OmniSwitch® 10K

Getting Started Guide

Alcatel·Lucent

Attention.

Only personnel knowledgeable in basic electrical and mechanical procedures should install or maintain this equipment.

The features and specifications described in this guide are subject to change without notice.

Alcatel·Lucent

Table of Contents

OmniSwitch 10K

OmniSwitch 10K Front Panel

The Alcatel-Lucent OmniSwitch 10K (OS10K) is a high-capacity, high-performance modular Ethernet LAN switch based on the state-of-the-art Alcatel Operating System (AOS).

The OS10K's class-leading low-power consumption, front-to-back cooling, compact form-factor, and all front-accessible components make it a perfect fit for data center applications, as well as a long-term upgrade for legacy core platforms.

Related Documentation

The following user documentation is provided for the OmniSwitch 10K.

- *OmniSwitch 10K Getting Started Guide*

  Describes the procedures for getting an OmniSwitch 10K up and running. Also provides information on fundamental aspects of hardware components and basic setup commands.

- *OmniSwitch 10K Hardware Users Guide*

  Technical specifications and procedures for the OmniSwitch 10K chassis, power supplies, fans, Chassis Management Modules (CMMs), Chassis Fabric Modules (CFMs) and Network Interface (NI) modules.

- *OmniSwitch CLI Reference Guide*

  Complete reference to all CLI commands supported on the OmniSwitch 10K. Includes syntax definitions, default values, examples, usage guidelines, and CLI-to-MIB variable mappings.

- *OmniSwitch AOS Release 7 Switch Management Guide*

  Includes procedures for readying an individual switch for integration into a network. Topics include software directory architecture, image rollback protections, authenticated switch access, managing switch files, system configuration, SNMP, and WebView management software.

- *OmniSwitch AOS Release 7 Network Configuration Guide*

  Includes network configuration procedures and descriptive information on all the major software features and protocols included in the base software package. Chapters cover Layer 2 information (Ethernet and VLAN configuration), Layer 3 information (routing protocols, such as RIP and VRRP), security options (authenticated switch access), Quality of Service (QoS), link aggregation, and server load balancing.

- *OmniSwitch AOS Release 7 Advanced Routing Configuration Guide*

  Includes network configuration procedures and descriptive information on advanced routing protocols such as OSPF, BGP, DVMRP and PIM-SM.

- *OmniSwitch AOS Release 7 Transceivers Guide*

  Includes information on Small Form Factor Pluggable (SFP) and 10 Gbps Small Form Factor Pluggable (SFP+) transceivers.

Installing the Hardware

Items Required

- Grounding wrist strap (included)
- Phillips screwdriver
- Flat-blade screwdriver
- Serial cable

Site Preparation

Environmental Requirements

OmniSwitch 10K switches have the following environmental and airflow requirements:

- The installation site must maintain a temperature between 0° and 45° Celsius (32° and 113° Fahrenheit) and not exceed 95 percent maximum humidity (non-condensing) at any time.

- Be sure to allow adequate room for proper air ventilation at the front, back, and sides of the switch. Refer to for minimum clearance requirements. No clearance is necessary at the top or bottom of the chassis.

Electrical Requirements

OmniSwitch 10K switches have the following general electrical requirements:

- Each switch requires one grounded electrical outlet for each power supply installed in the chassis. OmniSwitch 10K switches offer both AC and DC power supply support. Refer to the *OmniSwitch 10K Hardware Users Guide* for more information.

- For switches using AC power connections, each supplied AC power cord is 2 meters (approx. 6.5 feet). Do not use extension cords.

Redundant AC Power. It is recommended that each AC outlet resides on a separate circuit. With redundant AC, if a single circuit fails, the switch's remaining power supplies (on separate circuits) can remain operational.

- For switches using DC power, refer to the *OmniSwitch 10K Hardware Users Guide* for more information.

Unpacking and Installing the Switch

To protect your switch components from damage, read all unpacking recommendations and instructions carefully before beginning.

Unpack your OmniSwitch 10K chassis as close as possible to the location where it will be installed.

Items Included

Your OmniSwitch 10K includes the following items:

- OmniSwitch chassis with factory-installed power supplies, per order
- CMM module(s), per order
- CFM module(s), per order
- NI modules, per order
- Transceivers, per order
- Blank cover panels, if applicable
- Grounding wrist strap
- RJ45-to-DB9 console adapter
- Country-specific power cord(s)
- Hard copy of the *OmniSwitch 10K Getting Started Guide*

Weight Considerations

The empty OmniSwitch 10K chassis weighs approximately 46 lbs (21 Kgs). When fully populated (i.e., with components installed in all available chassis slots), the OmniSwitch 10K can weigh up to approximately 200 lbs (90.5 Kgs).

Lifting the Chassis

Lifting the chassis requires two people. When lifting, use the recessed hand grip provided on the rear panel and the reinforced area immediately under the front air intake plenum.
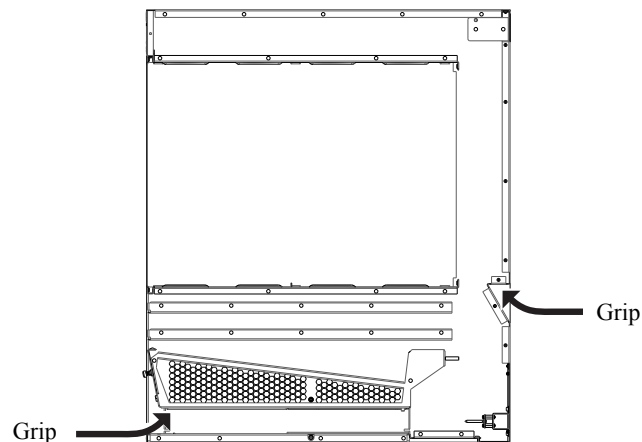
Chassis Cross Section

Note. Lifting the OmniSwitch 10K chassis improperly can cause personal injury and/or damage to the unit.

Airflow Considerations

To ensure proper airflow, be sure that your switch is placed in a well-ventilated area and provide minimum recommended clearance at the front, back and sides of the switch.

Rear. 6 inches minimum at rear of chassis.
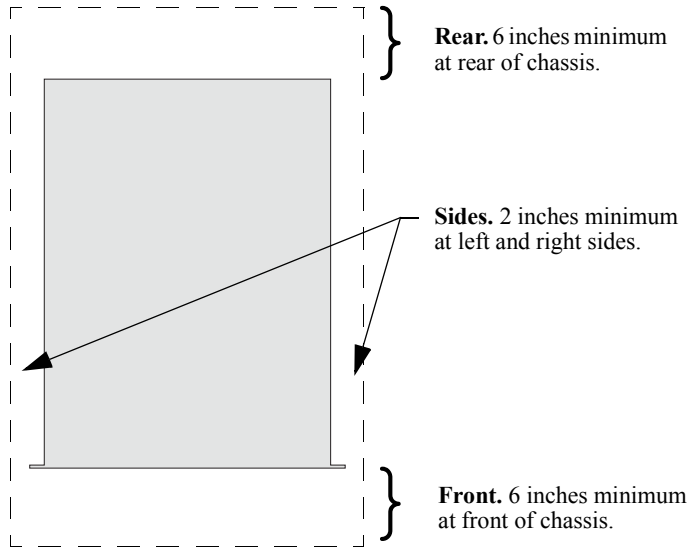
Sides. 2 inches minimum at left and right sides.

Front. 6 inches minimum at front of chassis.

Chassis Top View

Never obstruct the air intake vents located at the bottom-front and bottom-sides of the chassis or the fan unit's air output vents located at the rear of the chassis.

Note. Clearance is not required at the top and bottom of the chassis.

Mounting the Switch

Rack Mounting

Refer to the following important guidelines before installing the chassis in a rack:

- Three people are required to rack mount the switch: Two people to lift the chassis into position and one person to secure the chassis to the rack using the rack mount screws.

- The chassis has two integral rack-mount flanges that support standard 19-inch rack mount installations.

- Alcatel-Lucent does not provide rack-mount screws. Use the screws supplied by the rack vendor.

- To prevent a rack from becoming top heavy, it is recommended that you install the switch at the bottom of the rack whenever possible.

- If you are installing the switch in a relay rack, be sure to install and secure the rack per rack manufacturer's specifications.

Note. Due to its weight and airflow requirements, the OmniSwitch 10K cannot be wall-mounted.

To rack mount the switch, follow the steps below.

1 Mark the holes on the rack where the chassis is to be installed.

2 Using two people, lift and position the chassis until the rack-mount flanges are flush with the rack post. Refer to page 4 for information on properly lifting the chassis.

3 Align the holes in the flanges with the rack holes marked in step 1.

4 Once the holes are aligned, use a third person to insert a screw through the *bottom hole on each flange*. Tighten both screws until they are secure.

5 Once the screws at the bottom of each flange are secure, install the remaining screws. Be sure that all screws are securely tightened.

Optional Rack-Mounting Hardware

All OmniSwitch 10K switches are shipped with integral front rack mount flanges. These flanges support standard 19" rack mount installations. If you have non-standard rack mount requirements, contact your Alcatel-Lucent representative for information on optional hardware availability.

Standalone (Non-Rack Mounted) Installations

The chassis can also be placed unmounted on a stable, flat surface as a standalone unit. Be sure that the surface can accommodate the full, populated weight of all switches being installed. Approximate chassis weights are provided on page 4.

For a standalone unit, use two or more people to move and position the unpopulated chassis upright on the surface where it is to be installed. Be sure that adequate clearance has been provided for chassis airflow and that you have placed the chassis within reach of all required AC outlets. For recommended airflow allowances, refer to page 5.

Note. Chassis must be placed "right side up." Never attempt to operate a switch while it is lying on its side or back.

Installing Chassis Components

Electrostatic Discharge (ESD) Notice. Be sure to follow proper procedures to eliminate electrostatic discharge (ESD) from your person and the surrounding area before installing chassis components.

Blank Cover Plates

Blank cover plates are factory-installed in the chassis and are used to cover empty CMM, CFM and NI slots, as well as empty power supply and fan bays. These cover plates play an important role in chassis airflow and temperature management. They also provide protection for module processor boards and other sensitive internal switch components by closing off a chassis that is not fully populated.

Because they regulate airflow and help protect internal chassis components, blank cover plates should remain in place at all times.

Installing CMM, CFM and NI Modules

Before installing modules in the OmniSwitch 10K, locate their slot positions in the chassis. Slot numbers are clearly marked on the OmniSwitch 10K front panel.

CMM modules may be installed in slots A and B. If two CMM modules are installed in a chassis, the CMM occupying slot A is the primary CMM by default. CFM modules may be installed in slots C and D. NI modules may be installed in slots 1 through 8.

To install an CMM, CFM or NI module, follow the steps below:

1 Insert the module into the slot along the chassis card guides. The component side of the board should face right. The module should slide in easily.
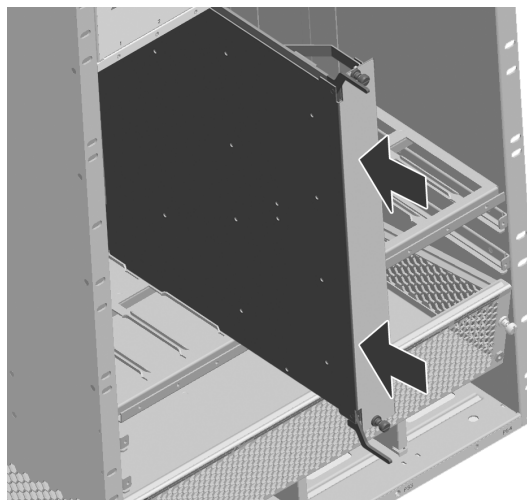
**Note.** Do not force the module into the slot. If any resistance is encountered, make sure the module is aligned properly in the card guides.

2 When the module is nearly seated in the slot, be sure that the two extractor levers—one on top of the module and one on the bottom—are open (approximately 90 degrees). This allows the notch on each extractor lever to grasp the rail on the chassis.

3 Once the notches have grasped the rail, press both extractor levers inward simultaneously until the module is firmly seated.
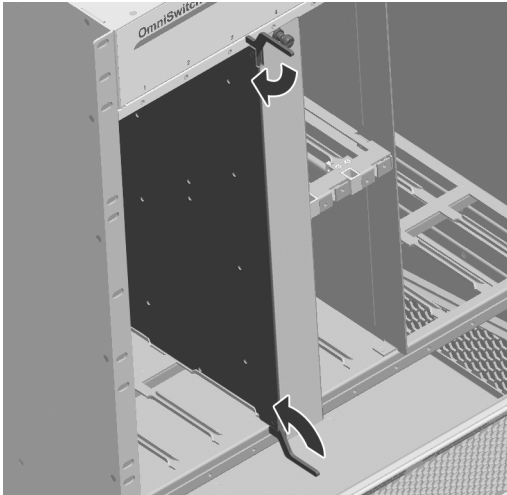
4 Once the module is firmly seated, secure the module to the chassis by tightening the two captive screws.

Installing Transceivers

For detailed information on installing transceivers, refer to the *OmniSwitch AOS Release 7 Transceivers Guide*.

Installing Fan Trays

1 Insert the tray into the chassis slot and slide it straight back until it meets the chassis backplane connectors.
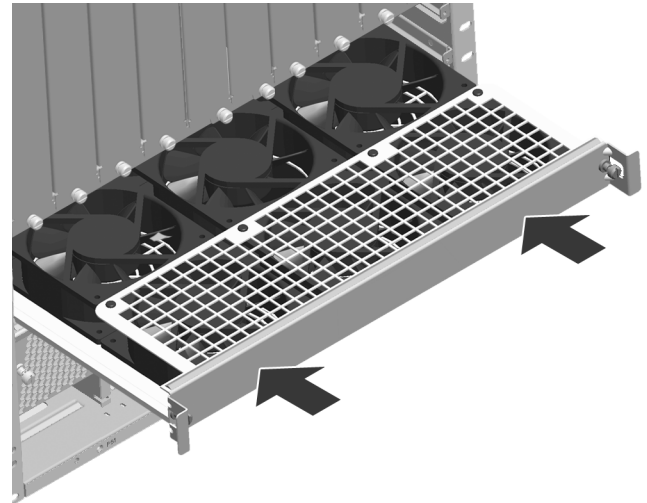
2 When the fan tray is firmly seated, tighten the two captive screws at the left and right sides of the fan tray's front panel.

Installing Power Supplies

1 Orient the power supply so that the power cord socket is situated at the right of the power supply. Also, for the power supply to seat properly, make sure that the handle is in the open (horizontal) position as shown.
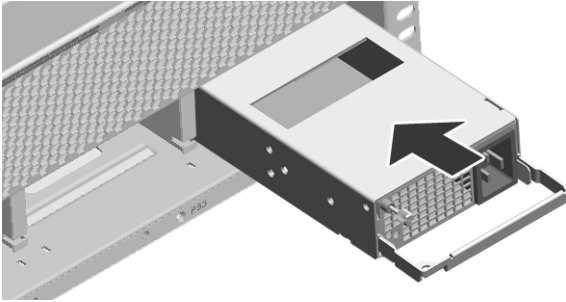
2 Slide the power supply back until its connector meets the chassis backplane.

3 When the power supply is fully seated, rotate the handle 90 degrees to the closed (vertical) position.
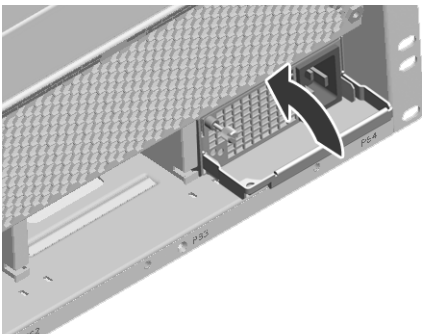
4 Tighten the captive screw, located at the top-left of the power supply's front panel.

5 Plug the power cord (provided) into the power supply's socket.
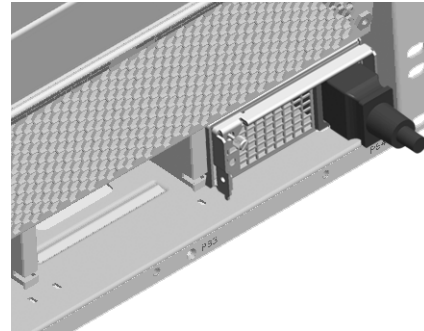
6 Place the cord retainer bracket over the power supply.
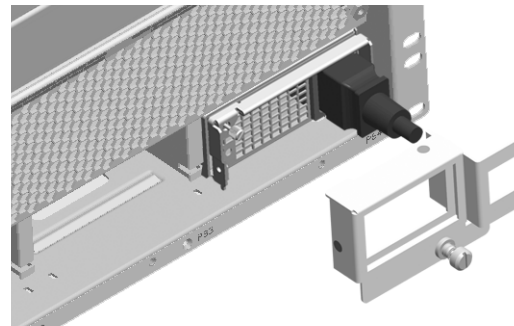
7 Secure the bracket to the bottom rail of the chassis using the captive screw. The bracket's prongs should hold the power cord securely in place.
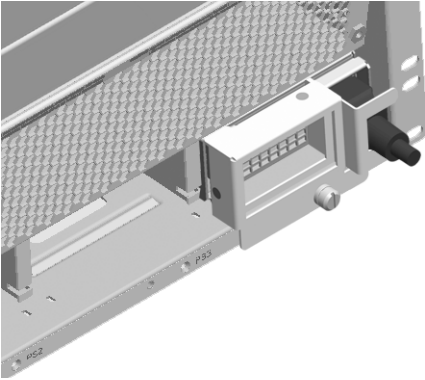
8 Repeat steps 1 though 7 for any additional power supplies being installed.

Important. Do not plug any power cords into a power source at this time as this will boot the chassis. Connecting the power cord(s) to a power source and the switch's boot sequence are covered on .

Connections and Cabling

Once your switch is properly installed, you should connect all network and management cables required for your network applications. Connections may include:

- RJ-45 straight-through cable to the console port
- Ethernet cable to the Ethernet Management Port (EMP) on the CMM
- Cables to NIs or transceivers

Serial Connection to the Console Port

The console port, located on the CMM module, provides a serial connection to the switch and is required when logging into the switch for the first time. By default, this RJ-45 connector provides a DCE console connection.

Serial Connection Default Settings

baud rate	9600
parity	none
data bits (word size)	8
stop bits	1

For information on modifying these settings, refer to the *OmniSwitch AOS Release 7 Switch Management Guide.*

Ethernet Management Port (EMP) Cable Requirements

There are specific cable type requirements (i.e., straight-through or crossover) based on the location of the Ethernet Management Port (EMP) and the type of device to which it is connecting. Refer to the information below:

EMP to a Switch	Straight-through
EMP to a Computer or Workstation	Crossover

For information on manually configuring Ethernet ports for cabling requirements, refer to the *OmniSwitch AOS Release 7 Network Configuration Guide*.

For detailed information on all port types, including console, EMP, Gigabit Ethernet, and 10 Gigabit Ethernet, refer to the *OmniSwitch 10K Hardware Users Guide*.

Booting the Switch

Now that you have installed the switch components and connected network and management cables, you can boot the switch. To boot the switch, plug all power supply cords into easily-accessible, properly grounded power outlets. (Do not use extension cords.) The switch will power on and boot automatically.

Note. If you have more than one power supply installed, be sure to plug in each power supply in rapid succession, (i.e., within a few seconds of each other). This ensures that there will be adequate power for all modules throughout the boot process.

Component LEDs

During the boot process, component LEDs will flash and change color, indicating different stages of the boot. Following a successful boot, the LEDs on all switch components, including power supplies, should display as follows:

CMM OK1	Solid Green
CMM OK2	Blinking Green
CMM CONTROL	Solid Green
CMM FABRIC	Solid Green
CMM TEMP	Solid Green

CFM OK1	Solid Green
CFM OK2	Blinking Green
NI OK1	Solid Green
NI OK2	Blinking Green
Power Supply AC	Solid Green
Power Supply DC	Solid Green

Note. If a secondary CMM is installed in the chassis (typically in slot B), its CMM CONTROL LED should be blinking green.

If the LEDs do not display as indicated, make sure the boot process is completed. If the LEDs do not display as indicated following a complete boot sequence, contact Alcatel-Lucent Customer Support. For information on fan tray LED states, refer to the *OmniSwitch 10K Hardware Users Guide*.

Once the switch has completely booted and you have accessed your computer's terminal emulation software via the console port, you are ready to log in to the switch's Command Line Interface (CLI) and configure basic information. Continue to .

Your First Login Session

In order to complete the setup process for the switch, you must complete the following steps during your first login session:

- Log in to the switch

- Set IP address information for the Ethernet Management Port (EMP)

- Unlock session types

- Change the login password

- Set the date and time

- Set optional system information

- Save your changes

Important. You must be connected to the switch via the console port before initiating your first login session.

Logging In to the Switch

When you first log in to the switch, you will be prompted for a CMM login name and password. Use the switch's default settings:

- CMM login: **admin**

- Password: **switch**

The default welcome banner, which includes information such as the current software version and system date, is displayed followed by the CLI command prompt:

```
+++ WARNING! Switch Access Vulnerability.

+++ WARNING! Admin user authentication using
default password.
Welcome to the Alcatel-Lucent OS10K
7.1.1.1198.R01, October 15, 2010.

Copyright (c) 1994-2010 Alcatel-Lucent. All
Rights Reserved.

OmniSwitch(tm) is a trademark of Alcatel-Lucent,
registered in the United States Patent and
Trademark Office.
->
```

More Information On User Accounts. A user account includes a login name, password, and user privileges. Privileges determine whether the user has read or write access to the switch and which commands the user is authorized to execute. For detailed information on setting up and modifying user accounts, refer to the *OmniSwitch AOS Release 7 Switch Management Guide*

Setting IP Address Information for the EMP

The Ethernet Management Port (EMP) is located on the CMM module. The EMP allows you to bypass the Network Interface (NI) modules and manage the switch over the network directly through the CMM.

In order to ping the switch through the EMP Ethernet connection, you must change the port's default IP and gateway addresses.

Note. You must be connected to the switch via the console port before attempting to change IP address information. Otherwise, an error message will display.

To change the default IP and gateway addresses, use the **ip interface** command. For example:

```
-> ip interface emp address 168.22.2.120 mask
   255.255.255.0
```

Verify your settings using the **show ip interface** command.

Note. Although you have configured the EMP with valid IP address information, you will not be able to access the switch through this port for Telnet, FTP, WebView, or SNMP sessions until you have unlocked these remote session types. See for more information.

Unlocking Session Types

Security is a key feature on OmniSwitch 10K switches. As described on page 13, when you access the switch for the first time, you must use a *direct console port connection*. All other session types (Telnet, FTP, WebView, and SNMP) are locked out until they are manually unlocked by the user.

The CLI command used to unlock session types is **aaa authentication**.

Note. When you unlock session types, you are granting switch access to non-local sessions (e.g., Telnet). As a result, users who know the correct user login and password will have remote access to the switch. For more information on switch security, refer to the *OmniSwitch AOS Release 7 Switch Management Guide.*

Unlocking All Session Types

To unlock all session types, enter the following command syntax at the CLI prompt:

```
-> aaa authentication default local
```

Unlocking Specified Session Types

You can also unlock session types on a one-by-one basis. For example, to unlock Telnet sessions only, enter the following command:

```
-> aaa authentication telnet local
```

To unlock WebView (HTTP) sessions only, enter the following command:

```
-> aaa authentication http local
```

You cannot specify more than one session type in a single command line. However, you can still unlock multiple session types by using the **aaa authentication** command in succession. For example:

```
-> aaa authentication http local
-> aaa authentication telnet local
-> aaa authentication ftp local
```

Refer to the *OmniSwitch CLI Reference Guide* for complete **aaa authentication** command syntax options.

Changing the Login Password

Change the login password for **admin** user sessions by following the steps below:

1 Be sure that you have logged into the switch as user type **admin** (see "Logging In to the Switch" on page 13).

2 Enter the keyword **password** and press **Enter**.

3 Enter your new password at the prompt.

Note. Be sure to remember or securely record all new passwords; overriding configured passwords on OmniSwitch 10K switches is restricted.

---

4 You will be prompted to re-enter the password. Enter the password a second time.

New password settings are automatically saved in real time to the local user database; the user is not required to enter an additional command in order to save the password information. Also note that new password information is retained following a reboot. All subsequent login sessions, including those through the console port, will require the new password to access the switch.

For detailed information on managing login information, including user names and passwords, refer to the *OmniSwitch AOS Release 7 Switch Management Guide*.

Setting the System Time Zone

The switch's default time zone is UTC. If you require a time zone that is specific to your region, or if you need to enable Daylight Savings Time (DST) on the switch, you can configure these settings via the **system timezone** and **system daylight-savings-time** commands.

For detailed information on configuring a time zone for the switch, refer to the *OmniSwitch AOS Release 7 Switch Management Guide*.

Setting the Date and Time

Set the current time for the switch by entering **system time**, followed by the current time in *hh:mm:ss*.

To set the current date for the switch, enter **system date**, followed by the current date in *mm/dd/yyyy*.

Setting Optional Parameters

Specifying an Administrative Contact

An administrative contact is the person or department in charge of the switch. If a contact is specified, users can easily find the appropriate network administrator if they have questions or comments about the switch.

To specify an administrative contact, use the **system contact** command.

Specifying a System Name

The system name is a simple, user-defined text description for the switch. To specify a system name, use the **system name** command.

Specifying the Switch's Location

It is recommended that you use a physical labeling system for locating and identifying your switch(es). Examples include placing a sticker or placard with a unique identifier (e.g., the switch's default IP address) on each chassis.

However, if no labeling system has been implemented or if you need to determine a switch's location from a remote site, entering a system location can be very useful.

To specify a system location, use the **system location** command.

Viewing Your Changes

To view your current changes, enter **show system** at the CLI prompt.

Saving Your Changes

Once you have configured this basic switch information, save your changes by entering **write memory** at the CLI command prompt.

Using WebView

OmniSwitch 10K switches can be configured and monitored using WebView, Alcatel-Lucent's web-based device management tool.

Logging In to WebView

Note. Before attempting to establish a WebView session, be sure that you have first unlocked the HTTP session type using the **aaa authentication** command. Otherwise, a login error will occur. See "Unlocking Session Types" on page 14 for more information.

To access WebView and log in to a switch:

1 Enter the switch's IP address in your web browser. If a certificate warning error occurs, accept the certificate and allow the page to load. The login screen displays.

2 Next, enter the user name and password at the login prompt.

Navigating WebView

After you have successfully logged in, the Chassis Management home page displays.
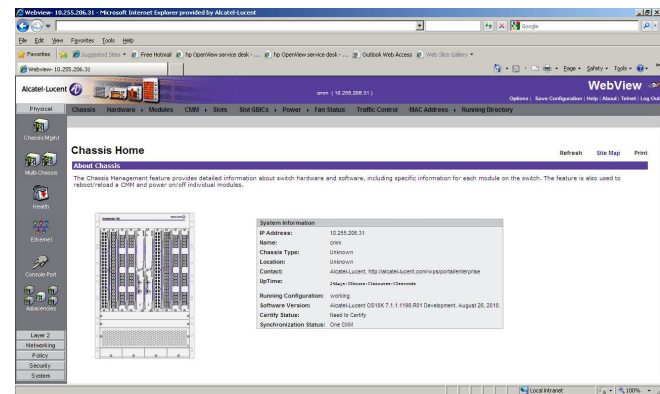
The Chassis Management home page provides a physical representation of the switch as well as basic system information. This is the main launching point for WebView.

Note. For more information on using WebView, refer to the *OmniSwitch AOS Release 7 Switch Management Guide*.

Troubleshooting WebView

The WebView login screen does not display.

This suggests either a physical or network connection issue. Try the following options:

- Be sure that there is a good physical Ethernet cable connection to the Ethernet port used for managing the switch (EMP or NI port).

- Be sure your computer has a valid Ethernet connection and IP address. See for information on configuring the IP address for the EMP.

The login screen displays, but login attempts fail.

This suggests either a user name and password or Authenticated Switch Access error. Try the following options:

- Check that you are using the correct user name and password. If you have already changed the user name and password for your switch, be sure to use the new information. If you have not changed the user name and password, the factory defaults are **admin** and **switch**, respectively.

- Be sure that you have unlocked HTTP sessions on the switch. To unlock HTTP sessions, enter the following command:

```
-> aaa authentication http local
```

For more information on unlocking session types, see .