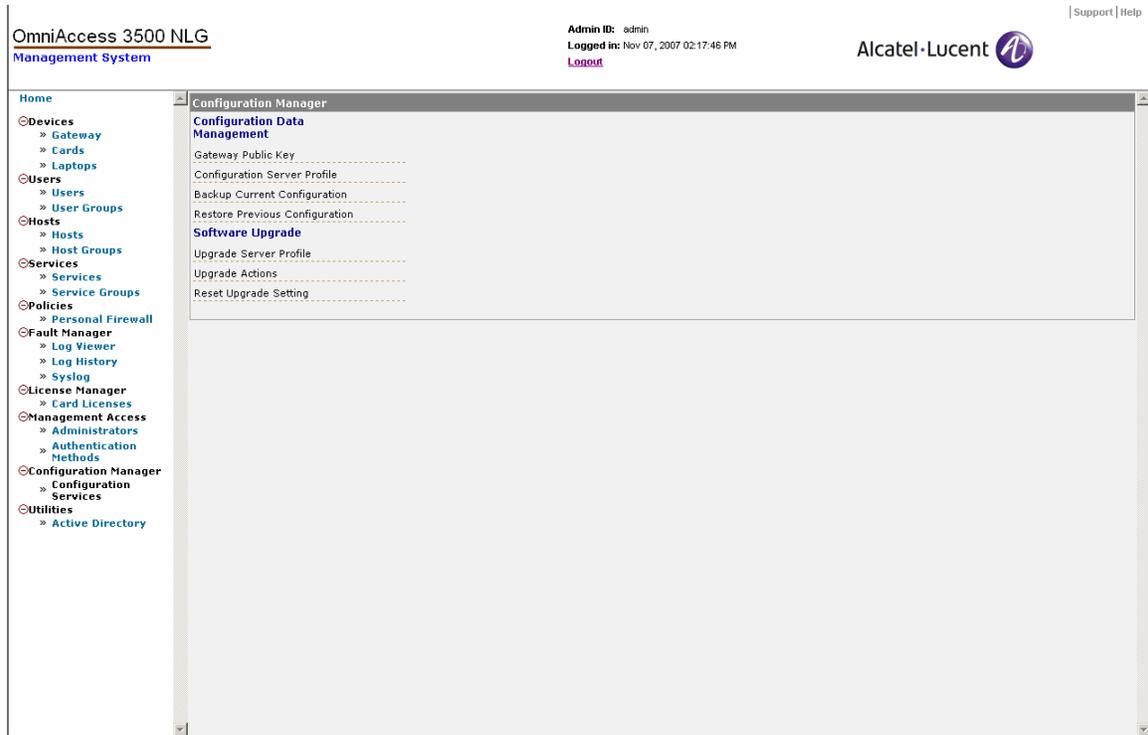


Figure 55 - Configuration Manager

3. The File Server - Public Key window appears (Figure 56). The text box on this window contains the Public Key for the Backup File Server. The text is read-only and is populated by the "SSH Public Key" generated internally when the gateway is configured for the first time.

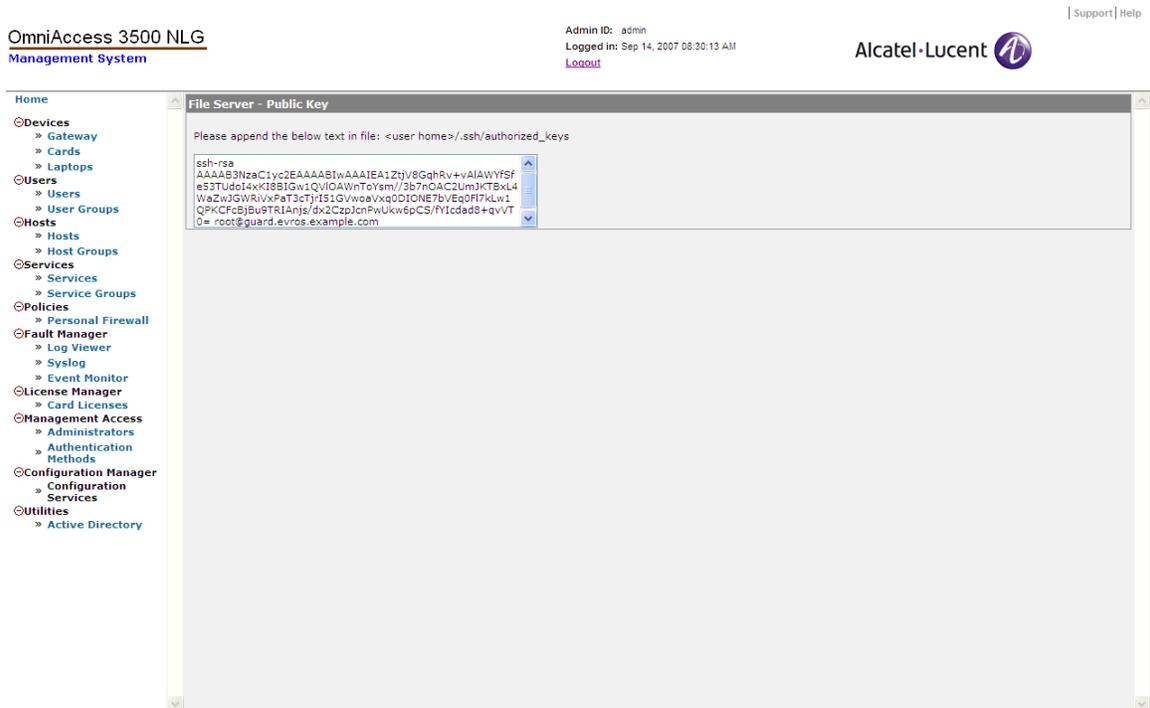


Figure 56 - File Server Public Key

4. Copy the contents of the text box into the “<user home>/ssh/authorized_keys” file on the backup server where the backup files are to be stored.
5. Click **Configuration Services** on the main menu.
6. On the Configuration Manager menu, click **Configuration Server Profile**. The Backup Configuration window appears (Figure 57), where you can set the following parameters for the backup server:
 - Backup File Name: Name assigned to the backup file, where all of the configuration settings are saved.
 - Primary Server IP Address: IP address of the first server where the backup file is uploaded.
 - Primary Server Username: Login account on Server 1 where the backup file is stored.
 - Primary Server Path: Directory path where the backup file is stored when uploaded to Server 1.
 - Secondary Server IP Address: IP address of a second server where the backup file may be uploaded.
 - Secondary Server Username: Login account on Server 2 where the backup file may be stored.
 - Secondary Server Path: Directory path where the backup file is stored if it is uploaded to Server 2.
 - Start Time (hh:mm:ss): Reference start time for periodic backups (the mm/dd/yyyy portion, combined with the Backup Frequency value, determines

the mm/dd/yyyy value for all future backups; the hh:mm:ss portion is also the hh:mm:ss value for all future backups).

- Backup Frequency: Frequency of generation and uploading of configuration backups.

7. Click Save to save the backup settings.

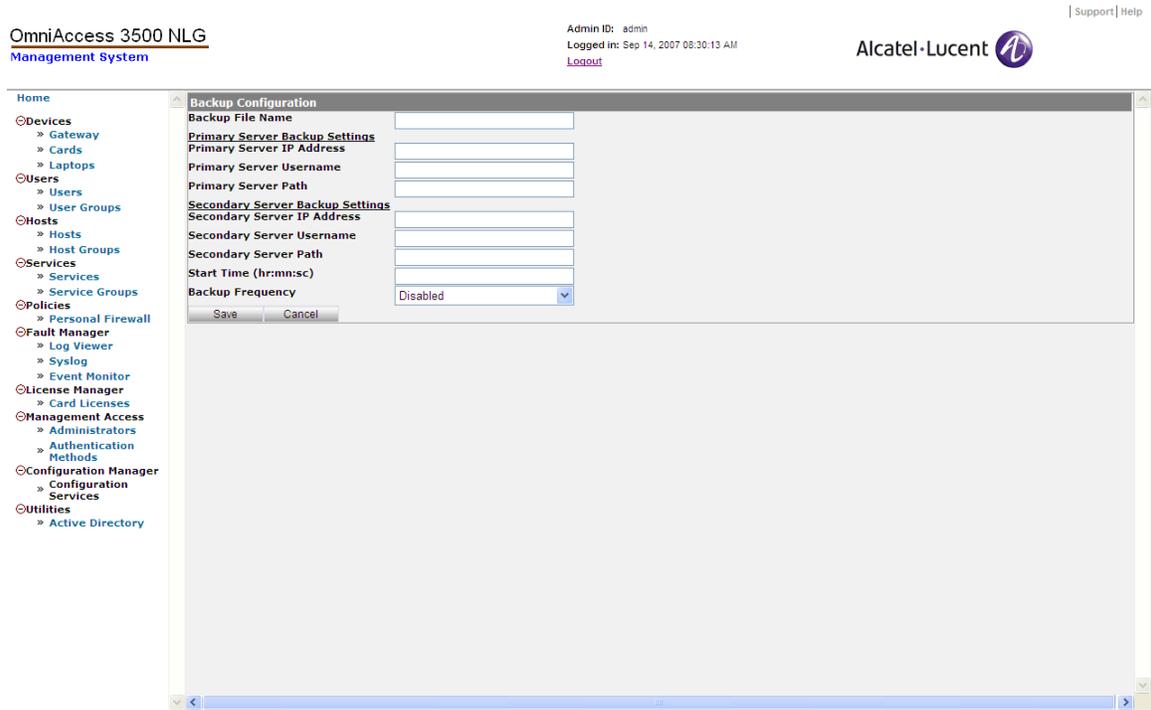


Figure 57 - Backup Configuration (Periodic Backup)

8. To start an immediate backup instead of waiting for a periodic one, click **Configuration Services** on the main menu and then click **Backup Current Configuration**. The Backup Configuration window appears (Figure 58), showing read-only information that you previously entered.

OmniAccess 3500 NLG Management System

Admin ID: admin
Logged in: Sep 14, 2007 08:30:13 AM
[Logout](#)

| Support | Help

Alcatel-Lucent

Home

- ⊖ Devices
 - Gateway
 - Cards
 - Laptops
- ⊖ Users
 - User Groups
- ⊖ Hosts
 - Hosts
 - Host Groups
- ⊖ Services
 - Services
 - Service Groups
- ⊖ Policies
 - Personal Firewall
- ⊖ Fault Manager
 - Log Viewer
 - Syslog
 - Event Monitor
- ⊖ License Manager
 - Card Licenses
- ⊖ Management Access
 - Administrators
 - Authentication Methods
- ⊖ Configuration Manager
 - Configuration Services
- ⊖ Utilities
 - Active Directory

Backup Configuration

Backup File Name

Primary Server IP Address

Primary Server Username

Primary Server Path

Secondary Server IP Address

Secondary Server Username

Secondary Server Path

Start Time (hr:min:sec)

Backup Frequency

Backup Status

Figure 58 - Backup Configuration (Immediate Backup)

9. Click **Start Backup** to start the backup procedure immediately.

Restoration Procedure

The restoration procedure consists of the following steps:

1. Click **Configuration Services** on the main menu.
2. Click **Restore Previous Configuration**. The Configuration Restore - Step 1 window appears (Figure 59).
3. From the drop-down list, select the IP address for the backup server from which to download the backed-up configuration. *Note: The IP addresses that appear are taken from the values you entered previously in the Backup Configuration window (Figure 57).*

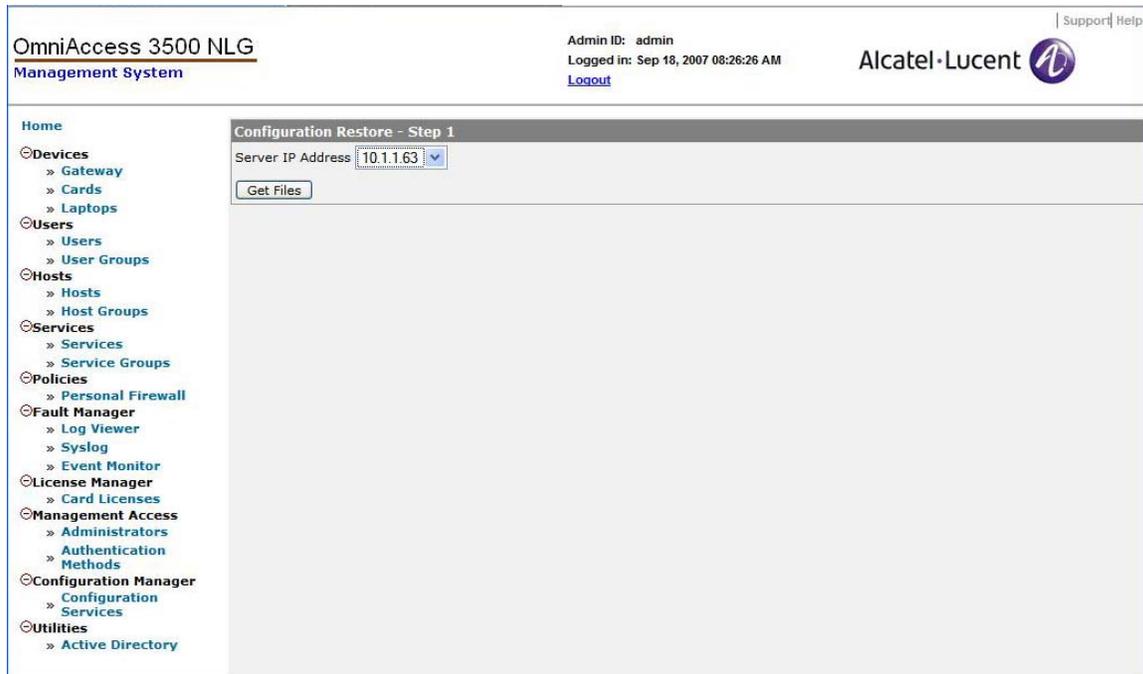


Figure 59 - Configuration Restore - Step 1

4. Click Get Files. The Configuration Restore - Step 2 window appears (Figure 60).

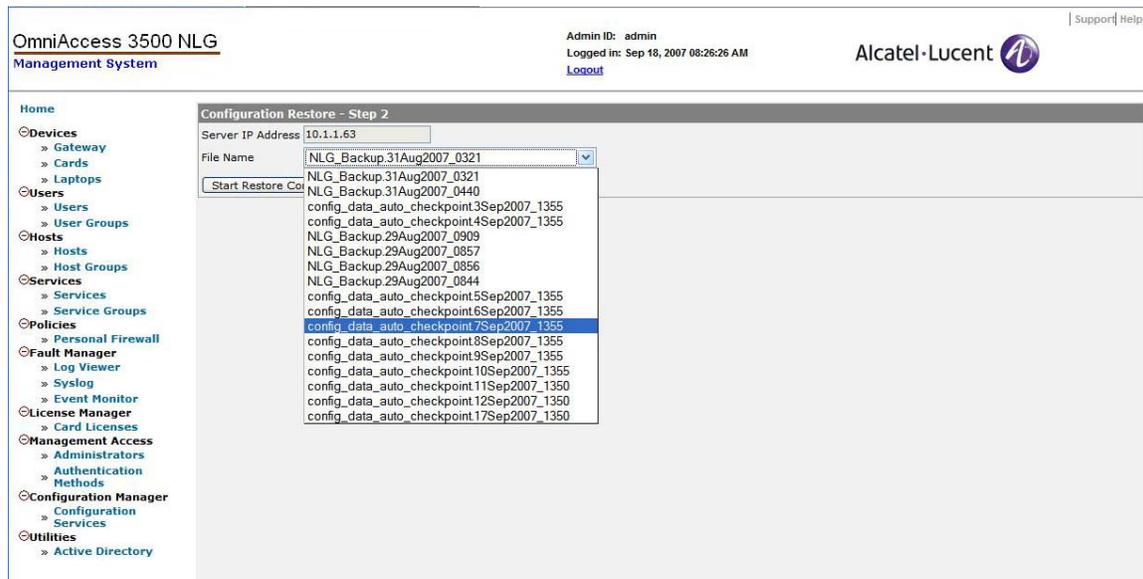


Figure 60 - Configuration Restore - Step 2

5. This window displays the backup files available to restore the configuration. Select a backup file and click **Start Restore Configuration**. The corresponding configuration is automatically restored. Once the restore is done, refresh the page, and log in again to see the restored configuration.

Upgrading the OmniAccess 3500 NLG Gateway Configuration

The procedure in this section describes how to upgrade the software package running on your OmniAccess 3500 NLG gateway.

Configuration Upgrade

The following steps are required for upgrading the OmniAccess 3500 NLG software package that runs on the gateway appliance:

1. Click **Configuration Services** on the main menu.
2. Click **Upgrade Server Profile**. The Configure Upgrade Profile (New) window appears (Figure 61) where you can set the following configuration parameters for the gateway:
 - Server Name: IP address of the Package Distribution Server where the upgrade package is stored.
 - User Name: The user name used to access the Package Distribution Server.
 - Package Name: The name of the package that contains all information needed for the upgrade.
 - Path: The path where the package is stored in the Package Distribution Server.

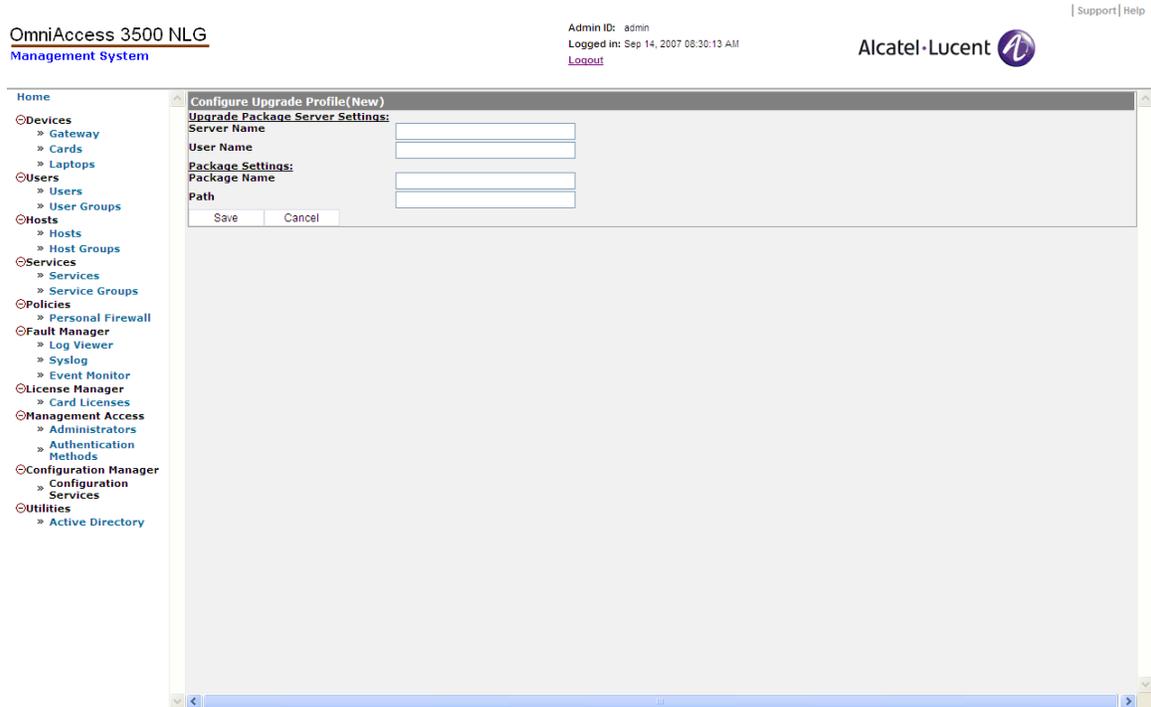


Figure 61 - Configure Upgrade Profile (New)

3. Click **Save** to save the parameters.
4. Click **Configuration Services** on the main menu.

5. Click **Upgrade Actions**. The Upgrade Actions window appears (Figure 62), displaying information about the upgrade, as well as upgrade status information.

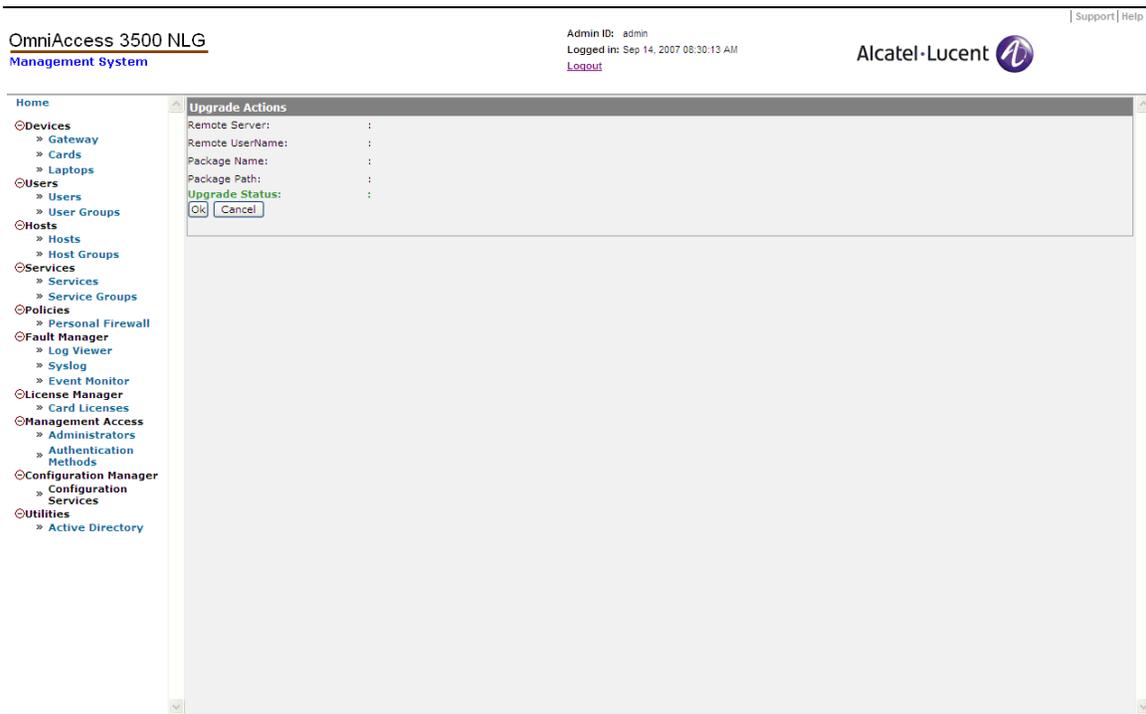


Figure 62 - Upgrade Actions

6. Click **Start Upgrade** to begin the configuration upgrade process. The **Start Upgrade** button appears only if an upgrade is possible (that is, if you have previously saved the configuration upgrade parameters on the Upgrade Server Profile window).

Connectivity will be lost during the upgrade as all processes are temporarily shut down. After the upgrade completes, connectivity will become available again. If an error occurs during the upgrade process, the previous software package will be used.

Note: After the upgrade starts, an **Abort** button appears. Click this button to stop the upgrade. To start the upgrade again, click **Configuration Services** on the main menu and then click **Reset Upgrade Setting**. This changes the upgrade status back to an idle state. The upgrade can then be re-attempted.

7. If a "Failed" message appears in the Upgrade Status field on the Upgrade Actions window, click **Configuration Services** on the main menu, then click **Reset Upgrade Setting**. This changes the upgrade status back to an idle state. The upgrade can then be re-attempted.

Chapter 5. OmniAccess 3500 NLG Administrative Information Base

This chapter presents the complete set of objects that can be observed and configured through the management system GUI.

Every object that is not a leaf in the management system GUI information base tree is presented in the following format:

- **Object Name** – [Path], [Window Title], [Action(s)]

Where:

- **Object Name** is the name of the object on display.
- [Path] is the list of consecutive GUI selections that lead to the information on display. An underlined path segment indicates that the corresponding object must be checked (✓) on the GUI window before clicking on the path segment that immediately follows.
- [Window Title] is the title shown on the window when the information is displayed.
- [Action(s)] is the type of action allowed on the object being displayed. Possible values are <r> (for read-only), <rw> (for read and write), and <x> (for execute, in the case of displayed objects that represent functions and not data).

The objects are presented below in the same order as they appear in the main menu of the management system GUI, from top to bottom.

Devices

The Devices section of the management system GUI provides access to the network nodes: gateways, cards, and laptops.

- **Gateway** – [Gateway], [Gateway Settings], [r]

In the OmniAccess 3500 NLG R1.2, each management system instance only controls the OmniAccess 3500 NLG gateway where it is installed. The Gateway Settings window lists the configuration parameters for the gateway where the management system software is installed.

The following parameters can be edited for the gateway upon selection of the <Edit Gateway Settings> option:

- **Gateway FQDN** – Fully Qualified Domain Name (FQDN) of the gateway.
- **WAN Interface IP** – IP address assigned to the WAN Ethernet interface of the gateway. The WAN interface is connected to a public subnet.
- **WAN Interface Netmask** – Network mask for identification of the public subnet of attachment of the WAN gateway interface.
- **WAN Interface Next-hop Router** – IP address of the next-hop-router within the public subnet of attachment of the WAN gateway interface.

- **LAN Interface IP** – IP address assigned to the LAN Ethernet interface of the gateway. The LAN interface is connected to a private subnet of the enterprise.
- **LAN Interface Netmask** – Network mask for identification of the private subnet of attachment of the LAN gateway interface.
- **LAN Interface Next-hop Router** – IP address of the next-hop-router within the private subnet of attachment of the LAN gateway interface (the next-hop router, or default gateway, should not be confused with the OmniAccess 3500 NLG gateway itself).
- **LAN Interface Secondary IP** – VPN address of the gateway, associated with the LAN:1 virtual interface. The VPN address is used by cards and laptops to communicate with the gateway (and vice versa) through the IPsec tunnel. It is included in the inner IP header of the packets exchanged by the gateway with the card and laptop over the IPsec tunnel. This entry must be filled with one IP address when the gateway is first configured. Later on, any modification of the VPN IP address of the gateway must be executed on the <GUARD_PRIVATE_IP> server type of the [Gateway Configure-> Server Table Information] window, reachable through the [Gateway|Configure Advanced Settings|Server Table] path.
- **LAN Interface Secondary Netmask** – Network mask for the private subnet of attachment of the LAN:1 virtual interface of the gateway.
- **Root Password** – Password for the root account on the OmniAccess 3500 NLG gateway.
- **Confirm Password** – Confirmation replica of the root account password.
- **Active Directory Server IP** – IP address of the Active Directory server used by the enterprise for authentication of the laptop users.
- **User Authentication Type** – The method used for authentication of the end users. Possible values are <DOMAIN>, <RADIUS-LAX>, and <RADIUS-STRIC>. If <DOMAIN> is selected, all users will be authenticated using KDC. If <RADIUS-LAX> or <RADIUS-STRIC> is selected, a RADIUS server will authenticate all users. More specifically, with <RADIUS-LAX> the user's laptop obtains its network parameters before submission of the authentication credentials by the end user. With <RADIUS-STRIC>, instead, the network parameters will only be granted after success of the RADIUS authentication.
- **Radius IP Address** – The IP address of the RADIUS server being used for authentication.
- **Radius Port** –The destination port for authentication requests.
- **Radius Secret** –The authentication and encryption key for all RADIUS communications between the gateway and the RADIUS server.
- **Kerberos Realm**– KDC domain of the OmniAccess 3500 NLG gateway. The KDC domain name is the same as the enterprise domain name, but must be written in uppercase letters.
- **KDC FQDN** – Fully Qualified Domain Name (FQDN) of the Active Directory server.

- **Admin Server** – Administration server for the enterprise domain; in most cases the administration server coincides with the Active Directory server, except when the KDC realm administrator has not made the administration server name available through DNS.
- **Primary DNS** – IP address of the primary DNS name server for laptop user traffic. This entry must be filled with one IP address when the gateway is first configured. Later on, any modification of the primary DNS name server address must be executed on the [Gateway Configure-> Server Table Information] window, reachable through the [Gateway|Configure Advanced Settings|Server Table] path.
- **Secondary DNS** – IP address of the secondary DNS name server (optional). This entry must be filled with one IP address when the gateway is first configured. Later on, any modification of the secondary DNS name server address must be executed on the [Gateway Configure-> Server Table Information] window, reachable through the [Gateway|Configure Advanced Settings|Server Table] path.
- **Primary NTP Server** – IP address of the Network Time Protocol (NTP) server used by the OmniAccess 3500 NLG gateway for time synchronization. Since the time on the OmniAccess 3500 NLG gateway is critically bound to the time on the Active Directory server, the Active Directory server typically acts as the primary NTP server for the OmniAccess 3500 NLG gateway.
- **Secondary NTP Server** – IP address of the secondary NTP server (optional).
- **SMTP Access Type** – Settings for the Simple Mail Transfer Protocol (SMTP) server used for the exchange of emails to and from the OmniAccess 3500 NLG gateway. The gateway uses emails (transmitted as SMS text messages over the 3G wireless network) to wake up dormant cards when urgent remote management tasks are due. The options for the SMTP Access Type are <Direct>, <Login>, and <TLS>. The <Direct> option enables access to the SMTP server without submission of a <login, password> pair. The <Login> option requires instead the submission of the <login, password> pair. The <TLS> option (for Transport Layer Security) requires the <login, password> submission and encrypts the communication between the gateway and the SMTP server.
- **SMTP Server** – IP address of the SMTP server.
- **SMTP Port** – Number of the port used by the mail server to listen for e-mail requests. The port number is typically <25>, but the administrator can change it for security purposes.
- **Mail From** – Email address used in the 'From' field of the SMS messages sent to wake up the dormant cards.
- **Mail Domain** – Domain within which all email addresses used for SMS messaging are exchanged.
- **SMTP Login** – Login name assigned to the OmniAccess 3500 NLG gateway for its email account with the SMTP server.
- **SMTP Password** – Password associated with the email account of the OmniAccess 3500 NLG gateway with the SMTP server.

- **Confirm Password** – Confirmation replica of the SMTP password.
- **SNMP Enable** – The OmniAccess 3500 NLG gateway offers MIB-II support for its native functional components (i.e., components that are not part of the OmniAccess 3500 NLG platform). If the <SNMP Enable> option is set, it is possible to use a third-party network management system to manage and monitor the MIB-II objects of the gateway through SNMP.
- **Port Number** – Port over which the third-party network-management system can exchange get and set SNMP messages with the OmniAccess 3500 NLG gateway for retrieving and setting the values of the MIB-II objects. The port number is typically 161, but the administrator can change it for security purposes.
- **Trap Port Number** – Port over which the third-party network management system can receive the trap messages generated by the OmniAccess 3500 NLG gateway. The port number is typically 162, but the administrator can change it for security purposes.
- **Read Community** – This string is used for SNMP authentication and works like a password that any remote SNMP client must use when accessing objects of the gateway MIB in read-only mode.
- **Confirm Read Community** – Confirmation replica of the read community string.
- **Read-Write Community** – This string is used for SNMP authentication and works like a password that any remote SNMP client must use when accessing objects of the gateway MIB in read-write mode. It is recommended to setup different values for the read community string and for the read-write community string.
- **Confirm Read-Write Community** – Confirmation replica of the read-write community string.
- **HTTPS Port** – The port on which you can securely access the management system GUI from a web browser. The default value is <443>, in which case you don't have to specify the port in the URL. If you set a different port, you will have to use the port number in the URL while accessing the management system. For example, if you specify the HTTPS port as <8443>, and the address of the LAN interface (accessible from within the enterprise network) is <10.1.1.1>, then you can open the management system GUI by typing the following URL in the address box of your browser: <https://10.1.1.1:8443>.
- **Card Address Range** – IP address pool for assignment to the cards when they connect to the gateway. This entry must be filled with one address range when the gateway is first configured. Later on, the editing of the initial card address range or the introduction of new address ranges must be executed on the [Gateway Configure-> Address Pool Information] window, reachable through the [Gateway|Configure Advanced Settings|Address Pool] path.
- **Card Address Mask** – Network mask for identification of the card address pool set upon initial configuration of the gateway.
- **Laptop Address Range** – IP address pool for assignment to the laptop when the corresponding Card connects to the gateway. This entry must be filled with one

address range when the gateway is first configured. Later on, the editing of the initial card address range or the introduction of new address ranges must be executed on the [Gateway Configure-> Address Pool Information] window, reachable through the [Gateway|Configure Advanced Settings|Address Pool] path.

- **Laptop Address Mask** – Network mask for identification of the laptop address pool set upon initial configuration of the gateway.
- **Gateway Certificate ID Type** – Type of identifier for the digital certificate that is used by the OmniAccess 3500 NLG gateway for mutual authentication with the OmniAccess 3500 NLG cards. Options available (choose one): <EMAIL>, <FQDN>, <DN>. This entry must be set when the gateway is first configured. Later on, the setting of the Gateway Certificate ID Type (possibly with a different value than the initial one) must be executed on the [Connection Manager Tunnel Table (Add)] window, reachable through the [Gateway|Configure Advanced Settings|Tunnel Table|New] path.
- **Gateway Certificate ID** – Identifier of the certificate that the OmniAccess 3500 NLG gateway uses for mutual authentication with the OmniAccess 3500 NLG cards. This entry must be set when the gateway is first configured. Later on, the setting of the Gateway Certificate ID (possibly with a different value than the initial one) must be executed on the [Connection Manager Tunnel Table (Add)] window, reachable through the [Gateway|Configure Advanced Settings|Tunnel Table|New] path. *Please note that this parameter is case-sensitive.*

OmniAccess 3500 NLG Management System

Admin ID: admin
Logged in: Sep 14, 2007 10:27:01 AM
Logout

Alcatel-Lucent

Home

- ⊖ Devices
 - Gateway
 - Cards
 - Laptops
- ⊖ Users
 - Users
 - User Groups
- ⊖ Hosts
 - Hosts
 - Host Groups
- ⊖ Services
 - Services
 - Service Groups
- ⊖ Policies
 - Personal Firewall
- ⊖ Fault Manager
 - Log Viewer
 - Syslog
 - Event Monitor
- ⊖ License Manager
 - Card Licenses
- ⊖ Management Access
 - Administrators
 - Authentication Methods
- ⊖ Configuration Manager
 - Configuration Services
- ⊖ Utilities
 - Active Directory

Gateway Configurations (Edit)

Gateway FQDN	guard.evros.example.com
WAN Interface IP	204.178.22.108
WAN Interface Netmask	255.255.255.0
WAN Interface Next-Hop Router	204.178.22.97
LAN Interface IP	10.1.1.1
LAN Interface Netmask	255.255.255.0
LAN Interface Next-Hop Router	10.1.1.30
LAN Interface Secondary IP	10.1.1.11
LAN Interface Secondary Netmask	255.255.255.0
Root Password	*****
Confirm Password	*****
Active Directory Server IP	10.1.1.20
User Authentication Type	DOMAIN
Radius Authentication Settings:	
Radius IP Address	
Radius Port	
Radius Secret	
Kerberos configuration	
Kerberos realm	EVROS.EXAMPLE.COM
KDC FQDN	kdc.evros.example.com
Admin Server	kdc.evros.example.com
DNS Settings:	
Primary DNS	10.1.1.20
Secondary DNS	
NTP Server Settings:	
Primary NTP Server	10.1.1.20
Secondary NTP Server	
SMTP Settings:	
SMTP Access Type	TLS
SMTP Server	209.85.129.109
SMTP Port	25
Mail From	evros.project@gmail.com
Mail Domain	mail.com

Figure 63 - Gateway Configurations (Edit)

The following gateway information objects can be accessed upon selection of the <Configure Advanced Settings> tab:

- **Connection Manager - Settings** – [Gateway| Configure Advanced Settings], [Configure:], [r]

Objects needed for configuration of the remote access connections.

- **Address Pool** – [Gateway| Configure Advanced Settings| Gateway Configure:-> Address Pool Information], [rw]

Sets of IP addresses from which the OmniAccess 3500 NLG gateway draws the pair of VPN addresses that it assigns to the OmniAccess 3500 NLG card and associated laptop upon establishment of the IPsec tunnel. The addresses for the card and for the laptop are drawn from different, disjoint sets. Multiple sets can be assigned to the cards (Card sets) and to the laptops (Laptop sets). The address sets are expressed in the format <IP address>, <Netmask>, as in <10.1.1.1>, <255.255.255.0>. The <IP Address> value can also be expressed as a range (as in <10.1.1.1 - 10.1.1.255>) or as a host (as in <10.1.1.1/24>). The <Netmask> value must be specified in all cases. The <Type> value designates the assignment of the IP address set to the OmniAccess 3500 NLG cards (<Card>) or to the laptops (<Laptop>).

Each address pool requires the configuration of the following set of parameters:

- ◆ **IP Address** – The IP address from which the gateway draws the pair of VPN addresses it assigns to the card and to the laptop upon establishment of the IPsec tunnel.
- ◆ **Netmask(x.x.x.x)** – The Netmask address used to designate the IP subnet from which the gateway draws the pair of VPN addresses it assigns to the card and to the laptop upon establishment of the IPsec tunnel.
- ◆ **Type** – Select <Card> or <Laptop> from the drop-down menu.

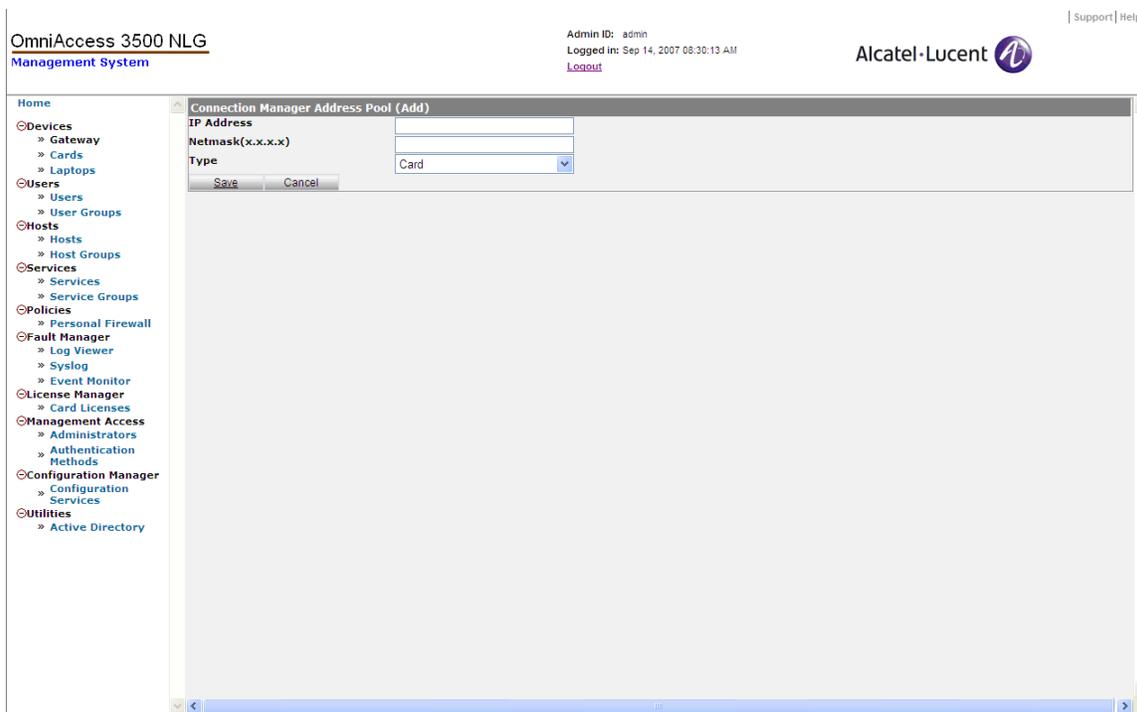


Figure 64 - Connection Manager Address Pool (Add)

- **Server Table** — [Gateway|Configure Advanced Settings|Server Table], [Gateway Configure:-> Server Table Information], [rw]

Configuration of the DNS, WINS, and default gateway addresses that the OmniAccess 3500 NLG gateway passes to the card and laptop together with the VPN addresses. Only one value can be set for each type of address.

- ◆ **Type** — Network server for which the IP address is specified. Options (choose one): <DNS> (DNS server), <WINS> (WINS server), and <GUARD_PRIVATE_IP> (IP address of the LAN:1 virtual interface of the gateway).
- ◆ **Primary IP Address** — IP address of the first network server being configured.
- ◆ **Secondary IP Address** — IP address of the second network server being configured.

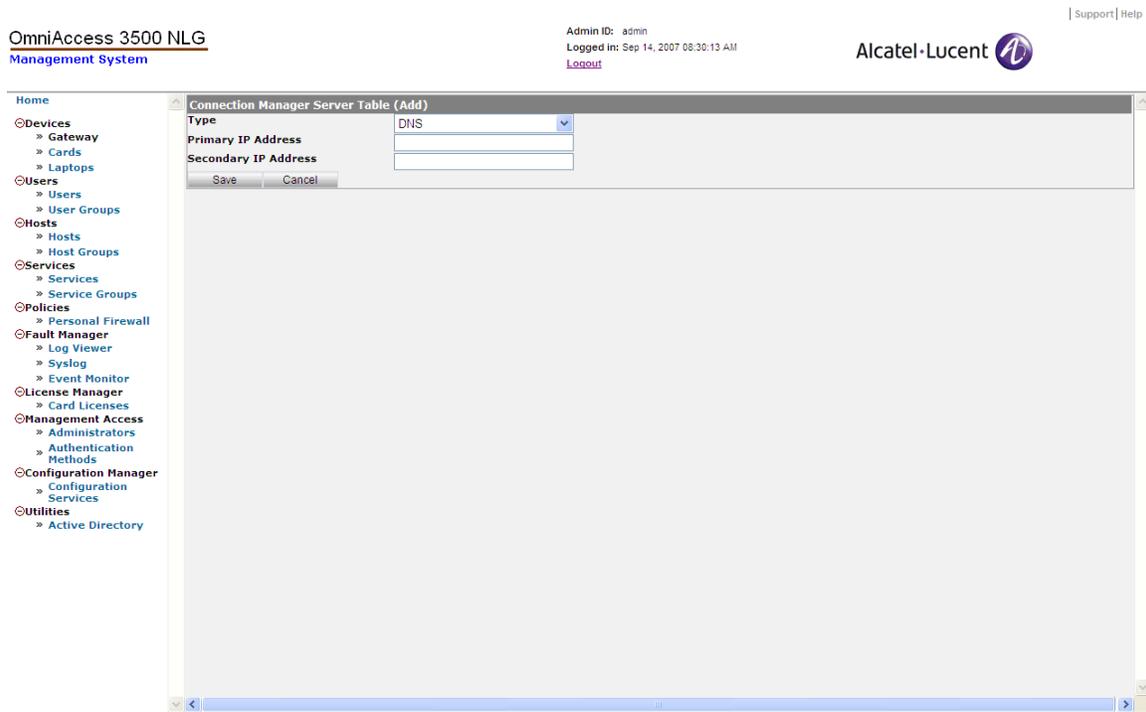


Figure 65 - Connection Manager Server Table (Add)

- **Rules** – [Gateway|Configure Advanced Settings|Rules], [Gateway Configure:-> Rule Information], [rw]

Packet classification rules for the firewall and IPsec endpoint that are embedded in the OmniAccess 3500 NLG gateway.

The embedded firewall can be used to restrict the network traffic that the OmniAccess 3500 NLG gateway exchanges over its interfaces, assuming the function of an enterprise firewall in a network where an enterprise firewall is not already deployed. The firewall rules may or may not be associated with existing IPsec tunnels.

The embedded IPsec endpoint handles the requests to open IKEv2 and IPsec security associations that the OmniAccess 3500 NLG cards originate from their current locations. The OmniAccess 3500 NLG gateway uses the IPsec endpoint rules to match incoming IKEv2 requests with sets of IKEv2/IPsec parameters to be used in the configuration of the security associations that may result from the negotiations.

Each rule requires the configuration of the following set of parameters:

- ◆ **Precedence** – Rule precedence with respect to other rules defined in the same context. The priority of the rule is higher with a higher precedence value. The highest-precedence rule that matches a packet is the rule that defines how the packet is handled.
- ◆ **Type** – Rule type, to be chosen among <Pass> (accept all packets matching the rule), <Drop> (drop all packets matching the rule), and

<Reject> (drop all packets matching the rule, and for each dropped packet notify the corresponding sender).

- ◆ **Protocol** – Protocol Identifier value carried by the packets that match the rule. Options (choose one): <ANY>, <TCP>, <UDP>, <ICMP>.
- ◆ **Source IP/[Mask]** – Range of IP addresses to be checked against the source IP field in the packet header.
- ◆ **Source Port Low, Source Port High** – Range of port values to be checked against the source port field in the packet header.
- ◆ **Destination IP/[Mask]** – Range of IP addresses to be checked against the destination IP field in the packet header.
- ◆ **Destination Port Low, Destination Port High** – Range of port values to be checked against the destination port field in the packet header.
- ◆ **Interface Name** – Network interface on the OmniAccess 3500 NLG gateway where the packet filter rule applies. For the target interface, the name must be consistent with the interface labels on the gateway's back panel (<WAN> and <LAN>).
- ◆ **Local Stack Direction** – Packet direction with respect to the local IP stack of the OmniAccess 3500 NLG gateway. Options (choose one): <ANY> (the rule applies to traffic in any direction), <From> (the rule only applies to traffic from the local IP stack, i.e., outgoing traffic), <To> (the rule only applies to traffic to the local IP stack, i.e., incoming traffic).
- ◆ **Tunnel Direction** – This object enables the association of the packet classification rule with a tunnel profile. Options (choose one): <None> (no tunnel is to be associated with the rule, which is therefore strictly a packet filtering rule), <To Tunnel> (packets matching the rule are dispatched through an IPsec tunnel whose profile is identified by the <To Tunnel> value; if an existing IPsec tunnel is not found for a matching packet, the IPsec tunnel is created before the packet is delivered), <From Tunnel> (packets matching the rule are received from an IPsec tunnel whose profile is identified by the <From Tunnel> value; if a remote request to open an IPsec tunnel is received on a packet whose header matches the rule, the OmniAccess 3500 NLG gateway uses the tunnel profile specified in the <From Tunnel> value to conduct the subsequent negotiations).
- ◆ **To Tunnel** – Name of the tunnel profile for the IPsec tunnel that dispatches the matching packet.
- ◆ **From Tunnel** – Name of the tunnel profile for the IPsec tunnel over which the matching packet is received.

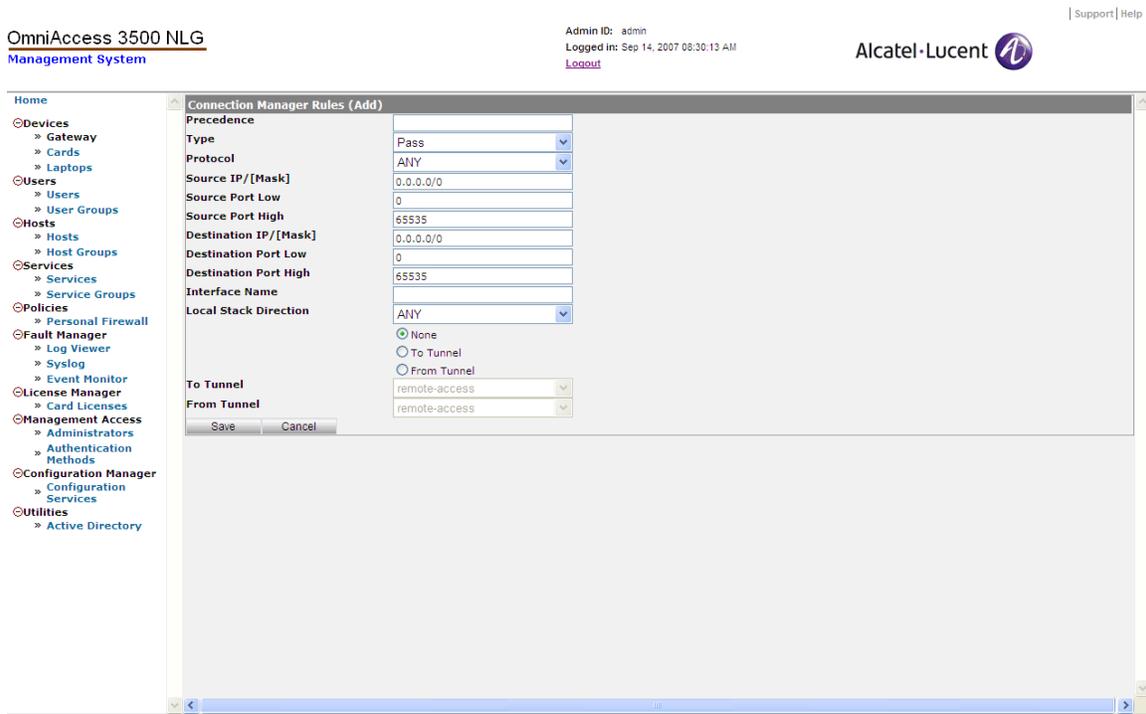


Figure 66 - Connection Manager Rules (Add)

- **Tunnel Table** — [Gateway|Configure Advanced Settings|Tunnel Table], [Gateway Configure:-> Tunnel Table], [rw]

List of profiles used to define the parameters of the IKE and IPsec Security Associations that are created either by the OmniAccess 3500 NLG gateway (<To Tunnel> option in the Rule definition) or by request of the OmniAccess 3500 NLG cards (<From Tunnel> option in the Rule definition).

- ◆ **Name** — Name of the tunnel profile.
- ◆ **Identity Type** — Type of identifier used to designate the local tunnel endpoint (residing on the OmniAccess 3500 NLG gateway) in the security association negotiations. Options (choose one): <EMAIL> (email address, as in <user@domain.ext>), <FQDN> (Fully Qualified Domain Name, as in <hostname.localdomain.ext.>), <DN> (Distinguished Name, used for identification of an entry in an LDAP directory, as in <dn: cn=John Doe,dc=example,dc=com>, where <cn=John Doe> is the Relative Distinguished Name of the entry and <dc=example,dc=com> is the Distinguished Name of the parent entry).
- ◆ **Identity** — Identity value for the local tunnel endpoint, specified in the format required by the <Identity Type> value.
- ◆ **Algorithms to be used for IPsec Negotiations** — Encryption algorithm to be used on the IPsec tunnel. Options (choose one): <3DES-SHA1>, <AES128-SHA1>, <AES192-SHA1>, <AES256-SHA1>.

- ◆ **Algorithms to be used for IKE Negotiations** – Encryption algorithm to be used for protection of the IKEv2 exchanges. Options (choose one): <3DES-SHA1>, <AES128-SHA1>, <AES192-SHA1>, <AES256-SHA1>.
- ◆ **Lifetime of the IKE SA in seconds** – Maximum duration of the IKEv2 Security Association that controls the IPsec tunnel between the OmniAccess 3500 NLG card and the OmniAccess 3500 NLG gateway.
- ◆ **Lifetime of the IPsec SA in seconds** – Maximum duration of the IPsec Security Association that carries encrypted packets from one end of the secure remote access connection to the other.

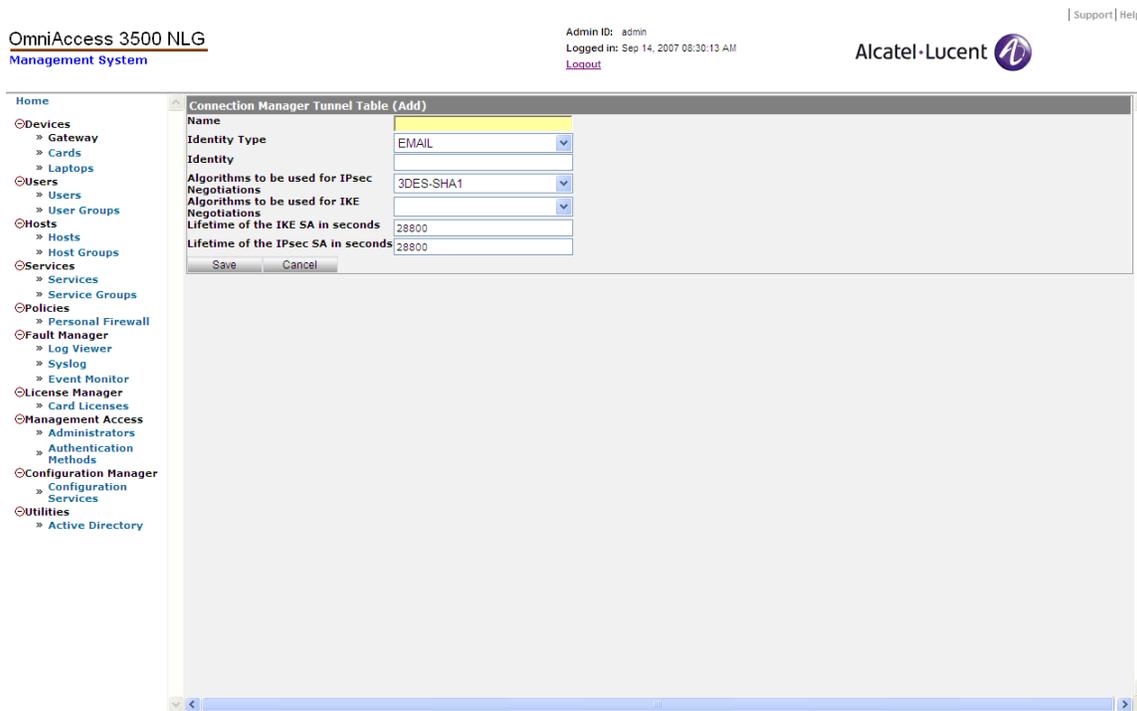


Figure 67 - Connection Manager Tunnel Table (Add)

- **Assisted File Transfer** – [Gateway|Configure Advanced Settings], [Configure:], [r]

Configuration of the OmniAccess 3500 NLG Assisted File Transfer facility for IT applications integrated in the OmniAccess 3500 NLG platform. The OmniAccess 3500 NLG gateway allocates a fixed amount of storage space for each application. The other configuration parameters drive the transport aspects of the file transfer transactions.

- **Application Table** – [Gateway|Configure Advanced Settings|Application Table], [Gateway:-> Application Table Information], [rw]

List of applications that utilize the Assisted File Transfer utility. The following information items are displayed for every application listed: Application Name, Share Path, User Name, Domain Name, Laptop Directory, Laptop Directory Owner, Direction, and Max Disk Space (MB).

- ◆ **Application Name** – Name of the application that will use the Assisted File Transfer facility (e.g., testapp).
- ◆ **Application Password** – Password associated with the application.
- ◆ **Share Path** – Directory path in the application server that leads to the Windows share to be mounted (e.g., //server1/testappdir).
- ◆ **Share User Name** – User name with permission to mount this share.
- ◆ **Share Password** – Password corresponding to this user.
- ◆ **Domain Name** – Domain of the application server that includes the Windows share.
- ◆ **Laptop Directory** – Path of the laptop folder that is created for this application (if it does not already exist).
- ◆ **Laptop Directory Owner** – The domain account to which the ownership of files in this folder should be set. (Currently unused. All files are stored and accessed using the SYSTEM account).
- ◆ **Direction** – Determines if the direction of the contents replication is from the laptop to the enterprise or vice versa.
- ◆ **Maximum Disk Size (MB)** – The maximum size of the folder allocated to the application.
- ◆ **User Groups** – User Groups that the file replication is restricted to. The BROADCAST group includes all user groups.

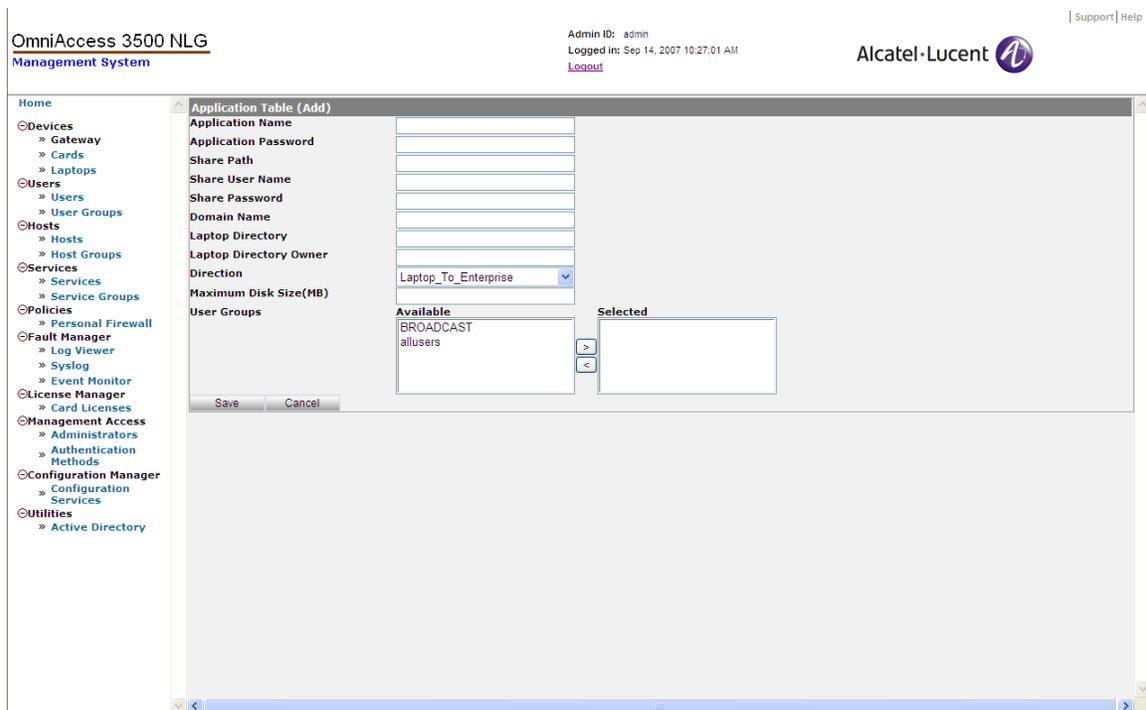


Figure 68 - Application Table Information

- o **Connection Manager - Show Information** — [Gateway|Configure Advanced Settings], [Configure:], [r]

Read-only state information for a number of functional components of the OmniAccess 3500 NLG platform.

- **SA - IKE** — [Gateway|Configure Advanced Settings|SA — IKE], [Gateway:-> SA IKE Information], [r]

List of the IKE Security Associations that currently exist between the OmniAccess 3500 NLG gateway and remotely connected OmniAccess 3500 NLG cards. Each row in the table corresponds to one OmniAccess 3500 NLG card and shows the following information items:

- ◆ **Child SAs** — Number of existing IPsec Security Associations that were established under control of this IKE Security Association.
 - ◆ **Creation Time** — Time of establishment of the IKE Security Association, in the format: <yyyymmddhhmmss>.
 - ◆ **Local IP** — IP address (outer header) of the local endpoint of the IKE Security Association (on the OmniAccess 3500 NLG gateway).
 - ◆ **Remote IP** — IP address (outer header) of the remote endpoint of the IKE Security Association (on the OmniAccess 3500 NLG card).
 - ◆ **Local Identity** — Certificate ID for the local endpoint of the IKE Security Association.
 - ◆ **Remote Identity** — Certificate ID for the remote endpoint of the IKE Security Association.
 - ◆ **Encryption Algorithm** — Algorithm used for the encryption of packets exchanged over the IKE Security Association.
 - ◆ **Hash Algorithm** — Algorithm used for the exchange of credentials over the IKE Security Association.
- **SA - IPsec** — [Gateway|Configure Advanced Settings|SA - IPsec], [Gateway:-> SA IPsec Information], [r]

List of the IPsec Security Associations that currently exist between the OmniAccess 3500 NLG gateway and remotely connected OmniAccess 3500 NLG cards. Each row in the table corresponds to one OmniAccess 3500 NLG card (i.e., one IPsec tunnel, consisting of two IPsec security associations) and shows the following information items:

- ◆ **Local IP** — IP address (outer header) of the local endpoint of the IPsec tunnel (on the OmniAccess 3500 NLG gateway).
- ◆ **Remote IP** — IP address (outer header) of the remote endpoint of the IPsec tunnel (on the OmniAccess 3500 NLG card).
- ◆ **ESP SPI-In** — Security Parameter Index (SPI) found in incoming IPsec packets with ESP protection (not available with AH protection).
- ◆ **ESP SPI-Out** — Security Parameter Index inserted in outgoing IPsec packets with ESP protection (not available with AH protection).

- ◆ **AH SPI-In** – Security Parameter Index found in incoming IPsec packets with AH protection (not available with ESP protection).
 - ◆ **AH SPI-Out** – Security Parameter Index inserted in outgoing IPsec packets with AH protection (not available with ESP protection).
 - ◆ **Algorithm Cipher** – Algorithm used for the encryption of packets exchanged over the IPsec tunnel.
 - ◆ **Algorithm Hash** – Algorithm used for the exchange of credentials over the IPsec tunnel.
- **Flows** – [Gateway|Configure Advanced Settings|Flows], [Gateway:->Flows], [r]

List of the objects that the OmniAccess 3500 NLG gateway instantiates for stateful packet inspection purposes. When a packet arrives at the firewall embedded in the OmniAccess 3500 NLG gateway, the firewall first tries to match it with a previously established flow object. If no matching flow object is found, the firewall tries to match the packet with one of its configured rules. If one or more matches are found, a new flow object is created according to the matching rule with the highest precedence. If no matching rule is found, the default rule (drop) is applied to the packet and no new flow is created. Each row in the table corresponds to one stateful-inspection flow object and shows the following information items:

- ◆ **Idle Time** – Time elapsed since the last packet associated with the flow was received (in seconds).
 - ◆ **IP Protocol** – IP-encapsulated protocol of the connection associated with the flow object. Some of the possible values are <TCP>, <UDP>, <ESP>, <AH>.
 - ◆ **Source IP** – Source IP Address (outer IP header) identifying the flow object.
 - ◆ **Source Port** – Source Port (if protocol is TCP or UDP) identifying the flow object.
 - ◆ **Dest. IP** – Destination IP Address (outer IP header) identifying the flow object.
 - ◆ **Dest. Port** – Destination Port (if protocol is TCP or UDP) identifying the flow object.
 - ◆ **Rule Index** – Internal identifier of the rule that originated the flow object.
- **Global Information** – [Gateway|Configure Advanced Settings|Global Information], [Gateway: -> Global Information], [r]

List of statistics collected since the OmniAccess 3500 NLG gateway was last restarted and current status indicators.

- ◆ **Active IKE SAs** – Number of IKE Security Associations that are currently active.

- ◆ **Total No. of IKE nego done** – Number of IKE negotiations successfully completed since the OmniAccess 3500 NLG gateway was last restarted.
- ◆ **Total No. of IKE nego failed** – Number of IKE negotiations failed since the OmniAccess 3500 NLG gateway was last restarted.
- ◆ **No. of Phase-1 Initiator SA's** – Number of Phase-1 negotiations initiated by the OmniAccess 3500 NLG gateway since it was last restarted.
- ◆ **No. of Phase-1 Responder SA's** – Number of Phase-1 negotiations initiated by a remote OmniAccess 3500 NLG card since it was last restarted.
- ◆ **No. of Active IPsec SA's** – Number of IPsec Security Associations that are currently active.
- ◆ **No. of Quick Mode nego done** – Number of successful negotiations for the creation of an IPsec Security Association since the OmniAccess 3500 NLG gateway was last restarted.
- ◆ **No. of Quick Mode nego failed** – Number of failed negotiations for the creation of an IPsec Security Association since the OmniAccess 3500 NLG gateway was last restarted.
- ◆ **No. of Bytes received** – Number of bytes received by the OmniAccess 3500 NLG gateway since it was last restarted.
- ◆ **No. of Bytes sent** – Number of bytes transmitted by the OmniAccess 3500 NLG gateway since it was last restarted.
- ◆ **No. of Bytes Forwarded** – Number of bytes forwarded from one interface to another since the OmniAccess 3500 NLG gateway was last restarted.
- ◆ **No. of Packets Received** – Number of packets received by the OmniAccess 3500 NLG gateway since it was last restarted.
- ◆ **No. of Packets Sent** – Number of packets transmitted by the OmniAccess 3500 NLG gateway since it was last restarted.
- ◆ **No. of Packets Forwarded** – Number of packets forwarded from one interface to another since the OmniAccess 3500 NLG gateway was last restarted.
- ◆ **No. of Packets Dropped** – Number of packets dropped at the OmniAccess 3500 NLG gateway since it was last restarted.
- ◆ **No. of Active flows** – Number of currently allocated stateful-inspection flow objects.
- ◆ **No. of Free flows** – Number of stateful-inspection flow objects that the OmniAccess 3500 NLG gateway can still allocate.
- ◆ **No. of Total flows** – Number of stateful-inspection flow objects allocated since the OmniAccess 3500 NLG gateway was last restarted.
- ◆ **No. of Active transforms** – Number of IPsec transforms (either ESP or AH) currently allocated.

- ◆ **No. of Free transforms** – Number of IPsec transforms (ESP or AH) that the OmniAccess 3500 NLG gateway can additionally allocate.
- ◆ **No. of Total transforms** – Number of IPsec transforms (ESP or AH) allocated by the OmniAccess 3500 NLG gateway since it was last restarted.
- ◆ **No. of Active rules** – Number of rules that are currently active.
- ◆ **No. of Free rules** – Number of rules that the OmniAccess 3500 NLG gateway can additionally allocate.

The following fields appear upon selection of the <**File upload**> menu item:

- **Gateway Configuration File Upload** – [Gateway|Configure Advanced Settings|File Upload], [Gateway -> File Upload], [rw]
 - **Keytab File** – File containing the credentials of the gateway for authentication with the Active Directory server. The file must necessarily be uploaded to the gateway before any interaction with the Active Directory (AD) infrastructure can start. This includes the case where the method used for authentication of one or more user groups changes from RADIUS to AD.
 - **CA Certificate** – Digital certificate of the Certificate Authority (CA), which includes the CA's public key and digital signature. The same CA certificate is installed in the OmniAccess 3500 NLG cards.
 - **CA Certificate Revocation List** – List of certificates issued by the Certificate Authority that have been revoked before their natural expiration.
 - **Gateway Certificate** – Certificate (public key) of the gateway, used by peer network nodes for encryption of the messages they send to the gateway.
 - **Gateway Private Key** – Secret key used by the gateway to decrypt the messages it receives from peer network nodes (including the OmniAccess 3500 NLG cards).

OmniAccess 3500 NLG Management System

Admin ID: admin
 Logged in: Sep 14, 2007 08:30:13 AM
[Logout](#)

| Support | Help

Alcatel-Lucent

Home

- ⊖ Devices
 - Gateway
 - Cards
 - Laptops
- ⊖ Users
 - User Groups
- ⊖ Hosts
 - Hosts
 - Host Groups
- ⊖ Services
 - Services
 - Service Groups
- ⊖ Policies
 - Personal Firewall
- ⊖ Fault Manager
 - Log Viewer
 - Syslog
- ⊖ Event Monitor
 - Event Monitor
- ⊖ License Manager
 - Card Licenses
- ⊖ Management Access
 - Administrators
 - Authentication Methods
- ⊖ Configuration Manager
 - Configuration Services
- ⊖ Utilities
 - Active Directory

Gateway Configuration File Upload

Keytab File

CA Certificate

CA Certificate Revocation List

Gateway Certificate

Gateway Private Key

Note: If any changes in the Key tab file; the Gateway will be **rebooted** automatically and Management System is temporarily inaccessible.

Figure 69 - Gateway Configuration File Upload

The following fields appear upon selection of the <Edit Support Information> menu item:

- **Edit Gateway Support Information** – [Gateway|Edit Support Information], [Edit Gateway Support Information], [rw]
 - **Contact Person** – Name of the person to contact for gateway support.
 - **Telephone** – Telephone number of the person to contact for gateway support.
 - **Web Site URL** – Web site where gateway support information can be found.
 - **Email** – E-mail address of the person to contact for gateway support.

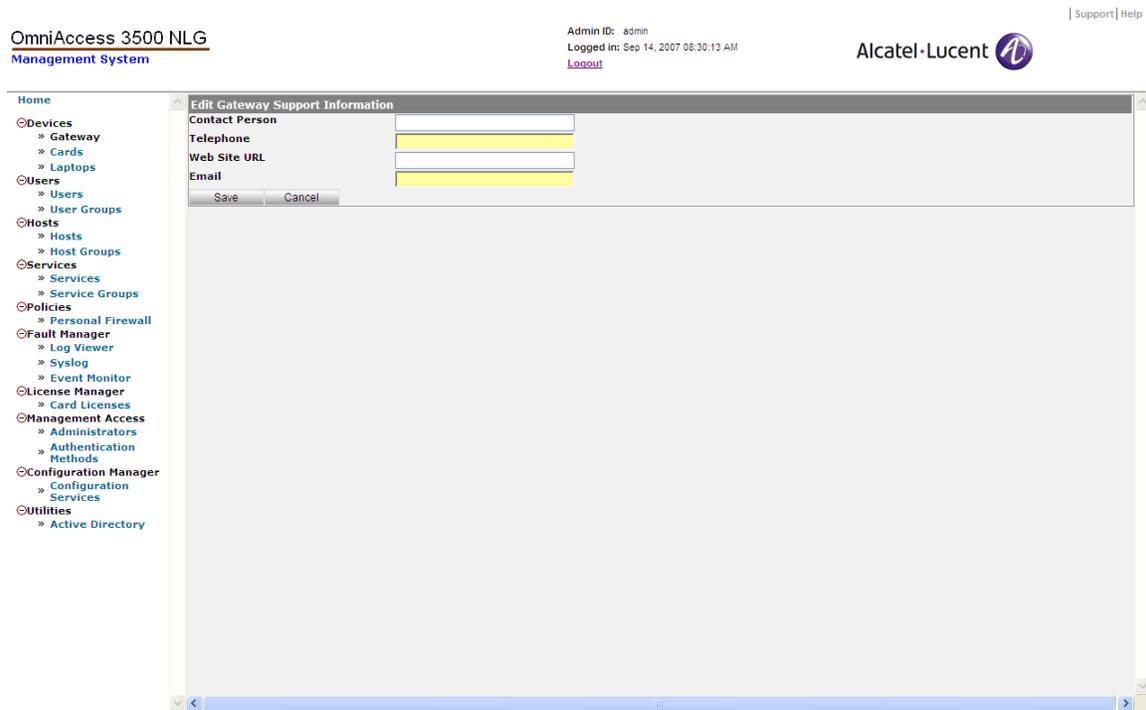


Figure 70 - Edit Gateway Support Information

- **Cards** – [Cards], [Card Information], [rwx]

List of the OmniAccess 3500 NLG cards that are currently under administrative control of the management system instance. Each row in the table corresponds to one OmniAccess 3500 NLG card and shows the following information items:

- **Card ID** – Electronic Serial Number (ESN) of the OmniAccess 3500 NLG card, an 8-digit (hexadecimal) numeric identifier assigned by the card manufacturer.
- **Phone** – The 10-digit telephone number associated with the OmniAccess 3500 NLG card, assigned by the service provider.
- **Description** – Space for additional card information (optional).

The Card Information window offers access to functions that can be applied to individual entries in the list: <New> (creates new entry), <Edit> (modifies provisioned parameters for existing entry), <Delete> (removes existing entry from list), <Status> (updates status variables for existing entry).

The following parameters are provisioned with the <New> or <Edit> functions:

- **Card ID (ESN #)** – Electronic Serial Number (ESN) of the OmniAccess 3500 NLG card, an 8-digit (hexadecimal) numeric identifier assigned by the card manufacturer.
- **Service Provider** – The company that is providing 3G wireless service to the card.
- **Description** – Optional field for additional card information.
- **Phone # (MSID)** – The 10-digit telephone number associated with the card.

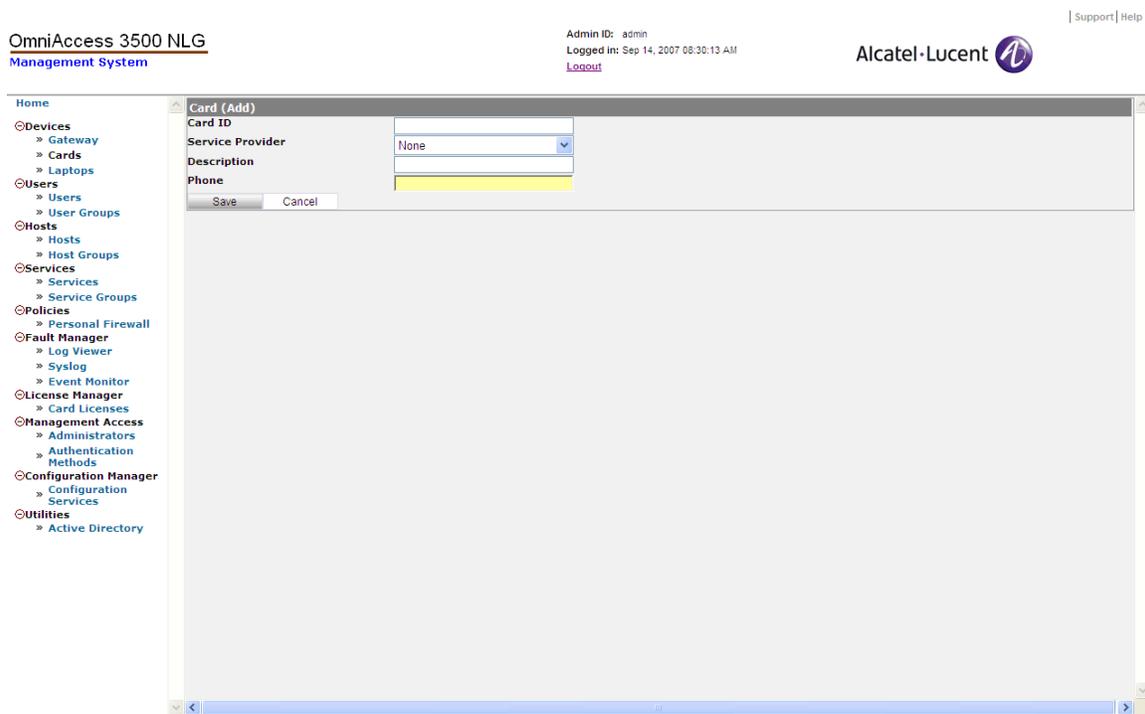


Figure 71 - Card (Add)

The following status indicators can be observed on the target OmniAccess 3500 NLG card upon selection of the <Status> tab:

- **Card ID** — The ESN (Electronic Serial Number) of the card. ESN is a unique identification number for the card provided by the manufacturer.
- **VPN IP Address** — The VPN IP Address assigned to the card when the tunnel is established (no address is visible if the tunnel is down).
- **VPN Status** — Current status of the IPsec tunnel between the OmniAccess 3500 NLG card and the OmniAccess 3500 NLG Gateway.
- **Last Connection Status** — Indicates whether the card is plugged into the laptop or not. Possible values are <CARD_INSIDE_LAPTOP> and <CARD_OUTSIDE_LAPTOP>.
- **Modem Activation Time** — Time when the card was activated with the Service Provider.
- **Last Connection Time** — Time when the card was last connected to the gateway.

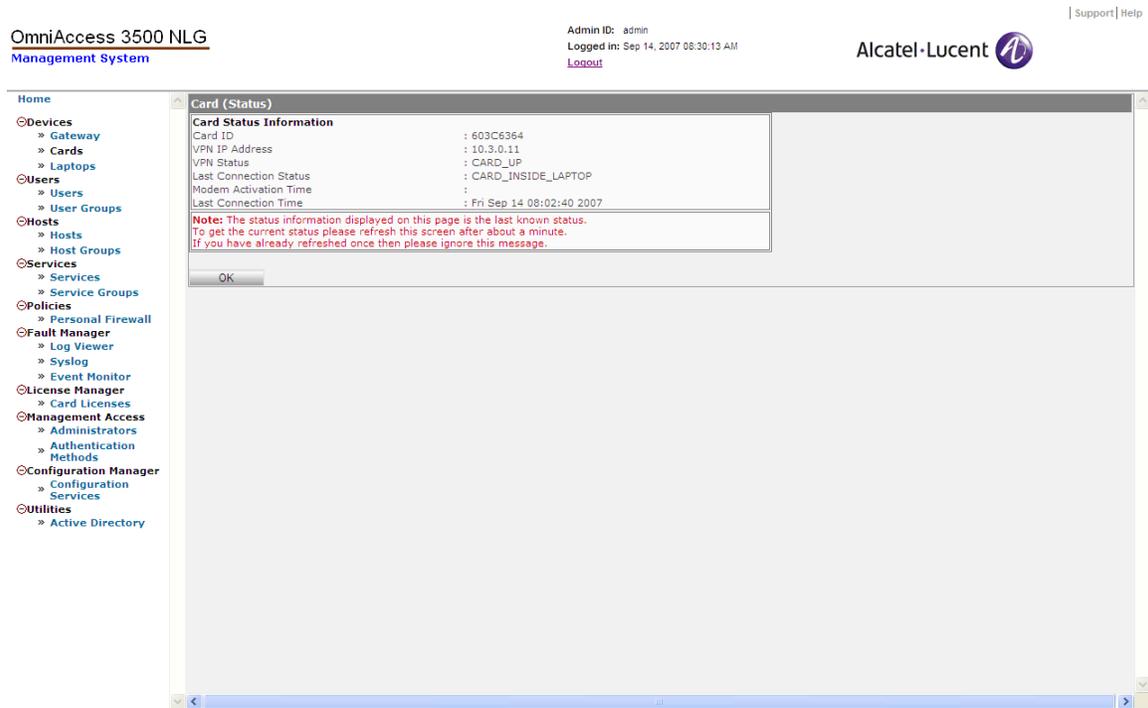


Figure 72 - Card (Status)

- **Laptops** – [Laptops], [Active Laptop Information], [rwx]

List of laptops associated with OmniAccess 3500 NLG cards that are currently connected to the gateway. The <New> and <Edit> tabs provide access to the following information items for the selected laptop. The <Delete> tab removes the selected entry.

 - **Laptop ID** – A unique name for the laptop.
 - **Description** – Field for additional laptop information (optional).

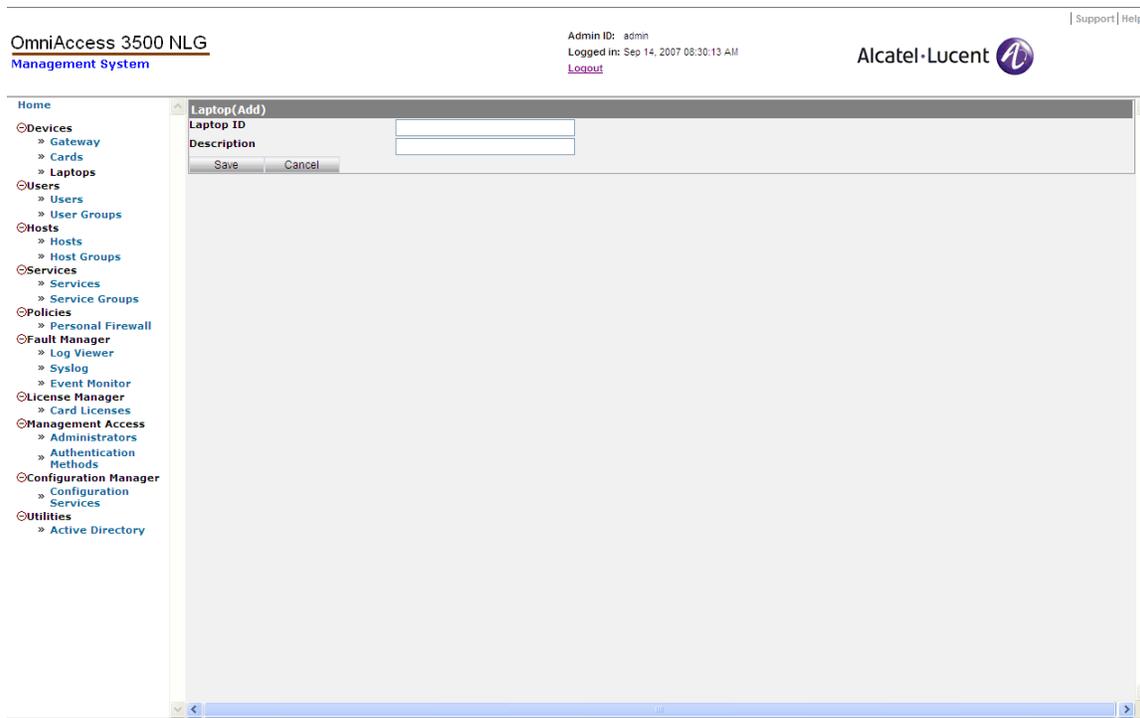


Figure 73 - Laptop (Add)

Users

The Users section of the management system GUI allows configuration and monitoring of users and user groups. In this section it is possible to add/edit and delete user/user group entries, check user status, and find the location of a user's laptop.

- **Users** – [Users], [User Information], [rw]

List of users that are currently configured under administrative control of the management system instance.

The <Open>, <New>, and <Edit> tabs provide access to the following information items for the selected user:

- **Login** – The login name of the user (e.g., jdoe).
- **Domain** – The name of the Windows domain that includes the user. If the enterprise uses a RADIUS-based method instead of an Active Directory infrastructure to authenticate the end users for network access, the Domain field should be filled with the Laptop ID as set up in the laptop configuration.
- **Full Name** – The real name of the user (e.g., John Doe).
- **Base Unlock Password** – Base password used to generate the one-time password. Do not use special characters (such as #, @, &) in this field.
- **Connectivity Timeout (sec.)** – Total laptop power-on time during which the laptop is allowed to work without VPN tunnel to the OmniAccess 3500 NLG gateway. The corresponding timer is reset every time the IPsec tunnel to the gateway is established while the laptop is powered on. A warning pops up on

- the laptop's screen five minutes before expiration of the connectivity timeout. If the timeout expires, the laptop locks and can only be unlocked with an OTP received from the IT helpdesk.
- **OTP Valid Time (sec)** – Amount of time that the laptop will remain unlocked and with reduced OmniAccess 3500 NLG controls after the one-time password has been successfully entered. All tamper checks are re-enabled after expiration of this time.
 - **Card ID** – The ESN of the card assigned to this user. Only one card can be assigned to a given user.
 - **Laptop ID** – The laptop assigned to this user. Only one OmniAccess 3500 NLG-enabled laptop can be assigned to a given user.
 - **User Group** – The user group that includes this user. A given user can belong to only one User Group.
 - **Certificate ID** – The identifier of the Digital Certificate that is used in the activation of the card. The identifier must be expressed in the format: <CN=value>, where *CN* stands for *common name* and *value* is the common name of the certificate (available in the *Subject* field of the certificate). *Please note that this parameter is case-sensitive.*
 - **License ID** – A license name can be selected from the pull-down menu. The user can connect to the enterprise between the start and end dates specified in the license selected.

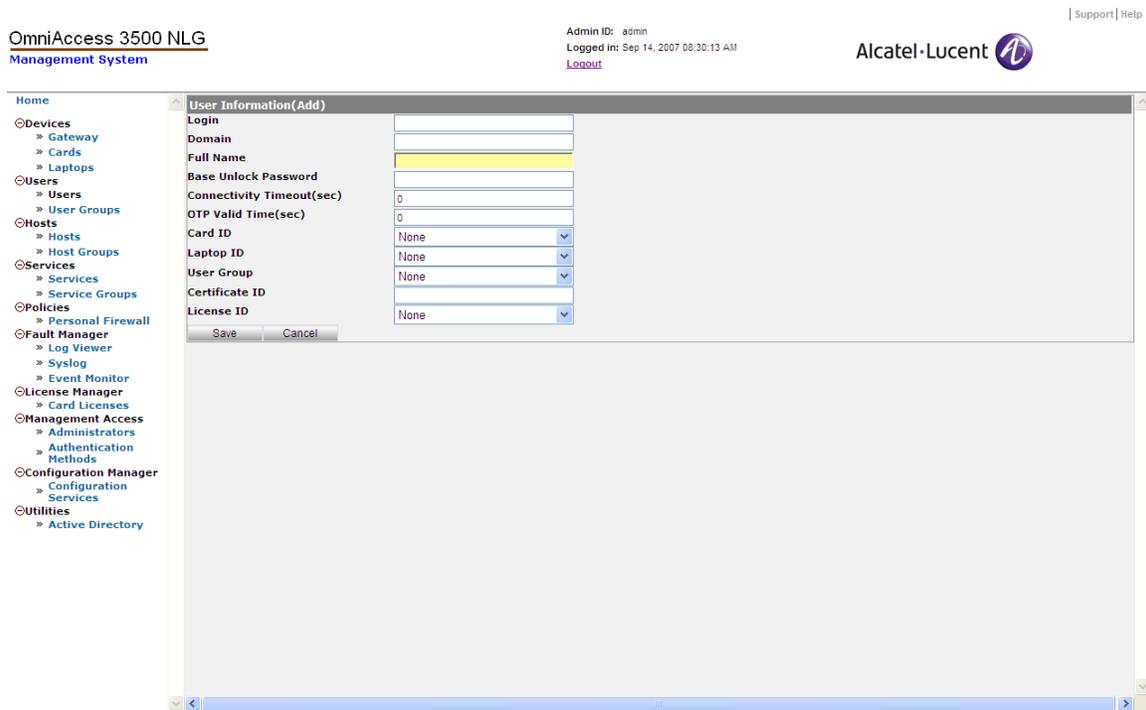


Figure 74 - User Information (Add)

The <Delete> tab removes the selected entry from the Users table.

The <Status> tab provides access to the following options: <User Status>, <View Current Location>, and <View Login Location>.

Clicking on <User Status> provides visual access to the following status indicators:

- **User Settings** – Information about the selected user.
 - **User ID** – Numeric identifier and full name of the user.
 - **User Status** – Whether or not logged into the laptop.
 - **Last Logged-in Time** – Time of completion of latest laptop login.
 - **Authentication Status** – Whether or not authenticated with the enterprise network.
- **Card Settings** – Information about the selected user’s card.
 - **Card ID** – Unique numeric identifier (ESN) of the card.
 - **Last Connection Status** – Whether or not plugged into the laptop.
 - **VPN Status** – Whether or not the IPsec tunnel between the card and the gateway is up.
 - **VPN IP Address** – Current VPN IP address of the card.
 - **Last Connection Time** – Time when the current connection was established.
 - **Modem Activation Time** – Time when the 3G modem was last switched on.
- **Laptop Settings** – Information about the selected user’s laptop:
 - **ID** – Laptop identifier.
 - **Name** – Laptop identifier.
 - **Status** – Whether or not powered on.
 - **IP Address** – Current VPN IP address of the laptop.
- **Tamper Proofing Settings** – Information about the selected user’s security settings:
 - **Lock Status** – Whether or not currently locked.
 - **Last Lock Time** – Time when the laptop was last locked.
 - **Last Unlock Time** – Time when the laptop was last unlocked.
 - **Last Remote Kill Status** – Status of the last remote kill command issued for the laptop.
 - **Last Remote Kill Time** – Time when a remote kill command was last issued for the laptop.
 - **Last Reboot Initiated** – Time when the laptop last started rebooting.
- **License Settings** – Information about the selected user’s license:
 - **License ID** – License identifier.

- State – Whether the license is in a valid state.
- Start Date – The start date for the license.
- End Date – The end date for the license.

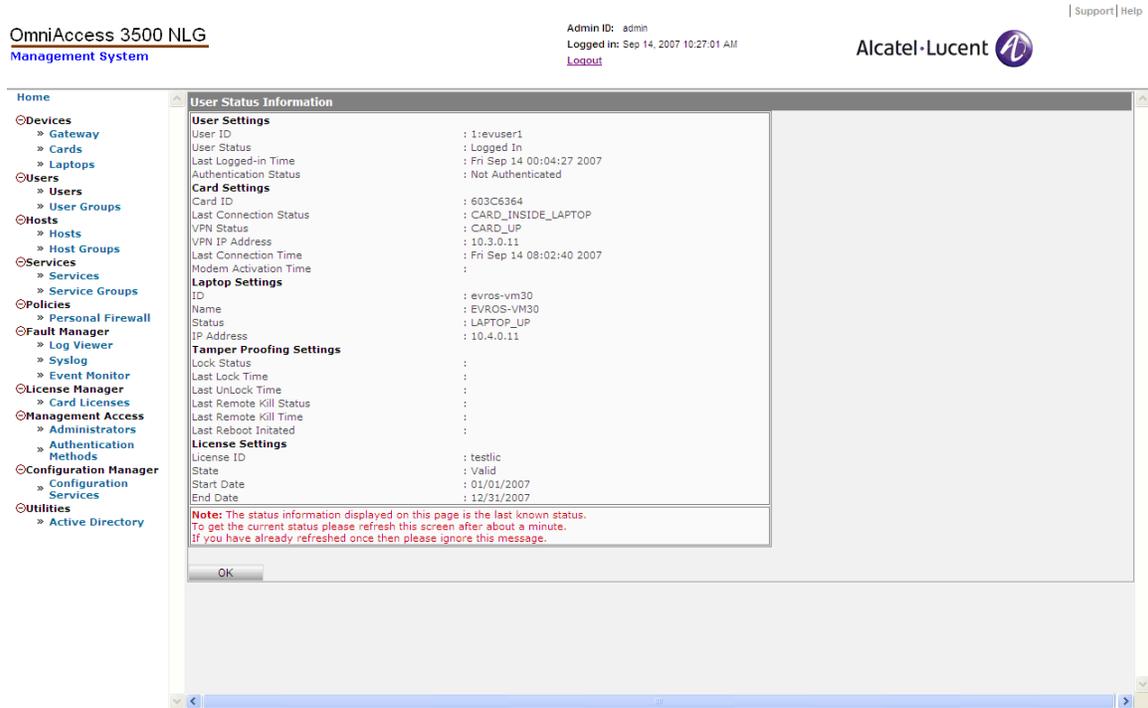


Figure 75 - User Status window

The <View Current Location> and <View Login Location> tabs provide geographic information about the laptop. Clicking on <View Login Location> shows a Proprietary Information page into which an administrator password must be typed, then displays the location of the last user login to the laptop, similar to the following map:

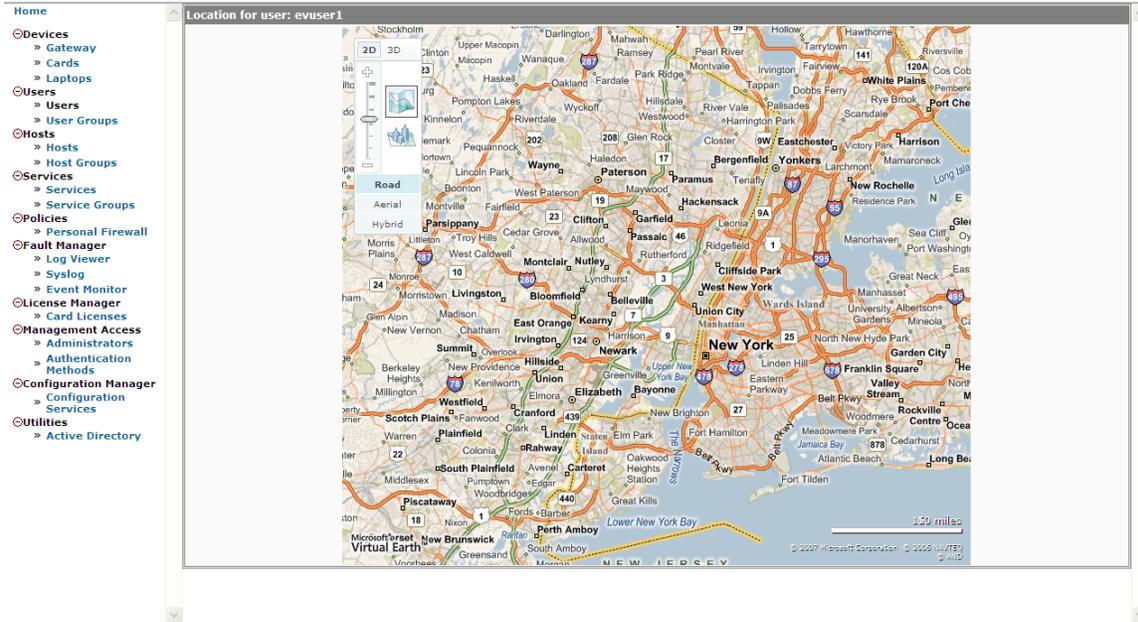


Figure 76 - View Login Location

Clicking on <View Current Location> shows a Proprietary Information page into which an administrator password must be typed, then displays the location of the current user login to the laptop, similar to the following map:

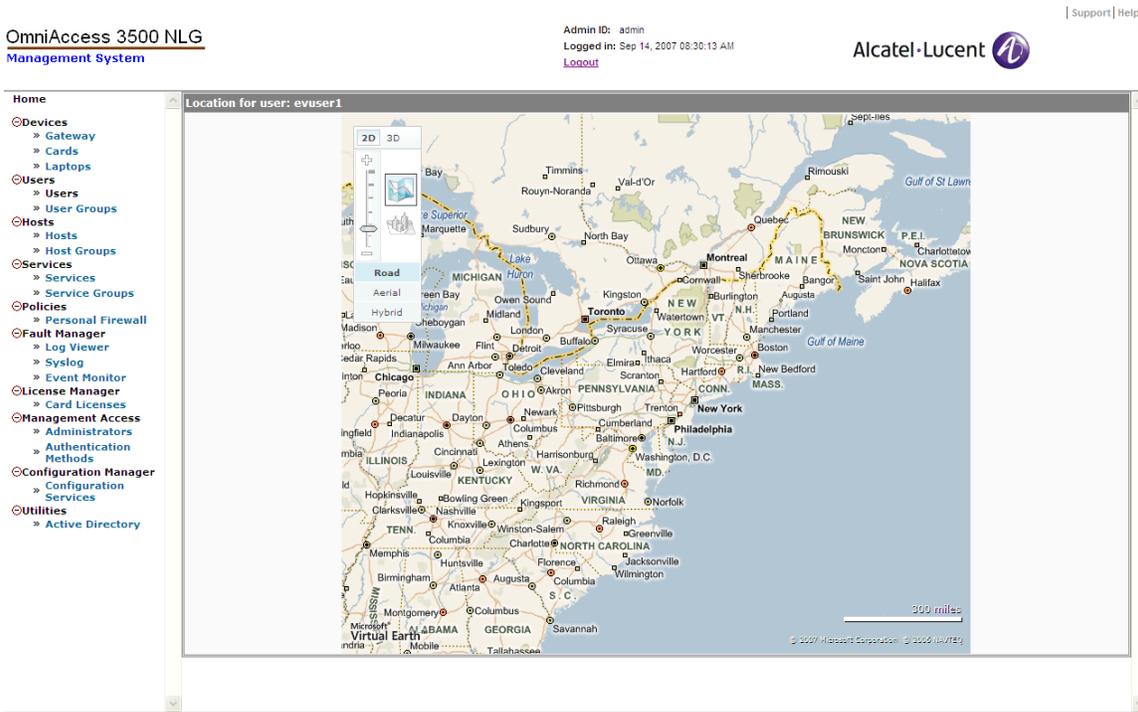


Figure 77 - View Current Location

The <Configure> tab provides access to the following items:

- o **Asset Management** :<Laptop local time of latest asset info refresh> – [Users|User|Configure], [User Configurations : <User ID :User Full Name>], [r]

This function runs on demand (see the Refresh Asset Info menu option below) and allows you to view information about user assets. Menu options available are:

- **Programs** – Applications that are currently running on the user's laptop.
- **Services** – State of the Windows Services installed in the user's laptop.
- **Processes** – Processes currently running on the user's laptop.
- **Partitions** – Partition table information.
- **System Information** – System information, such as Manufacturer. Model, CPU version, etc.
- **Operating System** – Operating system used on the user's laptop.
- **Personal Firewall** – Applications that are allowed network access by the application filter of the personal firewall.
- **Truecrypt File Information** – Information about files contained in the encrypted volume in the remote laptop.
- **Refresh Asset Info** – This command triggers a refresh of all the asset management entries.

- o **Tamper Proof Manager** – [Users|User|Configure], [User Configurations: <User ID: User Full Name>], [rwx]

This section of the management system GUI allows you to generate the one-time password that the end user can utilize to unlock a laptop recovered after being locked due to loss or theft.

- **Generate One Time Password** – [Users|User|Configure|Generate One Time Password], [Tamper Proofing Settings - Get One Time Password], [rwx]

Parameters needed for the immediate generation of a one-time password.

- ◆ **User ID** – User ID corresponding to the laptop for which the one-time password is being generated.
- ◆ **Current Date (mm/dd/yyyy)** – Date displayed on the lock screen of the laptop.
- ◆ **Current Time (hh:mm:ss)** – Time of the day displayed on the lock screen of the laptop.
- ◆ **Time Zone** – Time zone displayed on the lock screen of the laptop.
- ◆ **Screen Count** – Type the number seen by the end user in the upper right-hand corner of the window that appears on the screen of the locked laptop.

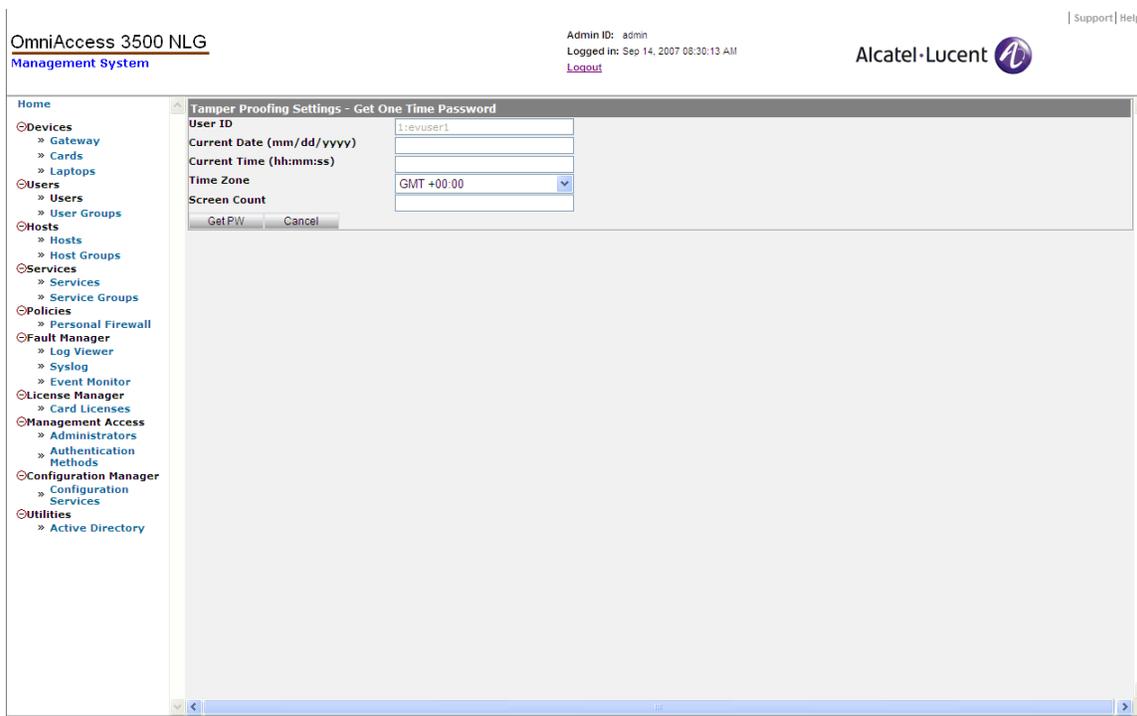


Figure 78 - Tamper Proofing Settings - Get One Time Password

- **TrueCrypt Volume Encryption** – [Users|User|Configure], [User Configurations: <User ID: User Full Name>], [rwx]

This section of the management system GUI allows you to configure the encrypted volume in the remote laptop and manage the secret password that the laptop needs to mount and access the encrypted volume.

- **Volume Settings** – [Users|User|Configure|Volume Settings], [TrueCrypt Settings], [rw]

Encrypted-volume configuration parameters that are set per user.

- ◆ **User ID** – Numeric identifier of the end user.
- ◆ **Volume Path** – Volume location in the laptop file system. The value can point to a file with any type of extension.
- ◆ **Mount Drive** – Drive identifier assigned to the encrypted volume once mounted.
- ◆ **Volume Size (MB)** – Total hard disk space allocated to the encrypted volume.
- ◆ **Volume Enabled** – Flag enabling/disabling the mounting of the encrypted volume upon authentication of the user's Windows Logon credentials.

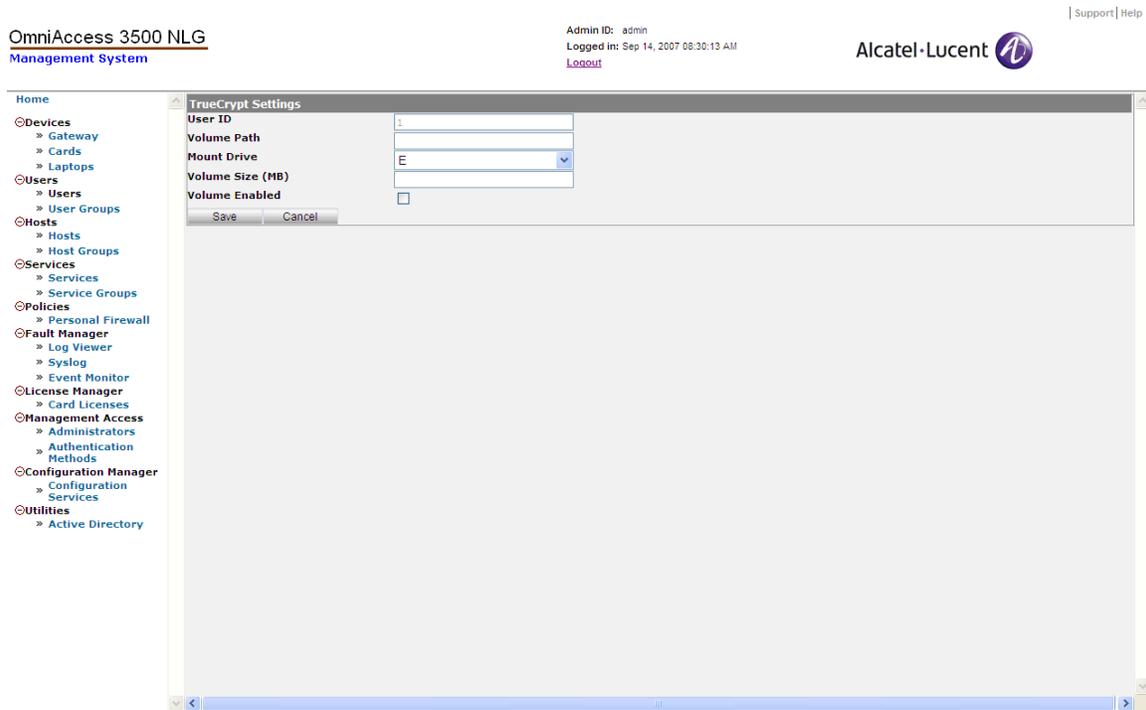


Figure 79 - TrueCrypt Settings

- **Change Volume Password** – [Users|User|Configure|Change Volume Password], [Change Password Confirmation], [rwx]
Facility for changing the secret password needed by the laptop to mount the encrypted volume and encrypt/decrypt the encrypted volume contents.
- **Remove Volume Password** – [Users|User|Configure|Remove Volume Password], [Delete Password Confirmation], [rwx]
Facility for deleting the secret password needed by the laptop to mount the encrypted volume and encrypt/decrypt the encrypted volume contents. Without the secret password the contents of the encrypted volume become inaccessible.
- **Restore Password** – [Users|User|Configure|Restore Password], [Restore Password Confirmation], [rwx]
Facility for restoring a deleted secret password needed by the laptop to mount the encrypted volume and encrypt/decrypt the encrypted volume contents.
- **Volume Status** – [Users|User|Configure|Volume Status], [TrueCrypt Status Information], [r]
 - List of status indicators for the encrypted volume:
 - ◆ **User ID** – Numeric identifier of the laptop user.
 - ◆ **Volume Path** – Location of the encrypted volume in the laptop file system. The value can point to a file with any type of extension.

- ◆ **Mount Drive** – Drive identifier assigned to the encrypted volume when mounted.
- ◆ **Volume Size (MB)** – Hard disk space allocated to the encrypted volume.
- ◆ **Volume Status** – Current status of the encrypted volume. Possible values indicate the following states: No Volume, Volume Mounted, Volume Dismounted, TrueCrypt Not Installed, Volume Creation Failed For Lack Of Space, Volume Creation Failed For Reasons Other Than Lack Of Space, Volume Mount Failed, Volume Dismount Failed.
- ◆ **Password Change Status** – Status of an ongoing password change or password removal procedure. Possible values indicate the following states: No Status, Password Change Successful, Password Change In Progress, Password Change Failed, Password Removal Successful, Password Removal In Progress, Password Removal Failed.
- ◆ **Password Change Time** – Time when the password was last changed.
- ◆ **Active Password** – Last password successfully stored in the OmniAccess 3500 NLG card.

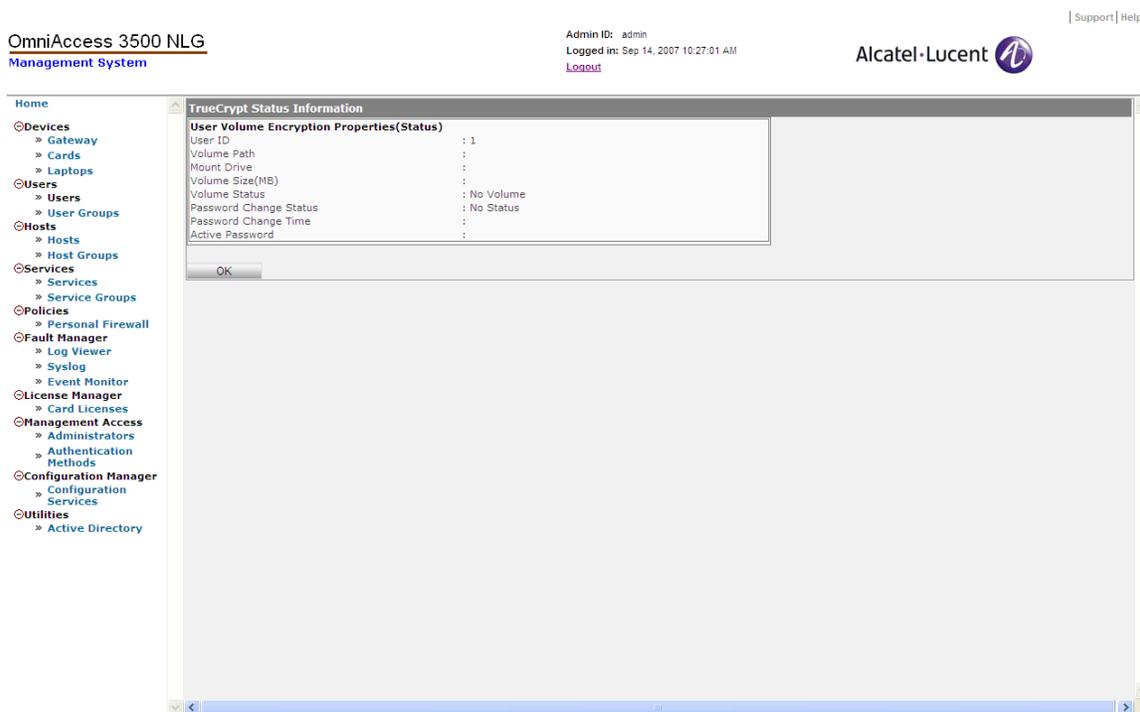


Figure 80 - TrueCrypt Status Information

- **Delete Volume** – [Users | User | Configure | Delete Volume], [Delete Volume Confirmation], [rwx]
Facility for removing the encrypted volume from the laptop hard disk.
- **Deleted Volume Properties** – [Users | User | Configure | Deleted Volume Properties], [Deleted Volume Information], [r]
Displays information about volumes that have previously been deleted.

- **System Management** – [Users|User Information|Configure], [System Management], [rw]

This set of commands allows you to lock or unlock the user's laptop.

- **Lock** – Locks the user's laptop.
- **Unlock** – Unlocks the user's laptop.

- **User Groups** – [User Groups], [User Groups Information], [rwx]

List of user groups that are currently configured under administrative control of the management system instance. Each row in the table corresponds to one user group and shows the following information items: <Group ID> (unique numerical identifier), <Name> (unique alphanumeric identifier, in no mandated format), <Description> (optional additional information), <Radio Timeout> (maximum allowed time with powered-off modem before the laptop screen locks).

The <Open> tab provides read access to the following information items for the selected user:

- **Name** – Unique alphanumeric identifier for the user group.
- **Description** – An optional field in which you can type any additional information.
- **Radio Timeout (sec)** – A switch on the OmniAccess 3500 NLG card turns the 3G modem on and off. The radio timeout field indicates how long the switch can remain in the off position with the laptop powered on before the Windows Lock screen appears on the laptop's monitor. The lock screen can be unlocked using the Windows Logon credentials, but only as long as the Connectivity Timeout does not expire.
- **Policy** – Personal firewall policy that applies to this user group.
- **Assigned Users** – Users assigned to this group.

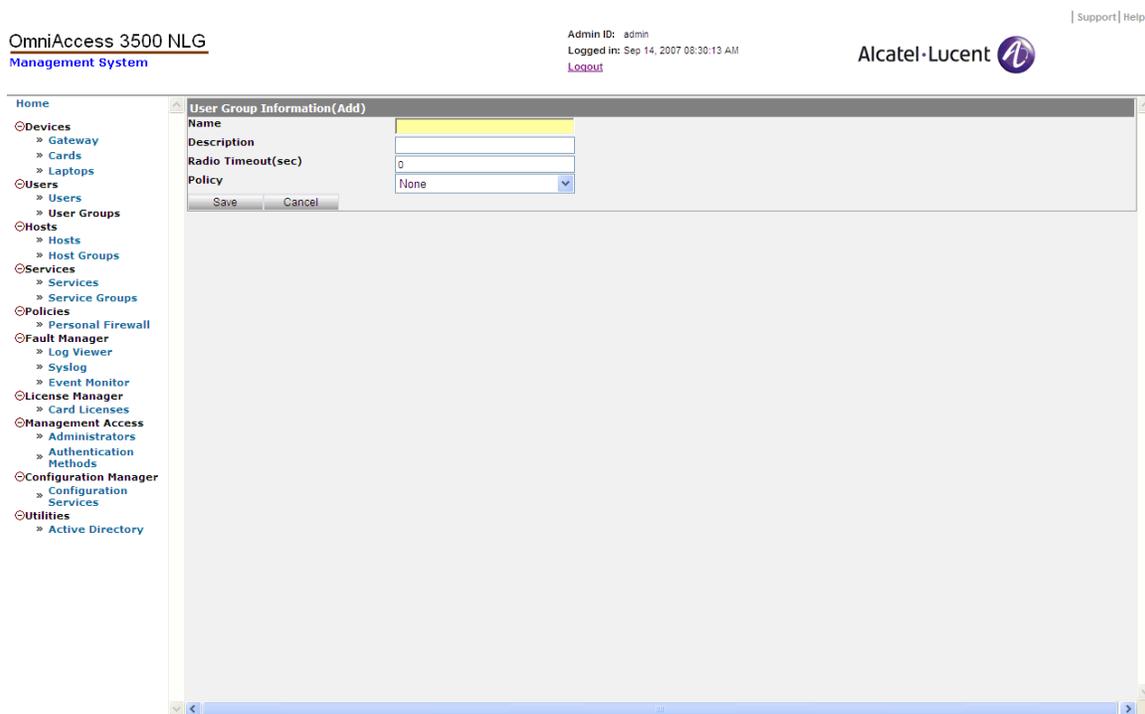


Figure 81 - User Group Information (Add)

The <New> tab allows the configuration of the above information items when a new user group is created. The <Edit> tab allows the modification of the settings for one or more of the above items for an existing User Group entry. The <Delete> tab removes the selected entry from the User Group table.

The <Configure> tab provides access to the section of the management GUI that allows you to assign TrueCrypt Volume Encryption information to a user group.

- o **Group Volume Settings** — [Users | User Groups Information | Configure | User Group Configurations], [Group TrueCrypt Settings], [rw]

Encrypted-volume configuration parameters that are set per user group.

- **Group Name** — Identifier of the user group, shown to remind the IT administrator of the user group for which the encrypted volume is being configured.
- **Encryption Algorithm** — Algorithm used for encryption of the volume contents. Available options are:
 - ◆ AES (default)
 - ◆ Serpent
 - ◆ Twofish
 - ◆ AES-Twofish
 - ◆ AES-Twofish-Serpent
 - ◆ Serpent-AES
 - ◆ Serpent-Twofish-AES

- ◆ Twofish-Serpent
- **Hash Algorithm** – Algorithm used for random generation of the volume master key. Available options are:
 - ◆ RIPEMD-160 (default)
 - ◆ SHA-1
 - ◆ Whirlpool
- **File Format** – Type of file system for the encrypted volume. Available options are:
 - ◆ FAT (default)
 - ◆ NTFS (this option does not work for end users that do not have administrator privileges on their laptops).

Note: Windows XP supports NTFS. Earlier Windows versions and Linux support FAT.

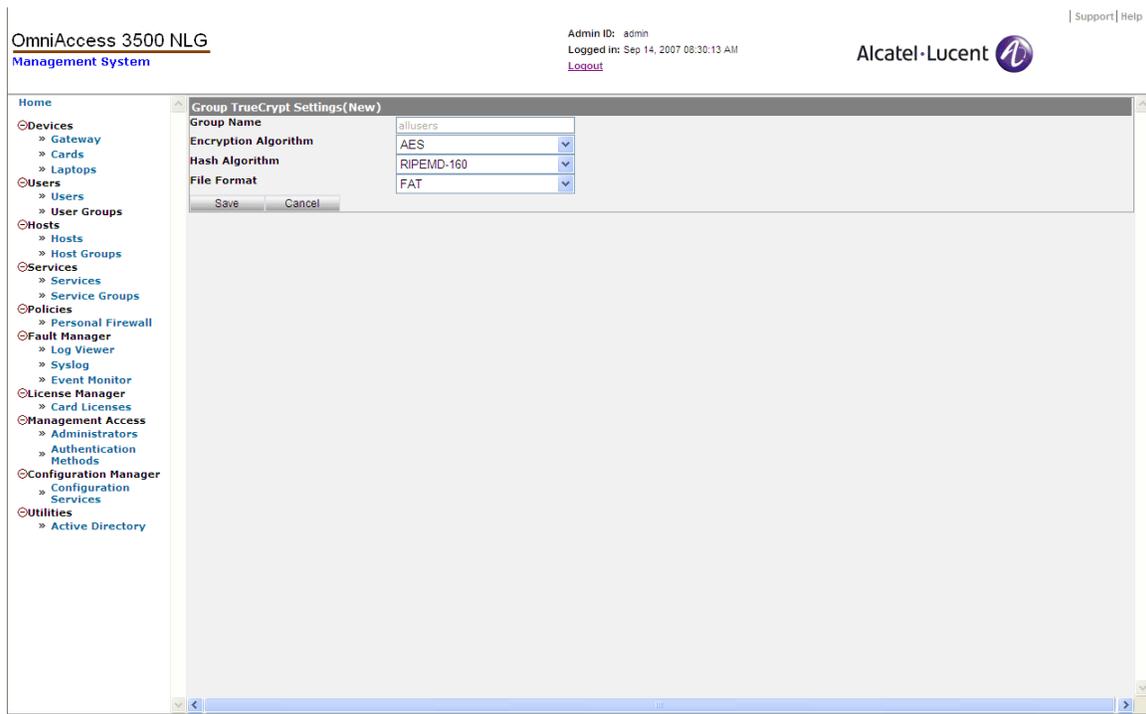


Figure 82 - Group TrueCrypt Settings (New)

- **Delete Group Volume** – [Users|User Groups Information|Configure|User Group Configurations], [Delete Group Volume Settings], [rw]

Click this to delete volume settings from the selected user group.

Hosts

The Hosts section of the management system GUI allows access to information and management actions that apply to the groups of IP addresses to be included in the specification of the packet filter rules for the personal firewall policies.

Through the Hosts section, you can view, add, edit, and delete hosts (i.e., ranges of IP addresses) and host groups (i.e., groups of non-contiguous IP address ranges).

- **Hosts** – [Hosts], [Hosts], [rw]

List of IP address ranges that are currently configured for inclusion in the packet filtering rules for the personal firewall policies. Each row in the table corresponds to one range of IP addresses and shows the following information items for identification purposes: <Host Name> (unique alphanumeric identifier of the IP address range, in no mandated format), <Description> (information note further describing the IP address range), <Host> (a valid address in the IP address range), <Mask> (network mask used for identification of the entire range, expressed as the number of initial invariant bits in the IP address; valid range: <1..32>).

The <Open> tab provides read access to the following information items for the selected host:

- **Host Name** – Unique name identifying the IP address range.
- **Description** – Descriptive text about the IP address range.
- **Host** – A valid IP address in the IP address range.
- **Mask (1-32)** – The network mask used for identification of the entire range.

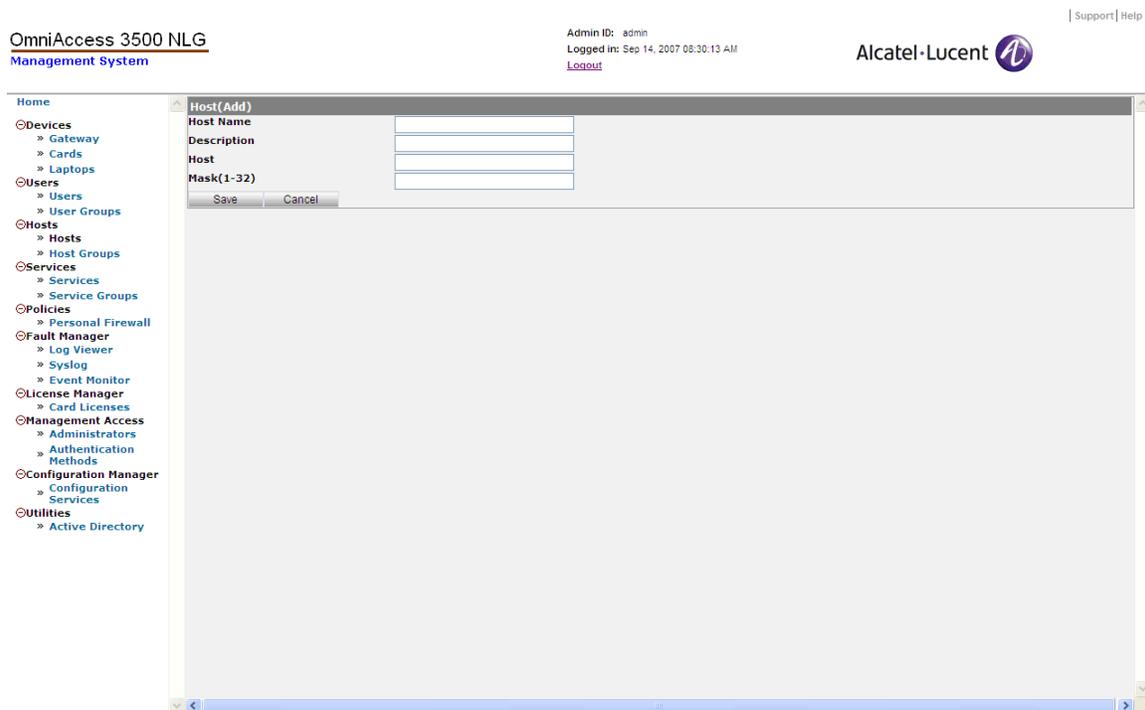


Figure 83 - Host (Add)

The <New> tab allows the configuration of the above information items when a new group of IP address ranges is created. The <Edit> tab allows the modification of the settings for one or more of the above items for an existing Host entry. The <Delete> tab removes the selected entry from the Hosts table.

- **Host Groups** – [Host Groups], [Host Groups], [rw]

List of IP address range groups that are currently configured for inclusion in the packet filtering rules for the personal firewall policies. Each row in the table corresponds to one host group and shows the following information items for identification purposes: <Host Group Name> (unique alphanumeric identifier of the IP address range group, in no mandated format), <Description> (information note further describing the IP address range group).

The <Open> tab provides access to the following information items for the selected host group:

- **Host Group Name** – Unique alphanumeric identifier for the group of IP address ranges.
- **Description** – Information note detailing the nature and purpose of the group of address ranges.
- **Hosts** – Set of IP address ranges included in the group.

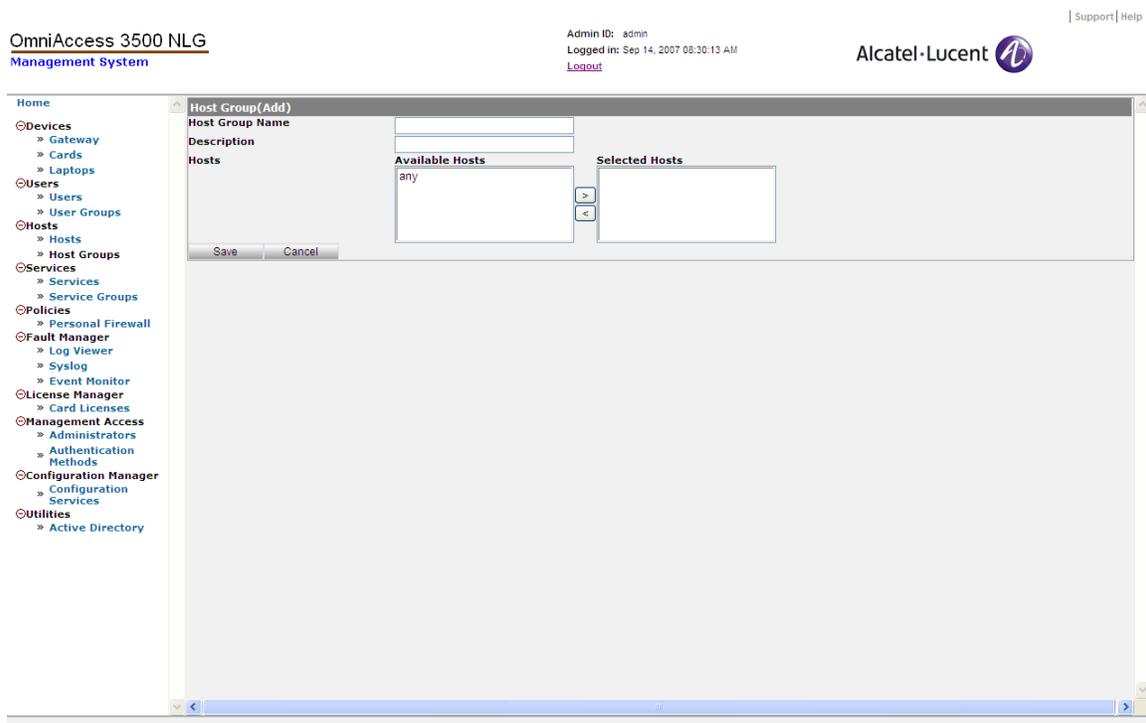


Figure 84 - Host Group (Add)

The <New> tab allows the configuration of the above information items when a new group of IP address ranges is created. The <Edit> tab allows the modification of the settings for one or more of the above items for an existing Host Group entry. The <Delete> tab removes the selected entry from the Host Groups table.

Services

The Services section of the management system GUI provides access to information and management actions that apply to the groups of UDP and TCP ports to be included in the specification of the packet filter rules for the personal firewall policies.

Through the Services section, you can view, add, edit, and delete services and service groups.

- **Services** – [Services], [Services Information], [rw]

List of layer-4 ports that are configured for inclusion in service groups. The service specification does not include indication of the target layer-4 protocol. Each row in the table corresponds to one service and shows the following information items: <Name> (descriptive alphanumeric identifier of the service), <Port> (port number of the service, with <0> representing all port numbers between <1> and <65535>).

The following items are set upon creation of a new table entry through the <New> tab:

- **Name** – Unique name for the service you want to add.
- **Port** – The port number of the service.

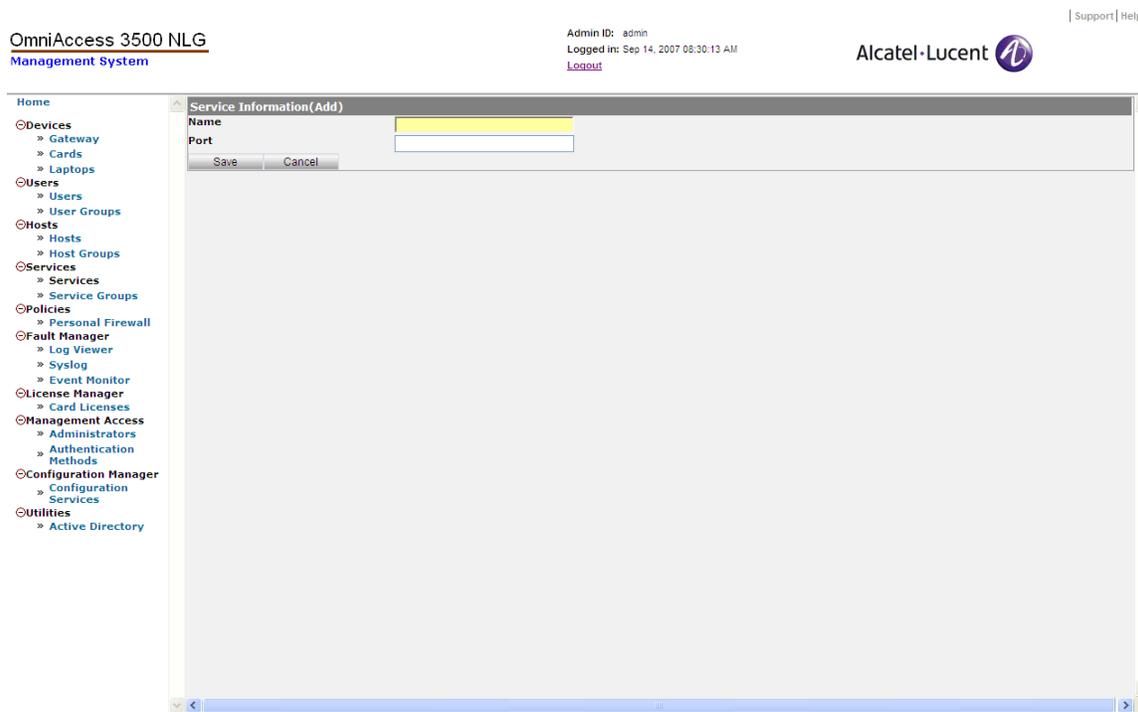


Figure 85 - Service Information (Add)

The <Open>, <Edit>, and <Delete> tabs can be used to view, modify, and delete an existing entry, respectively.

- **Service Groups** – [Service Groups], [Service Group Information], [rw]

A service group is a collection of layer-4 port numbers to be included in the specification of personal firewall policies. The service group specification does not

include indication of the target layer-4 protocol. Each row in the table corresponds to one service group and shows the following information items: <Group ID> (unique numerical identifier of the service group), <Name> (descriptive alphanumeric identifier of the service group).

The <New> tab enables the configuration of the following fields upon instantiation of a new service group:

- **Group ID** – Unique alphanumeric identifier for the group of layer-4 ports.
- **Name** – Name identifying the service group.
- **Services** – Set of layer-4 ports included in the group.

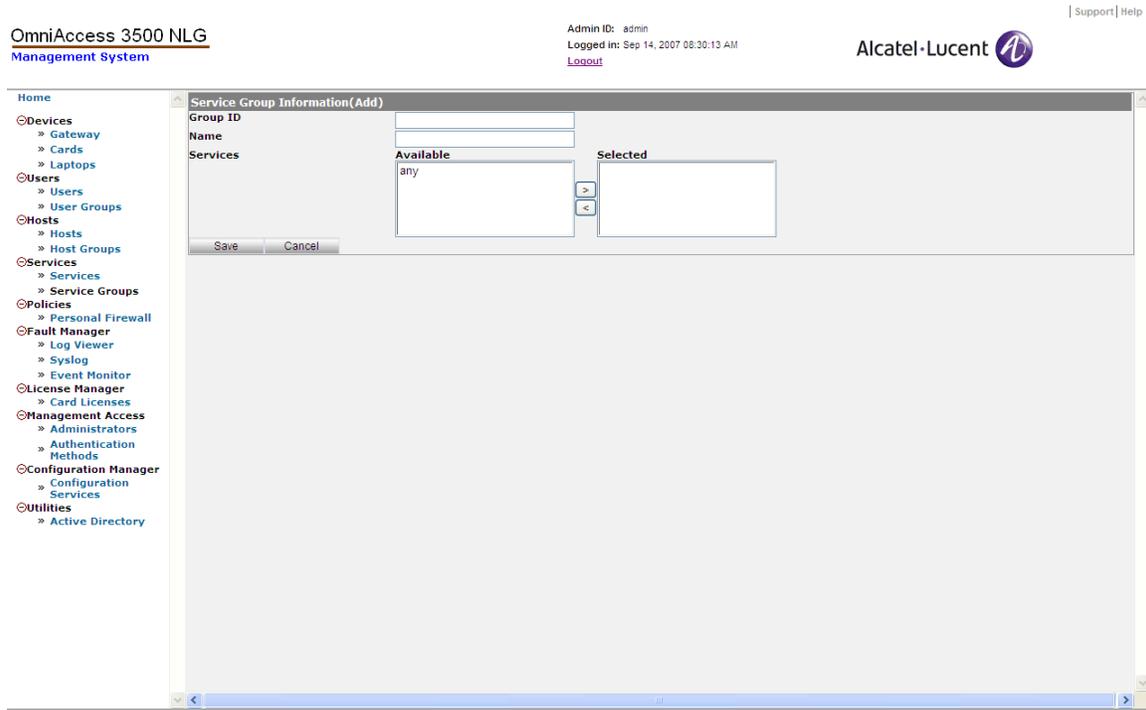


Figure 86 - Service Group Information (Add)

The <Open>, <Edit>, and <Delete> tabs can be used to view, modify, and delete an existing entry, respectively.

Policies

The Policies section of the management system GUI provides access to information and management actions that apply to the personal firewall policies to be installed in the OmniAccess 3500 NLG cards. A personal firewall policy has scope exclusively over the network traffic exchanged by the OmniAccess 3500 NLG laptop and not over the traffic that terminates at the OmniAccess 3500 NLG card.

Through the Policies section, you can view, add, edit, and delete packet filter rules, application filter rules, and personal firewall policies.

- **Personal Firewall** – [Personal Firewall], [Policies - Personal Firewall], [rw]

Configuration of packet filter rules, application lists, and personal firewall policies.

- o **Packet Filter Rules** — [Personal Firewall|Packet Filter Rules], [Packet Filter Rules Definitions], [rw]

List of packet filter rules to be included in the personal firewall policies. All packet filter rules are allow-rules: only packets that match one of the configured packet filter rules are allowed through the personal firewall. The <New> tab allows the creation of a new table entry. The <Open>, <Edit> and <Delete> tabs allow the inspection, modification, and deletion of an existing entry, respectively. Each entry in the table shows the following information items:

- **Rule Name** — Unique alphanumeric name of the packet filter rule.
- **Direction** — Direction of the traffic that is subject to the packet filter rule. Options (choose one): <In> (from the network to the laptop), <Out> (from the laptop to the network).
- **IP Addresses** — Set of IP address ranges including the address of a packet matching the packet filter rule. The address must be found in the Source IP Address field in the case of a packet filter rule with <In> direction, and in the Destination IP Address field in the case of a packet filter rule with <Out> direction.
- **Source Ports** — Set of port values including the source port number of a packet matching the packet filter rule. This field is only relevant for packet filter rules whose <Protocol> selection is either <TCP> or <UDP>.
- **Destination Ports** — Set of port values including the destination port number of a packet matching the packet filter rule. This field is only relevant for packet filter rules whose <Protocol> selection is either <TCP> or <UDP>.
- **Protocol** — Protocol identifier carried in the header of a packet that matches the packet filter rule. Options (choose one): <TCP>, <UDP>, <ICMP>, <IP>.
- **Rule Action** — Select an action to take from the drop-down list (Accept or Drop).

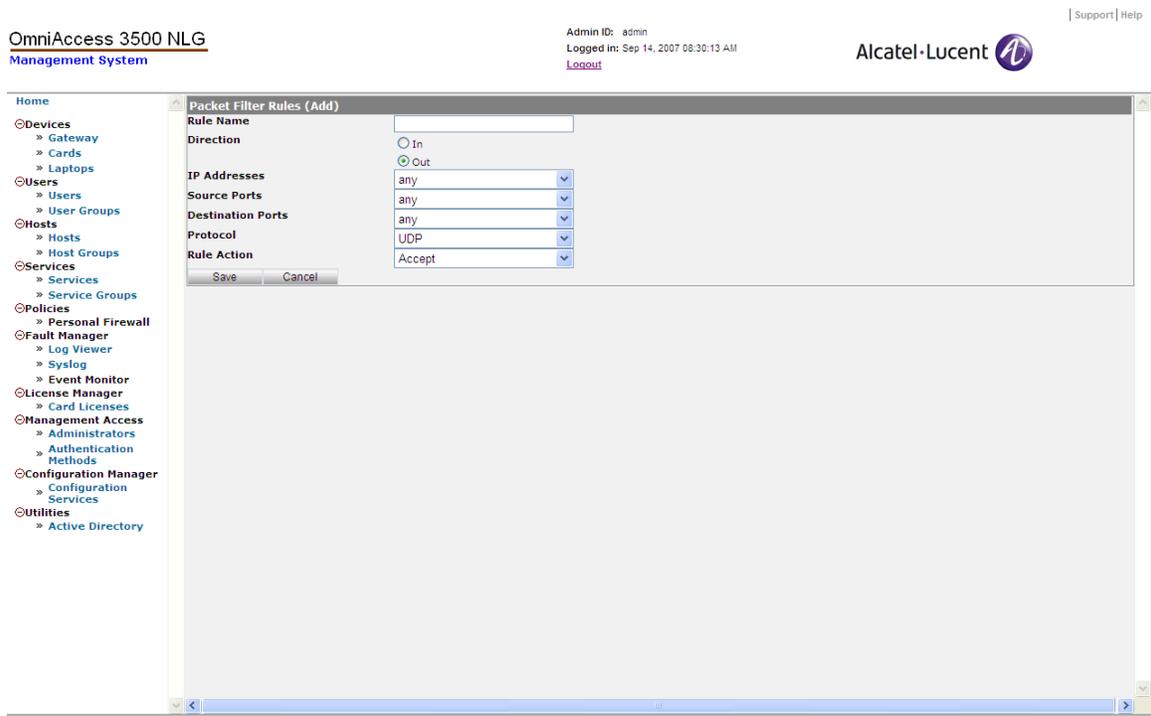


Figure 87 - Packet Filter Rules (Add)

- o **Applications** – [Personal Firewall|Applications], [Applications], [rw]
 Configuration of applications to be included in the personal firewall policies. This utility enables the coupling of MS Windows executable file names (<Executable File>) with their corresponding application names (<Application Name>). A pre-populated list of common applications is available by default. The following information items are set upon instantiation of a new table entry using the <New> tab:
 - **Application Name** – Unique alphanumeric name for the new application.
 - **Executable File** – Name of the MS Windows executable file that corresponds to the Application Name.

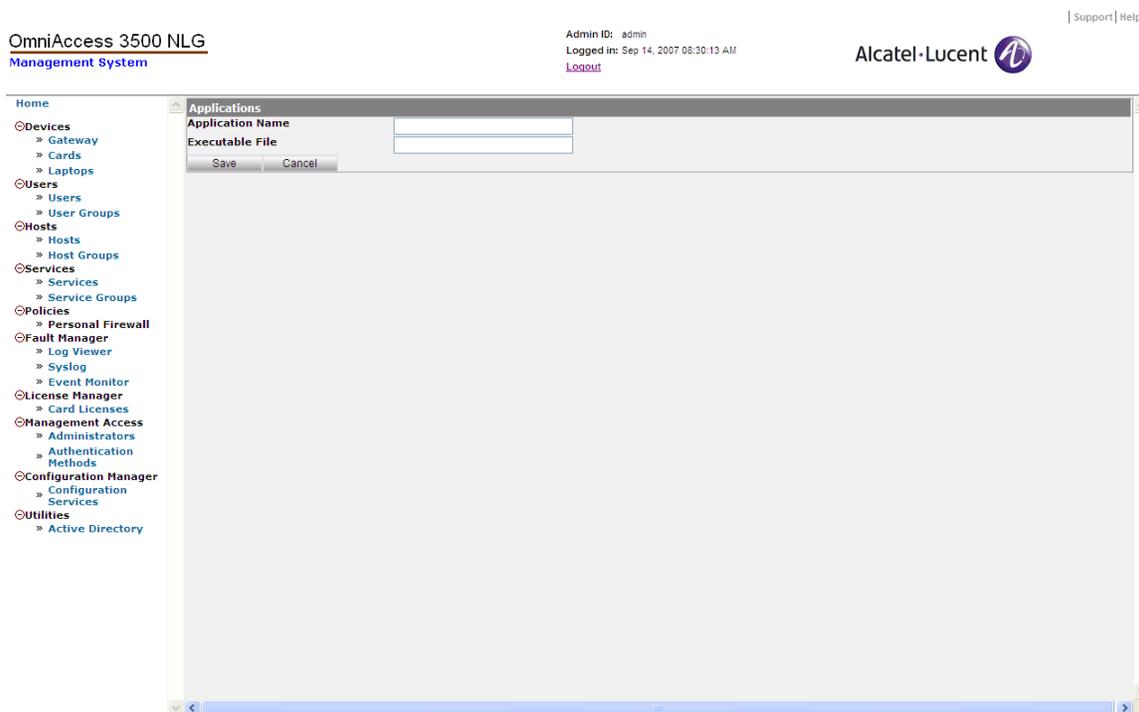


Figure 88 - Applications

- **Application Group** — [Personal Firewall | Application Group], [Application Group Information], [rw]

Configuration of groups of applications with homogeneous treatment in the application filter. The inclusion of an application group in a personal firewall policy works the same way as the inclusion of an individual application. This utility makes the specification of Personal Firewall rules faster by avoiding the necessity of explicitly listing the required firewall behavior for every application that is relevant to the rule. The creation of an application group requires the prior insertion of its component applications in the list that maps application names onto executable file names.

The following information items can be set through the <New> or <Edit> tabs:

- **Group Name** — Unique alphanumeric name for the new application group.
- **Applications** — Drop-down list of applications that are available for inclusion in the Application Group. Click the <Add> button to add the application to the group.

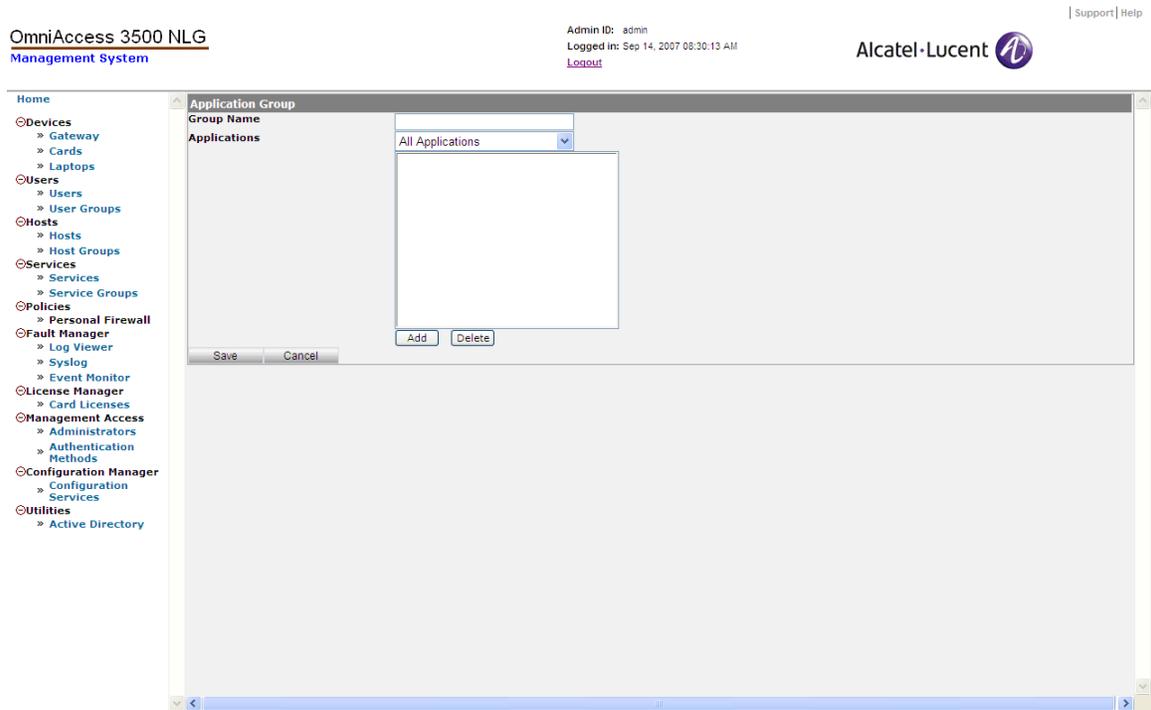


Figure 89 - Application Group

- o **Firewall Policy** – [Personal Firewall|Firewall Policy], [Firewall Policy Definitions], [rw]

List of personal firewall policies. A personal firewall policy consists of a set of packet filter rules and a set of application filter rules. A packet filter rule decides on the treatment of individual packets that traverse the personal firewall on the OmniAccess 3500 NLG card. An application filter rule decides on the opening of laptop-terminated connections for the target application whenever the application requests such opening. Each user group is bound to a single personal firewall policy. Whenever the policy changes, the same modification applies to the personal firewalls of all users in the group. Each entry in the table shows the following information items for identification purposes: <Policy Name> (unique alphanumeric identifier of the firewall policy), <User Control> (indicates whether to allow user control over the firewall policy).

Clicking the <New> tab brings up several tabs which allow the creation of a new personal firewall policy with the configuration of the following objects:

- **General** – [Personal Firewall|Firewall Policy|New|General], [Firewall Policy Settings (Add)], [rw]
 - ◆ **Policy Name** – Unique alphanumeric identifier for the personal firewall policy.
 - ◆ **User Control** – Whether the user will have control to allow or deny applications. Possible values are Allow and Deny.

- ◆ **Unsecured Connectivity Duration** – First timeout used in the Captive Portal Management algorithm, which regulates open access to the Internet during the negotiation of local access credentials with an access point provider. The timeout, expressed in seconds, defines the extension of the time window during which the end user can negotiate the access credentials with the access point provider, in a connectivity scenario that is not secured by the inclusion of the OmniAccess 3500 NLG Gateway in the data path.
- ◆ **Re-activation Wait Period** – Second timeout used in the Captive Portal Management algorithm, which regulates open access to the Internet during the negotiation of local access credentials with an access point provider. The timeout, expressed in seconds, defines the extension of the blackout interval between consecutive attempts to obtain access credentials from the access point provider. The blackout interval prevents the end user from causing continuous exposure of the laptop to external attacks with lengthy credential negotiation procedures.

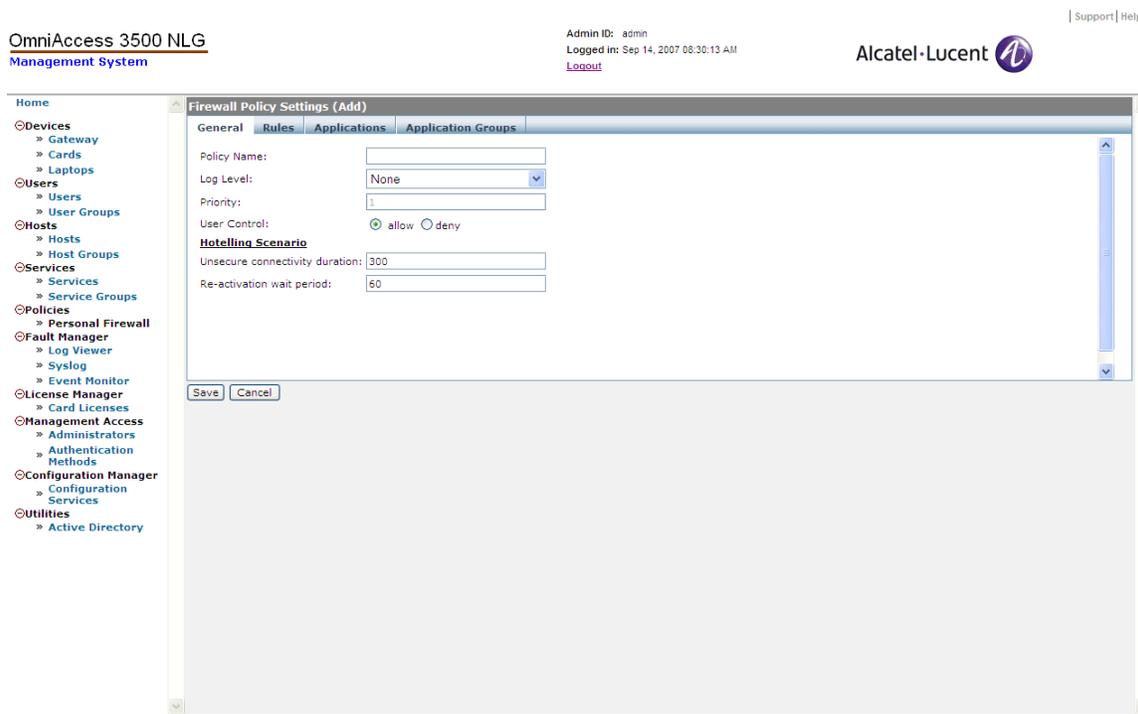


Figure 90 - Firewall Policy Settings General tab

- **Rules** – [Personal Firewall | Firewall Policy | New | Rules], [Firewall Policy Settings (Add)], [rw]
 - ◆ **Rule name** – Unique alphanumeric identifier for the packet filter rule being included in the personal firewall policy.
 - ◆ **Precedence** – The order in which the packet filter rule will be executed. Higher precedence means that the rule will be executed first.

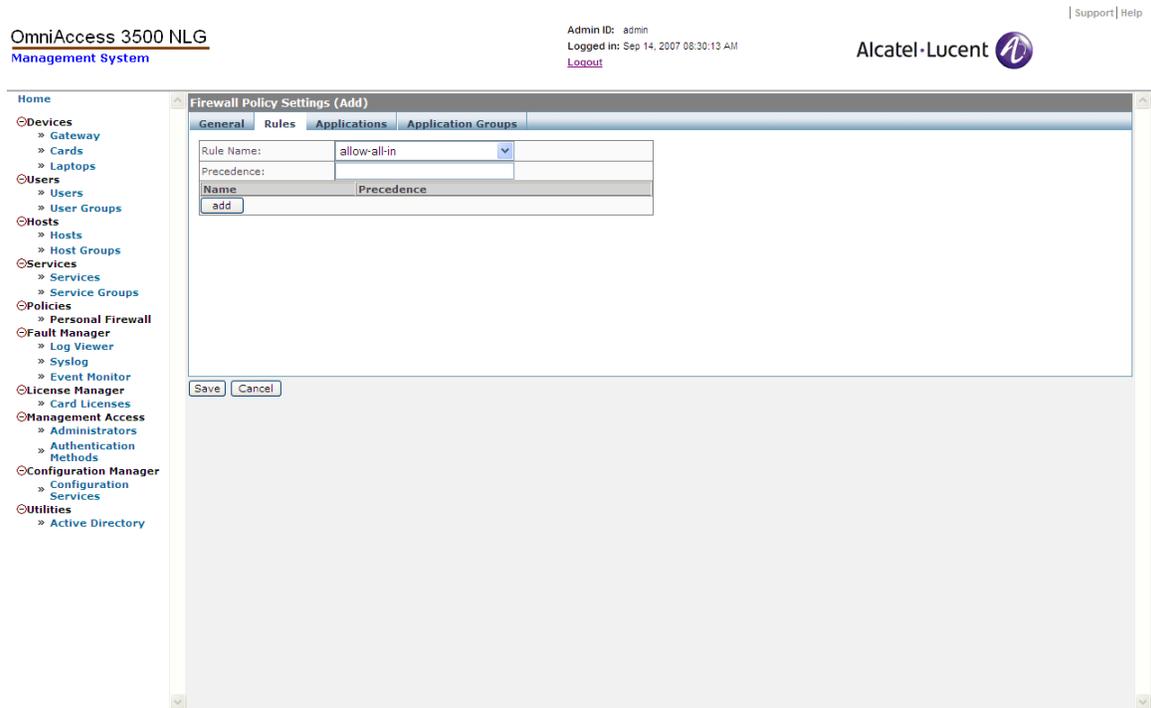


Figure 91 - Firewall Policy Settings Rules tab

- **Applications** — [Personal Firewall|Firewall Policy|New|Applications], [Firewall Policy Settings (Add)], [rw]
 - ◆ **Applications** — List of applications in the application filter table that contributes to the definition of the personal firewall policy.
 - ◆ **Network Access** — An application filter rule can be set as either an allow rule (the application is always allowed to open a remote connection) or a deny rule (the application is never allowed to open a remote connection).

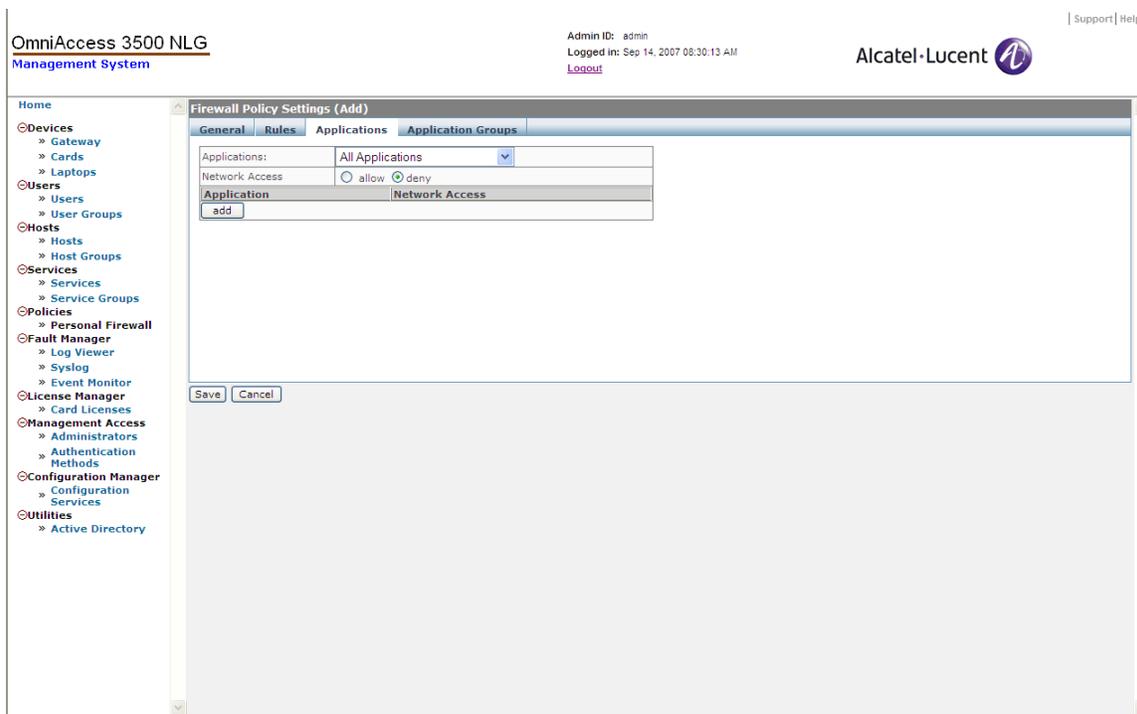


Figure 92 - Firewall Policy Settings Applications tab

- **Application Groups** – [Personal Firewall|Firewall Policy|New|Application Groups], [Firewall Policy Settings (Add)], [rw]
 - ◆ **Application Groups** – List of applications groups in the application filter table that contribute to the definition of the personal firewall policy. Application groups are used to simplify the specification of personal firewall policies, especially when a large number of applications require explicit inclusion in the application filter table.
 - ◆ **Network Access** – The application filter treatment is the same for all the applications in the application group. The network access decision can be set as either an allow rule (the applications in the group are always allowed to open a remote connection) or a deny rule (the applications in the group are never allowed to open a remote connection).

The <Open>, <Edit>, and <Delete> tabs allow to inspect, modify, or remove an existing personal firewall policy.

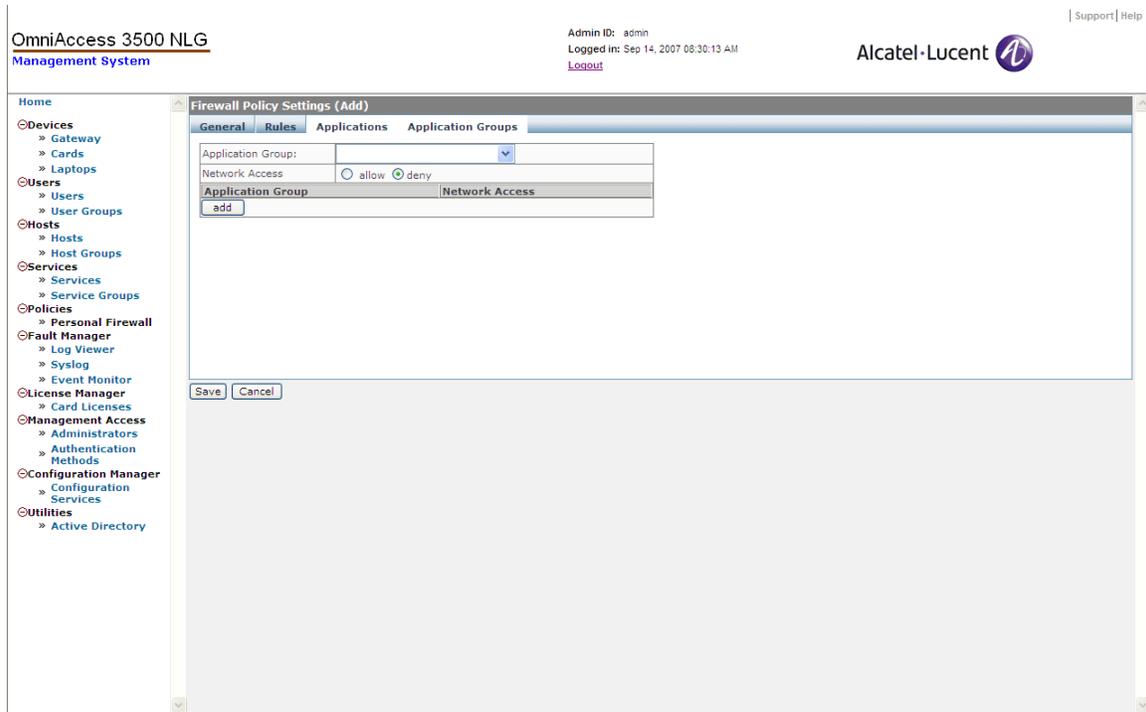


Figure 93 - Firewall Policy Settings Application Groups tab

Fault Manager

In the Fault Manager section of the management system GUI you can access system status information. Through the Fault Manager section, you can view logs and events and configure the interoperation of the OmniAccess 3500 NLG with a syslog server.

- **Log Viewer** – [Log Viewer], [Server Log Viewer], [r]

Logs collected from various portions of the OmniAccess 3500 NLG system. The <Log Viewer> command brings up records containing the following information:

- **Local Time** – Local time of generation of the log record (time zone of the source OmniAccess 3500 NLG node). Format: <yyyy-mm-dd hh:mm:ss>.
- **IP Address** – IP address of the OmniAccess 3500 NLG node (gateway, card, laptop) that generated the log.
- **Event ID** – The type of the logged event.
- **Module Name** – Name of the software module that generated the log.
- **Severity** – Severity of the event reported in the log record.
- **Message** – Additional information describing the event.

OmniAccess 3500 NLG Management System

Admin ID: admin
 Logged in: Nov 07, 2007 09:03:52 PM
 Logout

Alcatel-Lucent

Time	IP Address	Event ID	Module Name	Severity	Message
11/07/2007 09:03:52	10.1.1.13	MS_SERVER_LOGIN1860623611	MS_SERVER_LOGIN	INFO	Successfully logged in to the Management Server
11/07/2007 09:03:52	10.1.1.13	MS_SERVER_LOGIN155579627	MS_SERVER_LOGIN	INFO	Start verifying the admin logon credentials
11/07/2007 08:03:29	10.1.1.13	MS_SERVER_LOGIN-199163439	MS_SERVER_LOGIN	INFO	Successfully logged in to the Management Server
11/07/2007 08:03:29	10.1.1.13	MS_SERVER_LOGIN-1289785888	MS_SERVER_LOGIN	INFO	Start verifying the admin logon credentials
11/07/2007 02:17:46	10.1.1.13	MS_SERVER_LOGIN1096829240	MS_SERVER_LOGIN	INFO	Successfully logged in to the Management Server
11/07/2007 02:17:46	10.1.1.13	MS_SERVER_LOGIN-1979617803	MS_SERVER_LOGIN	INFO	Start verifying the admin logon credentials
11/06/2007 10:28:08	10.1.1.13	MS_SERVER_LOGIN-896537793	MS_SERVER_LOGIN	INFO	Successfully logged in to the Management Server
11/06/2007 10:28:08	10.1.1.13	MS_SERVER_LOGIN-1576015036	MS_SERVER_LOGIN	INFO	Start verifying the admin logon credentials

Refresh (mins.):

Navigation menu:

- Home
- Devices
 - Gateway
 - Cards
 - Laptops
- Users
 - User Groups
- Hosts
 - Hosts
 - Host Groups
- Services
 - Services
 - Service Groups
- Policies
 - Personal Firewall
- Fault Manager
 - Log Viewer
 - Log History
 - Syslog
- License Manager
 - Card Licenses
- Management Access
 - Administrators
 - Authentication Methods
- Configuration Manager
 - Configuration Services
- Utilities
 - Active Directory

Figure 94 - Server Log Viewer

- Syslog — [Syslog], [Syslog Server Settings], [rw]
 Syslog service configuration parameters.
 - Primary Server — First Syslog Server IP address.
 - Secondary Server — Second Syslog Server IP address.
 - Port — The port number to which you want to forward logs.
 - Forward Logs — Set whether or not the Syslog Logs should be forwarded.

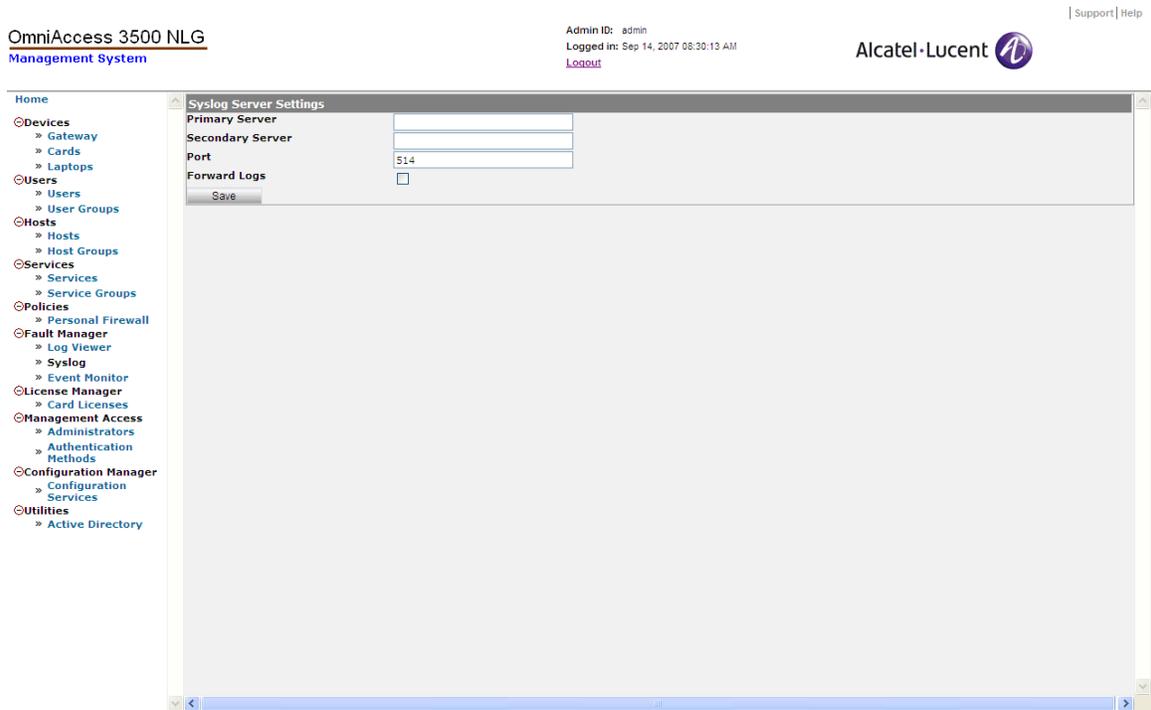


Figure 95 - Syslog Server Settings

- **Log History** – [Server Log History], [r]
 - List of archived event logs. Each entry in the list shows the following information objects:
 - **Time** – Time of generation of the log record (format: <yyyy-mm-dd hh:mm:ss>).
 - **GMT Time** – GMT time of generation of the log record (format: <yyyy-mm-dd hh:mm:ss>).
 - **IP Address** – IP address of the OmniAccess 3500 NLG node (gateway, card, laptop) that generated the event log.
 - **Event ID** – The type of the logged event.
 - **Module Name** – Name of the software module that generated the event log
 - **Severity** – Severity of the event reported in the event log.
 - **Message** – Any additional information about the event.
 - **Refresh (mins.)** – Type a number in this field to indicate how often (in minutes) you would like this window to refresh (default: 1).

OmniAccess 3500 NLG Management System

Admin ID: admin
 Logged in: Nov 07, 2007 09:03:52 PM
 Logout

Alcatel-Lucent

Support | Help

Home

- Devices
 - Gateway
 - Cards
 - Laptops
- Users
 - Users
 - User Groups
- Hosts
 - Hosts
 - Host Groups
- Services
 - Services
 - Service Groups
- Policies
 - Personal Firewall
- Fault Manager
 - Log Viewer
 - Log History
- System
 - License Manager
 - Card Licenses
- Management Access
 - Administrators
 - Authentication Methods
- Configuration Manager
 - Configuration Services
- Utilities
 - Active Directory

Server Log History

Local Time	GMT Time	IP Address	Event ID	Module Name	Severity	Message
11/06/2007 08:25:48	11/06/2007 08:25:48GMT	20.3.0.3	TUNNEL DOWN	USERMGR	INFO	User: evuser1@EVROS, Card: 603C6364
11/06/2007 08:23:41	11/06/2007 08:23:41GMT	20.4.0.3	USER LOGIN	USERMGR	INFO	User: evuser1@EVROS
11/06/2007 08:21:22	11/06/2007 08:21:22GMT	20.3.0.3	CARD INSIDE LAPTOP	USERMGR	INFO	Card 603C6364 inserted into laptop
11/06/2007 08:21:22	11/06/2007 08:21:22GMT	20.3.0.3	PFW SYNC UP MSG	PFWMGR	INFO	SYNC UP msg received from the client 20.3.0.3 Policy= allow-all checksum= 5328
11/06/2007 08:21:29	11/06/2007 08:21:29GMT	20.4.0.3	LAPTOP UP	USERMGR	INFO	User: evuser1@EVROS, Laptop: evros-vm35
11/06/2007 08:15:57	11/06/2007 08:15:57GMT	20.3.0.3	CARD INSIDE LAPTOP	USERMGR	INFO	Card 603C6364 inserted into laptop
11/06/2007 08:15:57	11/06/2007 08:15:57GMT	20.3.0.3	PFW SYNC UP MSG	PFWMGR	INFO	SYNC UP msg received from the client 20.3.0.3 Policy= allow-all checksum= 5371
11/06/2007 08:15:54	11/06/2007 08:15:54GMT	20.4.0.3	LAPTOP DOWN	USERMGR	INFO	User: evuser1@EVROS, Laptop: evros-vm35
11/06/2007 08:15:50	11/06/2007 08:15:50GMT	20.3.0.3	TUNNEL UP	USERMGR	INFO	User: evuser1@EVROS, Card: 603C6364
11/06/2007 06:56:28	11/06/2007 06:56:28GMT	10.1.1.13	MS_SERVER_LOGIN380069104	MS_SERVER_LOGIN	INFO	Successfully logged in to the Management Server
11/06/2007 06:56:28	11/06/2007 06:56:28GMT	10.1.1.13	MS_SERVER_LOGIN2024414216	MS_SERVER_LOGIN	INFO	Start verifying the admin logon credentials
11/06/2007 11:10:10	11/06/2007 11:10:10GMT	20.3.0.4	TUNNEL DOWN	USERMGR	INFO	User: evuser2@EVROS, Card: 1234
11/06/2007 11:03:39	11/06/2007 11:03:39GMT	20.3.0.3	TUNNEL DOWN	USERMGR	INFO	User: evuser@EVROS, Card: 12344321
11/06/2007 11:03:39	11/06/2007 11:03:39GMT	20.3.0.3	PFW SYNC UP MSG	PFWMGR	INFO	SYNC UP msg received from the client 20.3.0.3 Policy= allow-all checksum= 5328
11/06/2007 11:03:39	11/06/2007 11:03:39GMT	20.3.0.3	CARD INSIDE LAPTOP	USERMGR	INFO	Card 12344321 inserted into laptop
11/06/2007 11:03:37	11/06/2007 11:03:37GMT	20.3.0.3	UNKNOWN LAPTOP	USERMGR	MAJOR	Laptop CHENNAITOSHIBA not assigned to user 1
11/06/2007 11:03:34	11/06/2007 11:03:34GMT	20.3.0.3	TUNNEL UP	USERMGR	INFO	User: evuser@EVROS, Card: 12344321
11/06/2007 11:02:47	11/06/2007 11:02:47GMT	20.3.0.3	TUNNEL UP	USERMGR	INFO	User: evuser@EVROS, Card: 12344321
11/06/2007 11:01:56	11/06/2007 11:01:56GMT	20.3.0.4	CARD INSIDE LAPTOP	USERMGR	INFO	Card 1234 inserted into laptop
11/06/2007 11:01:56	11/06/2007 11:01:56GMT	20.3.0.4	PFW SYNC UP MSG	PFWMGR	INFO	SYNC UP msg received from the client 20.3.0.4 Policy= allow-all checksum= 5328
11/06/2007 11:01:54	11/06/2007 11:01:54GMT	20.3.0.4	UNKNOWN LAPTOP	USERMGR	MAJOR	Laptop TOSHIBA-USER not assigned to user 3
11/06/2007 11:01:50	11/06/2007 11:01:50GMT	20.3.0.4	TUNNEL UP	USERMGR	INFO	User: evuser2@EVROS, Card: 1234
11/06/2007 11:01:50	11/06/2007 11:01:50GMT	20.3.0.4	TUNNEL UP	USERMGR	INFO	User: evuser2@EVROS, Card: 1234

Figure 96 - Server Log History

License Manager

Allows for management of user card licenses.

- Card Licenses – [Card Licenses], [Card Licenses], [r]

List of currently active card licenses. Existing licenses can be inspected, renewed, and deleted using the <Open>, <Renew>, and <Delete> tabs respectively. The following information items are shown in the table for each entry:

- Name – A unique name that identifies a particular license.
- Service Provider – The service provider for which this license is valid.
- Max. Licenses – The maximum number of users who can be provisioned into the gateway at any given time.
- Available – Initially displays the same value as the Max. Licenses field. When a license is issued to a user, this field is decremented by one.
- Start Date – The start date for this license in the mm/dd/yyyy format.
- End Date – The end date for this license in the mm/dd/yyyy format

OmniAccess 3500 NLG Management System

Admin ID: admin
 Logged in: Sep 14, 2007 08:30:13 AM
[Logout](#)

Alcatel-Lucent

Home

- Devices
 - Gateway
 - Cards
 - Laptops
- Users
 - User Groups
- Hosts
 - Hosts
 - Host Groups
- Services
 - Service Groups
- Policies
 - Personal Firewall
- Fault Manager
 - Log Viewer
 - Syslog
 - Event Monitor
- License Manager
 - Card Licenses
- Management Access
 - Administrators
 - Authentication Methods
- Configuration Manager
 - Configuration Services
- Utilities
 - Active Directory

Card Licenses

Open New Renew Delete

<input type="checkbox"/>	Name	Service Provider	Max. Licenses	Available	Start Date	End Date
<input type="checkbox"/>	testlic-sprint	sprint	100	100	01/01/2007	12/31/2007
<input type="checkbox"/>	testlic	verizon	100	99	01/01/2007	12/31/2007

Figure 97 - Card Licenses

Upon selection of the <New> tab, the following field appears:

- o **License File** — Presents a text box into which the license file that has been obtained from Alcatel-Lucent can be typed. If this license is valid, a new entry will appear on the Card Licenses window after **Upload License** is clicked.

Upon selection of the <Renew> tab, the License File window appears as described above. Follow the same procedure described above for adding a new license in order to replace the old license file with a new one.

Management Access

In the Management Access section of the management system GUI, you can configure OmniAccess 3500 NLG administrator accounts. In the OmniAccess 3500 NLG R1.2 only one administrator account exists with super-administrator privileges, i.e., with the capability to setup other administrator accounts. Interoperation with a RADIUS server can be configured for authentication of the OmniAccess 3500 NLG administrators.

Through the Management Access section, you can view, add, edit, and delete administrator information and authentication methods.

- **Administrators** — [Administrators], [Administrators Information], [rw]

List of currently configured OmniAccess 3500 NLG administrator accounts. Existing entries can be inspected, modified, and deleted using the <Open>, <Edit>, and <Delete> tabs respectively. The following information items are shown in the table for each entry for identification purposes: <Login ID>, <Name>, <Email>, <Super Admin>, <Account Status>. These and other items are configured upon creation of the administrator account using the <New> tab.

- **Login ID** – Account name used for logging into the management system GUI.
- **Authentication Method** – Method used for authentication of the administrator upon login. Options (choose one): <Local> and <RADIUS>.
- **RADIUS Server** – Select <None> if RADIUS is not selected as the authentication method, or select the IP address of the preferred RADIUS server.
- **First Name** – First name of the account owner.
- **Last Name** – Last name of the account owner.
- **Password** – Password used by the new administrator for logging into the management system GUI.
- **Re-enter Password** – Confirmation replica for the login password.
- **Email** – The corporate e-mail address of the account owner.
- **Address** – Street address of the account owner.
- **City** – Address city of the account owner.
- **State** – Address state of the account owner.
- **Country** – Address country of the account owner.
- **Zip** – Address Zip code of the account owner.
- **Phone** – Wire-line phone number of the account owner.
- **Mobile** – Wireless phone number of the account owner.

OmniAccess 3500 NLG Management System

Admin ID: admin
Logged in: Sep 14, 2007 08:30:13 AM
[Logout](#)

Alcatel-Lucent 

| [Support](#) | [Help](#)

Home

- ⊖ Devices
 - » Gateway
 - » Cards
 - » Laptops
- ⊖ Users
 - » Users
 - » User Groups
- ⊖ Hosts
 - » Hosts
 - » Host Groups
- ⊖ Services
 - » Services
 - » Service Groups
- ⊖ Policies
 - » Personal Firewall
- ⊖ Fault Manager
 - » Log Viewer
 - » Syslog
 - » Event Monitor
- ⊖ License Manager
 - » Card Licenses
- ⊖ Management Access
 - » Administrators
 - » Authentication Methods
- ⊖ Configuration Manager
 - » Configuration Services
- ⊖ Utilities
 - » Active Directory

Administrator Information(Add)

Login ID	<input type="text"/>
Authentication Method	<input type="text" value="Local"/>
Radius Server	<input type="text" value="None"/>
First Name	<input type="text"/>
Last Name	<input type="text"/>
Password	<input type="text"/>
ReEnter Password	<input type="text"/>
Email	<input type="text"/>
Address	<input type="text"/>
	<input type="text"/>
City	<input type="text"/>
State	<input type="text"/>
Country	<input type="text"/>
Zip	<input type="text"/>
Phone	<input type="text"/>
Mobile	<input type="text"/>

Save Cancel

Figure 98 - Administrator Information (Add)

- **Authentication Methods** – [Authentication Methods], [Authentication Methods], [rw]

Clicking on the <RADIUS Server> link provides access to the configuration of RADIUS servers for the authentication of end user and management system administrators. Existing entries can be inspected, modified, and deleted using the <Open>, <Edit>, and <Delete> tabs respectively.

- **Server IP Address** – IP address of the RADIUS server.
- **Authentication Port** – Specifies the UDP destination port for authentication requests (the default value is 1812).
- **Accounting Port** – Currently not used - specifies the UDP destination port for accounting requests (Default 1813).
- **Timeout (secs.)** – The time interval (in seconds) that the OmniAccess 3500 NLG gateway waits for the Radius server to reply before retransmitting (Default 30).
- **Shared Secret** – Specifies the authentication and encryption key for all RADIUS communications between the gateway and the RADIUS server. This key must match the encryption used on the RADIUS daemon.
- **Authentication Method** – Authentication method used - CHAP (use challenge) or PAP (simple password).

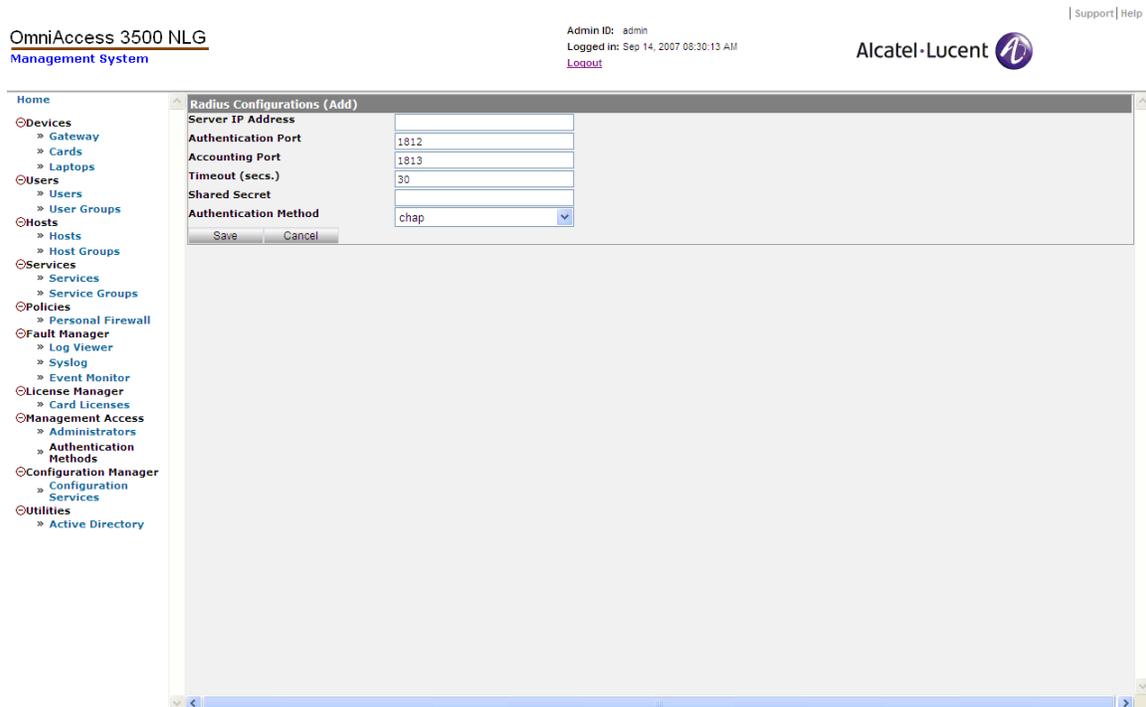


Figure 99 - Radius Configuration (Add)

Configuration Manager

This utility allows the administrator to run gateway maintenance tasks from the EMS GUI.

- **Configuration Services** – [Configuration Manager], [Configuration Services], [r]

The <Gateway Public Key> tab brings up the File Server - Public Key window. The text box on this window contains the Public Key for the Backup File Server. The text is read-only and is populated by the "SSH Public Key" generated internally when the gateway is configured for the first time.

The <Configuration Server Profile> tab brings up the Backup Configuration window, where you can set parameters for the backup server.

- **Backup File Name** – Name assigned to the backup file, where all of the configuration settings are saved.
- **Primary Server IP Address** – IP address of the first server where the backup file is uploaded.
- **Primary Server Username** – Login account on Server 1 where the backup file is stored.
- **Primary Server Path** – Directory path where the backup file is stored when uploaded to Server 1.
- **Secondary Server IP Address** – IP address of a second server where the backup file may be uploaded.
- **Secondary Server Username** – Login account on Server 2 where the backup file may be stored.
- **Secondary Server Path** – Directory path where the backup file is stored if it is uploaded to Server 2.
- **Start Time (hr:mn:sc)** – Reference start time for periodic backups (the mm/dd/yyyy portion, combined with the Backup Frequency value, determines the mm/dd/yyyy value for all future backups; the hr:mm:ss portion is also the hr:mm:ss value for all future backups).
- **Backup Frequency** – Frequency of generation and uploading of configuration backups.

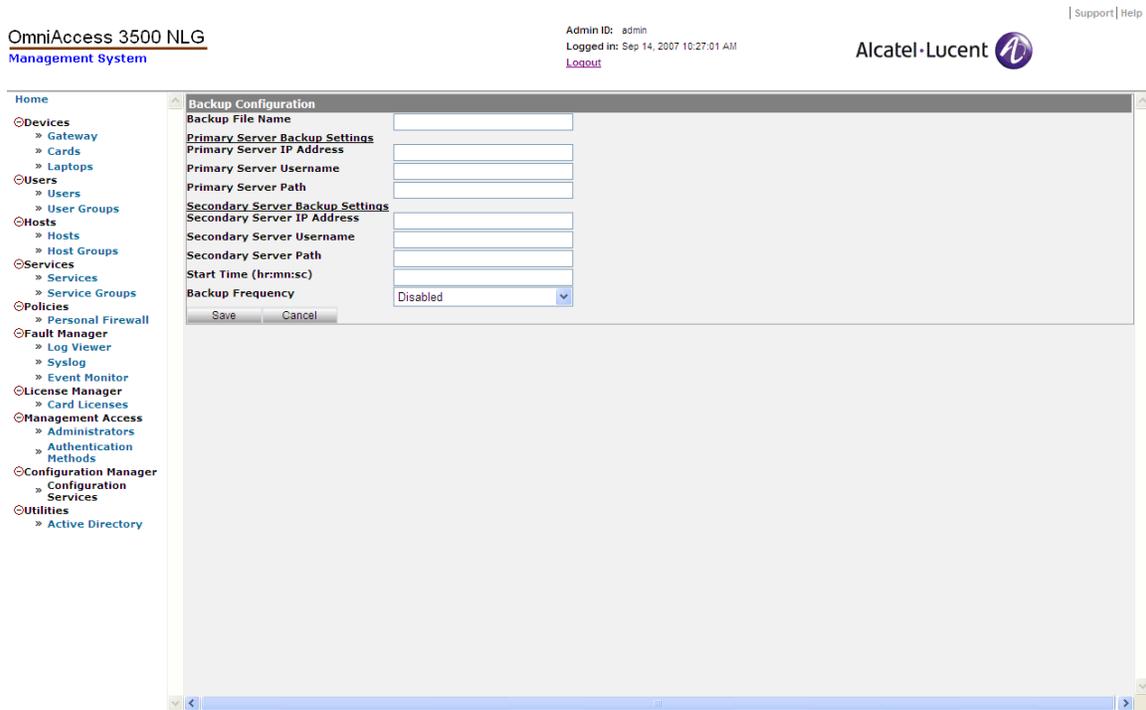


Figure 100 - Backup Configuration

- The <Backup Current Configuration> tab brings up the Backup Configuration window, which is used to request an immediate backup. The values shown on this window are read-only and are taken from the values you entered previously in the Backup Configuration window.
- The <Restore Previous Configuration> tab brings up the Configuration Restore - Step 1 window. From the drop-down list, you can select the IP address for the backup server from which to download a backed-up configuration. The IP addresses that appear are taken from the values you entered previously in the Backup Configuration window.
- The Configuration Restore - Step 2 window displays the backup files available to restore the configuration in a drop-down list.
- The <Upgrade Server Profile> tab brings up the Configure Upgrade Profile (Edit) window, where you can set the following configuration parameters for the gateway:

Upgrade Package Server Settings:

- ◆ **Server Name** – IP address of the Package Distribution Server where the upgrade package is stored.
- ◆ **User Name** – The user name used to access the Package Distribution Server.

Package Settings:

- ◆ **Package Name** – The name of the package that contains all information needed for the upgrade.

- ◆ **Path** – The path where the package is stored in the Package Distribution Server.

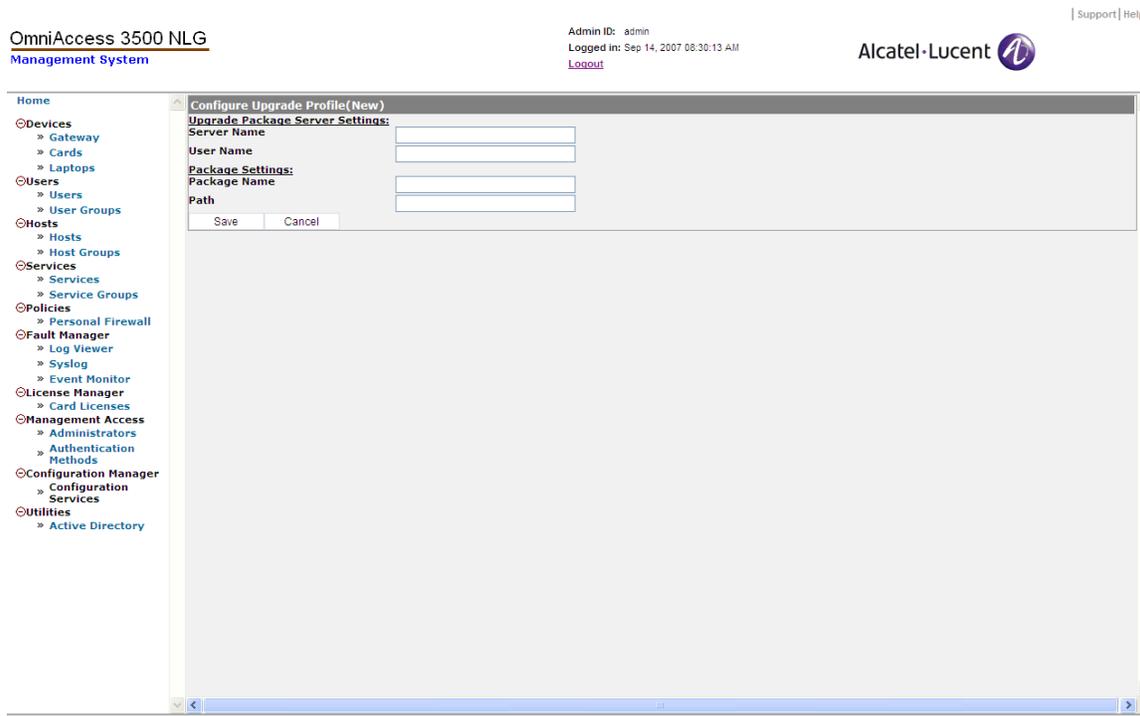


Figure 101 - Configure Upgrade Profile (New)

- The <Upgrade Actions> tab brings up the Upgrade Actions window, which shows the status of the upgrade, and allows the user to start the upgrade.

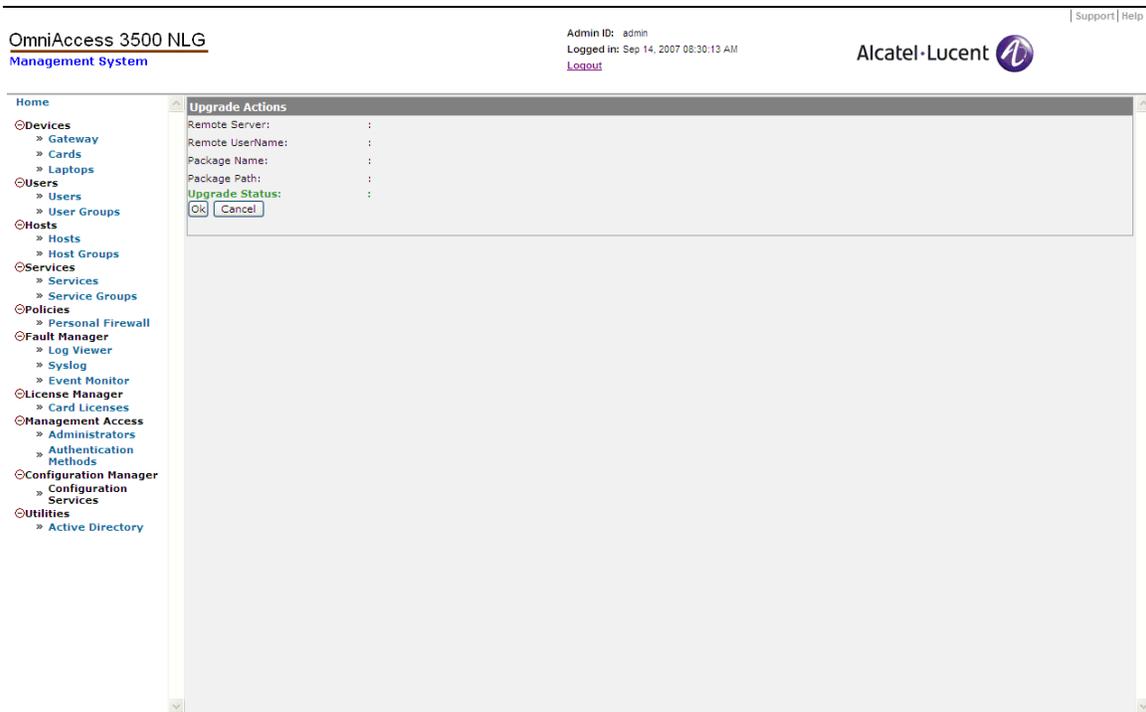


Figure 102 - Upgrade Actions

- The <Reset Upgrade Setting> tab brings up the Reset Upgrade Configuration window, which initiates the command to change the upgrade status on the module back to the idle state.

Utilities

The Utilities section of the management system GUI contains utilities needed for streamlining the most time-consuming functions expected from the OmniAccess 3500 NLG administrator, such as configuring the end user records. Debugging utilities are also included in this section, but are deemed for removal once the system stabilizes.

- **Active Directory** – [Active Directory], [Active Directory - Server Configuration], [rwx]

This utility allows the administrator to import user records directly from the Active Directory server of the enterprise instead of having to enter them manually one by one. The <New> tab enables the configuration of the following parameters:

- **Server IP** – IP address of the Active Directory server to be used as the source of the user record.
- **Password** – Password needed for access to the Active Directory server.
- **Authentication** – Type of authentication required for access by the Active Directory server. The <Simple> option is typical for Active Directory.
- **Search Base CN** – Common name; for example, Administrator, Users.
- **DC** – Domain name (e.g., evros.example.com).

- **NetBIOS** – The NetBIOS name corresponding to the Domain name (e.g., “evros” in the domain name evros.example.com).
- **Directory Name** – Directory name (group to be imported from the Active Directory Server).

The screenshot displays the 'Active Directory Import User Information' form within the OmniAccess 3500 NLG Management System. The form includes the following fields and controls:

- Server IP**: Text input field.
- Password**: Text input field.
- Authentication**: Dropdown menu with 'None' selected.
- Search Base**: Text input field containing 'Administrator,Users'.
- CN**: Text input field.
- DC**: Text input field.
- NetBIOS**: Text input field.
- User Group**: Text input field.
- Save** and **Cancel**: Buttons at the bottom of the form.

The left sidebar shows a navigation tree with categories like Home, Devices, Users, Hosts, Services, Policies, Fault Manager, License Manager, Management Access, Configuration Manager, and Utilities. The top right corner shows the Alcatel-Lucent logo and user information: Admin ID: admin, Logged in: Sep 14, 2007 10:27:01 AM, and a Logout link.

Figure 103 - Active Directory Import User Information

The <Delete> tab removes the selected entry from the Active Directory.

The <Import> tab triggers the automatic import from the Active Directory server of all OmniAccess 3500 NLG-relevant information about users and user groups, so that it doesn't have to be manually entered through the management system GUI.