Alcatel·Lucent

OmniAccess 3500
Nonstop Laptop Guardian
Release 1.2
Gateway Installation Guide

Document Version: 25.05

Part Number: 060227-10 Rev C

Published: 12.19.2007

Alcatel-Lucent Proprietary

Table of Contents

Chapter 1. Introduction

The OmniAccess 3500 Nonstop Laptop Guardian (NLG) gateway is the server component of the OmniAccess 3500 NLG platform. The gateway terminates the secure tunnels initiated by the OmniAccess 3500 NLG cards, manages user credentials and security policies, and provides storage and file-transfer capabilities in support of third-party remote-access and device-management applications. The gateway cooperates with the OmniAccess 3500 NLG card in ensuring that interface switchovers at the user endpoint of the secure tunnels do not disrupt any ongoing network application.

In the OmniAccess 3500 NLG Release 1.2 (R1.2), every instance of the gateway integrates one instance of the OmniAccess 3500 NLG management system. Accordingly, each OmniAccess 3500 NLG R1.2 card depends exclusively on one gateway for access connectivity and on the corresponding management system instance for all OAM&P functions.

This document provides all the information needed for installation and initial configuration of the gateway. The document includes the following sections:

- *Safety Information*: Precautions against the risk of fire, electric shock, and injury.
- *Hardware Overview*: Description of appliance, front and back panels, and interfaces.
- *Installation*: Rack mounting, power connections, and network connections.
- *Initial Configuration*: Software installation and configuration information.
- *Troubleshooting*: Problems that may occur while you are using the gateway, along with solutions.
- *Specification and Compliance Data*: Product dimensions, operating temperatures, electrical specifications, safety regulation compliance, EMC regulation compliance, and disclaimers.

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 2. Safety Information

When installing, operating, or maintaining this equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons, including the following:

- Read and understand all instructions contained in this guide.
- Handle this product in conformity with the applicable building code.
- Follow all warnings and instructions marked on the gateway appliance and accessories.
- Do not place this product on an unstable cart, stand or table. The product may fall and receive serious damage.
- This product should be operated only from the type of power source indicated on the marking label. If you are not sure of the type of power supply, consult your dealer or local Power Company.
- Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
- Do not use this product near water (e.g., in a wet basement).
- Never push objects of any kind into this product through slots as they may touch dangerous voltage points or short-out parts, which could result in a risk of fire or electrical shock. Never spill liquids of any kind on the product.
- Slots and openings in the unit are provided for ventilation, to protect it from overheating; these openings must not be blocked or covered. This product should not be placed in a built-in installation unless proper ventilation is provided.
- **Never disassemble this product.** The product does not contain serviceable parts. Opening or removing covers and/or circuit boards may expose you to dangerous voltages or other risks. Incorrect reassembly can cause electric shock when the unit is subsequently used.
- This product is equipped with a three-wire grounding type plug, a plug having a third (grounding) pin. This plug is intended to fit only into a grounding type power outlet. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not defeat the safety purpose of the grounding type plug. Do not use a 3-to-2-prong adapter at the receptacle. Use of this type of adapter may result in risk of electrical shock and/or damage to this product.
- Do not allow anything to rest on the power cord. Do not locate this product where a person can walk on the cord and abuse it.
- Do not overload wall outlets and extension cords as this can result in the risk of fire or electric shock.
- Unplug this product from the wall outlet and refer to qualified service personnel under the following conditions:
  - When the power supply cord or plug is damaged or frayed.
  - If liquid has been spilled into the product.

- If the product has been exposed to rain or water.
- If the product does not operate normally by following the operating instructions. Adjust only those controls that are covered by the operating instructions.
- If the product has been dropped or the cabinet has been damaged.
- If the product exhibits a distinct change in performance.

Chapter 3. Hardware Overview

The gateway is best deployed as a stub of the enterprise firewall at the edge 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. The physical location of the gateway can be either intra-premises or extra-premises (for example, in a data center).

The gateway comes in a 1U rack-mount appliance (Figure 1) that can be installed in a standard 19-inch rack. The shipment package includes two rack-mounting brackets that attach to the sides of the appliance.

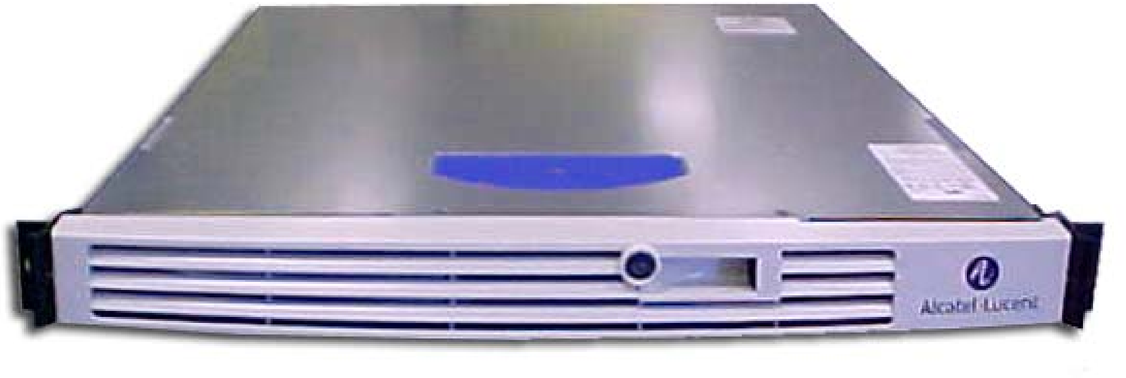


Figure 1: OmniAccess 3500 NLG gateway appliance

Front Panel

A front bezel with the Alcatel-Lucent logo covers the front control panel of the appliance, preventing accidental contact with the power button and visual access to all LEDs. In the product packaging, the key that opens the front bezel is taped to the appliance. For safety purposes, the bezel should be kept in place at all times and only opened to power the product on and off.

The power button and the LEDs on the front control panel of the gateway (normally hidden by the front bezel) are shown in Figure 2 and listed in Table 1.

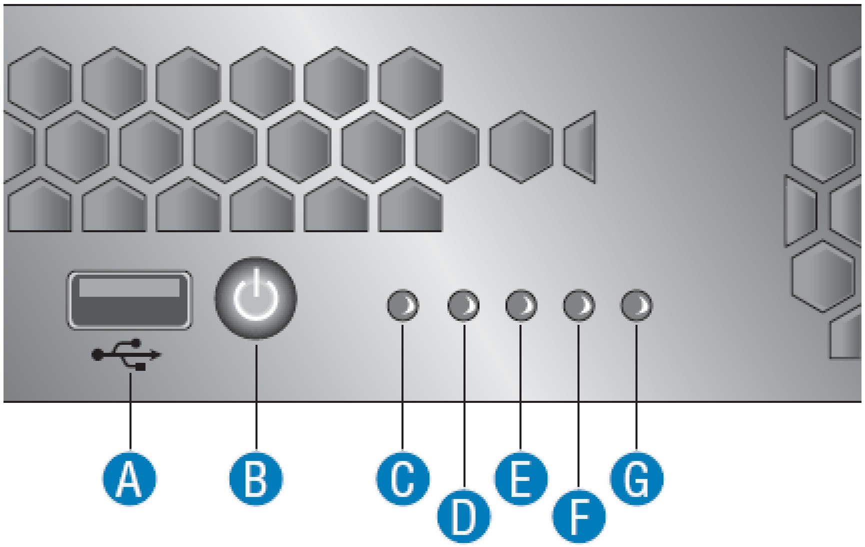


Figure 2: View of the front control panel

Item	Feature
A	USB 2.0 Port (not used)
B	Power Button
C	System Status (not used)
D	System Power LED
E	Hard Disk Drive Activity LED
F	Public Network Interface (WAN) LED
G	Private Network Interface (LAN) LED

Table 1: Front control panel buttons and LEDs

The function of the LEDs on the front control panel of the gateway (normally hidden by the front bezel) is described in Table 2.

LED	Color	State	Description
F, G — Public Network Interface (WAN) and Private Network Interface (LAN) Activity	Green	On	NIC Link / no access
	Green	Blink	Network access
D — Power / Sleep (on standby power)	Green	On	Power on
		Blink	Sleep / ACPI S1 state
	Off	Off	Power Off / ACPI S4 state

C — System Status (on standby power)	Status LED is not used		
E — Disk Activity	Green	Random blink	HDD access
	Off	Off	No hard disk activity

Table 2: Function of the front control panel LEDs

Back Panel

The connectors and data ports on the back panel of the gateway are shown in Figure 3 and listed in Table 3. The WAN and LAN interfaces are labeled on the back panel for immediate identification.

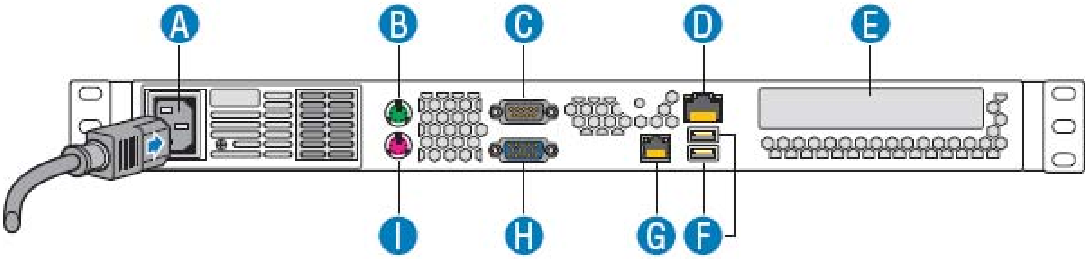


Figure 3: View of the back panel

A	AC power connector	F	USB 2.0 ports 0 and 1 (not used)
B	PS 2 Mouse port (not used)	G	Private Network Interface (LAN)
C	Serial Port (DB9) (not used)	H	Video connector (not used)
D	Public Network Interface (WAN)	I	PS2 Keyboard port (not used)
E	PCI-E/X Add-in Card Slot (not used)		

Table 3: Back panel connectors and data ports

Chapter 4. Installation

Installing the gateway requires two people. To prevent damage to components from electrostatic discharge, always follow the proper guidelines for equipment handling and storage.

Caution: *In order to reduce the static potential, any person installing, removing, or handling the gateway should be properly grounded through the use of an approved antistatic wrist strap.*

Items Required

The following items are required at the installation site:

- Phillips screwdriver
- Three Cat6 Ethernet cables (long enough to run between the gateway and the target network outlets)

  Note: Additional cabling may be required for connectivity through a patch panel.
- A PC with an Ethernet port and a web browser
- The capability to execute the **ktpass** command on the Active Directory Server of the enterprise
- A certificate and associated private key file for the gateway
- A license file for the gateway
- The certificate of the issuing authority for the gateway certificate.

Site Preparation

The gateway has the following environmental and airflow requirements:

- The installation site must maintain at any time the operational temperature and the humidity levels listed in the *Specification and Compliance Data* section of this document.
- Adequate room for proper air ventilation must be allowed at the front, back, and sides of the appliance. No clearance is necessary at the top or bottom of the appliance.

The gateway has the following general electrical requirements:

- One grounded electrical outlet must be available for the AC power supply of gateway.
- To connect the gateway to the grounded electrical outlet, use the supplied AC power cord. Do not use extension cords.

Items Included

Your gateway order includes the following items:

- OmniAccess 3500 NLG Gateway appliance

- AC power cord
- Two side-mount brackets
- Mid-point mounting brackets
- Wrist strap
- Hard copy of the *OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Gateway Quick Start Guide*.

Unpacking the Appliance

To protect the gateway components from electrostatic discharge (ESD) and physical damage, read all the following instructions carefully before beginning.

- Unpack the gateway as close as possible to the location where it will be installed.
- Carefully cut the tape along the seam marked “OPEN HERE FIRST”.
- Carefully remove the protective plastic from the appliance.
- Lift the appliance from the packaging material and move it to the location where it is to be installed.

Rack-Mounting

The gateway can be mounted in the following rack systems:

- Four-post rack system
- Two-post rack system (both mid-mounted and front-mounted).

Rack-mounting the appliance requires two people: one person to hold the appliance and position it in the rack and one person to secure the appliance to the rack by using the attachment screws.

Modify these instructions as appropriate for a cabinet mount.

Mounting in a Four-Post Rack System

Refer to the guidelines below to install the gateway appliance in a 4-post 19” rack.

REMOVE THE APPLIANCE HANDLES

1. Remove two screws (Figure 4) from each handle.
2. Set the handles and screws aside for reattachment later.

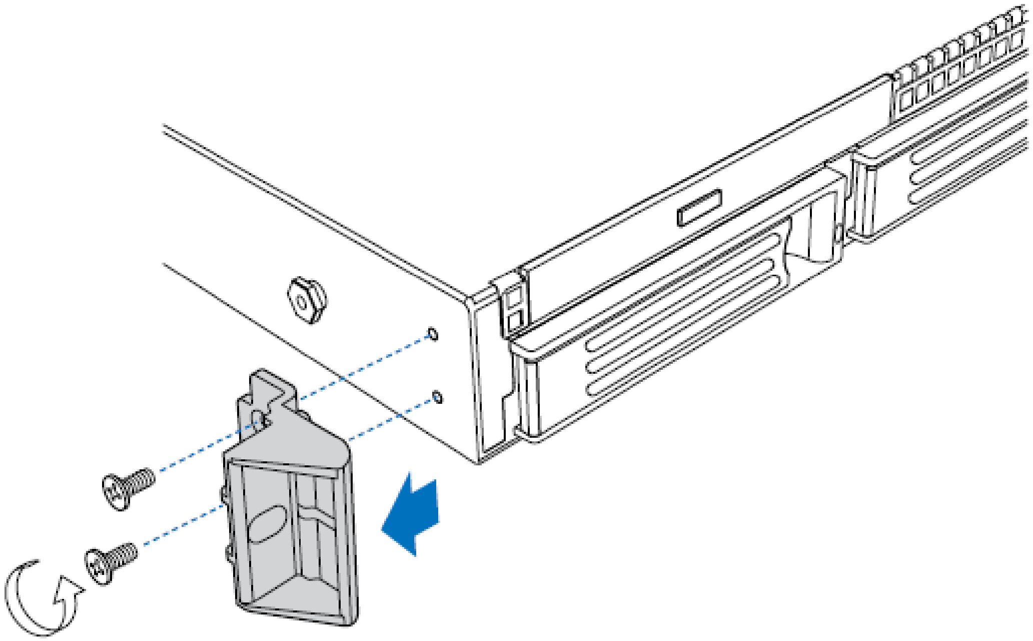
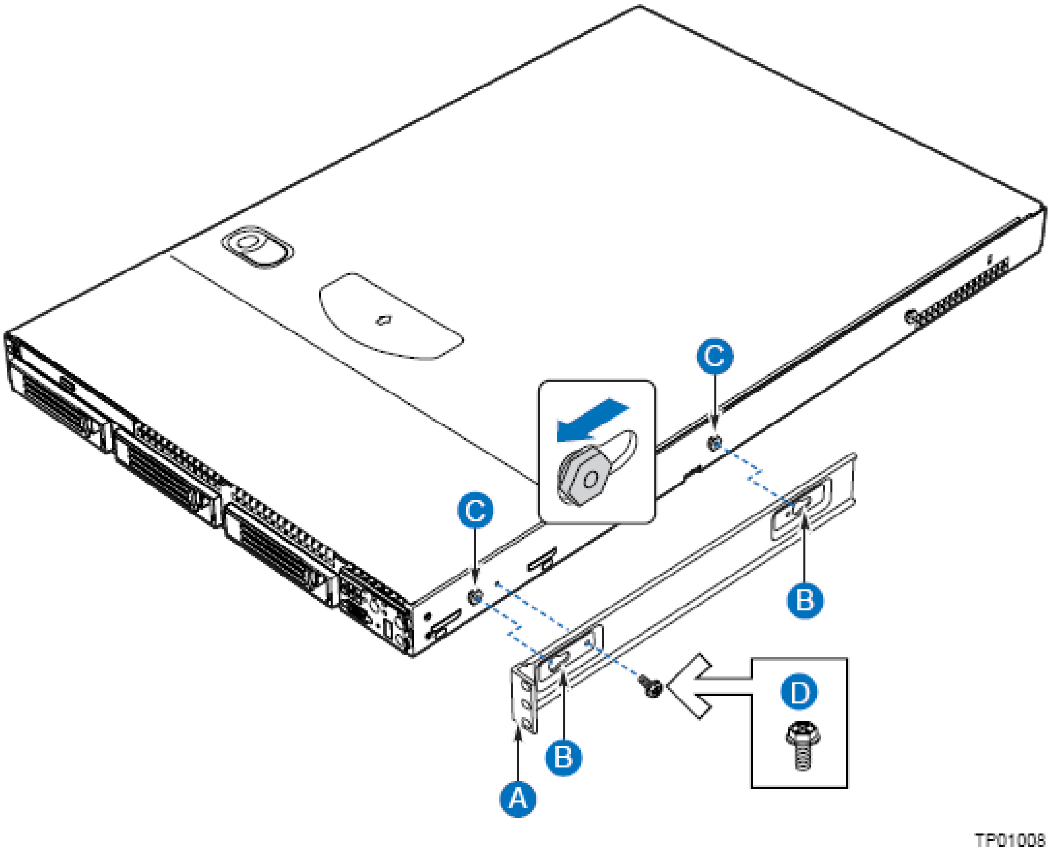


Figure 4: Removing a handle from the appliance

ATTACH BRACKETS TO APPLIANCE

1. Place an appliance bracket along one side of the appliance in the front-mount position (Figure 5, A).
2. Align the holes (B) in the bracket with the tabs (C) on the appliance and place the bracket against the appliance.
3. Slide the bracket as far as it will go toward the front of the appliance.
4. Fasten the bracket to the appliance using screw (D).
5. In the same manner, attach an appliance bracket to the other side of the appliance.

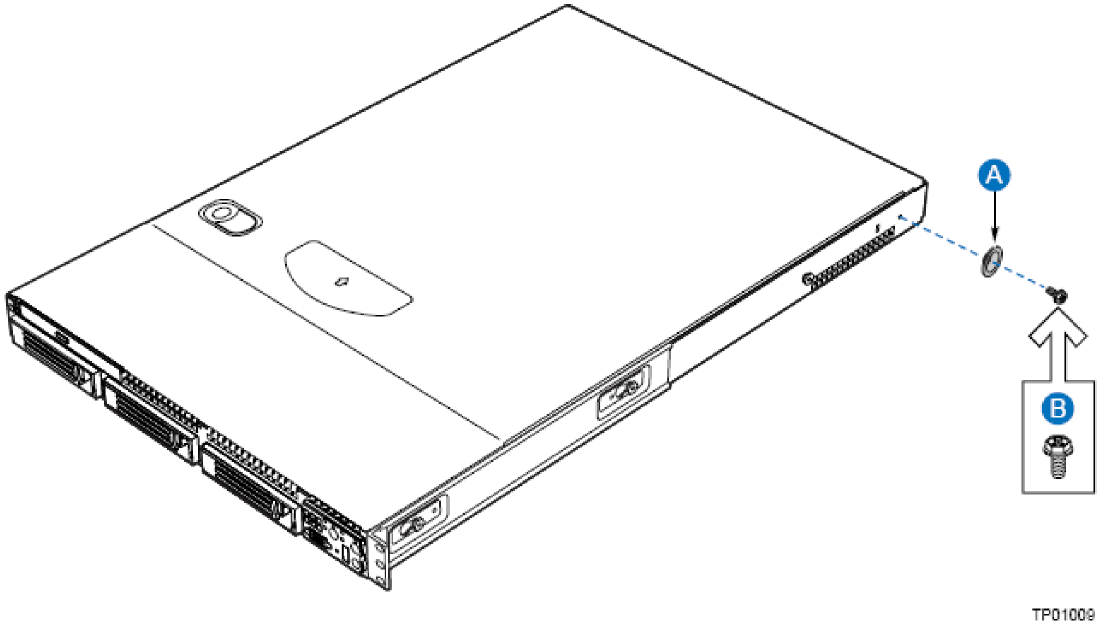


A. Chassis bracket in front-mount position
B. Bracket holes
C. Chassis tabs
D. Hex head screw

Figure 5: Installing an appliance bracket in the front-mount position

ATTACH DISKS TO APPLIANCE

1. Place an appliance disk at the side of the appliance towards the rear (see Figure 6, A).
2. Install screw (B) and tighten.
3. In the same manner, attach an appliance disk to the opposite side of the appliance.

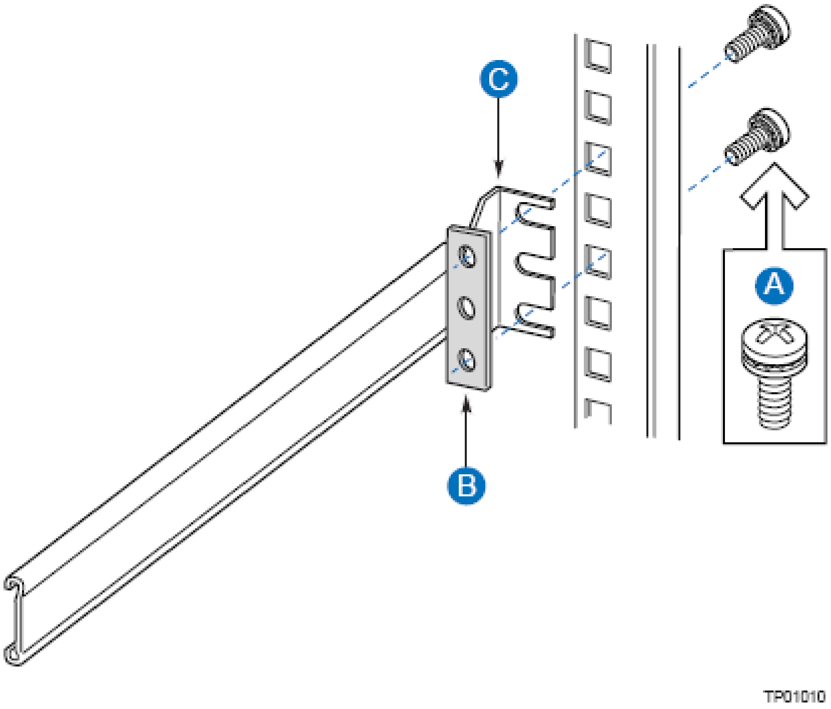


A. Chassis disk
B. Hex head screw

Figure 6: Attaching an appliance disk to the appliance

ATTACH BRACKETS TO REAR POSTS

1. Attach a nut bar (Figure 7, C) on the inside of the two rear rack posts using screws (A). Do not completely tighten the screws—leave them loose enough to allow insertion of the brackets in step 2.
2. Insert the slotted foot of a rear bracket (B) between each nut bar and post.
3. Align the face of the bracket foot with the edge of the rack post and firmly tighten the screws.



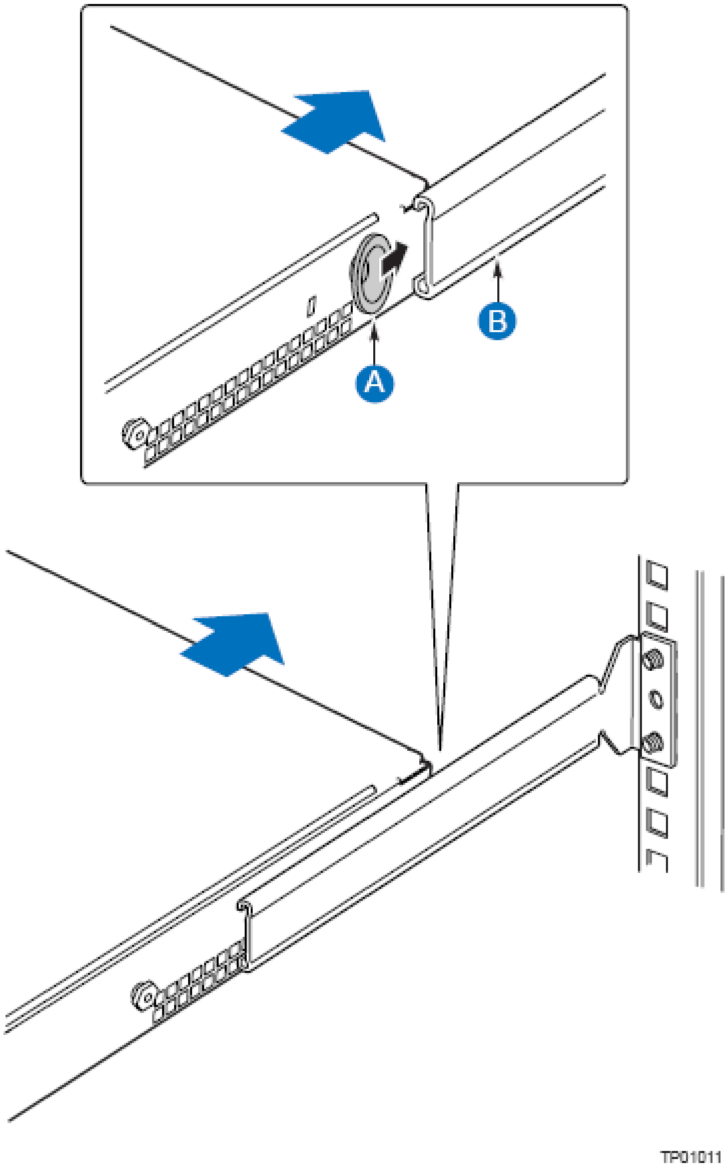
A. #10-32 x ½-inch screw
B. Nut bar
C. Rear bracket

Figure 7: Attaching a rear bracket to a rear post

INSTALL APPLIANCE IN RACK

Caution: Lifting the appliance and attaching it to the rack is a two-person job. If needed, use an appropriate lifting device.

1. With the appliance front facing you, lift the appliance and position the appliance disks (Figure 8, A) so they fit in the rear brackets (B).).

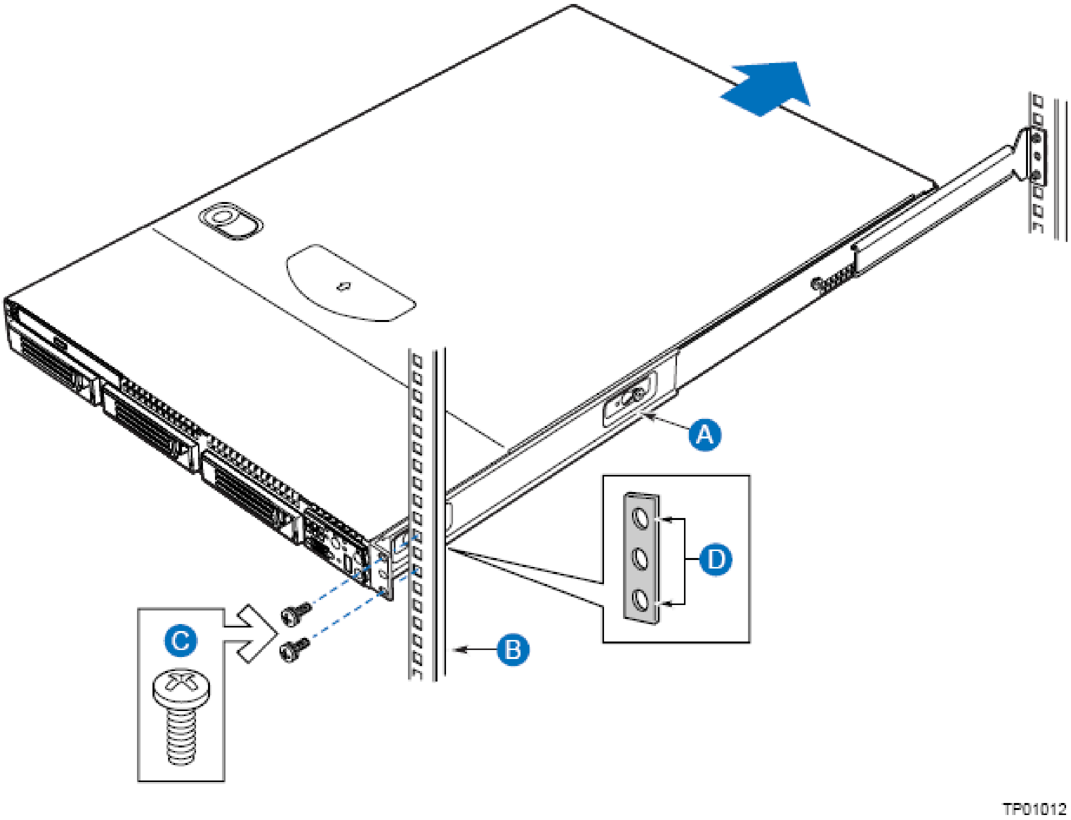


A. Chassis disk
B. Rear bracket

Figure 8: Installing the appliance in the rear brackets

2. Slide the appliance toward the rear of the rack until the front of the appliance brackets contact the front posts.

3. Attach the appliance brackets (Figure 9, A) to the front posts (B) using two screws (C) and one nut bar (D) per side.



A. Chassis bracket
B. Front post
C. #10-32 x ½-inch screw
D. Nut bar

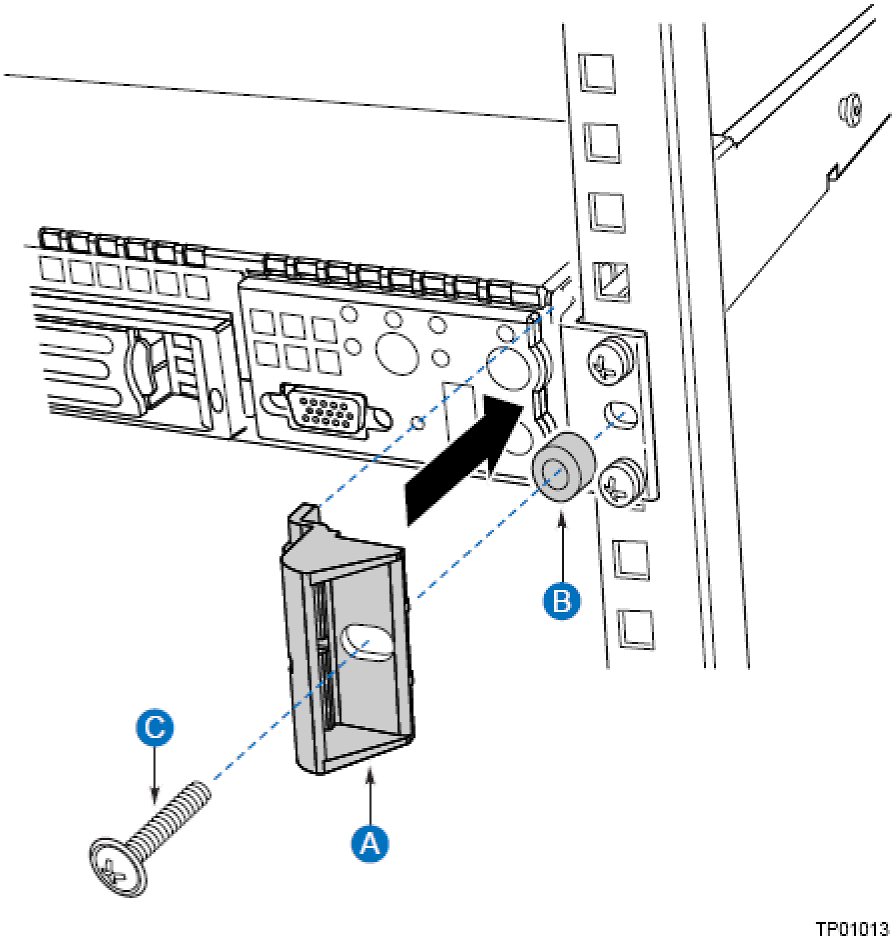
Figure 9: Attaching a front bracket to a front post

INSTALL APPLIANCE HANDLES

NOTE: The handles are required to hold the bezel on. If you will not be installing a bezel, you do not need to install the handles.

1. Slide a handle (Figure 10, A) between the appliance and the appliance bracket.
2. Align the hole in the handle with the unused hole in the appliance bracket.
3. Install a spacer (B) between the handle and the appliance bracket.
4. Install and tighten screw (C) to secure the handle.
5. In the same manner, attach the other handle to the opposite side.

You have completed the installation of your appliance in a four-post rack system.



A. Chassis handle
B. Spacer
C. #10-32 x 7/8-inch screw with washer

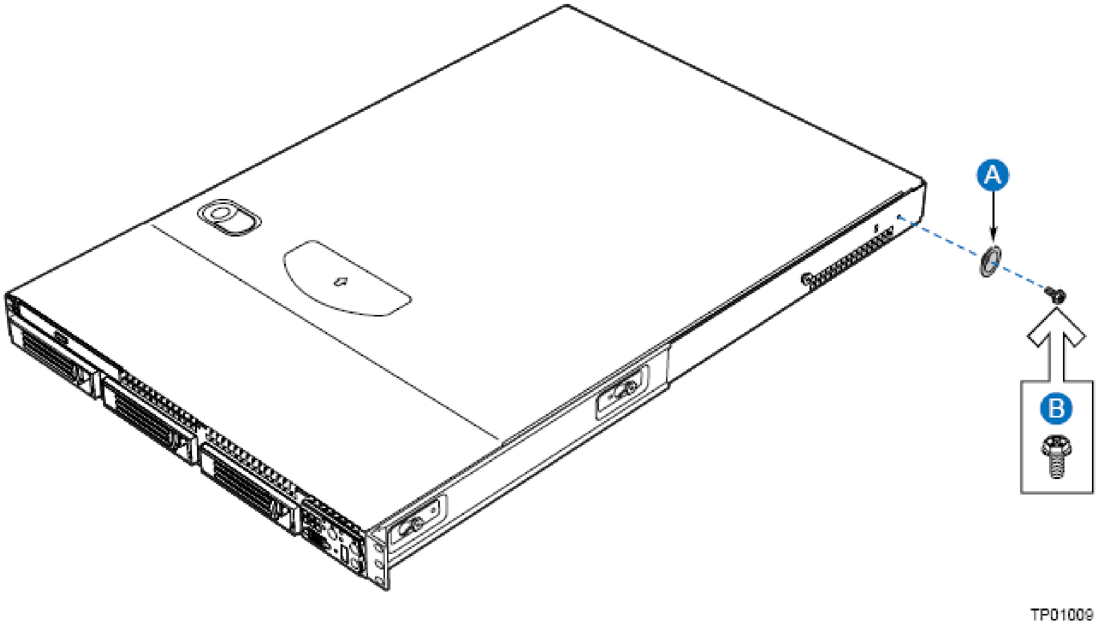
Figure 10: Attaching an appliance handle to a front post

Mid-Mounting in a Two-Post Rack System

Refer to the guidelines below to mid-mount the gateway appliance in a 2-post 19” rack.

REMOVE THE APPLIANCE HANDLES

1. Remove two screws (Figure 11) from each handle.
2. Save the handles and screws for possible future reattachment. You will not reattach them as part of this process.

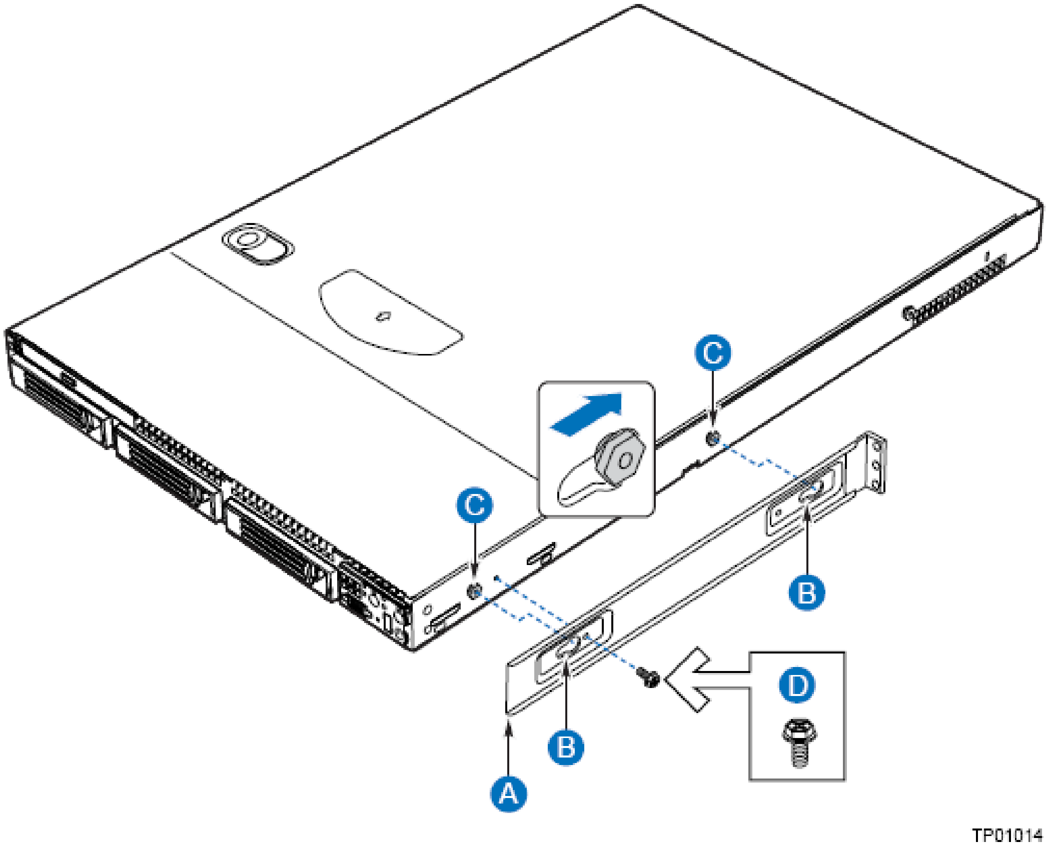


A. Chassis disk
B. Hex head screw

Figure 11: Removing a handle from the appliance

Attach Brackets to Appliance

1. Place a mounting bracket (Figure 12, A) along one side of the appliance in the mid-mount position.
2. Align the holes (B) in the bracket with the tabs (C) on the appliance and place the bracket against the appliance.
3. Slide the bracket as far as it will go toward the front of the appliance.
4. Fasten the bracket to the appliance using screw (D).
5. In the same manner, attach a bracket to the other side of the appliance.

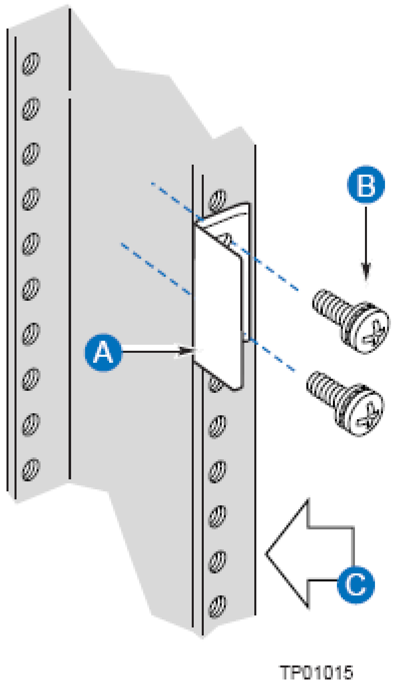


A. Chassis bracket in mid-mount position
B. Bracket holes
C. Chassis tabs
D. Hex head screw

Figure 12: Installing an appliance bracket in the mid-mount position

ATTACH L BRACKETS TO CENTER POSTS

1. Position an L bracket (Figure 13, A) on the backside of the center post (C).
2. Attach the L bracket to the center post using the screws (B) supplied with your rack. Do not fully tighten at this time.
3. In the same manner, attach an L bracket to the other center post.



A. L bracket
B. Screw
C. Front side of typical right center post

Figure 13: Attaching an L bracket to a center post

Install Appliance in Rack

Caution: Lifting the appliance and attaching it to the rack is a two-person job. If needed, use an appropriate lifting device.

1. Locate one person at the front of the rack and one at the rear.
2. Position the appliance so that the L brackets (Figure 14, A) are inserted into the appliance mounting brackets (B).
3. While supporting the weight of the appliance, adjust the L brackets to fit tightly into the appliance brackets (C).

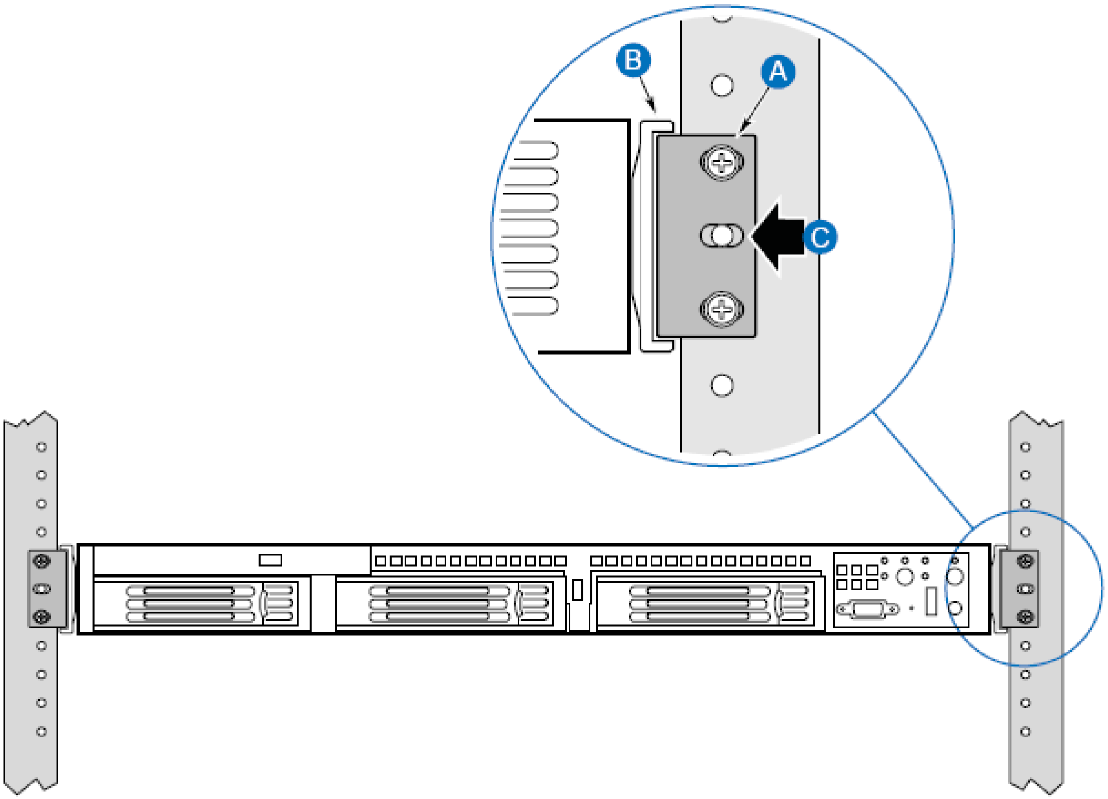
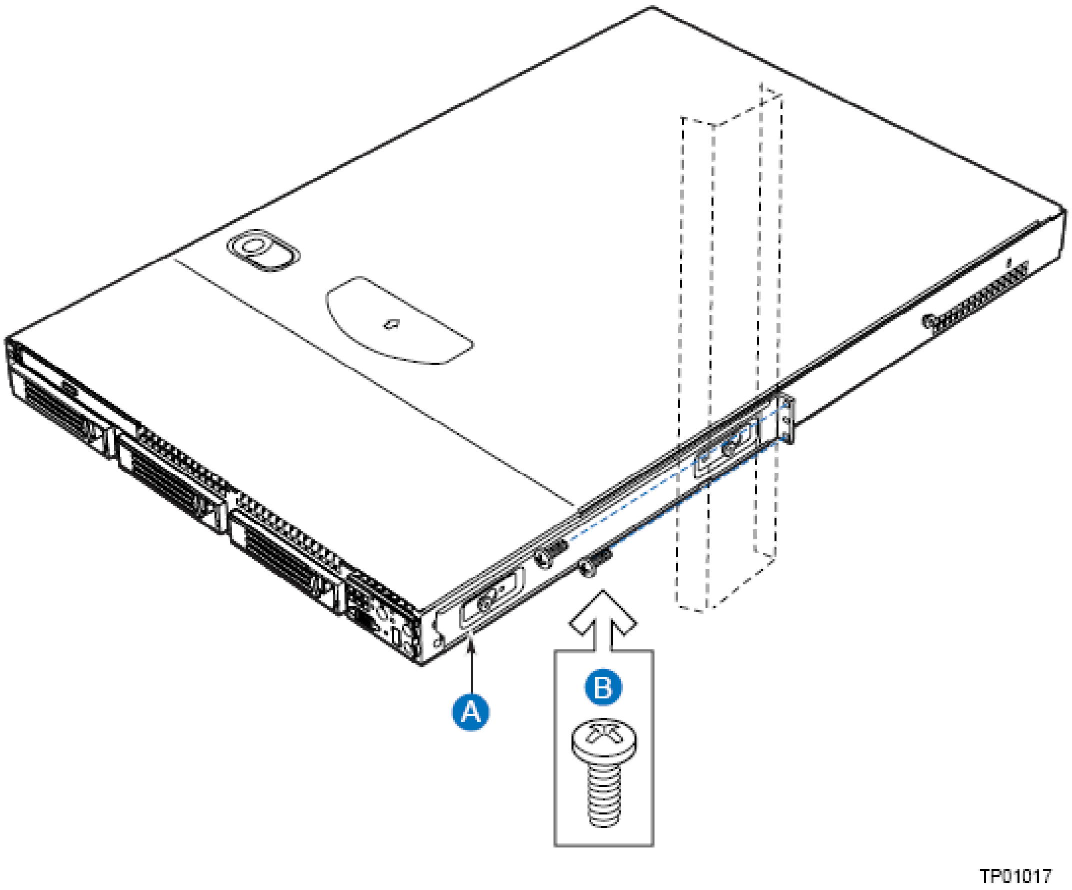


Figure 14: L brackets inserted into appliance mounting bracket (front view)

4. Slide the appliance toward the front of the rack until the front of the appliance mounting brackets contact the rear of the center posts.
5. Using the screws (Figure 15, C) supplied with your rack, attach the front of the mounting brackets to the front of the center posts.



A. Chassis bracket in mid-mount position
B. L bracket
C. Screw

Figure 15: Installing the appliance in the rack

You have completed the mid-mount installation of your appliance in a two-post rack system.

Front-Mounting in a Two-Post Rack System

Refer to the guidelines below to front-mount the gateway appliance in a 2-post 19" rack.

WARNING: *Your appliance's rack mount kit provides the option for mounting the system in a two post front-mount-only configuration. However, mounting your appliance using this option is not recommended for use in most rack systems. If a front-mount-only configuration is desired, it is highly recommended that you verify through your rack vendor that your specific rack is designed to support the excessive weight and stresses this type of mounting configuration imposes on the rack.*

Structural failure of the rack is likely if it is not designed for this type of load. A four-post or a two-post mid-mount configuration should be used when possible.

REMOVE THE APPLIANCE HANDLES

1. Remove two screws from each handle (see Figure 16).
2. Set the handles and screws aside for reattachment later.

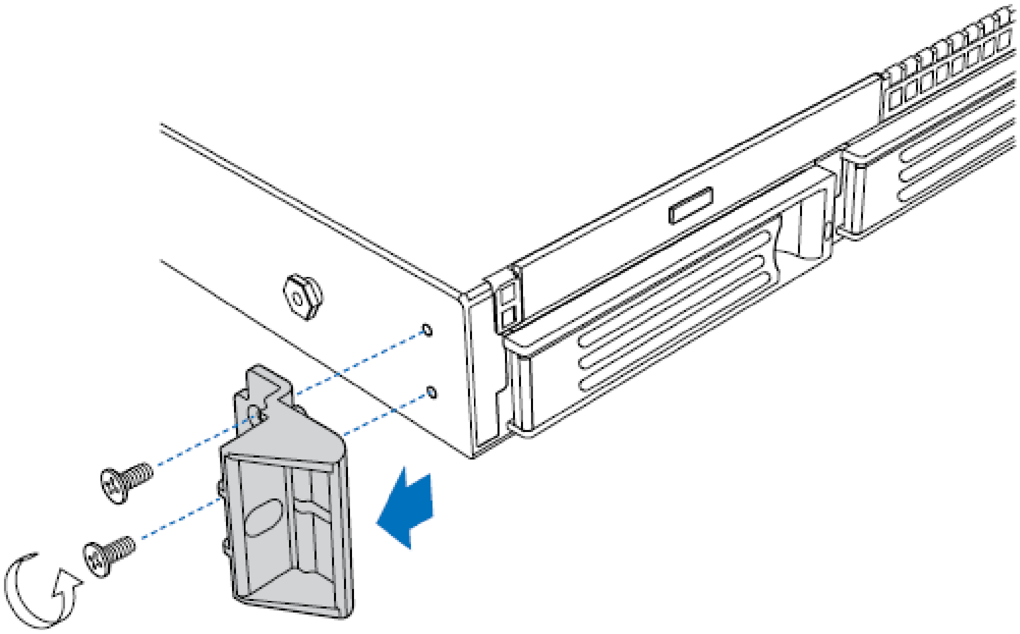
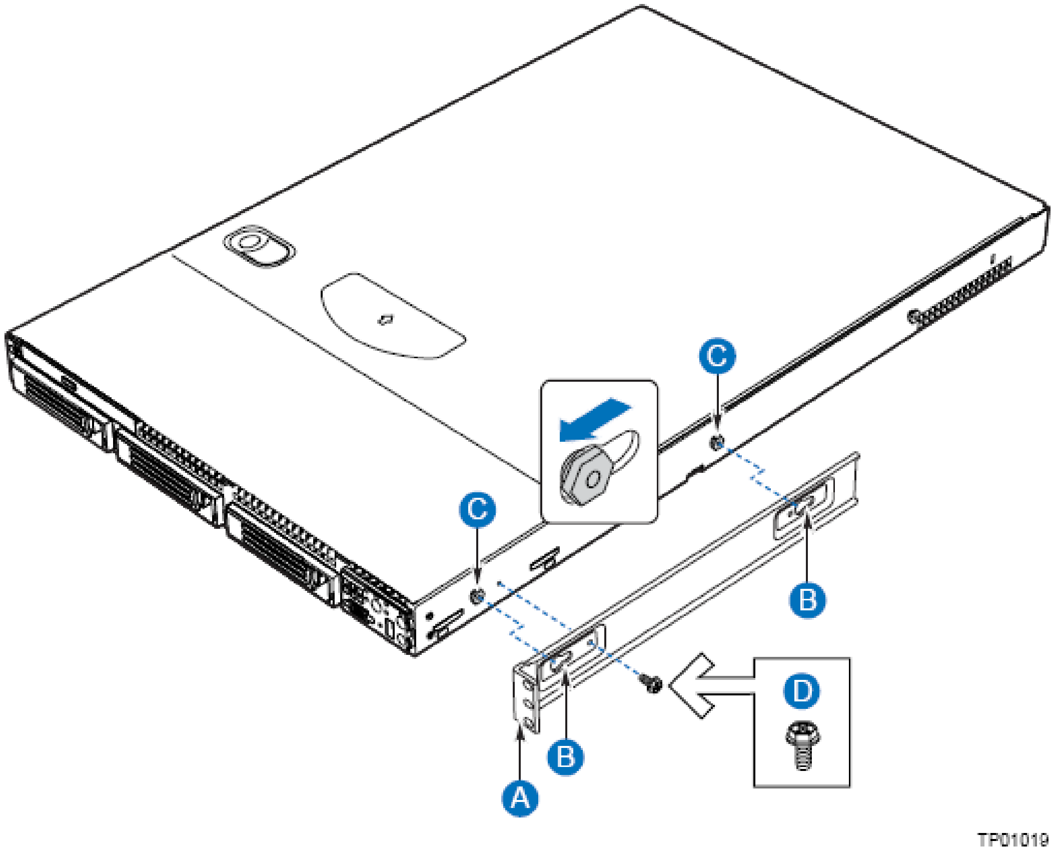


Figure 16: Removing a handle from the appliance

ATTACH BRACKETS TO APPLIANCE

1. Place a mounting bracket (Figure 17, A) along one side of the appliance in the front-mount position.
2. Align the holes (B) in the bracket with the tabs (C) on the appliance and place the bracket against the appliance.
3. Slide the bracket as far as it will go toward the front of the appliance.
4. Attach the bracket to the appliance using screw (D).
5. In the same manner, attach a bracket to the other side of the appliance.

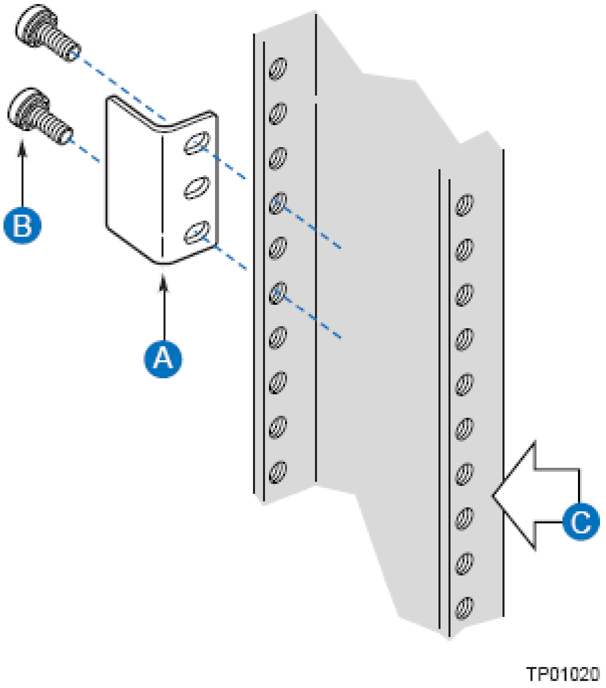


A. Chassis bracket in front-mount position
B. Bracket holes
C. Chassis tabs
D. Hex head screw

Figure 17: Installing an appliance bracket in the front-mount position

ATTACH L BRACKETS TO CENTER POSTS

1. Position an L bracket (Figure 18, A) on the backside of the center post (C).
2. Attach the L bracket to the center post using the screws (B) supplied with your rack. Do not fully tighten at this time.
3. In the same manner, attach an L bracket to the other center post.



A. L bracket
B. Screw
C. Front flange of typical right center post

Figure 18: Attaching an L bracket to a center post

INSTALL APPLIANCE IN RACK

Caution: Lifting the appliance and attaching it to the rack is a two-person job. If needed, use an appropriate lifting device.

1. Locate one person at the front of the rack and one at the rear.
2. Position the appliance so that the L brackets (Figure 19, A) are inserted into the appliance mounting brackets (B).
3. While supporting the weight of the appliance, adjust the L brackets to fit tightly into the appliance brackets (C).

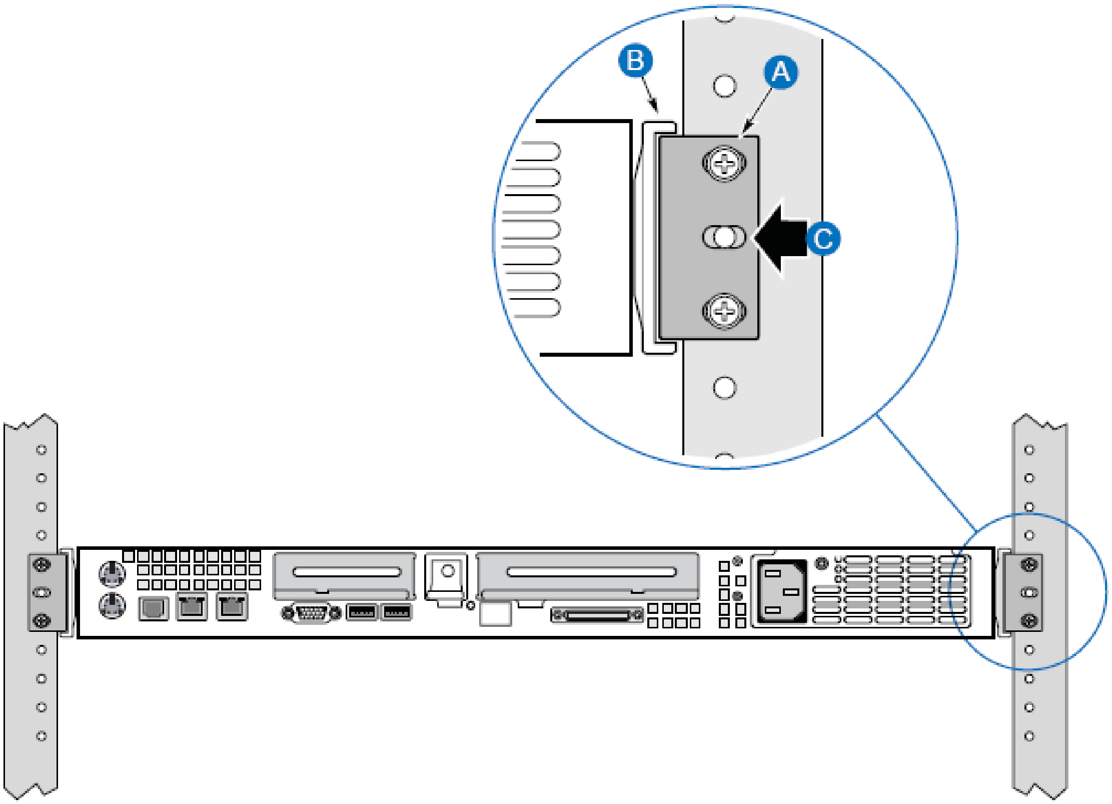
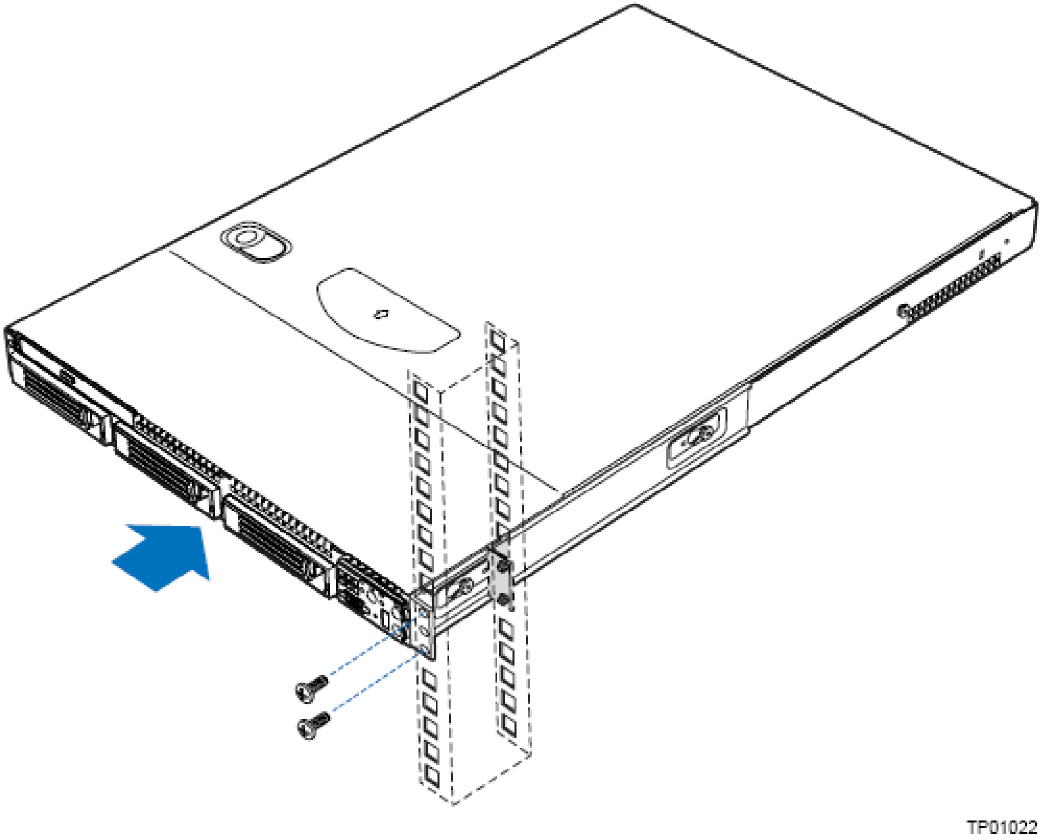


Figure 19: L brackets inserted into appliance mounting brackets (rear view)

4. Slide the appliance toward the rear of the rack until the front of the appliance brackets contact the front of the center posts.
5. Using the fasteners (Figure 20, C) supplied with your rack, attach the front of the mounting brackets to the front of the center posts.



A. Chassis bracket in front-mount position
B. L bracket
C. Screw (supplied by rack manufacturer)

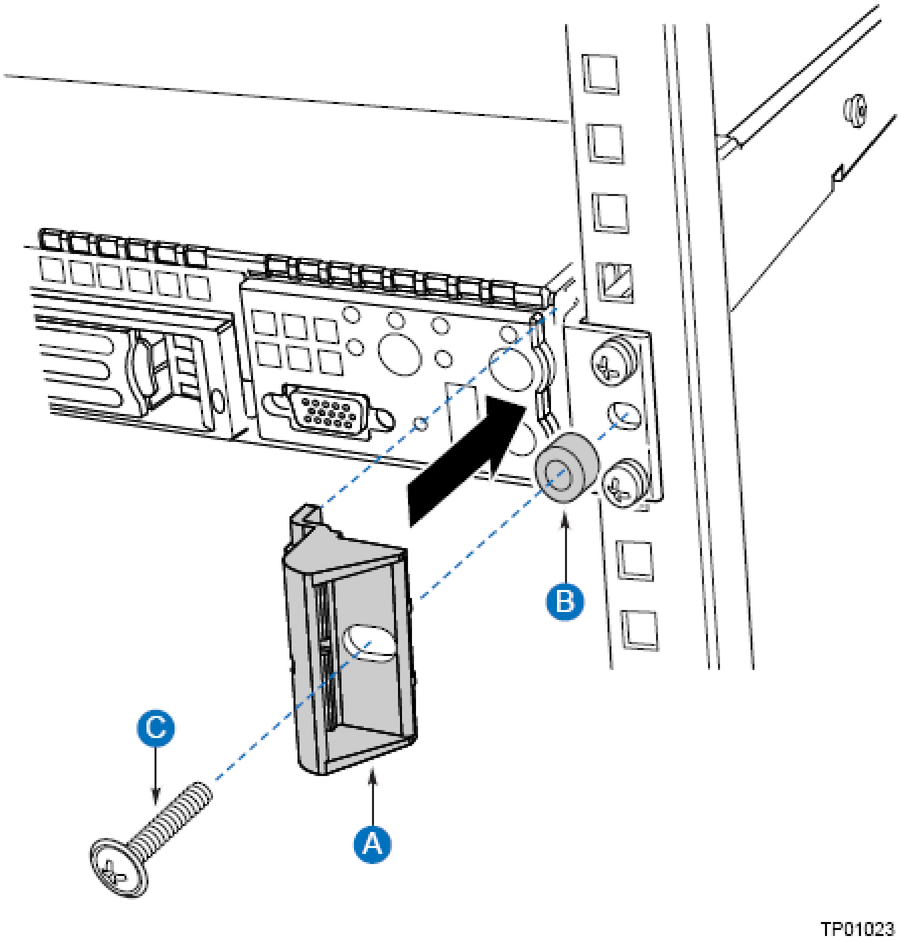
Figure 20: Installing the appliance in the rack

INSTALL APPLIANCE HANDLES

Note: The handles are only required to hold the bezel on. If you will not be installing a bezel, you do not need to install the handles.

1. Slide a handle (Figure 21, A) between the appliance and the appliance bracket.
2. Align the hole in the handle with the unused hole in the appliance bracket.
3. Install a spacer (B) between the handle and the bracket.
4. Install and tighten screw (C) to secure the handle.
5. In the same manner, attach the other handle to the opposite side.

You have completed the front-mount installation of your appliance in a two-post rack system.



A. Chassis handle
B. Spacer
C. #10-32 x 7/8-inch screw with washer

Figure 21: Attaching an appliance handle to a front post

Power Supply Connections

Take the power cord that comes with the unit and connect it to the power supply connector on the back.

Data Connections

The network and management cables should be connected once the gateway is properly installed. Connections may include:

- One Ethernet connection exchanging traffic with the public Internet via the enterprise firewall (WAN interface, item D in Figure 3).
- One Ethernet connection facing the private network (LAN interface, item G in Figure 3).

Ethernet specifications are as follows:

- WAN (NIC1): Intel® 10/100/1000 82573E Gigabit Ethernet Controller:
  - Integrated for 10/100/1000 Mb/s full- and half-duplex operation
  - IEEE 802.3ab Auto-Negotiation and PHY compliance and compatibility
  - Optimized transmit and receive queues
  - IEEE 802.3x-compliant flow control with software controlled pause times and threshold value
- LAN (NIC2): Intel® 10/100/1000 82541PI Gigabit Ethernet Controller:
  - Integrated for 10/100/1000 Mb/s full- and half-duplex operation
  - IEEE 802.3ab Auto-Negotiation and PHY compliance and compatibility
  - IEEE 802.3x-compliant flow-control support with software-controllable thresholds
  - Jumbo frame support up to 16 KB

Chapter 5. Initial Configuration

The initial configuration of the gateway is driven by the deployment scenario and by the network architecture. Please refer to the *OmniAccess 3500 Nonstop Laptop Guardian Technical Overview* document for more information on possible deployment scenarios.

This section describes the necessary configuration steps for the most common deployment scenario, where the gateway is located in the demilitarized zone (DMZ) of the enterprise network and other enterprise resources, e.g., the Active Directory Server (ADS), DNS, etc., are located in the secure zone, behind the enterprise firewall. Figure 22 shows the installation of the OmniAccess 3500 NLG gateway as a stub of the enterprise firewall in such a deployment scenario.

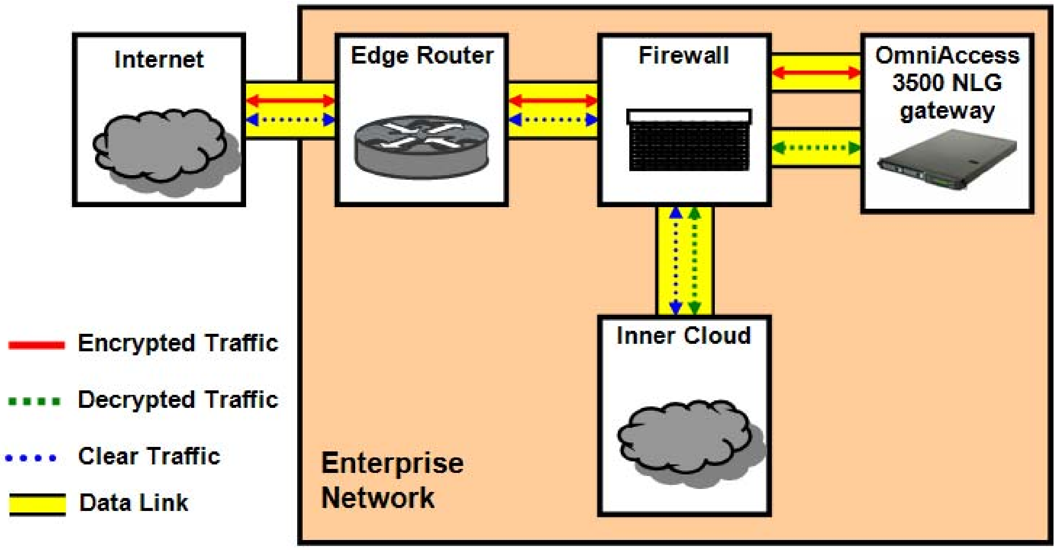


Figure 22: Sample network for the configuration examples

The configuration steps described in this section are sufficient to make (i) the gateway operational within the network and (ii) the web-based management system GUI accessible from a remote PC. Any subsequent configuration step relies on the management system GUI and is detailed in the *OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Administration Guide*.

Gateway Configuration Overview

The following configuration steps are **STRICTLY NECESSARY** to make the gateway fully operational within your network:

1. **Keytab File Generation** — Log into your Active Directory Server (ADS) and generate the keytab file that the gateway will use for automatic authentication with the ADS.
2. **DNS Configuration** — Apply a split DNS configuration to the DNS server of your enterprise network for resolution of the gateway's FQDN.

3. **Router Configuration** — Add a static route to the enterprise router adjacent to the gateway for every pool of VPN addresses that you allocate for the laptops and cards (see the description of the Card/Laptop Address Range/Mask parameters in the *Configuration of Basic Parameters* section below).
4. **Basic Gateway Configuration** — Use the pre-configured IP address of the gateway to set its networking parameters (including the permanent IP addresses of the two network interfaces) and other basic parameters.

Keytab File Generation on the Active Directory Server

To support the Single Sign-On (SSO) feature of the OmniAccess 3500 NLG platform, it is necessary that the gateway communicate with the authentication infrastructure of the enterprise. The OmniAccess 3500 NLG R1.2 only supports Microsoft Active Directory and RADIUS for end-user authentication. The integration of the OmniAccess 3500 NLG platform with the Active Directory infrastructure of the enterprise requires the establishment of a trust relationship between the gateway and the Active Directory Server (ADS). The following configuration steps enable the establishment of the trust relationship:

1. Log into the Active Directory Server (ADS) and create a user account (e.g., **evauth1**) and password (e.g., **evros123#** — do not use this password in practice) in the Active Directory database. The user account name (**evauth1** in the example) is also called the Service Principal Name (SPN) of the OmniAccess 3500 NLG authentication service. For the new user account, set the options that the user (i.e., the OmniAccess 3500 NLG authentication service) is not required to change the password on the next login and that the password never expires. This set of credentials will be used by the gateway for authenticating itself with the ADS every time a laptop user seeks Windows NT authentication: if the gateway credentials were instead set to expire, the authentication of laptop users would start failing with no apparent reason.
2. Create in the ADS the keytab file for the gateway by executing the command **ktpass** on the command prompt of the Windows Active Directory Server. Copy the keytab file in the computer that you will use for initial configuration of the gateway. You will eventually upload the keytab file to the gateway, so that the gateway can use it for authentication with the ADS.

   Use the following sample command to generate the keytab file in the ADS:

   ```
   $ ktpass -princ EVAUTH1/guard1.evros.sample-net.com@EVROS.SAMPLE-NET.COM -
   mapuser EVROS\evauth1 -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -mapop
   set +desonly -pass evros123# -out C:\evauthkeytab1
   ```

   In this command, replace the sample parameter values with your own as follows:

   o **evauth1** — The Service Principal Name created in the Active Directory (AD) database for the gateway. In the **-princ** declaration of the **ktpass** command, the name must be written entirely in uppercase letters (**EVAUTH1** in the example). The choice of the Service Principal Name (**evauth1** in the example) is arbitrary.

   o **guard1.evros.sample-net.com** — The fully qualified domain name (FQDN) of the gateway (shortly named **guard1**). In the **-princ** declaration of the **ktpass** command, the name must be written entirely in lowercase letters (**guard1.evros.sample-net.com** in the example).

- **evros.sample-net.com** — The full domain name served by the AD instance, also referred to as the *Kerberos realm*. In the **-princ** declaration of the **ktpass** command, the name must be written entirely in uppercase letters (**EVROS.SAMPLE-NET.COM** in the example).
- **EVROS** — The NetBIOS name of the domain served by the AD instance (as given in the **EVROS\evauth1** username). Note that the NetBIOS name of the domain may have nothing in common with the FQDN of the gateway (the example shows instead a common "evros" component).
- **evros123#** — The password for the user **evauth1** created in the AD instance.
- **c:\evauthkeytab1** — The output filename (to be eventually copied in the gateway). The name used as the output file name is arbitrary.

  Warning: All parameters in the **ktpass** command are case sensitive.

To further clarify the use of the **ktpass** command, the following example shows how the command can be specified when a second OmniAccess 3500 NLG gateway (named **guard2**) is added to the authentication domain:

```
$ ktpass -princ EVAUTH2/guard2.evros.sample-net.com@EVROS.SAMPLE-NET.COM -
mapuser EVROS\evauth2 -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -mapop
set +desonly -pass evros456# -out C:\evauthkeytab2
```

Please note the following:

- A separate user account must be created on the Active Directory Server for every OmniAccess 3500 NLG gateway in the domain. With reference to the latter example above, the **evauth2** account must be created on the ADS before invoking the **ktpass** command.
- The user account associated with the gateway does not need to be a domain administrator account. In general it is preferable to setup a regular user account, because an administrator account typically requires a more complex configuration procedure to comply with the security policy of the enterprise.
- Each invocation of the **ktpass** command causes the credentials of the user account to change. It is therefore necessary to upload a new keytab file to the gateway every time the **ktpass** command is invoked for that gateway.
- To avoid the multiplication of the keytab files uploaded to a given gateway for a specific AD domain, the name of the keytab file should always be the same for that gateway-domain pair. This way, when an updated version of the keytab file is generated and uploaded to the gateway, the previous version of the same keytab file is immediately overridden.
- The `ktpass.exe` file is not included by default in Windows Server 2003, but can be found in the Windows Server 2003 support tools package, distributed with the Windows Server 2003 CD ROM or available on the web at: http://www.microsoft.com/downloads/details.aspx?FamilyId=6EC50B78-8BE1-4E81-B3BE-4E7AC4F0912D&displaylang=en
- The DNS name of the gateway must be associated with the IP address of the LAN (private) interface.

- The DNS name of the gateway and the ADS that generates the keytab file may belong to different DNS domains.

DNS Configuration

A split DNS configuration must be applied to the DNS server of your network for resolution of the gateway's FQDN. The split DNS configuration must resolve the FQDN of the gateway to the IP address of the WAN interface when the name resolution request comes from an external host and to the IP address of the LAN interface when the resolution request comes from an internal host.

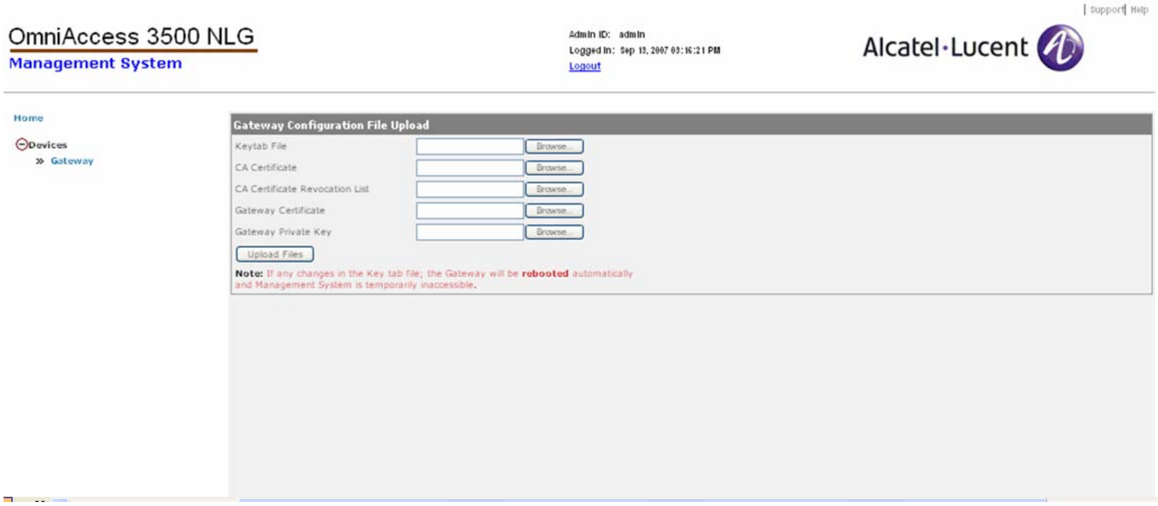
Router Configuration

The enterprise router in the subnet of attachment of the LAN interface of the OmniAccess 3500 NLG gateway must be provisioned with static routes for the address pools that the gateway allocates as VPN addresses for the cards and laptops. The routes must have the IP address of the LAN interface of the gateway as the next-hop IP address.

Configuration of Basic Parameters

You must configure the network and other basic parameters using the pre-configured IP address of the gateway (192.168.1.1). This section explains how to perform this procedure.

1. Connect a computer to the LAN (private) port of the gateway using an Ethernet cable. Ensure that the LED on the LAN interface is lit.
2. Open a web browser on your computer.
3. Type the following IP address in the address bar of the browser: https://192.168.1.1
4. You will be asked to enter the login ID and password for the super administrator (the default login ID is "admin" and the default password is "evros").
5. The initial Gateway Configuration File Upload window appears (Figure 23).



Admin ID: admin
Logged In: Sep 13, 2007 03:16:21 PM

Gateway Configuration File Upload

Keytab File

CA Certificate

CA Certificate Revocation List

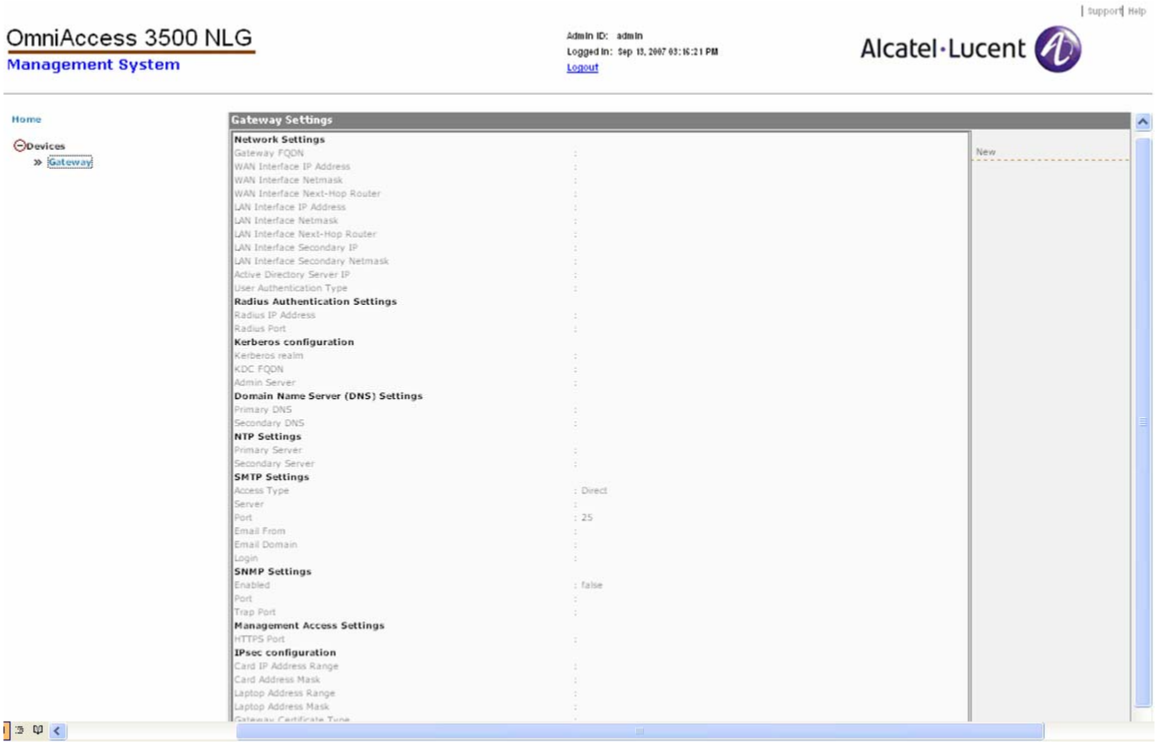
Gateway Certificate

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 23: Gateway Configuration File Upload window

6. Browse to the appropriate files in the file system of your computer to fill out the following fields:
   - **Keytab File**: File containing the credentials of the gateway for its authentication with the Active Directory server.
   - **CA Certificate**: Digital certificate of the Certificate Authority, 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 (including the OmniAccess 3500 NLG cards) 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).
7. Click **Upload Files**.
8. The Gateway Settings GUI window appears (Figure 24). Click **New**.



Admin ID: admin
Logged In: Sep 13, 2007 03:16:21 PM
Logout

Gateway Settings

Network Settings
Gateway FQDN :
WAN Interface IP Address :
WAN Interface Netmask :
WAN Interface Next-Hop Router :
LAN Interface IP Address :
LAN Interface Netmask :
LAN Interface Next-Hop Router :
LAN Interface Secondary IP :
LAN Interface Secondary Netmask :
Active Directory Server IP :
User Authentication Type :

Radius Authentication Settings
Radius IP Address :
Radius Port :

Kerberos configuration
Kerberos realm :
KDC FQDN :
Admin Server :

Domain Name Server (DNS) Settings
Primary DNS :
Secondary DNS :

NTP Settings
Primary Server :
Secondary Server :

SMTP Settings
Access Type : Direct
Server :
Port : 25
Email From :
Email Domain :
Login :

SNMP Settings
Enabled : false
Port :
Trap Port :

Management Access Settings
HTTPS Port :

IPsec configuration
Card IP Address Range :
Card Address Mask :
Laptop Address Range :
Laptop Address Mask :
Gateway Certificate Type :

Figure 24: Gateway Settings window

9. The Gateway Configuration (Add) window appears (Figure 25), displaying the following fields:

   Network Settings

- **Gateway FQDN**: Fully Qualified Domain Name (FQDN) of the gateway.
- **WAN Interface IP**: IP address assigned to the WAN 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 interface of the gateway. The LAN interface is connected to a private subnet of the enterprise.

  Note: Your current management system GUI session is interrupted after you set and save a new value for the LAN interface IP address. To open a new management system GUI session you must use the new value of the LAN interface IP address.
- **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 (LAN:1 virtual interface). The VPN address is used by cards and laptops to communicate with applications that run on 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 applied to 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 virtual interface (LAN:1) associated with the VPN address of the gateway.
- **Root Password**: Password for the root account on the OmniAccess 3500 NLG gateway.

  Warning: You MUST set a safe value for the root login password the first time you are presented with this configurable parameter. Failure to set the root password upon initial configuration of the gateway parameters is a security violation that exposes the appliance and your entire network to severe damage. It is critical to secure and remember the new password. If this password is lost it cannot be recovered.
- **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**: Method used for authentication of the end users. Possible values are <DOMAIN>, <RADIUS-LAX>, and <RADIUS-STRICT>. If <DOMAIN> is selected, the end users will be authenticated using KDC. With the other two values, a RADIUS server will authenticate the end users. More specifically, if <RADIUS-LAX> is selected the end-user laptop obtains the usual network parameters (VPN address and mask, next-hop router, DNS and WINS servers) before the end user submits the authentication credentials. If <RADIUS-STRICT> is selected, the network parameters will only be given after the RADIUS authentication succeeds.

RADIUS Authentication Settings

- **Radius IP Address:** IP address of the RADIUS server used for authentication of the end users (relevant only if the User Authentication Type field is set to one of the RADIUS methods).
- **Radius Port:** RADIUS server port where the authentication requests must be addresses.
- **Radius Secret:** Authentication and encryption key to be used in all RADIUS communications between the gateway and the RADIUS server.

Kerberos Configuration

- **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**: Admin server for the Domain; in most cases it is the same as the Active Directory Server except when the realm administrator has not made the information available through DNS.

DNS Settings

- **Primary DNS**: IP address of the primary DNS name server for end-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 applied 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 applied on the [Gateway Configure-> Server Table Information] window, reachable through the [Gateway|Configure Advanced Settings|Server Table] path.

NTP Server Settings

- **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 Settings

- **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 mail server that will forward the SMS emails sent for waking up the cards.
- **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 remotely wake up the cards.
- **Mail Domain**: Domain within which all email addresses used for SMS messaging are defined.
- **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 Settings

- **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 is similar to a password used by the SNMP clients to access information. If an SNMP Client uses a Read Community, it is allowed read-only access to the Information. It is recommended that the Read Community and Read-Write Community strings are different.
- **Confirm Read Community**: Re-type the Read Community string in this field.
- **Read-Write Community**: This string is used for SNMP authentication and is similar to a password used by the SNMP clients to access information. If an SNMP client uses a Read-Write Community, it is allowed to read information as well as modify it. It is recommended that the Read Community and Read-Write Community strings are different.
- **Confirm Read-Write Community**: Re-type the Read-Write Community string in this field.

HTTPS Settings

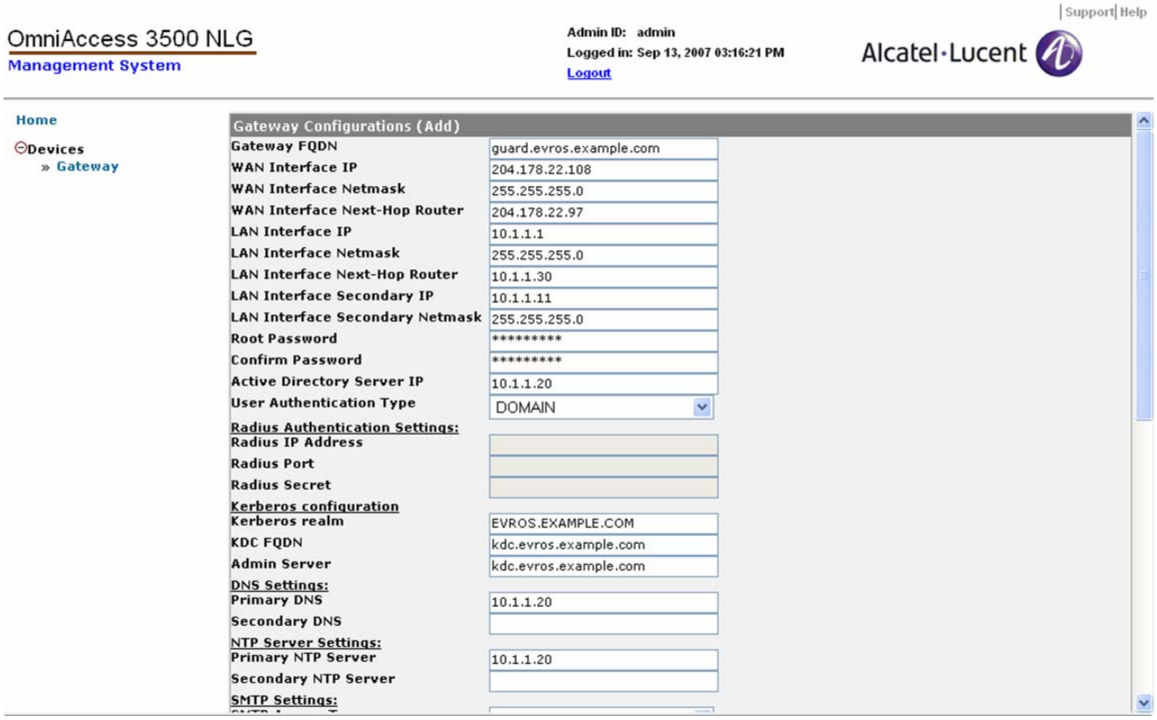
- **HTTPS Port**: The port on which you can securely access the management system GUI from a web browser. The default value is <443>, in which case you don't have to specify the port in the URL. If you set a different port, you will have to indicate the port number in the URL while accessing the management 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>.

IPsec Configuration

- **Card Address Range:** IP address pool for assignment to the OmniAccess 3500 NLG 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 applied 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 applied 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 digital certificate used by the OmniAccess 3500 NLG gateway for mutual authentication with the OmniAccess 3500 NLG cards. This entry must be set when the gateway is first configured. Later on, any modification of the Gateway Certificate ID Type must be applied

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, any modification of the Gateway Certificate ID must be applied on the [Connection Manager Tunnel Table (Add)] window, reachable through the [Gateway|Configure Advanced Settings|Tunnel Table|New] path.



Admin ID: admin
Logged in: Sep 13, 2007 03:16:21 PM

Gateway Configurations (Add)

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:	

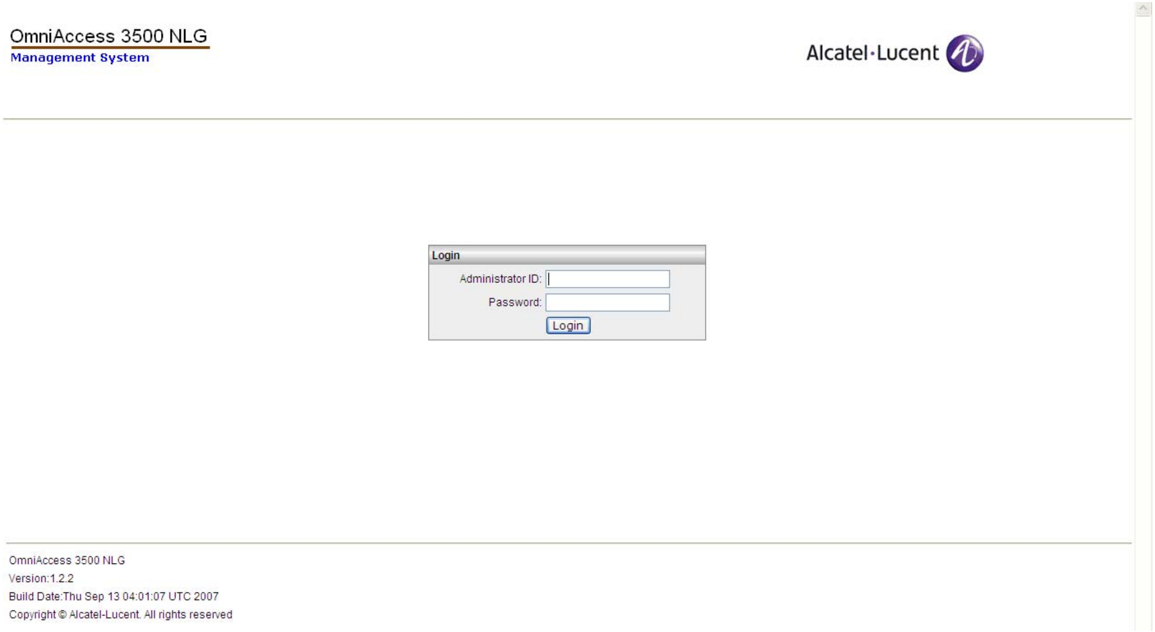
Figure 25: Gateway Configuration (Add) window

10. Type the appropriate information into the fields that do not contain default values.
11. Click **Save** when you are finished entering information.
12. A window appears stating that the operation has been successful.
13. Connect the WAN and LAN interfaces of the gateway to the gateway's preferred network outlets.
14. The gateway will reboot and then resume operation with the overall configuration that was most recently saved.

Accessing the Management System GUI

After rebooting the gateway, any subsequent administrative action can be completed through the management system GUI from a Web Browser. Please note that in OmniAccess 3500 NLG R1.2 the management system functionality is integrated in the gateway and automatically configured with the configuration of the gateway.

To access the management system GUI, open your web browser (any type will work) at the HTTPS URL that you have configured for the gateway (FQDN or LAN interface IP address; please note that HTTP won't work). The management system GUI login screen appears (Figure 26).



OmniAccess 3500 NLG
Version:1.2.2
Build Date:Thu Sep 13 04:01:07 UTC 2007
Copyright © Alcatel-Lucent. All rights reserved

Figure 26: Management system GUI login screen

You will be prompted for the Admin ID and the Password. The default values of Admin ID and Password are **admin** and **evros**, respectively.

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

Please refer to the *OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Administration Guide* for further operation, administration, and management of the OmniAccess 3500 NLG platform.

Upgrading the OmniAccess 3500 NLG Software

The gateway is shipped with the latest version of the software already installed. If the installation of new software is required for any reason, please follow the instructions contained in the *OmniAccess 3500 Nonstop Laptop Guardian Release 1.2 Administration Guide.*

Chapter 6. Troubleshooting

This chapter helps you identify and solve problems that might occur while you are using the gateway.

Resetting the System

Before going through in-depth troubleshooting, attempt first to reset your system using one of the methods below.

To do this….	**Press…**
Cold boot reset. Turn the system power off and then on. This clears system memory, reloads the operating system, and halts power to all peripherals	Power off/on button
Reset the BMC and get it back to a stable state	Remove AC power from the gateway for one minute

Table 4: Resetting the system

Problems following Initial System Installation

Problems that occur at initial system startup are usually caused by an incorrect installation or configuration. Hardware failure is a less frequent cause.

Here is a first-step troubleshooting checklist:

- Is AC power available at the wall outlet?
- Are the power supplies plugged in? Check the AC cable(s) on the back of the appliance and at the AC source.
- Are all cables correctly connected and secured?

If the above items are OK, please contact the customer support team at 800-995-2696 for further troubleshooting assistance.

Note: The gateway does not contain any field-serviceable components.

Chapter 7. Specification and Compliance Data

This section provides detailed specifications and compliance information for the gateway.

Physical Specifications

Dimensions

Height: 1.67” (4.24 cm)

Width: 16.930” (43 cm)

Depth: 20” (50.8 cm)

Maximum weight: approx. 33 lb (15 kg).

Cooling

2550 BTU/Hr

Operating Temperature

50°F (+10°C) to 95°F (+35°C), with the maximum rate of change not to exceed 50°F (10°C) per hour

Non-Operating Temperature

-40°F (-40°C) to +158°F (+70°C)

Non-Operating Humidity

90%, non-condensing at 95°F (35°C)

Operating Shock

Half sine, 2 g peak, 11 ms

Shock, Unpackaged

Trapezoidal, 25 g, velocity change 136 inches/s (3.45 m/s) (>40 lb/18 kg to >80 lb/36 kg)

Shock, Packaged

Non-palletized free fall in height 24 inches (>40 lbs to >80 lbs)

Vibration, Unpackaged

5 Hz to 500 Hz, 2.20 g RMS random

Power Supply

The following power supply configuration is supported on the gateway:

- Internal AC to DC Power Supply: Rated 300 watts max
- Auto-ranging: 100 to 254 VAC, 47 to 63 Hz
- Typical Consumption: 8A @ 120VAC; 5A @ 240VAC

Compliance Data

Product Safety Compliance

The gateway complies with the following safety requirements:

- UL60950 – CSA 60950(USA / Canada)
- EN60950 (Europe)
- IEC60950 (International)
- CB Certificate & Report, IEC60950 (report to include all country national deviations)
- GS License (Germany)
- GOST R 50377-92 - License (Russia)
- Belarus License (Belarus)
- Ukraine License (Ukraine)
- CE - Low Voltage Directive 73/23/EEE (Europe)
- IRAM Certification (Argentina)
- GB4943- CNCA Certification (China)

Product EMC Compliance

The platform has been tested and verified to comply with the following electromagnetic compatibility (EMC) regulations:

- FCC (Class A Verification) – Radiated & Conducted Emissions (USA)
- CISPR 22 – Emissions (International)
- EN55022 - Emissions (Europe)
- EN55024 - Immunity (Europe)
- EN61000-3-2 - Harmonics (Europe)
- EN61000-3-3 - Voltage Flicker (Europe)
- CE – EMC Directive 89/336/EEC (Europe)
- VCCI Emissions (Japan)
- AS/NZS 3548 Emissions (Australia / New Zealand)
- BSMI CNS13438 Emissions (Taiwan)
- GOST R 29216-91 Emissions (Russia)

- GOST R 50628-95 Immunity (Russia)
- Belarus License (Belarus)
- Ukraine License (Ukraine)
- RRL MIC Notice No. 1997-41 (EMC) & 1997-42 (EMI) (Korea)
- GB 9254 - CNCA Certification (China)
- GB 17625 - (Harmonics) CNCA Certification (China)

Electromagnetic Compatibility Notice

This platform complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. For questions related to the EMC performance of this product, contact your region's Alcatel-Lucent Enterprise Service and Support Desk (phone numbers and email addresses are listed at the end of this document).

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving radio/TV antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit other than the one to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment. The customer is responsible for ensuring compliance of the modified product.

Only peripherals (computer input/output devices, terminals, printers, etc.) that comply with FCC Class B limits may be attached to this computer product. Operation with noncompliant peripherals is likely to result in interference to radio and TV reception.

All cables used to connect to peripherals must be shielded and grounded. Operation with cables, connected to peripherals that are not shielded and grounded may result in interference to radio and TV reception.

FCC Verification Statement

Product Type: EG1.0

- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

OmniAccess 3500 NLG Enterprise Gateway Server: One Year Limited Warranty

Alcatel-Lucent warrants to Customer that the OmniAccess 3500 NLG Enterprise Gateway server sold by it is free from defects in material and workmanship under proper, normal use and service for a period of one year from the date of shipment by Alcatel-Lucent.

Alcatel-Lucent will, at its option, repair or replace failed or defective component parts or the entire system at no charge to Customer. If Alcatel-Lucent selects the replacement option, the parts will be the same or a later version, which perform substantially the same function(s) as the one being replaced. Alcatel-Lucent will make the final determination as to the existence and cause of any defect.

This warranty does not cover:

- Damage due to abuse, misuse, neglect, Customer's modifications, or accident;
- Improper wiring, repairing, splicing, alteration, installation, storage, or maintenance;
- Use in a manner not in accordance with Alcatel-Lucent or its vendor's specifications or operating instructions;
- Failure of Customer to apply previously applicable Alcatel-Lucent modifications or corrections;
- Problems with electrical power;
- Servicing not authorized by Alcatel-Lucent;
- Usage not in accordance with product instructions;
- Failure to perform required preventive maintenance;
- Problems caused by use of parts and components not supplied by Alcatel-Lucent;
- Products on which payment is past due.

In addition, Alcatel-Lucent makes no warranty with respect to Products which have had serial numbers or month and year of manufacturing removed or altered.

No guarantee is made by Alcatel-Lucent that third party software can be installed and run uninterrupted and error free on hardware purchased from Alcatel-Lucent. In addition, Alcatel-Lucent makes no warranty with respect to defects related to Customer’s software or database errors.

THE ALCATEL-LUCENT WARRANTY COVERS DEFECTS IN MATERIAL AND WORKMANSHIP ONLY. FAILURE OF SOFTWARE TO INSTALL AND RUN UNINTERRUPTED AND ERROR FREE DOES NOT RELIEVE CUSTOMER OF THE OBLIGATION TO PAY FOR THE HARDWARE IN ACCORDANCE WITH TERMS OF SALE. FAILURE OF CUSTOMER TO MAKE PAYMENT(S) IN A TIMELY MANNER WILL VOID ANY WARRANTY ON THE HARDWARE.

These terms, conditions, and warranties apply unless Customer has signed a separate purchase agreement or Statement of Work (SOW), in which case the separate agreement or SOW shall govern.

All software sold by Alcatel-Lucent is subject to the license agreement included with the software package. Opening the software package or breaking the seal subjects Customer to the terms of the license agreement. Alcatel-Lucent does not provide a warranty for any software. Software warranties, if any, are specified in the license agreement.

If Alcatel-Lucent determines that returned Product is not defective, Customer shall pay Alcatel-Lucent costs of handling, inspecting, testing, and transportation and, if applicable, travel and related expenses.

In repairing or replacing any Product, part of Product, or Software medium under this warranty, Alcatel-Lucent may use new, remanufactured, reconditioned, refurbished, or functionally equivalent Products or parts.

Parts returned must include all manuals, cables, software, and any related items. All shipping and insurance costs to return the parts to Alcatel-Lucent will be paid by Customer.

Repair or replacement shall constitute the fulfillment of all liabilities of Alcatel-Lucent with respect to warranty. Repair or replacement by Alcatel-Lucent is Customer's sole and exclusive remedy for any breach of warranty with respect to any integrated system sold hereunder.

ALCATEL-LUCENT PASSES THROUGH TO CUSTOMER WARRANTIES THAT ALCATEL-LUCENT HAS RECEIVED FROM THE MANUFACTURER OF COMPONENT PARTS. SUCH WARRANTIES MAY EXCEED THE LENGTH STATED IN THE OPENING PARAGRAPH AND WILL BE SUBJECT TO EVALUATION BY THE PARTS MANUFACTURER PRIOR TO ANY WARRANTY CREDIT BEING ISSUED.

EXCEPT AS PROVIDED HEREIN, ALCATEL-LUCENT MAKES NO WARRANTY OF ANY KIND WHATSOEVER INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PURPOSE OR USE. UNDER NO CIRCUMSTANCES WILL ALCATEL-LUCENT BE LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL ECONOMIC OR PROPERTY DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE SERVERS.

EXCEPT FOR THE EXCLUSIVE REMEDY SET FORTH ABOVE, IN NO EVENT SHALL ALCATEL-LUCENT HAVE ANY LIABILITY TO PURCHASER OR ANY THIRD PARTY FOR ANY CLAIM, LOSS, OR DAMAGE OF ANY KIND ARISING OUT OF OR IN CONNECTION WITH

- THE PERFORMANCE, USE OF, OR INABILITY TO USE ANY PRODUCT OR ANY DATA, SOFTWARE, OR RELATED PARTS, OR
- INFRINGEMENT OF ANY PATENT, COPYRIGHT, TRADEMARK, OR OTHER INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY.